kaspersky

Kaspersky Symphony XDR: Single Management Platform

Содержание

Kaspersky Symphony XDR

Kaspersky Symphony XDR – это комплексное решение для кибербезопасности бизнеса, которое включает в себя приложения "Лаборатории Касперского", с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты Kaspersky Symphony XDR развернуты на единой платформе управления Open Single Management Platform. Платформа обеспечивает выполнение кросс-программных сценариев в рамках единого интерфейса и позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности.

Один из центральных элементов решения – SIEM-система – позволяет отслеживать события, полученные от всех компонентов, и выполняет взаимную корреляцию этих событий с помощью готовых и пользовательских правил. На основании журналов и телеметрии, полученных от инфраструктуры организации, Kaspersky Symphony XDR автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в Kaspersky Symphony XDR события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Для реагирования на сложные инциденты Kaspersky Symphony XDR использует предустановленные и пользовательские сценарии. Также доступны действия по реагированию от приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

В решение включена базовая защита конечных точек, которая позволяет блокировать атаки, направленные на инфраструктуру конечных устройств (как физических, так и виртуальных). Также компоненты Kaspersky Symphony XDR обеспечивают специализированную защиту HTTP-, HTTPS- и FTP-трафика, проходящего через прокси-сервер, защиту почтовых серверов, входящей и исходящей почты от вредоносных объектов, спама и фишинга.

Решение позволяет централизованно устанавливать приложения безопасности "Лаборатории Касперского" на устройства инфраструктуры, удаленно запускать задачи проверки и обновления, а также настраивать политики безопасности управляемых приложений. В панели мониторинга отображается актуальное состояние системы безопасности, подробные отчеты и детальные параметры политик.

Kaspersky Symphony XDR позволяет компаниям соответствовать требованиям регуляторов (например, в сфере безопасности объектов КИИ) благодаря встроенному модулю ГосСОПКА.

Компоненты решения Kaspersky Symphony XDR

	Open Single Management Platform		Kaspersky Security Suite для Linux Mail Server
	Kaspersky Security Center		Kaspersky Secure Mail Gateway
	Kaspersky Unified Monitoring and Analysis Platform		Kaspersky Automated Security Awareness Platform
	Kaspersky Endpoint Detection and Response		Kaspersky CyberTrace
	Kaspersky Anti-Targeted Attack Platform		Kaspersky Web Traffic Security 6.0
	Kaspersky Endpoint Security для бизнеса		

Быстрые ссылки

Новые функции

- Что нового в Open Single Management Platform

Ключевые функции

- Управление алертами и инцидентами безопасности
- Инструменты Поиска угроз
- Граф расследования
- Предопределенные и пользовательские плейбуки
- Ручное реагирование на обнаруженные угрозы
- Панель мониторинга и веб-виджеты

Совместимость и аппаратные и программные требования

- Аппаратные и программные требования
- Совместимые приложения и решения
- Интеграция с другими решениями и системами сторонних производителей

Начало работы

- Пошаговый сценарий развертывания, активации и первоначальной настройки Open Single Management Platform
- Развертывание Open Single Management Platform
- Перенос данных в Open Single Management Platform
- Использование функций мониторинга, обнаружения и поиска угроз
- Пример расследования инцидента с помощью Open Single Management Platform

Работа с Open Single Management Platform

- Установка приложений безопасности "Лаборатории Касперского" на устройства в корпоративной сети
- Удаленный запуск задач поиска вредоносного ПО и обновления
- Управление политиками безопасности управляемых приложений

Что нового

Open Single Management Platform 1.2

В Open Single Management Platform реализовано несколько новых функций и улучшений:

- В приложении используется обновленная версия Bootstrap. Прежде чем установить новую версию Open Single Management Platform, обновите Bootstrap, выполнив следующую команду:

  ```
  ./kdt apply -k <путь_к_обновлениям_XDR-архива> -i <путь_к_конфигурационному_файлу> --force-bootstrap
  ```

- Гибкий рабочий процесс инцидентов. Вы можете настроить рабочий процесс инцидента и просмотреть его в визуальном редакторе.

- Теперь вы можете прикреплять файлы к алертами или инцидентам. При необходимости вы можете удалить или скачать прикрепленные файлы.

- Настраиваемый процесс обработки инцидентов с использованием типов инцидентов.

- Обновление Open Single Management Platform с версии 1.1 до версии 1.2.

- При создании плейбука вы можете настроить алгоритм плейбука для изменения свойств инцидента или свойств алерта.

- Вы можете экспортировать информацию обо всех инцидентах, которые отображаются в таблице инцидентов, в файл JSON. Это может потребоваться, когда вам нужно будет предоставить эту информацию третьим сторонам.

- Оптимизировано развертывание Open Single Management Platform: улучшен конфигурационный файл и мастер развертывания для упрощенной настройки параметров установки.

- AI-оценка активов. Механизм на основе машинного обучения помогает вам оценивать процессы, выполняемые на активе, и определять, является ли конкретный процесс нормальным или необычным и требует внимания аналитика SOC.

- Улучшен процесс настройки шаблонов для отправки уведомлений по электронной почте о событиях, происходящих в Open Single Management Platform.

- Вы можете уменьшать или увеличивать период хранения алертов и инцидентов в зависимости от ваших требований. По умолчанию период хранения алертов и инцидентов составляет 360 дней.

- Удаление Open Single Management Platform и всех созданных данных.

- Из контекстного меню окна деталей алерта или инцидента теперь можно открыть страницу **Поиск угроз** в новой вкладке браузера.

- В окне деталей алерта или в инцидента теперь можно выполнять поиск по затронутым активам и наблюдаемым объектам.

- Возможность настройки правил агрегации алертов с помощью REST API.

- При открытии страницы Поиск угроз из окна деталей алерта или окна деталей инцидента поиск теперь выполняется за период между первым и последним событием алерта или инцидента, а не за последние 24 часа.

- Предварительные проверки перед развертыванием. Перед развертыванием Open Single Management Platform теперь вы можете проверить, выполняются ли аппаратные и программные требования. Kaspersky Deployment Toolkit (KDT) проверяет ваше оборудование, операционную систему, программное обеспечение и сетевую среду. Если хотя бы одно требование не выполнено, KDT прерывает развертывание и предоставляет вам подробный отчет.
- Решение Open Single Management Platform теперь может быть установлено на платформе виртуализации Nutanix AHV.
- Оптимизация Консоли OSMP: окна консоли, страница входа и Панель мониторинга теперь загружаются быстрее.
- Теперь вы можете переключаться из окна деталей инцидента на события, связанные с инцидентом, на странице **Поиск угроз**.
- Open Single Management Platform теперь поддерживает следующие EPP-программы:
  - Kaspersky Endpoint Security для Windows, версии 12.5, 12.6, 12.7
  - Kaspersky Endpoint Security 12.1 для Linux
  - Kaspersky Endpoint Security 12.1 для Mac
  - Kaspersky Industrial CyberSecurity for Nodes 4.0
  - Kaspersky Endpoint Agent 4.0
- Open Single Management Platform теперь совместим с Kaspersky Anti Targeted Attack Platform 7.0.
- Теперь вы можете обновить информацию в окне деталей алерта и окне деталей инцидента, нажав на значок обновления.
- В окнах деталей алерта и инцидента в таблицу с устройствами добавлен атрибут КИИ.
- Добавлено ручное обновление данных в окнах деталей алерта, инцидента, инцидента НКЦКИ.

Open Single Management Platform 1.1

В Open Single Management Platform реализовано несколько новых функций и улучшений:

- В приложении используется обновленная версия Bootstrap. Прежде чем установить новую версию Open Single Management Platform, обновите Bootstrap, выполнив следующую команду:

  ```
  ./kdt apply -k <путь_к_обновлениям_XDR-архива> -i <путь_к_конфигурационному_файлу> --force-bootstrap
  ```

- Реализован новый дизайн пользовательского интерфейса.
- Снижены требования к аппаратному и программному обеспечению.
- Повышена стабильность работы приложения.
- Реализован мастер развертывания для упрощенной настройки параметров установки.
- Добавлены предустановленные плейбуки.

- Open Single Management Platform теперь поддерживает следующие EPP-программы:
  - Kaspersky Endpoint Security 12.0 для Mac
  - Kaspersky Industrial CyberSecurity for Nodes 3.2
  - Kaspersky Endpoint Agent 3.16
- Реализованы новые веб-виджеты в Панели мониторинга для контроля действий по реагированию с помощью плейбуков.
- Перенос данных из KUMA или Kaspersky Security Center в Open Single Management Platform, включая перенос пользователей и тенантов, а также привязку тенантов к Серверам администрирования Kaspersky Security Center.
- Open Single Management Platform теперь совместим с Kaspersky Anti Targeted Attack Platform 6.0.
- Поддержка модели статусов инцидентов, совместимой с ГОСТ.
- Поддержка совместимости с новой версией swagger-контракта НКЦКИ.
- Термин "обнаружение" заменен на термин "алерт".

Об Open Single Management Platform

Open Single Management Platform – это надежное решение для кибербезопасности, которое защищает вашу корпоративную ИТ-инфраструктуру от сложных киберугроз, в том числе тех, которые не могут быть обнаружены EPP-программами, установленными на корпоративных активах. Решение обеспечивает полную видимость, корреляцию и автоматизацию, используя широкий спектр инструментов реагирования и источников данных, включая активы конечных точек, данные сети и облачного окружения. Чтобы эффективно защитить вашу ИТ-инфраструктуру, Open Single Management Platform анализирует данные из этих источников для выявления угроз, создает алерты о потенциальных инцидентах и предоставляет инструменты для реагирования на них. Open Single Management Platform обладает расширенными аналитическими возможностями и богатым опытом в области безопасности.

Это решение обеспечивает единый процесс обнаружения и реагирования с помощью интегрированных компонентов и целостных сценариев в едином интерфейсе для повышения эффективности специалистов по безопасности.

Средства обнаружения включают:

- Инструменты поиска угроз для автоматического поиска угроз и уязвимостей путем анализа событий.
- Расширенное обнаружение угроз и взаимная корреляция: корреляция событий из разных источников в режиме реального времени, более 350 готовых правил корреляции для разных сценариев с матричным отображением MITRE ATT&CK, возможность создавать новые правила и настраивать существующие, ретроспективное сканирование для обнаружения уязвимостей нулевого дня.
- Граф расследования для визуализации и облегчения расследования инцидента и определения первопричин алерта.
- Использование Kaspersky Threat Intelligence Portal для получения последней подробной информации об угрозах, касающейся веб-адресов, доменов, IP-адресов, хешей файлов, статистических и поведенческих данных, и данных WHOIS и данных DNS.

Инструменты действий по реагированию включают:

- Действия по реагированию, выполняемые вручную: изоляция активов, запуск команд, создание правил запрета, запуск задач на активе, пополнение репутации Kaspersky Threat Intelligence Portal и обучающие задания для пользователей.
- Плейбуки как предустановленные, так и созданные пользователем, для автоматизации типичных действий по реагированию.
- Действия по реагированию приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

Open Single Management Platform также использует компонент Open Single Management Platform для управления активами и централизованного выполнения задач по администрированию и обслуживанию:

- Развертывание приложений "Лаборатории Касперского" на активах в корпоративной сети.
- Удаленный запуск задач поиска вредоносного ПО и обновления.
- Получение подробной информации о защите активов.
- Настройка всех компонентов безопасности с помощью приложений "Лаборатории Касперского".

Open Single Management Platform поддерживает иерархию тенантов.

Open Single Management Platform интегрирован с Active Directory, включает API-интерфейсы и поддерживает широкий спектр интеграций как с приложениями "Лаборатории Касперского", так и с решениями сторонних производителей для получения данных и реагирования на них. Информацию о приложениях и решениях, которые поддерживает OSMP, см. в разделах Совместимые приложения "Лаборатории Касперского" и Интеграция с другими решениями.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Аппаратные и программные требования

В статье описаны аппаратные требования к схеме развертывания на одном узле и к схеме развертывания на нескольких узлах, программные требования Open Single Management Platform, аппаратные и программные требования Kaspersky Deployment Toolkit и компонентов OSMP.

Общие требования и рекомендации

Если вы используете виртуализацию, требуется выделить 100% vCPU сервера.

Для сетей, превышающих 40 000 устройств, используйте подчиненные Серверы администрирования.

Развертывание на одном узле не может быть обновлено до развертывания на нескольких узлах. Установка на нескольких узлах должна быть предпочтительной, если ожидается рост сети.

Эффективное устройство и расчет количества событий в секунду (EPS)

Требования к оборудованию могут изменяться в зависимости от операционной системы конечных устройств. Используйте следующую формулу для оценки эффективных устройств в вашей сети:

<количество устройств> = <конечные точки с операционной системой Windows> + 3* <конечные точки с операционной системой Linux и macOS> + 20 * <серверы>

Ожидается, что эффективное устройство будет вносить вклад в 0,5 EPS (событий в секунду) с параметрами по умолчанию. Общие количество событий в секунду (EPS) рассчитывается по следующей формуле:

<общее EPS> = <EPS от эффективных устройств> + <EPS от сторонних устройств>

Вы можете преобразовать общее EPS в эффективные устройства, используя следующую формулу:

<общее количество эффективных устройств> = <общее EPS> / 0,5

Развертывание на одном узле: аппаратные требования

Схема с одним узлом поддерживает только до 10 000 устройств в сети.

Для KATA/KEDR требуются дополнительные узлы.

При развертывании на одном узле рекомендуется сначала вручную установить СУБД на устройстве, которое будет выполнять роль первичного узла. После этого вы можете установить Open Single Management Platform на том же устройстве.

Минимальные аппаратные требования

Решение	250 устройств	1000 устройств	3000 устройств	5000 устройств	10 000 устройств
Решение, включающее в себя следующие приложения: • Open Single Management Platform • Kaspersky Unified Monitoring and Analysis Platform • Kaspersky Anti-Targeted Attack Platform / Kaspersky Endpoint Detection and Response Central Node*	1 первичный узел XDR**: • Процессор: 6 ядер, частота от 2,5 ГГц. • Оперативная память: 27 ГБ. • Объем свободного места на диске: 360 ГБ. 1 узел сервиса KUMA: • Процессор: 10 ядер. • Оперативная память: 16 ГБ. • Объем дискового пространства: 500 ГБ.	1 первичный узел XDR**: • Процессор: 8 ядер, частота от 2,5 ГГц. • Оперативная память: 32 ГБ. • Объем свободного места на диске: 400 ГБ. 1 узел сервиса KUMA: • Процессор: 10 ядер. • Оперативная память: 16 ГБ. • Объем дискового пространства: 600 ГБ.	1 первичный узел XDR**: • Процессор: 11 ядер, частота от 2,5 ГГц. • Оперативная память: 38 ГБ. • Объем свободного места на диске: 600 ГБ. 1 узел сервиса KUMA: • Процессор: 10 ядер. • Оперативная память: 16 ГБ. • Объем дискового пространства: 1000 ГБ.	1 первичный узел XDR**: • Процессор: 15 ядер, частота от 2,5 ГГц. • Оперативная память: 46 ГБ. • Объем свободного места на диске: 740 ГБ. 1 узел сервиса KUMA: • Процессор: 10 ядер. • Оперативная память: 16 ГБ. • Объем дискового пространства: 1400 ГБ.	1 первичный узел XDR**: • Процессор: 18 ядер, частота от 2,5 ГГц. • Оперативная память: 57 ГБ. • Объем свободного места на диске: 1500 ГБ. 1 узел сервиса KUMA: • Процессор: 10 ядер. • Оперативная память: 16 ГБ. • Объем дискового пространства: 2400 ГБ.

*Требования не учитывают устройства для сервисов KEDR.

База данных развернута на первичном узле XDR отдельно от установки OSMP.

Для корректного развертывания решения убедитесь, что процессор целевого устройства поддерживает набор инструкций BMI, AVX и SSE 4.2.

Развертывание на нескольких узлах: аппаратные требования

Схема кластера с несколькими узлами рекомендуется для сетей с количеством устройств более 10 000.

Минимальные аппаратные требования

Решение	20 000 устройств	30 000 устройств	50 000 устройств
Решение, включающее в себя следующие приложения: • Open Single Management Platform • Kaspersky Unified Monitoring and Analysis Platform • Kaspersky Anti-Targeted Attack Platform / Kaspersky Endpoint Detection and Response Central Node*	12 узлов: • 1 первичный узел XDR** • 3 рабочих узла XDR • 1 узел базы данных XDR** • 1 коллектор KUMA • 1 коррелятор KUMA • 3 кипера KUMA	12 узлов: • 1 первичный узел XDR** • 3 рабочих узла XDR • 1 узел базы данных XDR** • 1 коллектор KUMA • 1 коррелятор KUMA	12 узлов: • 1 первичный узел XDR** • 3 рабочих узла XDR • 1 узел базы данных XDR** • 1 коллектор KUMA

	• 2 хранилища KUMA	• 3 кипера KUMA • 2 хранилища KUMA	• 1 коррелятор KUMA • 3 кипера KUMA • 2 хранилища KUMA
	1 первичный узел XDR**: • Процессор: 4 ядра. • Оперативная память: 8 ГБ. • Объем свободного места на диске: 500 ГБ. 3 рабочих узла XDR: • Процессор: 8 ядер. • Оперативная память: 20 ГБ. • Объем свободного места на диске: 1 ТБ. 1 узел базы данных XDR**: • Процессор: 10 ядер. • Оперативная память: 21 ГБ. • Объем свободного места на диске: 1.6 ТБ. 1 узел с коллектором KUMA: • Процессор: 8 ядер. • Оперативная память: 16 ГБ. • Объем свободного места на диске: 500 ГБ. 1 узел с коррелятором KUMA: • Процессор: 8 ядер. • Оперативная память: 32 ГБ. • Объем свободного места на диске: 500 ГБ. 3 узла с кипером KUMA: • Процессор: 6 ядер. • Оперативная память: 12 ГБ. • Объем свободного места на диске: 150 ГБ. 2 узла с хранилищами KUMA:	1 первичный узел XDR**: • Процессор: 4 ядра. • Оперативная память: 8 ГБ. • Объем свободного места на диске: 500 ГБ. 3 рабочих узла XDR: • Процессор: 10 ядер. • Оперативная память: 24 ГБ. • Объем свободного места на диске: 1 ТБ. 1 узел базы данных XDR**: • Процессор: 12 ядер. • Оперативная память: 24 ГБ. • Объем свободного места на диске: 2.7 ТБ. 1 узел с коллектором KUMA: • Процессор: 8 ядер. • Оперативная память: 16 ГБ. • Объем свободного места на диске: 500 ГБ. 1 узел с коррелятором KUMA: • Процессор: 8 ядер. • Оперативная память: 32 ГБ. • Объем свободного места на диске: 500 ГБ. 3 узла с кипером KUMA: • Процессор: 6 ядер. • Оперативная память: 12 ГБ. • Объем свободного места на диске: 150 ГБ. 2 узла с хранилищами KUMA: • Процессор: 24 ядра.	1 первичный узел XDR**: • Процессор: 4 ядра. • Оперативная память: 8 ГБ. • Объем свободного места на диске: 500 ГБ. 3 рабочих узла XDR: • Процессор: 12 ядер. • Оперативная память: 28 ГБ. • Объем свободного места на диске: 1 ТБ. 1 узел базы данных XDR**: • Процессор: 16 ядер. • Оперативная память: 32 ГБ. • Объем свободного места на диске: 4.3 ТБ. 1 узел с коллектором KUMA: • Процессор: 8 ядер. • Оперативная память: 16 ГБ. • Объем свободного места на диске: 500 ГБ. 1 узел с коррелятором KUMA: • Процессор: 8 ядер. • Оперативная память: 32 ГБ. • Объем свободного места на диске: 500 ГБ. 3 узла с кипером KUMA: • Процессор: 6 ядер.

	• Процессор: 24 ядра. • Оперативная память: 64 ГБ. • Объем свободного места на диске SSD: 4,7 ТБ.	• Оперативная память: 64 ГБ. • Объем свободного места на диске SSD: 7 ТБ.	• Оперативная память: 12 ГБ. • Объем свободного места на диске: 150 ГБ. 2 узла с хранилищами KUMA: Процессор: 24 ядра. Оперативная память: 64 ГБ. Объем свободного места на диске SSD: 12 ТБ.

*Требования не учитывают устройства для сервисов KEDR.

** База данных может размещаться как внутри кластера, так и на отдельном устройстве вне кластера.

Для корректного развертывания решения убедитесь, что процессоры целевых устройств поддерживают набор инструкций BMI/AVX.

Open Single Management Platform: программные требования

Требования к программному обеспечению и поддерживаемым системам и платформам

Операционная система	Поддерживаются следующие 64-разрядные версии операционных систем: Astra Linux Special Edition РУСБ.10015-01 (2023-0426SE17 обновление 1.7.4). Ubuntu Server 22.04 LTS. Debian GNU/Linux 11.x (Bullseye).
Платформы виртуализации	VMWare vSphere 7. VMWare vSphere 8. Microsoft Hyper-V Server 2016. Microsoft Hyper-V Server 2019. Microsoft Hyper-V Server 2022. Kernel-based Virtual Machine. Proxmox Virtual Environment 7.2. Proxmox Virtual Environment 7.3. Nutanix AHV 20220304.242 и выше.
Система управления базами данных (СУБД)	PostgreSQL 13.x 64-разрядная. PostgreSQL 14.x 64-разрядная. PostgreSQL 15.x 64-разрядная. Postgres Pro 13.x (все редакции) 64-разрядная. Postgres Pro 14.x (все редакции) 64-разрядная. Postgres Pro 15.x (все редакции) 64-разрядная.

Поддерживаются высокодоступные кластеры PostgreSQL. Роль Postgres, используемая Сервером для доступа к СУБД, должна иметь права на чтение следующих представлений (по умолчанию права назначены):

- pg_stat_replication
- pg_stat_wal_receiver

Kaspersky Deployment Toolkit

Все компоненты Open Single Management Platform устанавливаются с помощью Kaspersky Deployment Toolkit.

Kaspersky Deployment Toolkit имеет следующие аппаратные и программные требования:

Спецификация	Системные требования
Оборудование	Процессор: 4 ядра, частота от 2500 МГц. Оперативная память: 8 ГБ. Объем свободного места на диске: 40 ГБ.
Операционная система	Поддерживаются следующие 64-разрядные версии операционных систем: • Astra Linux Special Edition РУСБ.10015-01 (2023-0426SE17 обновление 1.7.4). • Oracle Linux 9. • Ubuntu Server 22.04 LTS. • Debian GNU/Linux 11.x (Bullseye). • CentOS 7.x. • CentOS 8.x.

Компоненты Open Single Management Platform

Чтобы просмотреть аппаратные и программные требования для компонента Open Single Management Platform, нажмите на его название:

- Консоль OSMP
- Kaspersky Unified Monitoring and Analysis Platform (далее также KUMA)
- Подчиненные Серверы администрирования Kaspersky Security Center
- Агент администрирования Kaspersky Security Center
- Kaspersky Endpoint Security для Windows
- Kaspersky Anti Targeted Attack Platform (далее также KATA)
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky CyberTrace
- Kaspersky Threat Intelligence Portal
- Kaspersky Automated Security Awareness Platform (далее также KASAP)

Требования к устройствам с сервисами KUMA

Сервисы KUMA (коллекторы, коррелляторы и хранилища) устанавливаются на устройствах, находящихся за пределами кластера Kubernetes. Аппаратные и программные требования для этих устройств описаны в этой статье.

Рекомендованные аппаратные и программные требования

В этом разделе перечислены аппаратные и программные требования для обработки потока данных до 40 000 событий в секунду (EPS). Значение нагрузки KUMA зависит от типа анализируемых событий и эффективности нормализатора.

Для повышения эффективности обработки событий количество ядер процессора важнее тактовой чистоты. Например, 8 ядер процессора со средней тактовой частотой могут обрабатывать события эффективнее, чем 4 ядра процессора с высокой тактовой частотой. В таблице ниже перечислены аппаратные и программные требования компонентов KUMA.

Объем оперативной памяти, используемой коллектором, зависит от настроенных способов обогащения (DNS, учетные записи, активы, обогащение данными из Kaspersky CyberTrace) и от того, используется ли агрегирование. На потребление оперативной памяти влияют параметры окна агрегации данных, количество полей, используемых для агрегации данных, объем данных в агрегируемых полях.

Например, с потоком событий 1000 EPS и отключенным обогащением событий (обогащение событий отключено, агрегация событий отключена, 5000 учетных записей, 5000 активов на одного тенанта) одному коллектору требуются следующие ресурсы:

- 1 процессорное ядро или 1 виртуальный процессор;
- 512 МБ оперативной памяти;
- 1 ГБ дискового пространства (без учета кеша событий).

Например, для 5 коллекторов, которые не выполняют обогащение событий, потребуется выделить следующие ресурсы: 5 процессорных ядер, 2,5 ГБ оперативной памяти и 5 ГБ свободного дискового пространства.

Рекомендуемые аппаратные и программные требования для установки сервисов KUMA

	Коллектор	Коррелятор	Хранилище
Процессор	Intel или AMD с поддержкой SSE 4.2: от 4 ядер 8 потоков или 8 виртуальных процессоров.	Intel или AMD с поддержкой SSE 4.2: от 4 ядер 8 потоков или 8 виртуальных процессоров.	Intel или AMD с поддержкой SSE 4.2: от 12 ядер 24 потоков или 24 виртуальных процессоров.
ОЗУ	16 ГБ	16 ГБ	48 ГБ
Свободное место диске	Размер директории /opt: от 500 ГБ.	Размер директории /opt: от 500 ГБ.	Размер директории /opt: от 500 ГБ.
Операционные системы	• Ubuntu 22.04 LTS (Jammy Jellyfish). • Oracle Linux 8.6, 8.7, 9.2, 9.4. • Astra Linux Special Edition РУСБ.10015-01 (2021-1126SE17 обновление 1.7.1). • Astra Linux Special Edition РУСБ.10015-01 (2022-1011SE17MD обновление 1.7.2.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2022-1110SE17 обновление 1.7.3). Требуется версия ядра 5.15.0.33 или выше. • Astra Linux Special Edition РУСБ.10015-01 (2023-0630SE17MD обновление 1.7.4.UU.1). • Astra Linux Special Edition РУСБ.10015-01 (2023-1023SE17MD обновление 1.7.5).		

Пропускная способность сети	100 Мбит/с	100 Мбит/с	Скорость передачи данных между узлами ClickHouse должна быть не менее 10 Гбит/с, если поток данных превышает 20 000 EPS.

Установка KUMA поддерживается в следующих виртуальных средах:

- VMware 6.5 и выше.
- Hyper-V for Windows Server 2012 R2 и выше.
- QEMU-KVM 4.2 и выше.
- Программный комплекс средств виртуализации "Брест" РДЦП.10001-02.

Рекомендации "Лаборатории Касперского" для серверов хранения

Для серверов хранения данных специалисты "Лаборатории Касперского" рекомендуют следующее:

- Ставьте ClickHouse на твердотельные накопители (SSD). Твердотельные накопители помогают повысить скорость доступа к данным. Жесткие диски можно использовать для хранения данных с помощью технологии HDFS.
- Чтобы подключить систему хранения данных к серверам хранения, используйте высокоскоростные протоколы, такие как Fibre Channel или iSCSI 10G. Не рекомендуется использовать протоколы уровня приложений, например NFS и SMB, для подключения систем хранения данных.
- Используйте файловую систему ext4 на кластерных серверах ClickHouse.
- Если вы используете RAID-массивы, используйте RAID 0 для высокой производительности или RAID 10 для высокой производительности и отказоустойчивости.
- Для обеспечения отказоустойчивости и производительности подсистемы хранения данных, убедитесь, что узлы ClickHouse разворачиваются строго на разных дисковых массивах.
- Если вы используете виртуализированную инфраструктуру для размещения компонентов системы, разворачивайте узлы кластера ClickHouse на разных гипервизорах. В этом случае необходимо запретить двум виртуальным машинам с ClickHouse работать с одним гипервизором.
- Для высоконагруженных установок KUMA установите ClickHouse на физических серверах.

Требования к устройствам для установки агентов

Чтобы отправлять данные в коллектор KUMA, вам нужно установить агенты на устройствах сетевой инфраструктуры. Требования к аппаратному и программному обеспечению перечислены в таблице ниже.

Рекомендуемые аппаратные и программные требования для установки агентов

	Устройства с операционной системой Windows	**Устройства с операционной системой Linux**
Процессор	Одноядерный, 1.4 ГГц или выше	Одноядерный, 1.4 ГГц или выше
ОЗУ	512 МБ	512 МБ
Свободное место диске	1 ГБ	1 ГБ
Операционные системы	• Microsoft Windows 2012.	• Astra Linux Special Edition РУСБ.10015-01 (2023-0426SE17 обновление 1.7.4).

	• Microsoft Windows Server 2012 R2. • Microsoft Windows Server 2016. • Microsoft Windows Server 2019. • Microsoft Windows 10 20H2, 21H1.	• Ubuntu 22.04 LTS (Jammy Jellyfish). • Debian 11.7 (Bullseye).

Требования к операционной системе

Требования к операционной системе, перечисленные в таблице ниже.

Требования к установке операционной системы

	Astra Linux
Версия Python	3.6 и выше
Модуль SELinux	Выключен
Менеджер пакетов	pip3
Базовые пакеты	• python3-apt • curl • libcurl4 Пакеты можно установить с помощью следующей команды: `apt install python3-apt curl libcurl4`
Зависимые пакеты	• netaddr • python3-cffi-backend Пакеты можно установить с помощью следующей команды: `apt install python3-netaddr python3-cffi-backend` Если вы планируете запрашивать базы данных Oracle DB из KUMA, вам нужно установить пакет libaio1 Astra Linux.
Уровень прав пользователя, необходимый для установки приложения	Чтобы назначить необходимые права учетной записи пользователя, используемой для установки приложения, запустите следующую команду: `sudo pdpl-user -i 63 <имя учетной записи пользователя, используемой для установки приложения>`

Требования к Консоли OSMP

Сервер OSMP

Требования к оборудованию и программному обеспечению см. в требованиях к рабочему узлу.

Клиентские устройства

Клиентскому устройству для работы с Консолью OSMP требуется только браузер.

Минимальное разрешение экрана составляет 1366x768 пикселей.

Требования к аппаратному и программному обеспечению устройства совпадают с требованиями к браузеру, который используется для работы с Консолью OSMP.

Браузеры:

- Google Chrome 100.0.4896.88 или более поздняя версия (официальная сборка).
- Microsoft Edge 100 или более поздняя версия.
- Safari 15 для macOS.
- Яндекс Браузер 23.5.0.2271 и выше.
- Mozilla Firefox Extended Support Release 102.0 или выше.

Требования к Агенту администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Требования к программному обеспечению для устройств с операционной системой Linux: должен быть установлен интерпретатор языка Perl версии 5.10 и выше.

Агент администрирования. Поддерживаемые платформы

Операционные системы. Рабочие станции Microsoft Windows	Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная. Microsoft Windows Embedded 7 Standard Service Pack 1 32-разрядная/64-разрядная. Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1703, 1709, 1803, 1809 32-разрядная/64-разрядная. Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1909 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная. Microsoft Windows 10 TH1 (July 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.

	Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная. Microsoft Windows 8 Pro/Enterprise 32-разрядная/64-разрядная. Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium Service Pack 1 и выше 32-разрядная/64-разрядная. Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная (поддерживается Агентом администрирования версии 10.5.1781). Microsoft Windows XP Professional Service Pack 3 и выше 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023). Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023).
Операционные системы. Серверы Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-разрядная. Microsoft Windows Server 2003 SP1 32-разрядная/64-разрядная (поддерживаются только для Агента администрирования версии 10.5.1781, которую вы можете запросить в Службе технической поддержки). Microsoft Windows Server 2008 Foundation Service Pack 2 32-разрядная/64-разрядная. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter Service Pack 2 32-разрядная/64-разрядная. Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard Service Pack 1 и выше 64-разрядная. Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-разрядная. Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-разрядная. Windows Server 2016 Datacenter/Standard (вариант установки Server Core) (LTSB) 64-разрядная. Microsoft Windows Server 2019 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2019 RS5 Essentials/Standard 64-разрядная. Microsoft Windows Server 2022 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-разрядная. Microsoft Windows Storage Server 2019 64-разрядная. Microsoft Windows Small Business Server 2011 Standard 64-разрядная. Microsoft Windows Small Business Server 2011 Essentials 64-разрядная. Microsoft Windows Small Business Server 2011 Premium Add-on 64-разрядная.
Операционные системы. Linux	Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная. Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная. Debian GNU/Linux 12 (Bookworm) 32-разрядная/64-разрядная. Ubuntu Server 10.04 LTS (Lucid Lynx) 32-разрядная/64-разрядная. Ubuntu Server 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная. Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная. Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная. Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная. Ubuntu Server 22.04 LTS ARM 64-разрядная. Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.

Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32-разрядная/64-разрядная.
Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная.
CentOS 6.x 32-разрядная/64-разрядная.
CentOS 7.2 и выше 64-разрядная.
CentOS Stream 8 64-разрядная.
CentOS Stream 9 64-разрядная.
CentOS Stream 9 ARM 64-разрядная.
Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная.
Red Hat Enterprise Linux Server 7.2 и выше 64-разрядная.
Red Hat Enterprise Linux Server 8.x 64-разрядная.
Red Hat Enterprise Linux Server 9.x 64-разрядная.
SUSE Linux Enterprise Server 12.5 и выше (все пакеты обновлений) 64-разрядная.
SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
SUSE Linux Enterprise Server 15 (все пакеты обновлений) ARM 64-разрядная.
openSUSE Leap 15 64-разрядная.
EulerOS 2.0 SP10 64-разрядная.
EulerOS 2.0 SP10 ARM 64-разрядная.
Astra Linux Special Edition RUSB.10015-01 (обновление 1.5) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6) 64-разрядная.
Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7) ARM 64-разрядная.
Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
Альт Рабочая станция 10.1 64-разрядная.
Альт Сервер 10.1 64-разрядная.
ALT Education 10.1 64-разрядная.
Альт СП Сервер 10 32-разрядная/64-разрядная.
Альт СП Сервер 10 ARM 64-разрядная.
Альт СП Рабочая станция 10 32-разрядная/64-разрядная.
Альт СП Рабочая станция 10 ARM 64-разрядная.
Альт 8 СП Сервер (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
Альт 8 СП Сервер (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
Альт 8 СП Сервер (ЛКНВ.11100-03) 32-разрядная/64-разрядная.
Альт 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
Альт 8 СП Рабочая станция (ЛКНВ.11100-03) 32-разрядная/64-разрядная.
Mageia 4 32-разрядная.
Oracle Linux 7 64-разрядная.
Oracle Linux 8 64-разрядная.
Oracle Linux 9 64-разрядная.
Linux Mint 20.3 и выше 64-разрядная.
Linux Mint 21.1 и выше 64-разрядная.
Linux Mint 22.x 64-разрядная.
AlterOS 7.5 и выше 64-разрядная.
ГосЛинукс IC6/7.17 64-разрядная.
ГосЛинукс IC6/7.2 64-разрядная.
SberOS 3.3.3 64-разрядная.
Platform V SberLinux OS Server (SLO) 8.8 64-разрядная.
Platform V SberLinux OS Server (SLO) 8.9.2 64-разрядная.
РЕД ОС 7.3 ARM 64-разрядная.
РЕД ОС 7.3 Сервер 64-разрядная.
РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

	РЕД ОС 8 64-разрядная. РЕД ОС 8 ARM 64-разрядная. ROSA Enterprise Linux Server 7.9 64-разрядная. ROSA Enterprise Linux Desktop 7.9 64-разрядная. РОСА "КОБАЛЬТ" 7.9 64-разрядная. РОСА "ХРОМ" 12 64-разрядная. AlmaLinux 8 и выше 64-разрядная. AlmaLinux 9 и выше 64-разрядная. Rocky Linux 8 и выше 64-разрядная. Rocky Linux 9 и выше 64-разрядная. Atlant, Alcyone build, версия 2022.02 64-разрядная. MSVSPHERE 9.2 SERVER 64-разрядная. MSVSPHERE 9.2 ARM 64-разрядная. MSVSPHERE 9.4 SERVER 64-разрядная. MSVSPHERE 9.4 ARM 64-разрядная. SynthesisM Server 8.6 64-разрядная. SynthesisM Client 8.6 64-разрядная. ОСнова 2.* 64-разрядная. Kylin 10 64-разрядная. EMIAS 1.0 64-разрядная. Amazon Linux 2 64-разрядная. МосОС 15.4 Arbat 64-разрядная. M OC (Moscow Electronic School) 12 (для компьютеров и ноутбуков) 64-разрядная. M OC (Moscow Electronic School) 12 (для интерактивных панелей) 64-разрядная. M OC (Moscow Electronic School) 12 Сервер 64-разрядная. Mostech 64-разрядная. Mostech Server 64-разрядная. Fedora Linux Server 40 64-разрядная. Fedora Linux Workstation 40 64-разрядная.
Операционные системы. macOS	macOS Monterey (12.x). macOS Ventura (13.x). macOS Sonoma (14.x). macOS Catalina (15.x). Для Агента администрирования поддерживается архитектура Apple Silicon (M1), также, как и Intel.
Платформы виртуализации	VMware vSphere 6.7.0. VMware vSphere 7.0.3. Citrix XenServer 7.x. Citrix XenServer 8.2. Parallels Desktop 18. Oracle VM VirtualBox 7.0.12. Microsoft Hyper-V Server 2019 64-разрядная. Microsoft Hyper-V Server 2022 64-разрядная. Kernel-based Virtual Machine (все операционные системы Linux, поддерживаемые Агентом администрирования). См. требования к управляемым приложениям для других поддерживаемых платформ.

На устройствах под управлением Windows 10 версии RS4 или RS5 Kaspersky Security Center может не обнаруживать некоторые уязвимости в папках, в которых включен учет регистра.

Перед установкой Агента администрирования на устройства под управлением Windows 7, Windows Server 2008, Windows Server 2008 R2 или Windows MultiPoint Server 2011 убедитесь, что вы установили обновление безопасности KB3063858 для ОС Windows (Обновление безопасности для Windows 7 (KB3063858), Обновление безопасности для Windows 7 для систем на базе x64 (KB3063858), Обновление безопасности для Windows Server 2008 (KB3063858), Обновление безопасности для Windows Server 2008 x64 Edition (KB3063858), Обновление безопасности для Windows Server 2008 R2 x64 Edition (KB3063858).

В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно.

Вы можете установить или обновить Агент администрирования для Windows XP только в Microsoft Windows XP. Поддерживаемые редакции Microsoft Windows XP и соответствующие им версии Агента администрирования указаны в списке поддерживаемых операционных систем. Вы можете скачать необходимую версию Агента администрирования для Microsoft Windows XP с этой страницы.

Рекомендуется устанавливать ту же версию Агента администрирования для Linux, что и Open Single Management Platform.

Open Single Management Platform полностью поддерживает Агент администрирования той же или выше.

Агент администрирования для macOS поставляется вместе с приложением безопасности "Лаборатории Касперского" для этой операционной системы.

Совместимые приложения и решения

Open Single Management Platform может быть интегрирован со следующими версиями приложений и решений:

- Kaspersky Security Center 15 Linux (в качестве подчиненных Серверов администрирования)
- Kaspersky Security Center 14.2 Windows (в качестве подчиненных Серверов администрирования)
- Kaspersky Anti Targeted Attack Platform 5.1
- Kaspersky Anti Targeted Attack Platform 6.0
- Kaspersky Anti Targeted Attack Platform 7.0
- Kaspersky Endpoint Security для Windows 12.3 и выше (поддерживает файловые серверы)
- Kaspersky Endpoint Security 12.4 для Windows
- Kaspersky Endpoint Security 12.0 для Mac
- Kaspersky CyberTrace 4.2 (интеграция настраивается только в Консоли KUMA)

- Kaspersky Industrial CyberSecurity for Nodes 3.2 и выше
- Kaspersky Endpoint Agent 3.16
- Kaspersky Industrial CyberSecurity for Networks 4.0 (интеграция настраивается только в Консоли KUMA)
- Kaspersky Secure Mail Gateway 2.0 и выше (интеграция настраивается только в Консоли KUMA)
- Kaspersky Security для Linux Mail Server 10 и выше (интеграция настраивается только в Консоли KUMA)
- Kaspersky Web Traffic Security 6.0 и выше (интеграция настраивается только в Консоли KUMA)
- UserGate 7
- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal

Подробнее о версиях приложений и решений см. на странице "Жизненный цикл приложений".

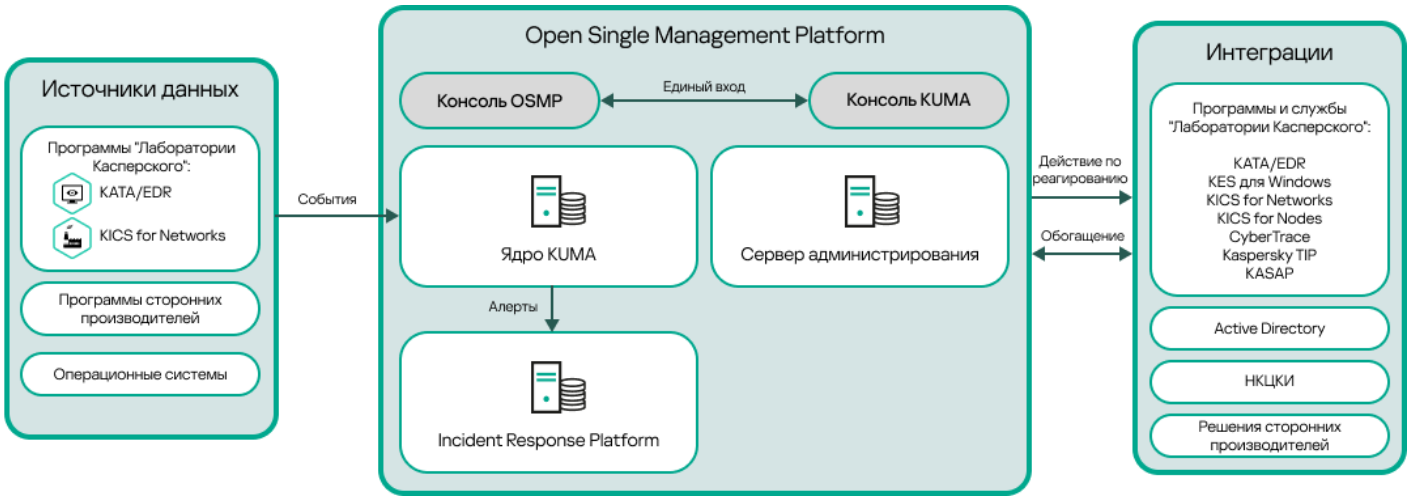
Список ограничений

Open Single Management Platform поддерживает управление Kaspersky Endpoint Security для Windows со следующими ограничениями:

- Компонент Адаптивный контроль аномалий не поддерживается. Open Single Management Platform не поддерживает правила Адаптивного контроля аномалий.
- Компоненты Kaspersky Sandbox не поддерживаются.

Архитектура Open Single Management Platform

Этот раздел содержит описание компонентов Open Single Management Platform и их взаимодействия.



Архитектура Open Single Management Platform

Open Single Management Platform включает в себя следующие основные компоненты:

- **OSMP**. Технологическая основа, на которой построен Open Single Management Platform. OSMP объединяет все компоненты решения и обеспечивает взаимодействие между компонентами. OSMP является масштабируемым и поддерживает интеграцию как с приложениями "Лаборатории Касперского", так и со сторонними решениями.

- **Консоль OSMP**. Представляет собой веб-интерфейс OSMP.

- **Консоль KUMA**. Представляет собой веб-интерфейс Kaspersky Unified Monitoring and Analysis Platform (KUMA).

- Ядро KUMA. Центральный компонент KUMA. KUMA получает, обрабатывает и хранит события информационной безопасности, а затем анализирует события с помощью правил корреляции. Если в результате анализа срабатывает правило корреляции, KUMA создает алерт и отправляет его в Incident Response Platform.

- **Incident Response Platform**. Компонент Open Single Management Platform, который позволяет создавать инциденты автоматически или вручную, управлять жизненным циклом алертов и инцидентов, назначать алерты и инциденты аналитикам SOC, а также автоматически или вручную реагировать на инциденты, включая действия по реагированию с помощью плейбуков.

- Сервер администрирования (далее также *Сервер*). Ключевой компонент защиты конечных точек организации-клиента. Сервер администрирования обеспечивает централизованное развертывание и управление защитой конечных точек с помощью EPP-программ, а также позволяет контролировать состояние защиты конечных точек.

- **Источники данных**. Аппаратное и программное обеспечение информационной безопасности, которое создает события. После интеграции Open Single Management Platform с необходимыми источниками данных, KUMA получает события для их хранения и анализа.

- Интеграции. Приложения "Лаборатории Касперского" и сторонние решения, интегрированные в OSMP. С помощью интегрированных решений аналитик SOC может обогащать данные, необходимые для расследования инцидентов и реагирования на них.

Интерфейс Консоли OSMP

Open Single Management Platform управляется с помощью интерфейса Консоли OSMP.

Окно Консоли OSMP содержит следующие элементы:

- главное меню в левой части окна;
- рабочая область в правой части окна.

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования**. Отображает имя Сервера администрирования, к которому вы сейчас подключены. Нажмите на значок параметров (), чтобы открыть свойства Сервера администрирования.
- **Мониторинг и отчеты**. Предоставляет сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.
- **Активы (Устройства)**. Содержит инструменты для активов, а также задачи и политики приложений "Лаборатории Касперского".
- **Пользователи и роли**. Позволяет управлять пользователями и ролями, настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями.
- **Операции**. Содержит различные параметры, включая лицензирование приложений, просмотр и управление зашифрованными дисками и событиями шифрования, а также управление приложениями сторонних производителей. Раздел также предоставляет вам доступ к хранилищам приложений.
- **Обнаружение устройств и развертывание**. Позволяет опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. Этот раздел содержит мастер первоначальной настройки и мастер развертывания защиты.
- **Marketplace**. Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".
- **Параметры**. Позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Содержит личные параметры, связанные с внешним видом интерфейса, такие как язык интерфейса или тема.
- **Меню вашей учетной записи**. Содержит ссылку на справку Open Single Management Platform. Также вы можете выйти из Open Single Management Platform и просмотреть версию Консоли OSMP и список установленных веб-плагинов управления.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окон интерфейса Консоли OSMP. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

Закрепление и отмена закрепления разделов главного меню

Вы можете закрепить разделы Консоли OSMP, чтобы добавить их в избранное и быстро получить к ним доступ из раздела **Закрепленное** в главном меню.

Если закрепленных элементов нет, раздел **Закрепленное** не отображается в главном меню.

Вы можете закрепить разделы, в которых отображаются только страницы. Например, если вы перейдете в раздел **Активы (Устройства)** → **Управляемые устройства**, откроется страница с таблицей устройств, что означает, что вы можете закрепить раздел **Управляемые устройства**. Если после выбора раздела в главном меню окно или элемент не отображается, то закрепить такой раздел нельзя.

Чтобы закрепить раздел:

1. В главном меню наведите курсор мыши на раздел, который вы хотите закрепить.

   Отображается значок булавки (📌).

2. Нажмите на значок булавки (📌).

Раздел закреплен и отображается в разделе **Закрепленное**.

Максимальное количество элементов, которые вы можете закрепить, равно пяти.

Вы также можете удалить элементы из избранных, отменив их закрепление.

Чтобы отменить закрепление раздела:

1. В главном окне приложения перейдите в раздел **Закрепленное**.
2. Наведите курсор мыши на раздел, для которого вы хотите отменить закрепление и нажмите на значок отмены закрепления (📌).

Раздел удален из избранных.

Изменение языка интерфейса Консоли OSMP

Вы можете выбрать язык интерфейса Консоли OSMP.

Чтобы изменить язык интерфейса:

1. В главном окне приложения перейдите в раздел **Параметры** → **Язык**.
2. Выберите необходимый язык интерфейса.

Лицензирование

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Open Single Management Platform.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Open Single Management Platform.
- Прочитав документ license.txt. Этот документ включен в комплект поставки приложения.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вам нужно прервать установку приложения и вы не должны использовать приложение.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Open Single Management Platform. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Open Single Management Platform или после заказа пробной версии Open Single Management Platform.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Open Single Management Platform или после заказа пробной версии Open Single Management Platform.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

Лицензионные ограничения

Приобретая лицензию на Open Single Management Platform, вы определяете количество пользователей, которых хотите защитить. Вы можете превысить лицензионное ограничение не более чем на 5%. Если вы превысите лицензионное ограничение более чем на 5%, дополнительные устройства и дополнительные учетные записи будут добавлены в список **Ограниченные активы**.

Если лицензионное ограничение превышено, в верхней части Консоли OSMP отображается уведомление.

Невозможно запустить действия по реагированию или сценарии для ограниченных активов.

Чтобы просмотреть список ограниченных активов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. В разделе **Тенанты** нажмите на корневой тенант.

   Откроется окно свойств корневого тенанта.
3. Выберите вкладку **Лицензии**.
4. Перейдите по ссылке с количеством ограниченных активов.

Откроется окно **Ограниченные активы**.

В списке отображается не более 2000 ограниченных активов.

Активация Open Single Management Platform

После установки Open Single Management Platform вам необходимо активировать приложение в свойствах Сервера администрирования.

Чтобы активировать Open Single Management Platform:

1. В главном меню нажмите на значок параметров () рядом с именем корневого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Лицензионные ключи**.
3. В разделе **Действующая лицензия** нажмите на кнопку **Выбрать**.
4. В открывшемся окне выберите лицензионный ключ, который вы хотите использовать для активации Open Single Management Platform. Если лицензионного ключа нет в списке, нажмите на кнопку **Добавить лицензионный ключ** и укажите новый лицензионный ключ.
5. При необходимости вы также можете добавить резервный лицензионный ключ. Для этого в разделе **Резервный лицензионный ключ** нажмите на кнопку **Выбрать** и выберите существующий лицензионный ключ или добавьте ключ. Обратите внимание, что вы не можете добавить резервный лицензионный ключ, если нет активного лицензионного ключа.
6. Нажмите на кнопку **Сохранить**.

Просмотр информации об используемых лицензионных ключах

Чтобы просмотреть информацию об активном и резервном лицензионных ключах:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. В разделе **Тенанты** нажмите на корневой тенант.

   Откроется окно свойств корневого тенанта.

3. Выберите вкладку **Лицензии**.

   Отображается информация об активном и резервном лицензионных ключах.

Отображаемый лицензионный ключ применяется ко всем дочерним тенантам корневого тенанта. Указать отдельный лицензионный ключ для дочернего тенанта невозможно. В окне свойств дочерних тенантов нет вкладки **Лицензии**.

Если лицензионное ограничение ключей превышено, отображается уведомление, а в информации о лицензионном ключе отображается предупреждение.

Вы можете нажать на кнопку **Перейти к Серверу администрирования**, чтобы управлять лицензионными ключами Open Single Management Platform.

Также можно просмотреть список объектов, используемых по лицензии на вкладке **Лицензии**. Для этого нажмите на кнопку ⓘ.

Доступность объекта, используемого по лицензии, зависит от типа приобретенной лицензии. Дополнительную информацию о типах лицензий см. в разделе Лицензирование и возможности Open Single Management Platform.

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить лицензии на Open Single Management Platform и включенные в него приложения "Лаборатории Касперского", такие как Kaspersky Unified Monitoring and Analysis Platform и Open Single Management Platform. Вы можете продлить лицензии, срок действия которых истек или истекает в течение 30 дней.

Письмо с архивом, содержащим новые лицензионные ключи, будет отправлено на ваш адрес электронной почты после покупки новой лицензии на Open Single Management Platform.

Чтобы продлить лицензию на Open Single Management Platform:

1. Извлеките новые лицензионные ключи из архива, отправленного на ваш адрес электронной почты.

2. Следуйте инструкциям в разделе Активация Open Single Management Platform.

   Срок действия лицензии продлен.

> Если вам необходимо продлить лицензии включенных приложений "Лаборатории Касперского", вам нужно добавить лицензионные ключи в веб-интерфейсы этих решений.

О том, как продлить лицензию на Kaspersky Unified Monitoring and Analysis Platform, см. раздел Добавление лицензионного ключа в веб-интерфейс приложения справки Kaspersky Unified Monitoring and Analysis Platform.

О том, как продлить лицензию на Kaspersky Endpoint Detection and Response Expert, см. раздел Добавление ключа справки Kaspersky Anti Targeted Attack Platform.

В Консоли OSMP уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;

- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;
- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

О предоставлении данных

Данные, обрабатываемые локально

Open Single Management Platform предназначен для оптимизации выявления угроз, расследования инцидентов, реагирования (в том числе автоматического), а также проактивного поиска угроз в реальном времени.

Open Single Management Platform выполняет следующие основные функции:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- расследование инцидентов и алертов, ручное реагирование;
- автоматическое реагирование с использованием предустановленных и пользовательских плейбуков;
- поиск угроз по событиям в реальном времени.

Для выполнения своих основных функций приложение Open Single Management Platform может принимать, хранить и обрабатывать следующую информацию:

- Информация об устройствах, на которые производится установка компонентов Open Single Management Platform:
  - Имя устройства, MAC-адрес, поставщик операционной системы, номер сборки операционной системы, версия ядра ОС, наличие требуемых установленных пакетов, наличие прав для учетной записи, тип средства управления службами, состояние портов. Данная информация собирается Kaspersky Deployment Toolkit при установке.
  - IPv4-адрес. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Имена учетных записей для доступа к устройствам, на которые производится установка компонентов Open Single Management Platform, и SSH ключи. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Имя и пароль учетной записи Open Single Management Platform. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Данные для доступа к СУБД: IP/DNS имя, порт, логин и пароль пользователя. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Файлы инвентаря и лицензии KUMA. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Зона DNS. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.
- Сертификаты безопасного подключения устройств к компонентам Open Single Management Platform. Данная информация заполняется пользователем в конфигурационном файле Kaspersky Deployment Toolkit.

- Гибкая модель статусов инцидентов, включая предустановленные (стандартная или ГОСТ). Наличие модель статусов по ГОСТ настраивается пользователем в конфигурационном файле Kaspersky Deployment Toolkit.

  Информация, которую заполняет пользователь в конфигурационном файле Kaspersky Deployment Toolkit и которую собирает Kaspersky Deployment Toolkit при установке, сохраняется в лог установки, который хранится в базе данных Kaspersky Deployment Toolkit. Лог установки первоначальной инфраструктуры сохраняется в файл на машине пользователя. Срок хранения не ограничен, файл будет удален при деинсталляции решения. Имена пользователей и пароли хранятся в зашифрованном виде.

- Информация о типах инцидентов: общая информация о типе, включая имя и описания типа; связь типа и модели статусов инцидентов.

- Информация об учетных записях пользователей: полное имя и адрес электронной почты. Данная информация вводится пользователем в Консоли OSMP и KUMA. Данные хранятся в базе данных неограниченное время, пока пользователь их не удалит.

- Данные об интеграционном токене.

- Информация о тенантах: название тенанта, название родительского тенанта, описание. Данная информация вводится пользователем в Консоли OSMP и KUMA. Данные хранятся в базе данных неограниченное время, пока пользователь их не удалит.

- Данные об алертах и инцидентах:

  - Данные об алертах: сработавшие правила, соответствие матрице MITRE, статус алерта, резолюция, назначенный оператор, затронутые активы (устройства и учетные записи), наблюдаемые объекты (IP, MD5, SHA256, URL, DNS-домен или DNS-имя, имя пользователя, имя хоста), признак наличия устройств КИИ в алерте, комментарии и журнал изменений, файлы. Данная информация формируется в Консоли OSMP автоматически на основании корреляционных событий из Kaspersky Unified Monitoring and Analysis Platform.

  - Данные об инцидентах: связанные алерты, сработавшие правила, соответствие матрице MITRE, статус инцидента, резолюция, затронутые активы (устройства и аккаунты), наблюдаемый объект (из алерта), признак наличия устройств КИИ в инциденте, комментарии и журнал изменений. Данная информация формируется в консоли OSMP автоматически по правилам или вручную пользователем, файлы, тип инцидента.

  - Данные об инцидентах НКЦКИ: сведения об атакованном ресурсе и о вредоносной системе, информацию из ГосСОПКА по экспортированному инциденту (уникальный идентификатор карточки уведомления в НКЦКИ, регистрационный номер уведомления, дата и время регистрации инцидента в ГосСОПКА, дата последнего обновления инцидента в ГосСОПКА) и журнал изменений. Данная информация формируется автоматически на основании инцидентов XDR для передачи в ГосСОПКА.

  - Данные о настройке правил формирования инцидентов из алертов: имя и условия срабатывания правила, шаблон имени нового инцидента, описание правила и приоритет запуска правила. Данная информация вводится пользователем в Консоли OSMP.

  - Данные о шаблонах уведомлений: имя шаблона, тема сообщения, шаблон текста сообщения, описание шаблона и правила детектирования, при срабатывании которых будут отправляться уведомления. Данная информация вводится пользователем в Консоли OSMP.

  Данные об алертах и инцидентах хранятся в соответствии с заданным пользователем сроком хранения.

  Данные об инцидентах НКЦКИ, настройке правил формирования инцидентов и шаблонах уведомлений хранятся в базе данных неограниченное время, пока пользователь не удалит их.

- Данные о настройках сроков хранения алертов и инцидентов
- Данные о плейбуках:
  - Операционные данные плейбука, в том числе данные о входных параметрах действий по реагированию: название, описание, теги, текст триггера и алгоритма. Данная информация вводится пользователем в Консоли OSMP.
  - Данные о результатах выполнения действий по реагированию в рамках исполнения плейбука: содержит данные из интегрированных систем, данные с устройств.
  - Полная история реагирований по всем алертам и инцидентам.

  Перечисленные выше данные о плейбуках хранятся в базе данных в течение трех дней, после чего удаляются. Данные полностью удаляются при деинсталляции Open Single Management Platform.
- Данные о параметрах интеграции (как с приложениями и службами "Лаборатории Касперского", так и со сторонними решениями, которые участвуют в сценариях Open Single Management Platform):
  - Интеграция с Kaspersky Threat Intelligence Portal: API-токен доступа для подключения к Kaspersky Threat Intelligence Portal, срок хранения кеша, признак подключения через прокси, тип сервиса. Данная информация вводится пользователем в Консоли OSMP.
  - Интеграция с НКЦКИ: URL-адрес, API-токен доступа для подключении к ГосСОПКА, наименование компании, сфера деятельности компании, сведения о местонахождении или географическом местоположении информационного ресурса или объекта, признак подключения через прокси. Данная информация вводится пользователем в Консоли OSMP.
  - Интеграция с KATA/EDR: адрес сервера KATA/EDR: IP адрес/имя устройства, порт, уникальный идентификатор для подключения к KATA/EDR, файл сертификата и закрытый ключ для подключения к KATA/EDR. Данная информация вводится пользователем в Консоли OSMP.
  - Подключение к устройству, где будет запускаться пользовательский скрипт: IP адрес/имя устройства, порт, логин пользователя и SSH ключ, пароль/ключ. Данная информация вводится пользователем в Консоли OSMP.
  - Интеграция с Сервером администрирования OSMP: имя Сервера администрирования, полный путь до Сервера администрирования в иерархии. Данная информация вводится пользователем в Консоли OSMP.
  - Интеграция с Kaspersky Cyber Trace: IPv4/Hostname и порт, по которому доступен Kaspersky Cyber Trace, имя и пароль для подключения. Данная информация вводится пользователем в Консоли KUMA.
  - Интеграция с Kaspersky Automated Security Awareness Platform (KASAP): API токен доступа при подключении к KASAP, URL портала KASAP, Email Администратора KASAP, признак подключения через прокси. Данная информация вводится пользователем в Консоли KUMA.
  - Интеграция с Active Directory: адреса контроллеров домена, логин и пароль для подключения к контроллерам домена, сертификат. Данная информация вводится пользователем в Консоли KUMA.
  - Интеграция с внешней системой (например UserGate): данные для подключения к удаленному клиентскому устройству: логин пользователя и SSH ключ, пароль/ключ.

  Перечисленные выше данные о настройках интеграции хранятся в базе данных неограниченное время, пока пользователь не удалит их. Данные полностью удаляются при деинсталляции приложения.

- IP-адрес, с которого пользователь подключается к консоли OSMP - фиксируется автоматически консолью, хранится до истечения времени хранения ревизий объектов, которые редактировал пользователь.

Подробную информацию о прочих данных, принимаемых, хранимых и обрабатываемых для выполнения основных функций решения Open Single Management Platform, см. в справке приложения:

- Kaspersky Security Center 15.2 Linux

- Kaspersky Unified Monitoring and Analysis Platform

Все перечисленные выше данные могут быть переданы в "Лабораторию Касперского" только посредством файлов дампа, файлов трассировки или файлов журналов компонентов Open Single Management Platform, включая файлы журналов, создаваемые инсталляторами и утилитами. Файлы дампов, файлы трассировки или файлы журналов компонентов Open Single Management Platform могут содержать персональные или конфиденциальные данные. Файлы дампов, файлы трассировки или файлы журналов хранятся в открытой форме на устройствах. Файлы дампов, файлы трассировки или файлы журналов не передаются в "Лабораторию Касперского" автоматически, но администратор может передать эти файлы в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Open Single Management Platform. "Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи. Срок хранения данной информации (период ротации) составляет, по умолчанию, 7 дней.

Данные, передаваемые в "Лабораторию Касперского"

Переходя по ссылкам из Консоли OSMP к справке OSMP, пользователь соглашается на автоматическую передачу в "Лабораторию Касперского" следующих данных: код OSMP, версия OSMP, локализация OSMP.

Для назначения обучающего курса сотруднику Open Single Management Platform передает в Kaspersky Automated Security Awareness Platform (KASAP) следующие данные: email пользователя, ID пользователя в KASAP, ID группы обучения.

Для получения дополнительных данных по алертам Open Single Management Platform передает в Threat Intelligence Portal следующую информацию: тип и значение наблюдаемых объектов из алертов, инцидентов, событий информационной безопасности.

Данные, передаваемые третьим сторонам

Для получения информации о тактике/технике MITRE при переходе по ссылке из карточки алерта/инцидента, Open Single Management Platform передает на сайт MITRE информацию о тактике/технике: ID и тип.

Для представления информации по инциденту НКЦКИ (Национальный координационный центр по компьютерным инцидентам) в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) Open Single Management Platform передает следующие данные:

- Краткое описание инцидента, категория инцидента, тип инцидента. Дата и время выявления компьютерного инцидента (признака инцидента), начала компьютерной атаки или выявления уязвимости (признака уязвимости), дата и время восстановления штатного режима работы контролируемого информационного ресурса (объекта КИИ) после компьютерного инцидента, окончания компьютерной атаки или устранения уязвимости.

- Наименование главной организации, в которой произошел инцидент. Наименование подчиненной организации, в которой произошел инцидент.

- Ограничительный маркер на распространение сведений из карточки компьютерной атаки, статус реагирования на инцидент.
- Название информационного ресурса, целевая функция или сфера деятельности, в которой функционирует информационный ресурс. Наличие одной из категорий у объекта КИИ или ее отсутствие. Сведения о месте нахождения или географического местоположения информационного ресурса или объекта КИИ. Город, в котором расположен объект КИИ, на котором произошел инцидент, атака или обнаружена уязвимость.
- Наименование уязвимого приложения, версия уязвимого приложения.
- Необходимость привлечения сил ГосСОПКА, сведения о средстве или способе выявления инцидента, наличие подключения к сети Интернет.
- Влияние на доступность, влияние на целостность, влияние на конфиденциальность. Описание иной формы последствий компьютерного инцидента или компьютерной атаки.
- IPv4-адрес и IPv6-адрес контролируемого ресурса, доменное имя контролируемого ресурса, URI-адрес контролируемого ресурса, Email-адрес контролируемого ресурса.
- Имя атакованной сетевой службы, порт/протокол сетевой службы.
- Тип активности, хеш-сумма вредоносного модуля, описание используемых уязвимостей, идентификатор уязвимости.
- IPv4-адрес и IPv6-адрес вредоносной системы, доменное имя вредоносной системы, URI-адрес вредоносной системы, Email-адрес вредоносной системы.
- AS-Path до атакованной Автономной системы (ASN), номер подставной Автономной системы (ASN), наименование LIR, наименование AS.
- Утечка ПДн, наименование оператора ПДн, ИНН оператора ПДн, адрес оператора ПДн, адрес электронной почты для отправки информации об уведомлении. Предполагаемые причины, повлекшие нарушение прав субъектов ПД. Предполагаемый вред, нанесенный правам субъектов ПД. Характеристики персональных данных, принятые меры по устранению последствий инцидента, информация о результатах внутреннего расследования инцидента, дополнительные сведения.

Для реагирования через внешние системы (например, UserGate) с помощью запуска сторонних скриптов на удаленных клиентских устройствах Open Single Management Platform передает во внешние системы следующую информацию: тип и значение наблюдаемых объектов из алертов, инцидентов.

Предоставление данных в Open Single Management Platform

Данные, обрабатываемые локально

Приложение Open Single Management Platform предназначено для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Open Single Management Platform предоставляет администратору доступ к подробной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского". Open Single Management Platform выполняет следующие основные функции:

- обнаружение устройств и их пользователей в сети организации;
- формирование иерархии групп администрирования для управления устройствами;

- установка приложений "Лаборатории Касперского" на устройства;
- управление параметрами работы и задачами установленных приложений;
- активация приложений "Лаборатории Касперского" на устройствах;
- управление учетными записями пользователей;
- просмотр информации о работе приложений "Лаборатории Касперского" на устройствах;
- просмотр отчетов.

Для выполнения своих основных функций приложение Open Single Management Platform может принимать, хранить и обрабатывать следующую информацию:

- Информация об устройствах в сети организации получена путем опроса контроллеров домена Active Directory или Samba или путем опроса IP-диапазонов. Сервер администрирования самостоятельно получает данные или передает Агенту администрирования.
- Информация из Active Directory и Samba об организационных подразделениях, доменах, пользователях и группах. Сервер администрирования самостоятельно получает данные, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Данные об управляемых устройствах. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные. Пользователь вводит отображаемое имя и описание устройства в интерфейсе Консоли OSMP:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, имя и тип (для устройств, принадлежащих Windows-домену), имя устройства в среде (для устройств, принадлежащих Windows-домену), DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, является ли устройство динамической виртуальной машиной как частью VDI.
  - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств: архитектура операционной системы, поставщик операционной системы, номер сборки операционной системы, идентификатор выпуска операционной системы, папка расположения операционной системы, если устройство является виртуальной машиной, то тип виртуальной машины, имя виртуального Сервера администрирования, под управлением которого находится устройство.
  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидания перезапуска, время включения устройства.
  - Данные об учетных записях пользователей устройств и их сеансах работы.
- Данные, полученные при запуске удаленной диагностики на управляемом устройстве: файлы трассировки, системная информация, сведения об установленных на устройстве приложениях "Лаборатории Касперского", файлы дампов, журналы событий, результаты запуска диагностических скриптов, полученные от Службы технической поддержки "Лаборатории Касперского".
- Статистику работы точки распространения, если устройство является точкой распространения. Агент администрирования передает данные от устройства на Сервер администрирования.
- Параметры точки распространения, которые Пользователь вводит в Консоли OSMP.

- Данные о приложениях "Лаборатории Касперского", установленных на устройстве. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования:

  - Параметры приложений "Лаборатории Касперского", установленных на управляемом устройстве: название и версия приложения "Лаборатории Касперского", статус, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, наличие и статус компонентов приложения, данные о параметрах и задачах приложения "Лаборатории Касперского", информация об активном и резервных лицензионных ключах, дата и идентификатор установки приложения.

  - Статистика работы приложения: события, связанные с изменениями статуса компонентов приложения "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных компонентами приложения.

  - Состояние устройства, определенное приложением "Лаборатории Касперского".

  - Теги, передаваемые приложением "Лаборатории Касперского".

- Данные, содержащиеся в событиях от компонентов Open Single Management Platform и управляемых приложений "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.

- Настройки компонентов Open Single Management Platform и управляемых приложений "Лаборатории Касперского", представленные в виде политик и профилей политик. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Настройки задач компонентов Open Single Management Platform и управляемых приложений "Лаборатории Касперского". Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает с устройства на Сервер администрирования следующую информацию:

  - Информация об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).

  - Данные о приложениях, установленных на управляемых устройствах (Реестр приложений). Приложения могут быть сопоставлены с информацией об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений.

- Пользовательские категории приложений. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Информация о шифровании устройств с операционной системой Windows и статусах шифрования. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.

- Информация об ошибках шифрования данных на устройствах с операционной системой Windows, выполняемого функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о файлах, помещенных в резервное хранилище. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных

представлен в справке соответствующего приложения.

- Данные о файлах, помещенных в Карантин. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о файлах, запрошенных специалистами "Лаборатории Касперского" для подробного анализа. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о внешних устройствах (устройствах памяти, инструментах передачи информации, инструментах превращения информации в твердую копию, шинах подключения), установленных или подключенных к управляемому устройству и обнаруженных функцией Контроль устройств. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Информация о зашифрованных устройствах и статусе шифрования. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.

- Информация об ошибках шифрования данных на устройствах. Шифрование выполняется функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Список управляемых программируемых логических контроллеров (ПЛК). Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные для создания цепочки развития угроз. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о введенных кодах активации или файлах ключей. Пользователь вводит данные в интерфейсе Консоли администрирования или Консоли OSMP.

- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной телефон, пароль. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Истории ревизий объектов управления. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Реестр удаленных объектов управления. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Инсталляционные пакеты, созданные из файла, и параметры установки. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Консоли OSMP. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Данные, необходимые для работы плагинов управляемых приложений в Консоли OSMP и сохраняемые плагинами в базе данных Сервера администрирования в процессе повседневной работы. Описание и способы предоставления данных приведены в файлах справки соответствующего приложения.

- Настройки пользователя в Консоли OSMP: язык локализации и тема пользовательского интерфейса, настройки отображения панели мониторинга, информации о состоянии нотификаций (прочитано/не прочитано), состояние столбцов в таблицах (скрыть/показать), прогресс прохождения режима обучения. Данная информация вводится пользователем в интерфейсе Консоли OSMP.

- Сертификат безопасного подключения управляемых устройств к компонентам Open Single Management Platform. Данная информация вводится пользователем в интерфейсе Консоли OSMP.
- Информация о принятии пользователем условий юридических соглашений с "Лабораторией Касперского".
- Данные Сервера администрирования, которые Пользователь вводит в интерфейсе Консоли OSMP или в программном интерфейсе Kaspersky Security Center OpenAPI.
- Любые данные, которые Пользователь вводит в интерфейсе Консоли OSMP.

Перечисленные выше данные могут попасть в Open Single Management Platform следующими способами:

- Данная информация вводится пользователем в интерфейсе Консоли OSMP.
- Агент администрирования самостоятельно получает данные с устройства и передает на Сервер администрирования.
- Агент администрирования получает данные от управляемого приложения "Лаборатории Касперского" и передает их на Сервер администрирования. Перечни данных, обрабатываемых управляемыми приложениями "Лаборатории Касперского", приведены в справках соответствующих приложений.
- Сервер администрирования самостоятельно получает данные о сетевых устройствах, или их передает ему Агент администрирования, который выполняет роль точки распространения.

Перечисленные данные хранятся в базе данных Сервера администрирования. Имена пользователей и пароли хранятся в зашифрованном виде.

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только посредством файлов дампа, файлов трассировки или файлов журналов компонентов Open Single Management Platform, включая файлы журналов, создаваемые инсталляторами и утилитами.

Файлы дампов, файлы трассировки или файлы журналов компонентов Open Single Management Platform содержат произвольные данные Сервера администрирования, Агента администрирования и Консоли OSMP. Эти файлы могут содержать персональные или прочие конфиденциальные данные. Файлы дампов, файлы трассировки или файлы журналов событий хранятся в незашифрованной форме на устройствах. Файлы дампов, файлы трассировки или файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти файлы в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Open Single Management Platform.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Переходя по ссылкам в Консоли администрирования или в Консоли OSMP, Пользователь соглашается на автоматическую передачу следующих данных:

- Код Open Single Management Platform.
- Версия Open Single Management Platform.
- Локализация Open Single Management Platform.
- Идентификатор лицензии.
- Тип лицензии.
- Признак покупки лицензии через партнера.

Список данных, предоставляемых по каждой ссылке, зависит от цели и местоположения ссылки.

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное время.

Предоставление данных в Kaspersky Unified Monitoring and Analysis Platform

Данные, передаваемые третьим сторонам

При использовании функциональности KUMA отсутствует автоматическая передача данных пользователя третьим сторонам.

Данные, обрабатываемые локально

Kaspersky Unified Monitoring and Analysis Platform (далее "KUMA" или "приложение") – это комплексное программное решение, сочетающее в себе следующие основные функции:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- поиск по полученным событиям;
- создание уведомлений о выявлении признаков угроз информационной безопасности;
- создание алертов и инцидентов для обработки угроз информационной безопасности;
- отображение информации о состоянии инфраструктуры заказчика на панели мониторинга и в отчетах;
- мониторинг источников событий;
- управление устройствами (активами): просмотр информации об активах, поиск, добавление, редактирование и удаление активов, экспорт данных об активах в файл формата CSV.

Для выполнения своих основных функций KUMA может принимать, хранить и обрабатывать следующую информацию:

- Данные об устройствах в сети организации.

  Сервер Ядра KUMA получает данные, если настроена соответствующая интеграция. Вы можете добавить активы в KUMA следующими способами:

  - Импортировать активы:
    - По запросу из MaxPatrol.
    - По расписанию: из Open Single Management Platform и KICS for Networks.
  - Создать активы вручную через веб-интерфейс или с помощью API.

KUMA хранит следующие данные об устройствах:

- Технические характеристики устройства.
- Уязвимости, обнаруженные на активе.
- Данные, специфичные для источника получения актива.

- Дополнительные технические характеристики устройств в сети организации, которые пользователь указывает для отправки инцидента в НКЦКИ: IP-адреса, доменные имена, URI-адреса, адрес электронной почты контролируемого объекта, атакованная сетевая служба и порт/протокол.
- Информация об организации: название, ИНН, почтовый адрес, адрес электронной почты для отправки уведомлений.
- Данные Active Directory об организационных единицах, доменах, пользователях, группах, полученные в результате опроса сети Active Directory.

  Сервер Ядра KUMA получает эти данные, если настроена соответствующая интеграция. Для обеспечения безопасного подключения к серверу LDAP пользователь вводит URL сервера, Base DN, учетные данные для подключения и сертификат в Консоли KUMA.
- Данные для доменой аутентификации пользователей в KUMA: корневой DN для поиска групп доступа в службе каталогов Active Directory, URL-адрес контроллера домена, сертификат (публичный ключ root, которым подписан сертификат AD), полный путь к группе доступа пользователей в AD (distinguished name).
- Данные, содержащиеся в событиях от настроенных источников.

  В коллекторе настраивается источник событий, формируются события KUMA и передаются далее в другие сервисы KUMA. Иногда события могут поступать сначала в сервис агент, который передает события от источника в коллектор. Также вы можете настроить сохранение адреса или имени устройства сервера, который агрегирует события.
- Данные, необходимые для интеграции KUMA с другими приложениями (Kaspersky Threat Lookup, Kaspersky CyberTrace, Open Single Management Platform, Kaspersky Industrial CyberSecurity for Networks, Kaspersky Automated Security Awareness Platform, Kaspersky Endpoint Detection and Response, Security Orchestration, Automation and Response: AI-оценка и статус, Kaspersky Investigation and Response Assistant).

  Это могут быть сертификаты, токены, URL или данные учетной записи для установки соединения с другим приложением, а также другие данные для обеспечения основной функциональности KUMA, например email. Пользователь вводит эти данные в Консоли KUMA.
- Данные об источниках, с которых настроено получение событий.

  Это могут быть название источника, имя устройства, IP-адрес, политика мониторинга, назначенная этому источнику. В политике мониторинга указывается адрес электронной почты ответственного, кому будет отправлено уведомление при нарушении политики.
- Учетные записи пользователей: имя, логин, адрес электронной почты. Пользователь может просмотреть свои данные в профиле в Консоли KUMA.
- Параметры профиля пользователя:
  - Роль пользователя в KUMA. Пользователь может видеть назначенную ему роль.
  - Язык локализации, параметры уведомлений, отображение непечатаемых символов.

    Пользователь вводит эти данные в интерфейсе KUMA.

- Список категорий активов в разделе **Активы**, панель мониторинга по умолчанию, признак режима ТВ для панели мониторинга, SQL-запрос по событиям по умолчанию, пресет по умолчанию.

  Пользователь указывает эти параметры в соответствующих разделах Консоли KUMA.

- Данные для доменной аутентификации пользователей в KUMA:

  - Active Directory: корневой DN для поиска групп доступа в службе каталогов Active Directory, URL-адрес контроллера домена, сертификат (публичный ключ root, которым подписан сертификат AD), полный путь к группе доступа пользователей в AD (distinguished name).

  - Active Directory Federation Services (ADFS): идентификатор доверенной стороны (идентификатор KUMA в ADFS), URI для получения метаданных Connect, URL для перенаправления из ADFS и сертификат сервера ADFS.

  - FreeIPA: Base DN, URL, сертификат (открытый корневой ключ, который использовался для подписи сертификата FreeIPA), пользовательские учетные данные для интеграции, учетные данные для подключения.

- События аудита.

  KUMA автоматически фиксирует события аудита.

- Журнал KUMA.

  Пользователь может включить ведение расширенных записей журналов в Консоли KUMA. Записи журнала хранятся на устройстве пользователя, автоматическая передача данных отсутствует.

- Информация о принятии пользователем условий юридических соглашений с "Лабораторией Касперского".

- Любые данные, которые пользователь вводит в интерфейсе KUMA.

Перечисленные выше данные могут попасть в KUMA следующими способами:

- Пользователь вводит данные в Консоли KUMA.

- Сервисы KUMA (агент или коллектор) получают данные при настроенном пользователем подключении к источникам событий.

- Через REST API KUMA.

- Данные об устройствах могут быть получены с помощью утилиты из MaxPatrol.

Перечисленные данные хранятся в базе данных KUMA (Mongo DB, Click House, SQLite). Пароли хранятся в зашифрованном виде (хранится хеш паролей).

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только в файлах дампа, файлах трассировки или файлах журналов компонентов KUMA, включая файлы журналов, создаваемые установщиком и утилитами.

Файлы дампа, файлы трассировки и файлы журналов компонентов KUMA могут содержать персональные и конфиденциальные данные. Файлы дампа, файлы трассировки и файлы журналов хранятся в открытом виде на устройстве. Файлы дампа, файлы трассировки и файлы журналов не передаются в "Лабораторию Касперского" автоматически, но администратор может передать эти данные в "Лабораторию Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе KUMA.

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное время.

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи.

Начало работы

Следующие сценарии представляют собой пошаговые инструкции от приобретения Open Single Management Platform до расследования инцидентов и поиска угроз.

Начните с установки и первоначальной настройки Open Single Management Platform, изучите функции обнаружения и поиска угроз Open Single Management Platform и ознакомьтесь с примером рабочего процесса расследования инцидентов.

Развертывание и первоначальная настройка Open Single Management Platform

Следуя этому сценарию, вы можете развернуть Open Single Management Platform со всеми компонентами, необходимыми для работы Open Single Management Platform, а также выполнить необходимые предварительные настройки и интеграции.

Предварительные требования

Перед тем как начать, убедитесь в следующем:

- Вам нужно использовать лицензионный ключ для Open Single Management Platform и совместимых EPP-программ.
- Ваша инфраструктура соответствует требованиям к аппаратному и программному обеспечению.

Этапы

Основной сценарий установки и первоначальной настройки состоит из следующих этапов:

1. **Развертывание**

   Подготовьте свою инфраструктуру к развертыванию Open Single Management Platform и всех необходимых компонентов для Open Single Management Platform и разверните решение с помощью утилиты Kaspersky Deployment Toolkit.

2. **Активация**

   Активируйте по лицензии решение Open Single Management Platform.

3. **Настройка мультитенантности**

   Если требуется, вы можете использовать возможности мультитенантности:

   1. Спланируйте и создайте требуемую иерархию тенантов.
   2. Создайте соответствующую иерархию Серверов администрирования в Open Single Management Platform.
   3. Привяжите тенанты к соответствующим Серверам администрирования.
   4. Создайте учетные записи для всех пользователей Open Single Management Platform и назначьте роли.

4. **Добавление активов**

Устройства в вашей инфраструктуре, которые необходимо защитить, представлены в Open Single Management Platform как активы. Open Single Management Platform позволяет обнаруживать устройства в вашей сети и управлять их защитой. Вы также сможете добавлять активы вручную или импортировать их из других источников на этапе 8.

Учетные записи пользователей также представлены как активы в Open Single Management Platform. Убедитесь что интеграция с Active Directory на этапе 9 настроена, чтобы включить отображение затронутых учетных записей пользователей в связанных событиях, алертах и инцидентах.

5. **Добавление пользователей и назначение ролей**

   Назначьте роли учетным записям пользователей, чтобы определить их права доступа к различным функциям Open Single Management Platform в зависимости от их задач.

6. **Подключение к SMTP-серверу**

   Настройте подключение к SMTP-серверу для получения уведомлений по электронной почте о событиях, возникающих в Open Single Management Platform.

7. **Установка приложений и решений для защиты конечных точек**

   Open Single Management Platform работает с событиями, полученными от приложений безопасности, установленных на ваших активах. Проверьте список совместимых приложений и решений "Лаборатории Касперского". Вы можете использовать Open Single Management Platform для развертывания приложений "Лаборатории Касперского" на устройствах в вашей инфраструктуре.

   Убедитесь, что приложения защиты конечных точек интегрированы с Kaspersky Anti Targeted Attack Platform. Например, если вы используете Kaspersky Endpoint Security на своих активах, обратитесь к одной из следующих справок, чтобы узнать, как настроить интеграцию с KATA:

   - Kaspersky Endpoint Security для Windows
   - Kaspersky Endpoint Security для Linux
   - Kaspersky Endpoint Security для Mac

8. **Настройка источников событий, хранения и корреляции**

   Укажите, откуда должны быть получены события, а также как они должны храниться и обрабатываться:

   1. Войдите в Консоль KUMA.
   2. Настройте интеграцию Kaspersky Unified Monitoring and Analysis Platform и Open Single Management Platform.
   3. Импортируйте активы из Open Single Management Platform.
   4. Добавьте активы вручную или импортируйте их из других источников (необязательно).
   5. Настройте источники событий, чтобы указать, откуда вы хотите получать события.
   6. Создайте хранилище для событий.
   7. Создайте коллекторы для приема, обработки (нормализации) и передачи событий.
   8. Создайте корреляторы для первоначального анализа нормализованных событий и их дальнейшей обработки.

      При создании коллектора вы можете создать правила корреляции, которые определяют правила обработки и реагирования на события, а также импортировать ранее сохраненные правила корреляции или использовать готовый набор правил корреляции, входящий в состав решения Open Single Management Platform. После создания коррелятора вы можете связать правила корреляции с коррелятором, если это необходимо.

Рекомендуется настроить исключения на этом этапе, чтобы избежать ложных срабатываний и нерелевантных данных.

9. **Настройка интеграций**

   Настройте интеграцию Open Single Management Platform с Active Directory и другими решениями "Лаборатории Касперского", чтобы расширить его возможности и обогатить данные, доступные для расследования инцидентов.

   1. Интеграция с Active Directory (рекомендуется).
   2. Интеграция с KATA/EDR (требуется лицензия).
   3. Интеграция с Kaspersky CyberTrace (необязательная интеграция; требуется лицензия).
   4. Интеграция с Kaspersky TIP (необязательная интеграция; требуется лицензия) или Kaspersky Open TIP.
   5. Интеграция с Kaspersky Automated Security Awareness Platform (необязательная интеграция; требуется лицензия).

10. **Настройка обновлений**

    Создайте задачу Загрузка обновлений в хранилище Сервера администрирования.

11. **Проверка корректности конфигурации**

    Используйте тестовый файл EICAR на одном из активов. Если первоначальная настройка была выполнена правильно и были настроены необходимые правила корреляции, это событие вызовет создание алерта в списке алертов.

После завершения первоначальной настройки события от защищаемых активов будут получены и обработаны Open Single Management Platform, а из событий правила корреляции будет создан алерт.

Проверка настройки Open Single Management Platform

Вы можете использовать тестовый "вирус" EICAR на одном из активов, чтобы убедиться, что Open Single Management Platform правильно развернут и настроен. Если первоначальная настройка была выполнена правильно и были настроены необходимые правила корреляции, соответствующее событие вызовет создание алерта в списке алертов.

Чтобы проверить настройку Open Single Management Platform:

1. Создайте коррелятор в Консоли KUMA.

   При создании коррелятора не указывайте параметры в разделе **Корреляция**.

2. Импортируйте правила корреляции из пакета SOC Content, чтобы получить предустановленные правила корреляции, используемые для обнаружения тестового "вируса" EICAR.

3. Укажите правило корреляции для созданного коррелятора.

   Вы можете указать правило корреляции одним из следующих способов:

   - Свяжите предустановленное правило корреляции с созданным коррелятором:

a. Перейдите в раздел **Ресурсы**, нажмите на **Правила корреляции** и выберите тенант, к которому будет применяться правило корреляции.

b. В списке предустановленных правил корреляции выберите правило **R077_02_KSC.Malware detected**, чтобы обнаруживать события Kaspersky Security Center.

c. Нажмите на **Связать с коррелятором** и выберите созданный коррелятор, чтобы связать выбранное правило корреляции с коррелятором.

- Создайте правило корреляции с предустановленными фильтрами вручную:

a. Откройте параметры созданного коррелятора, перейдите в раздел **Корреляция** и нажмите на кнопку **Добавить**.

b. В окне **Создание правила корреляции** на вкладке **Общие** задайте следующие параметры, так же как и другие параметры:

- **Вид**: простой.
- **Наследуемые поля**: DestinationAddress, DestinationHostName, DestinationAccountID, DestinationAssetID, DestinationNtDomain, DestinationProcessName, DestinationUserName, DestinationUserID, SourceAccountID, SourceUserName.

c. Перейдите в раздел **Селекторы** → **Параметры** и укажите выражение для фильтрации необходимых событий:

- В режиме конструктора добавьте фильтры событий **KSC**, **Обнаружен вирус приложением KSC** и **Базовые события** с помощью оператора AND.
- Также вы можете указать это выражение в режиме исходного кода следующим образом:

```
filter='b308fc22-fa79-4324-8fc6-291d94ef2999'
AND filter='a1bf2e45-75f4-45c1-920d-55f5e1b8843f'
AND filter='1ffa756c-e8d9-466a-a44b-ed8007ca80ca'
```

d. В разделе **Действия** в параметрах правила корреляции установите только флажок **Вывод** (флажки **Цикл для коррелятора** и **Нет алертов** должны быть сняты). В этом случае при обнаружении тестового "вируса" EICAR будет создано событие корреляции и в списке алертов Open Single Management Platform будет создан алерт.

e. Нажмите на кнопку **Создать сейчас**, чтобы сохранить параметры правила корреляции, связанные с коррелятором.

4. Создайте и настройте в Консоли KUMA коллектор для получения информации о событиях Сервера администрирования из базы данных MS SQL.

   Также вы можете использовать предустановленный коллектор [OOTB] KSC SQL.

5. В разделе параметров коллектора **Маршрутизация** установите **Тип коррелятора** и укажите созданный коррелятор в поле **URL**, чтобы пересылать ему обработанные события.

6. Установите Агент администрирования и приложение защиты конечных точек (например, Kaspersky Endpoint Security) на актив в сети вашей организации. Убедитесь, что актив подключен к Серверу администрирования.

7. Поместите тестовый файл EICAR на актив, а затем обнаружьте тестовый "вирус" с помощью приложения защиты конечных точек.

После этого Сервер администрирования получит уведомление о событии на активе. Это событие будет перенаправлено в компонент KUMA, преобразовано в событие корреляции, после чего в Open Single Management Platform будет создан алерт в списке алертов. Если алерт создан, значит Open Single Management Platform работает правильно.

Использование функций мониторинга, обнаружения и поиска угроз

После установки и настройки Open Single Management Platform вы можете использовать функции Open Single Management Platform для мониторинга безопасности вашей инфраструктуры, расследования инцидентов безопасности, автоматизации рабочих процессов и автоматического поиска угроз:

- **Использование панели мониторинга и настройка веб-виджетов**

  Вкладка **Обнаружение и реагирование** по панели мониторинга может содержать веб-виджеты, которые отображают информацию о зарегистрированных алертах и инцидентах, а также действиях по реагированию на них. Вы можете использовать и настраивать предварительно настроенные макеты веб-виджетов для своей панели мониторинга или создавать макеты и веб-виджеты.

  Open Single Management Platform также предоставляет различные инструменты для мониторинга безопасности и создания отчетов.

- **Использование отчетов**

  Вы можете настроить формирование отчетов в Kaspersky Unified Monitoring and Analysis Platform для получения необходимых сводных данных по указанному расписанию.

- **Использование поиска угроз**

  Вы можете использовать инструменты поиска угроз для анализа событий и поиска угроз и уязвимостей, которые не были обнаружены автоматически. Поиск угроз можно использовать как для расследования инцидентов и алертов, так и для предупреждающего поиска угроз.

- **Использование плейбуков**

  Вы можете использовать плейбуки для автоматизации действий по реагированию на алерты и инциденты в соответствии с заданным алгоритмом. Существует ряд предустановленных плейбуков, которые вы можете запускать в различных режимах работы. Вы можете создавать пользовательские плейбуки.

Пример расследования инцидента с помощью Open Single Management Platform

Этот сценарий представляет собой пример рабочего процесса расследования инцидента.

Расследование инцидента проходит поэтапно:

1. **Назначение алерта пользователю**

   Вы можете назначить алерт себе или другому пользователю.

2. **Проверка совпадения сработавшего правила корреляции с данными событий алерта**

   Просмотрите информацию об алерте и убедитесь, что данные о событии алерта соответствуют сработавшему правилу корреляции.

3. **Анализ информации об алерте**

Проанализируйте информацию об алерте, чтобы определить, какие данные требуются для дальнейшего анализа алерта.

4. **Обогащение вручную**

   Запустите доступные решения для дополнительного обогащения события (например, Kaspersky TIP).

5. **Проверка ложного срабатывания**

   Убедитесь, что действие, запустившее правило корреляции, является аномальным для ИТ-инфраструктуры организации.

6. **Создание инцидента**

   Если шаги с 3 по 5 показывают, что алерт требует расследования, вы можете создать инцидент или связать алерт с существующим инцидентом.

   Вы также можете объединить инциденты.

7. **Расследование**

   Этот шаг включает в себя просмотр информации об активах, учетных записях пользователей и алертах, связанных с инцидентом. Вы можете использовать граф расследования и инструменты поиска угроз, чтобы получить дополнительную информацию.

8. **Поиск связанных активов**

   Вы можете просмотреть алерты, которые возникли на активах, связанных с инцидентом.

9. **Поиск связанных событий**

   Вы можете расширить область расследования, выполнив поиск событий связанных алертов.

10. **Запись причин инцидента**

    Вы можете записать информацию, необходимую для расследования, в журнал изменений инцидента.

11. **Действие по реагированию**

    Вы можете выполнять действия по реагированию вручную.

12. **Закрытие инцидента**

    После принятия мер по удалению следов присутствия злоумышленника в ИТ-инфраструктуре организации можно закрыть инцидент.

Развертывание Open Single Management Platform

Следуя этому сценарию, вы можете подготовить свою инфраструктуру к развертыванию Open Single Management Platform и всех необходимых компонентов, подготовить конфигурационный файл, содержащий параметры установки, и развернуть решение с помощью утилиты Kaspersky Deployment Toolkit (далее также KDT).

Прежде чем приступить к развертыванию Open Single Management Platform и компонентов Open Single Management Platform, рекомендуется прочитать Руководство по усилению защиты.

Сценарий развертывания состоит из следующих этапов:

1. **Выбор варианта установки Open Single Management Platform**

   Выберите конфигурацию Open Single Management Platform, наиболее подходящую для вашей организации. Вы можете использовать руководство по масштабированию, в котором описаны требования к оборудованию и рекомендуемый вариант развертывания в зависимости от количества устройств в организации.

   В зависимости от выбранного варианта развертывания вам могут потребоваться следующие устройства для работы Open Single Management Platform:

   - **Устройство администратора**

     Устройство администратора – это физическая или виртуальная машина, которая используется для развертывания и управления кластером Kubernetes и Open Single Management Platform. Поскольку KDT работает на устройстве администратора, это устройство должно соответствовать требованиям KDT.

   - **Целевые устройства**

     Целевые устройства – это физические или виртуальные машины, на которые устанавливается Open Single Management Platform. Используются следующие целевые устройства:

     - Целевые устройства для установки компонентов Open Single Management Platform

       Устройства, входящие в кластер Kubernetes, между которыми распределяется рабочая нагрузка.

       Целевые устройства должны соответствовать требованиям для выбранного варианта развертывания (распределенное развертывание или развертывание на одном узле).

     - Целевые устройства KUMA для установки сервисов KUMA

       Целевые устройства, не входящие в кластер Kubernetes и используемые для установки сервисов KUMA (коррелляторы, коллекторы и хранилища). Количество целевых устройств KUMA зависит от количества событий которые Open Single Management Platform должен обработать.

       Целевые устройства KUMA должны соответствовать требованиям к оборудованию, программному обеспечению и требованиям установки, необходимым для установки сервисов KUMA.

   - **Устройство СУБД (только для развертывания на нескольких узлах)**

Устройством для установки СУБД рекомендуется сделать отдельный сервер, расположенный вне кластера Kubernetes. Устройство с СУБД может быть включено в кластер только для оценки и демонстрационных целей.

Требования к устройству СУБД одинаковы независимо от того, входит он в кластер или нет.

- **Устройство KATA/KEDR (необязательно)**

  Если вы хотите получать телеметрию от Kaspersky Anti Targeted Attack Platform и управлять действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response, вы можете установить и настроить Kaspersky Anti Targeted Attack Platform с функциональным блоком Kaspersky Endpoint Detection and Response. Kaspersky Anti Targeted Attack Platform – это автономное решение, которое необходимо установить на отдельный сервер, не входящий в кластер Kubernetes. Подробную информацию о сценариях развертывания KATA см. в документации KATA.

Доступны схемы развертывания на нескольких узлах и развертывания на одном узле:

- Развертывание на нескольких узлах

  Рекомендуемый вариант установки Open Single Management Platform. При развертывании на нескольких узлах компоненты Open Single Management Platform устанавливаются на нескольких рабочих узлах кластера Kubernetes, и при выходе из строя одного узла кластер может восстановить работу компонентов на другом узле.

  В этой конфигурации вам понадобится минимум семь устройств:

  - 1 устройство администратора;
  - 4 целевых устройства для установки кластера Kubernetes и компонентов Open Single Management Platform;
  - 1 устройство для установки СУБД;
  - 1 целевое устройство KUMA для установки сервисов KUMA.

- Развертывание на одном узле

  При развертывании на одном узле все компоненты Open Single Management Platform устанавливаются на одном узле кластера Kubernetes. Вы можете выполнить развертывание Open Single Management Platform на одном узле, чтобы решение потребовало меньше вычислительных ресурсов.

  В этой конфигурации вам понадобится минимум три устройства:

  - 1 устройство администратора;
  - 1 целевое устройство для установки кластера Kubernetes, компонентов Open Single Management Platform и СУБД;
  - 1 целевое устройство KUMA для установки сервисов KUMA.

  В этой конфигурации СУБД не требует отдельного узла, но она должна быть установлена вручную на целевом устройстве перед развертыванием Open Single Management Platform. Устройство с СУБД может быть включено в кластер только для оценки и демонстрационных целей.

2. **Загрузка дистрибутива с компонентами Open Single Management Platform**

В состав дистрибутива входят следующие компоненты:

- Транспортный архив, который содержит компоненты Open Single Management Platform и Лицензионные соглашения Open Single Management Platform и KDT.
- Архив с утилитой KDT, а также шаблоны конфигурационного файла и файл инвентаря KUMA.

3. **Установка системы управления базами данных (СУБД)**

   Для развертывания на нескольких узлах вручную установите СУБД на отдельном сервере за пределами кластера Kubernetes.

   Для развертывания на одном узле вручную установите СУБД на целевом устройстве перед развертыванием Open Single Management Platform. В этом случае компоненты СУБД и Open Single Management Platform устанавливаются на одном и том же целевом устройстве, но СУБД не будет включена в кластер Kubernetes.

   Если вы выполняете демонстрационное развертывание и хотите установить СУБД внутри кластера, пропустите этот шаг. KDT установит СУБД во время развертывания Open Single Management Platform.

4. **Подготовка устройства администратора и целевых устройств**

   С учетом выбранной схемы развертывания определите количество целевых устройств, на которых вы будете разворачивать кластер Kubernetes и компоненты Open Single Management Platform, входящие в этот кластер. Подготовьте выбранные устройства администратора и целевые машины к развертыванию Open Single Management Platform.

   Инструкции:

   - Развертывание на нескольких узлах: Подготовка устройства администратора и целевых устройств.
   - Развертывание на одном узле: Подготовка устройства администратора и целевых устройств.

5. **Подготовка устройств KUMA**

   Подготовьте целевые устройства KUMA для установки сервисов KUMA (коллекторы, корреляторы и хранилища).

   Инструкции: Подготовка устройств к установке сервисов KUMA.

6. **Подготовка файла инвентаря KUMA для установки сервисов KUMA**

   Подготовка файла инвентаря KUMA в формате YAML. Файл инвентаря KUMA содержит параметры для установки сервисов KUMA

   Инструкции: Подготовка файла инвентаря KUMA.

7. **Подготовка конфигурационного файла**

   Подготовка конфигурационного файла в формате YAML. Конфигурационный файл содержит список целевых устройств для развертывания и набор параметров для установки компонентов Open Single Management Platform.

   Если вы разворачиваете Open Single Management Platform на отдельном узле, используйте конфигурационный файл, содержащий параметры установки, предназначенные для развертывания на одном узле.

   Инструкции:

   - Развертывание на нескольких узлах: Указание параметров установки
   - Развертывание на одном узле: Указание параметров установки

   Вы можете заполнить шаблон конфигурационного файла вручную либо с помощью мастера настройки: укажите параметры установки, необходимые для развертывания Open Single Management Platform и сгенерируйте конфигурационный файл.

Инструкции: Указание параметров установки с помощью мастера настройки.

8. **Развертывание Open Single Management Platform**

   Разверните Open Single Management Platform с помощью KDT. KDT автоматически разворачивает кластер Kubernetes, в котором установлены компоненты Open Single Management Platform и другие компоненты инфраструктуры.

   Инструкции: Установка Open Single Management Platform.

9. **Установка сервисов KUMA**

   Установите сервисы KUMA (коллекторы, корреляторы и хранилища) на подготовленные целевые устройства KUMA, расположенные вне кластера Kubernetes.

   Инструкции: Установка сервисов KUMA.

10. **Настройка интеграции с Kaspersky Anti Targeted Attack Platform**

    Установите Central Node, чтобы получать телеметрию от Kaspersky Anti Targeted Attack Platform, а затем настройте интеграцию Open Single Management Platform и KATA/KEDR для управления действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response.

    При необходимости вы можете установить несколько компонентов Central Node, чтобы использовать их независимо друг от друга или объединить для централизованного управления в режиме **распределенного решения**. Чтобы объединить несколько компонентов Central Node, вам нужно организовать серверы с компонентами в иерархию.

    Двухуровневая иерархия серверов с установленными компонентами Central Node. Эта иерархия выделяет первичный управляющий сервер (Primary Central Node (PCN)) и вторичные серверы (Secondary Central Nodes (SCN)).

    При настройке серверов Central Node вам нужно указать минимально возможное значение в поле **Хранилище**, чтобы избежать дублирования данных между базами Open Single Management Platform и KEDR.

Руководство по усилению защиты

Приложение Open Single Management Platform предназначено для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к детальной информации об уровне безопасности сети организации. Open Single Management Platform позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского".

Сервер администрирования имеет полный доступ к управлению защитой клиентских устройств и является важнейшим компонентом системы защиты организации. Поэтому для Сервера администрирования требуются усиленные меры защиты.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Open Single Management Platform и его компонентов для снижения рисков его компрометации.

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;
- настройка безопасного подключения к Серверу Администрирования;

- настройка учетных записей для работы с Сервером администрирования;
- управление защитой Сервера администрирования;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы.;
- рекомендации по безопасности сторонних информационных систем.

Управление инфраструктурой Open Single Management Platform

В этом разделе описан общий принцип использования минимально необходимого количества приложений для работы операционной системы и Open Single Management Platform. Также в этом разделе описан принцип минимальных привилегий, который сводится к концепции нулевого доверия.

Управление учетными записями операционной системы

Для работы с кластером Kubernetes с помощью KDT рекомендуется создать отдельного пользователя с минимальными правами. Оптимальным способом является реализация управления учетными записями пользователей операционной системы с помощью LDAP, с возможностью отзыва прав пользователей через LDAP. Информацию о конкретной реализации отзыва прав и блокировки пользователей см. в руководстве пользователя/администратора в вашем решении LDAP. Рекомендуется использовать пароль длиной не менее 18 символов или физические средства аутентификации (например, токен) для аутентификации пользователя операционной системы.

Также рекомендуется защищать корневой каталог документов пользователя и все вложенные каталоги таким образом, чтобы только пользователь имел к ним доступ. Другие пользователи и группа пользователей не должны иметь прав на корневой каталог документов.

Рекомендуется не предоставлять права на запуск для директорий .ssh, .kube, .config и .kdt, а также для всех файлов, содержащихся в этих директориях в корневой директории документов пользователя.

Управление пакетами операционной системы

Рекомендуется использовать минимальный набор приложений, необходимый для работы KDT и Open Single Management Platform. Например, вам не нужно использовать графический пользовательский интерфейс для работы в кластере Kubernetes, поэтому не рекомендуется устанавливать графические пакеты. Если пакеты установлены, рекомендуется удалить эти пакеты, включая графические серверы, такие как Xorg или Wayland.

Рекомендуется регулярно устанавливать обновления безопасности для системного программного обеспечения и ядра Linux. Также рекомендуется включить автоматическое обновление следующим образом:

- Для операционных систем с диспетчером пакетов atp:

```
/etc/apt/apt.conf.d/50unattended-upgrades

Unattended-Upgrade::Allowed-Origins {
 "${distro_id}:${distro_codename}-security";
```

```
  "${distro_id}ESMApps:${distro_codename}-apps-security";
  "${distro_id}ESM:${distro_codename}-infra-security";
};
```

- Для операционных систем с диспетчером пакетов rp, dnf и yum:

/etc/dnf/automatic.conf

```
[commands]
# Какое обновление выполнить:
# default = все доступные обновления
# security = только обновления безопасности
upgrade_type = default

# Следует ли скачивать обновления, когда они будут доступны,
# dnf-automatic.timer. notifyonly.timer, download.timer и
# install.timer отменяют этот параметр.
download_updates = yes

# Следует ли применять обновления, когда они будут доступны,
# dnf-automatic.timer. notifyonly.timer, download.timer и
# install.timer отменяют этот параметр.
apply_updates = no
```

Параметры безопасности операционной системы

Параметры безопасности ядра Linux можно включить в файле `/etc/sysctl.conf` или с помощью команды `sysctl`. Рекомендуемые параметры безопасности ядра Linux перечислены во фрагменте файла `/etc/sysctl.conf`:

/etc/sysctl.conf

```
# Выключить execshield
kernel.randomize_va_space=2
# Включить защиту от IP-спуфинга
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
# Игнорировать широковещательные сетевые запросы
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_responses=1
# Включить ведение журнала событий сетевых спуфинговых пакетов
net.ipv4.conf.all.log_martians=1
# Скрыть указатели ядра
kernel.kptr_restrict=1
# Ограничить доступ к журналам событий ядра
kernel.dmesg_restrict = 1
# Запретить профилирование ядра для непривилегированных пользователей
kernel.perf_event_paranoid=3
# Увеличение бит энтропии ASLR
vm.mmap_rnd_bits=32
vm.mmap_rnd_compat_bits=16
```

Рекомендуется ограничить доступ к PID. Это уменьшит вероятность того, что один пользователь будет отслеживать процессы другого пользователя. Вы можете ограничить доступ к PID при монтировании файловой системы `/proc`, например, добавив следующую строку в файл `/etc/fstab`:

```
proc /proc proc nosuid,nodev,noexec,hidepid=2,gid=proc 0 0
```

Если процессы операционной системы управляются с помощью системы `systemd`, служба `systemd-logind` по-прежнему может контролировать процессы других пользователей. Для корректной работы пользовательских сессий в системе `systemd` необходимо создать файл `/etc/systemd/system/systemd-logind.service.d/hidepid.conf` и добавить в него следующие строки:

```
[Service]
SupplementaryGroups=proc
```

Так как в некоторых системах может не быть группы `proc`, рекомендуется добавить группу `proc` заранее.

Рекомендуется выключить комбинацию клавиш **`Ctrl`**+**`Alt`**+**`Del`**, чтобы предотвратить неожиданную перезагрузку операционной системы с помощью команды `systemctl mask ctrl-alt-del.target`.

Рекомендуется запретить аутентификацию привилегированных пользователей (пользователей root) для установления удаленного подключения пользователя.

Рекомендуется использовать сетевой экран для ограничения сетевой активности. Об используемых портах и протоколах см. в разделе Порты, используемые Open Single Management Platform.

Рекомендуется включить `auditd`, чтобы упростить расследование инцидентов безопасности. О включении перенаправления телеметрии см. в разделе Настройка получения событий Auditd.

Рекомендуется регулярно создавать резервные копии следующих конфигураций и директорий данных:

- Устройство администратора: `~/kdt`
- Целевое устройство: `/etc/k0s/`, `/var/lib/k0s`

Также рекомендуется зашифровать эти резервные копии.

Руководства по усилению защиты для различных операционных систем и СУБД

Если вам нужно настроить параметры безопасности вашей операционной системы и программного обеспечения, вы можете использовать рекомендации, предоставленные Center for Internet Security (CIS).

Если вы используете операционную систему Astra Linux, обратитесь к рекомендациям по безопасности, которые можно применить к вашей версии Astra Linux.

Если вам необходимо настроить параметры безопасности PostgreSQL, воспользуйтесь рекомендациями по администрированию сервера из официальной документации PostgreSQL.

Безопасность соединения

Строгие параметры TLS

Рекомендуется использовать протокол TLS версии 1.2 или выше и ограничить или запретить использование небезопасных алгоритмов шифрования.

Вы можете настроить протоколы шифрования (TLS), используемые Сервером администрирования. При этом учитывайте, что на момент выпуска определенной версии Open Single Management Platform параметры протокола шифрования по умолчанию настроены так, чтобы обеспечить безопасную передачу данных.

Ограничение доступа к базе данных Open Single Management Platform

Рекомендуется ограничить доступ к базе данных Open Single Management Platform. Например, разрешить доступ только с устройств, на которых установлен Open Single Management Platform. Это позволит снизить вероятность взлома базы данных Open Single Management Platform через известные уязвимости.

Вы можете настроить параметры в соответствии с руководством по эксплуатации используемой базы данных, а также предусмотреть закрытые порты на сетевых экранах.

Учетные записи и авторизация

Использование двухэтапной проверки Open Single Management Platform

Open Single Management Platform обеспечивает двухэтапную проверку для пользователей на основе стандарта RFC 6238 (TOTP: Time-Based One-Time Password Algorithm).

Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Open Single Management Platform с помощью браузера вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Для того чтобы получить одноразовый код безопасности, вам нужно установить приложение для аутентификации на своем компьютере или мобильном устройстве.

Существуют как программные, так и аппаратные аутентификаторы (токены), поддерживающие стандарт RFC 6238. Например, к программным аутентификаторам относятся Google Authenticator, Microsoft Authenticator, FreeOTP.

Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Open Single Management Platform. Например, вы можете установить приложение для аутентификации на мобильном устройстве.

Использование двухфакторной аутентификации операционной системы

Рекомендуется использовать многофакторную аутентификацию (MFA) на устройствах с развернутым Open Single Management Platform с помощью токена, смарт-карты или другим способом (если это возможно).

Запрет на сохранение пароля администратора

Также при работе с Open Single Management Platform через браузер не рекомендуется сохранять пароль администратора в браузере на устройстве пользователя.

Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Open Single Management Platform должен соответствовать следующим требованиям:

- Длина пароля должна быть от 8 до 16 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
  - верхний регистр (A-Z);
  - нижний регистр (a-z);

- числа (0-9);
- специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля.

Пользователь может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

Ограничение назначения роли Главного администратора

Пользователю назначается роль Главного администратора в списке контроля доступа (ACL) Open Single Management Platform. Не рекомендуется назначать роль Главного администратора большому количеству пользователей.

Настройка прав доступа к функциям приложения

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Open Single Management Platform.

Управление доступом на основе ролей позволяет создавать типовые роли пользователей с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Основные преимущества ролевой модели управления доступом:

- простота администрирования;
- иерархия ролей;
- принцип наименьшей привилегии;
- разделение обязанностей.

Вы можете воспользоваться встроенными ролями и присвоить их определенным сотрудникам на основе должностей либо создать полностью новые роли.

При настройке ролей требуется уделить особое внимание привилегиям, связанным с изменением состояния защиты устройства с Open Single Management Platform и удаленной установкой стороннего программного обеспечения:

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений.

  Эта привилегия позволяет настроить уведомления, которые запускают скрипт или исполняемый модуль на устройстве с OSMP при возникновении события.

Отдельная учетная запись для удаленной установки приложений

Помимо базового разграничения прав доступа, рекомендуется ограничить возможность удаленной установки приложений для всех учетных записей (кроме "Главного администратора" или иной специализированной учетной записи).

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль или разрешения отдельной учетной записи.

Регулярный аудит всех пользователей

Рекомендуется проводить регулярный аудит всех пользователей на устройстве, где развернут Open Single Management Platform. Это позволит реагировать на некоторые типы угроз безопасности, связанные с возможной компрометацией устройства.

Управление защитой Open Single Management Platform

Выбор программного обеспечения защиты Open Single Management Platform

В зависимости от типа развертывания Open Single Management Platform и общей стратегии защиты выберите приложение защиты устройств с развернутым Open Single Management Platform и устройство администратора.

Если вы разворачиваете Open Single Management Platform на выделенных устройствах, рекомендуется выбрать приложение Kaspersky Endpoint Security для защиты устройств с развернутым Open Single Management Platform и устройства администратора. Это позволит применить все имеющиеся технологии для защиты этих устройств, в том числе модули поведенческого анализа.

Если Open Single Management Platform разворачивается на устройствах, которые уже существуют в инфраструктуре и ранее использовались для выполнения других задач, рекомендуются следующие приложения защиты:

- Kaspersky Industrial CyberSecurity for Nodes. Это приложение рекомендуется устанавливать на устройства, входящие в промышленную сеть. Kaspersky Industrial CyberSecurity for Nodes – это приложение, имеющее сертификаты совместимости с различными производителями промышленного программного обеспечения.

- Рекомендованные приложения безопасности. Если Open Single Management Platform развернут на устройствах с другим программным обеспечением, нужно ознакомиться с рекомендациями производителя программного обеспечения по использованию антивирусных приложений (возможно, уже существуют рекомендации по выбору приложения защиты, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

Модули защиты

Если отсутствуют особые рекомендации от производителя стороннего программного обеспечения, установленного на тех же устройствах, что и Open Single Management Platform, рекомендуется активировать и настроить все доступные модули защиты (после проверки их работы в течение определенного времени).

Настройка сетевого экрана устройств с Open Single Management Platform

На устройствах с развернутым Open Single Management Platform рекомендуется настроить сетевой экран, чтобы ограничить количество устройств, с которых администраторы могут подключаться к Open Single Management Platform через браузер.

По умолчанию

Open Single Management Platform использует порт 443 для входа в систему через браузер. Рекомендуется ограничить число устройств, с которых Open Single Management Platform может управляться по этим портам.

Управление защитой клиентских устройств

Ограничение добавления лицензионных ключей в инсталляционные пакеты

Инсталляционные пакеты можно публиковать с помощью Веб-сервера, входящего в состав Open Single Management Platform. Если вы добавите лицензионный ключ в инсталляционный пакет, опубликованный на Веб-сервере, лицензионный ключ будет доступен для чтения всем пользователям.

Для того чтобы избежать компрометации лицензионного ключа, не рекомендуется добавлять лицензионные ключи в инсталляционные пакеты.

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства, выполнять развертывание с помощью задачи *Добавление лицензионного ключа* для управляемого приложения, и добавлять код активации или файл ключа на устройства вручную.

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования.

Использование правил автоматического перемещения может привести к тому, что на устройство будут распространены политики, предоставляющие более широкий набор привилегий, чем было до перемещения.

Перемещение клиентского устройства в другую группу администрирования может привести к распространению на него параметров политик. Эти параметры политик могут быть нежелательны к распространению на гостевые и недоверенные устройства.

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования.

Требования к безопасности к устройствам с точками распространения и шлюзам соединений

Устройства с установленным Агентом администрирования могут использоваться в качестве точки распространения и выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Open Single Management Platform, на клиентские устройства в группе.
- Выполнять удаленную установку приложений сторонних производителей и приложений "Лаборатории Касперского" на клиентские устройства.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Open Single Management Platform.

Размещение точек распространения в сети организации используется для следующего:

- снижение нагрузки на Open Single Management Platform;
- оптимизация трафика;
- предоставление Open Single Management Platform доступа к устройствам в труднодоступных частях сети.

С учетом доступных возможностей рекомендуется защитить, в том числе физически, устройства, выполняющие роль точек распространения, от любого типа несанкционированного доступа.

Ограничение автоматического назначения точек распространения

Для упрощения администрирования и сохранения работоспособности сети рекомендуется воспользоваться автоматическим назначением точек распространения. Однако в промышленных и небольших сетях рекомендуется избегать автоматического назначения точек распространения, так как на точки распространения могут быть, например, переданы конфиденциальные сведения учетных записей, используемых для работы задач принудительной удаленной установки средствами операционной системы.

В промышленных и небольших сетях вы можете назначить точки распространения вручную.

При необходимости вы также можете просмотреть Отчет о работе точек распространения.

Настройка защиты управляемых приложений

Политики управляемых приложений

Рекомендуется создать политику для каждого вида используемого приложения и всех компонентов Open Single Management Platform (Агент администрирования, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Agent и другие). Эта групповая политика должна применяться ко всем управляемым устройствам (корневой группе администрирования) или к отдельной группе, в которую автоматически попадают новые управляемые устройства в соответствии с настроенными правилами перемещения.

Установка пароля на выключение защиты и удаление приложения

Настоятельно рекомендуется включить защиту паролем, чтобы злоумышленники не смогли выключить или удалить приложения безопасности "Лаборатории Касперского". На платформах, где поддерживается защита паролем, вы можете установить пароль, например, для Kaspersky Endpoint Security, Агента администрирования и других приложений "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать соответствующие параметры, закрыв их "замком".

Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Open Single Management Platform рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN. При обновлении Open Single Management Platform вы также можете принять обновленное Положение о KSN. Когда использование облачных служб запрещено законодательством или иными нормативными актами, вы можете не включать KSN.

Регулярная проверка управляемых устройств

Для всех групп устройств вам нужно создать задачу, периодически запускающую полную проверку устройств.

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с контроллерами доменов и указать диапазоны IP-адресов для обнаружения новых устройств.

В целях безопасности вы можете использовать группу администрирования по умолчанию, в которую попадают все новые устройства, и политики по умолчанию, применяемые к этой группе.

Передача событий в сторонние системы

В этом разделе описаны особенности передачи проблем безопасности, обнаруженных на клиентских устройствах, в системы сторонних производителей.

Мониторинг и отчеты

Для своевременного реагирования на проблемы безопасности вы можете настроить функции мониторинга и параметры отчетов.

Экспорт событий в SIEM-системы

Для максимально быстрого выявления проблем безопасности до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему.

Уведомление по электронной почте о событиях аудита

Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Сервером администрирования уведомлений о публикуемых им событиях аудита, критических событиях, событиях отказа функционирования и предупреждениях.

Поскольку события аудита являются внутрисистемными, они регистрируются редко и количество уведомлений о подобных событиях вполне приемлемо для почтовой рассылки.

Схема развертывания: развертывание на нескольких узлах

Существует несколько вариантов развертывания Open Single Management Platform. Прежде чем начать, убедитесь, что вы знакомы с различными схемами развертывания, и выберите ту, которая лучше всего соответствует требованиям вашей организации.

В этом разделе приводится описание схемы развертывания на нескольких узлах.

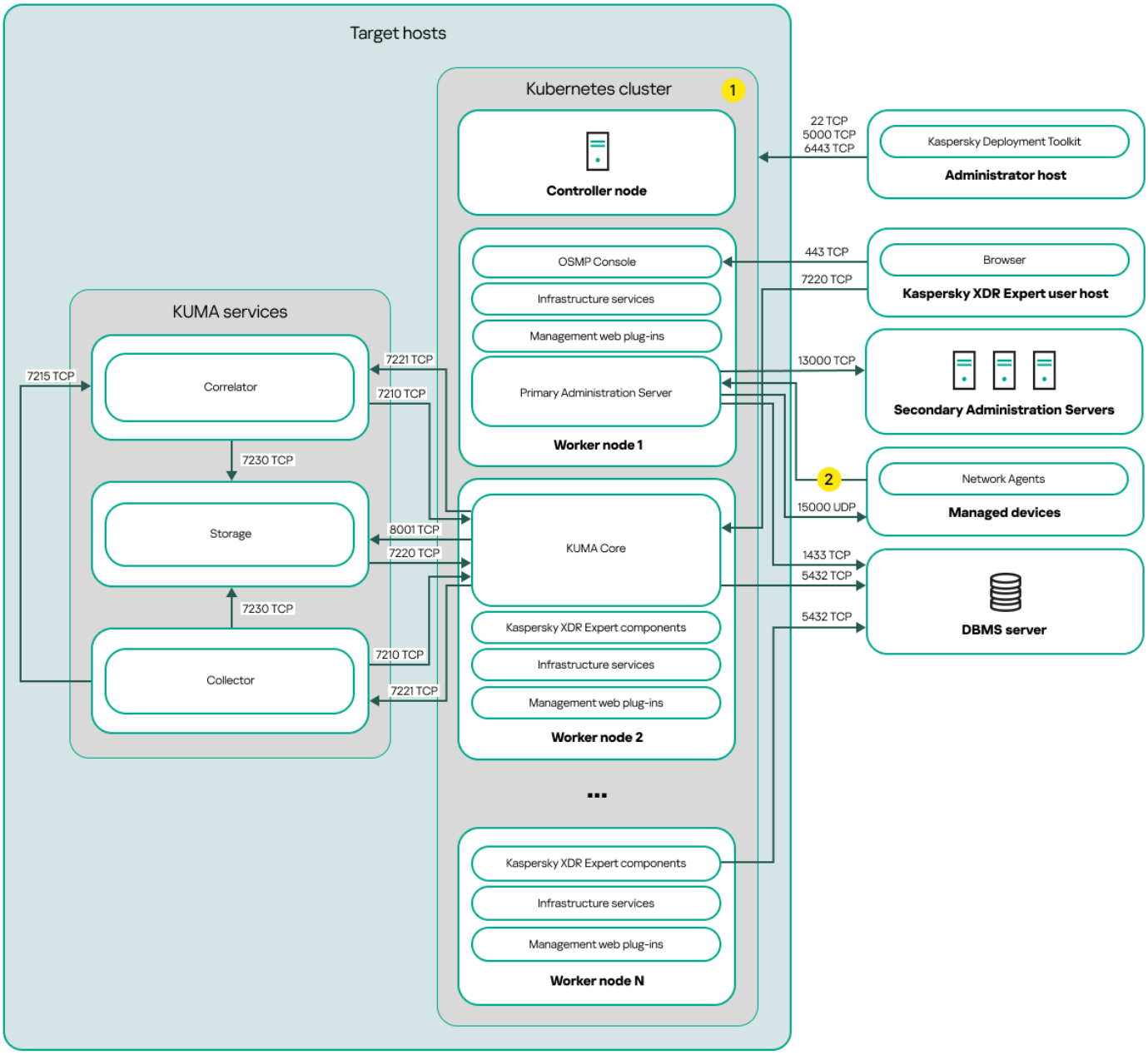


Схема развертывания Open Single Management Platform на нескольких узлах

Схема развертывания Open Single Management Platform на нескольких узлах включает следующие основные компоненты:

- **Устройство администратора**. На этом устройстве администратор использует Kaspersky Deployment Toolkit для развертывания и управления кластером Kubernetes и Open Single Management Platform. Устройство администратора не входит в кластер Kubernetes.

- **Кластер Kubernetes**. Кластер Kubernetes включает узел контроллера (также называемый первичным узлом во время процедуры развертывания) и как минимум три рабочих узла. Количество рабочих узлов может быть разным. На схеме в качестве примера показано распределение компонентов Open Single Management Platform по рабочим узлам. Фактическое распределение компонентов может отличаться.

- **Сервер СУБД**. Для корректной работы компонентов Open Single Management Platform необходим сервер с установленной системой управления базами данных. Администратор устанавливает СУБД вручную на отдельные серверы вне кластера Kubernetes.

- **Устройства с сервисами KUMA**. Сервисы KUMA (коллекторы, коррелляторы и хранилища) устанавливаются на устройства, расположенные вне кластера Kubernetes. Количество целевых устройств для сервисов KUMA может отличаться.

- **KATA с KEDR**. Kaspersky Anti-Targeted Attack Platform с функциональным блоком Kaspersky Endpoint Detection and Response. Подробную информацию о сценариях развертывания KATA см. в документации KATA.

- **Устройство пользователя с Open Single Management Platform**. Пользовательское устройство, которое используется для входа в Консоль OSMP или Консоль KUMA.

- **Подчиненные Серверы администрирования** (необязательно). Подчиненные Серверы администрирования используются для создания иерархии Серверов.

- **Управляемые устройства**. Клиентские устройства защищены Open Single Management Platform. На каждом управляемом устройстве установлен Агент администрирования.

Порты

Схема не предоставляет все порты, необходимые для успешного развертывания. Полный список портов приведен в разделе Порты, используемые Open Single Management Platform.

Условные обозначения схемы:

1 На схеме не показано взаимодействие внутри кластера Kubernetes между узлами и между компонентами Open Single Management Platform. Подробнее см. в разделе Порты, используемые Open Single Management Platform.

2 Список портов, которые необходимо открыть на управляемых устройствах, приведен в разделе Порты, используемые Open Single Management Platform.

3 Подробнее об интеграции с KATA, включая функциональный блок KEDR, см. в разделе Интеграция с KATA/KEDR.

4 На схеме сервисы KUMA развернуты по схеме развертывания на нескольких узлах. Количество целевых устройств для сервисов KUMA может отличаться. Список открываемых портов зависит от выбранной схемы развертывания. Полный список портов приведен в разделе Порты, используемые Open Single Management Platform.

5 TCP-порт 7221 и другие порты для установки служб. Вы указываете эти порты как значение для --api.point <port>.

Схема развертывания: развертывание на одном узле

Существует несколько вариантов развертывания Open Single Management Platform. Прежде чем начать, убедитесь, что вы знакомы с различными схемами развертывания, и выберите ту, которая лучше всего соответствует требованиям вашей организации.

В этом разделе приводится описание схемы развертывания на одном узле.

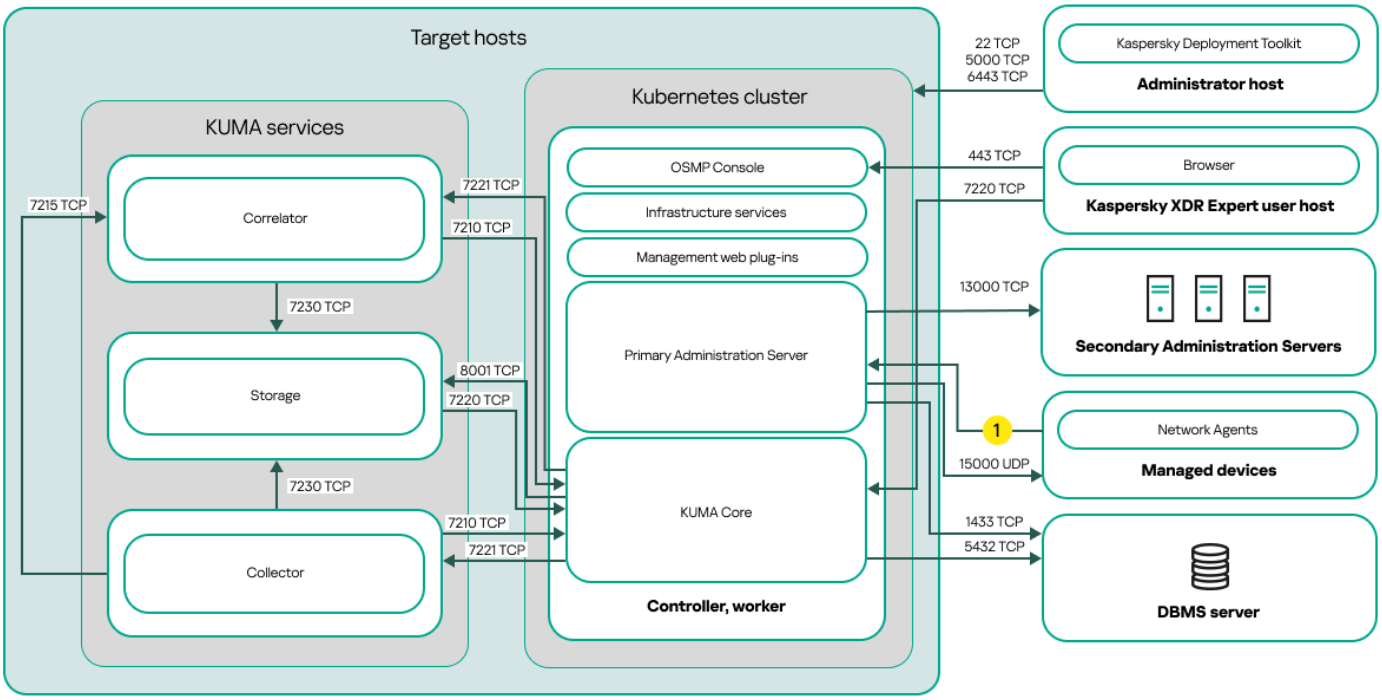


Схема развертывания Open Single Management Platform на одном узле

Схема развертывания Open Single Management Platform на одном узле включает следующие основные компоненты:

- **Устройство администратора**. На этом устройстве администратор использует Kaspersky Deployment Toolkit для развертывания и управления кластером Kubernetes и Open Single Management Platform. Устройство администратора не входит в кластер Kubernetes.
- **Кластер Kubernetes**. Кластер Kubernetes включает в себя устройство, которое действует как узел контроллера (далее также первичный узел во время процедуры развертывания) и как рабочий узел.
- **Сервер СУБД**. Для корректной работы компонентов Open Single Management Platform необходим сервер с установленной системой управления базами данных. Сервер СУБД не входит в кластер Kubernetes. Администратор устанавливает СУБД вручную на целевом устройстве, которое будет действовать как первичный рабочий узел перед развертыванием Open Single Management Platform.
- **Устройства с сервисами KUMA**. Сервисы KUMA (коллекторы, коррелляторы и хранилища) устанавливаются на устройства, расположенные вне кластера Kubernetes. Количество целевых устройств для сервисов KUMA может отличаться.
- **KATA с KEDR**. Kaspersky Anti-Targeted Attack Platform с функциональным блоком Kaspersky Endpoint Detection and Response. Подробную информацию о сценариях развертывания KATA см. в документации KATA.
- **Устройство пользователя с Open Single Management Platform**. Пользовательское устройство, которое используется для входа в Консоль OSMP или Консоль KUMA.
- **Подчиненные Серверы администрирования** (необязательно). Подчиненные Серверы администрирования используются для создания иерархии Серверов.
- **Управляемые устройства**. Клиентские устройства защищены Open Single Management Platform. На каждом управляемом устройстве установлен Агент администрирования.

Порты

Схема не предоставляет все порты, необходимые для успешного развертывания. Полный список портов приведен в разделе Порты, используемые Open Single Management Platform.

Условные обозначения схемы:

1 Список портов, которые необходимо открыть на управляемых устройствах, приведен в разделе Порты, используемые Open Single Management Platform.

2 Подробнее об интеграции с KATA, включая функциональный блок KEDR, см. в разделе Интеграция с KATA/KEDR.

3 На схеме сервисы KUMA развернуты по схеме развертывания на нескольких узлах. Количество целевых устройств для сервисов KUMA может отличаться. Список открываемых портов зависит от выбранной схемы развертывания. Полный список портов приведен в разделе Порты, используемые Open Single Management Platform.

4 TCP-порт 7221 и другие порты для установки служб. Вы указываете эти порты как значение для --api.point <port>.

Порты, используемые Open Single Management Platform

Для правильного взаимодействия между устройством администратора и целевыми устройствами вам нужно предоставить доступ к соединению между устройством администратора и целевыми устройствами через порты, перечисленные в таблице ниже. Эти порты невозможно изменить.

Для взаимодействия между устройством администратора и устройствами, которые используются для установки сервисов KUMA и находятся вне кластера Kubernetes, доступ предоставляется только по TCP-порту 22.

Порты, используемые для взаимодействия между устройством администратора и целевыми устройствами

Порт	Протокол	Назначение порта
22	TCP	Обеспечение SSH-соединения от устройства администратора к целевым устройствам. Обеспечение SSH-подключения от устройства администратора к устройствам, которые используются для установки внешних сервисов KUMA.
5000	TCP	Подключение к реестру Docker.
6443	TCP	Подключение к Kubernetes API.

Для корректной работы компонентов Open Single Management Platform целевые устройства должны находиться в одном широковещательном домене.

В таблице ниже указаны порты, которые должны быть открыты на сетевых экранах всех целевых устройств кластера. Эти порты невозможно изменить.

Если вы используете сетевой экран или сетевой экран UFW на целевых устройствах, KDT автоматически откроет требуемые порты на сетевых экранах. Или вы можете вручную открыть перечисленные порты перед развертыванием Open Single Management Platform.

Обязательные порты, используемые компонентами Open Single Management Platform

Порт	Протокол	Назначение порта
80	TCP (HTTP)	Прием соединений от браузера. Перенаправление на порт 443 TCP (HTTPS).
443	TCP (HTTPS)	Прием соединений от браузера. Прием соединений от Сервера администрирования по OpenAPI. Используется для автоматизации сценариев работы с Сервером администрирования.

13000	TCP	Прием соединений от Агентов администрирования и подчиненных Серверов администрирования.
13000	UDP	Прием информации от Агентов администрирования о выключении устройств.
14000	TCP	Прием подключений от Агентов администрирования.
17000	TCP	Прием подключений для активации приложений от управляемых устройств (кроме мобильных устройств).
7210	TCP	Получение конфигурации KUMA с сервера Ядра KUMA.
7220	TCP	Прием соединений от браузера.
7222	TCP	Реверсивный прокси в системе CyberTrace.
7224	TCP	Ответные вызовы для Identity and Access Manager (IAM).

В таблице ниже указаны порты, которые по умолчанию не открываются на сетевых экранах при развертывании Open Single Management Platform. Эти порты невозможно изменить.

Если вам нужно выполнить действия, перечисленные в столбце **Назначение порта** в таблице ниже, вы можете открыть соответствующие порты на сетевых экранах всех целевых устройств вручную.

Необязательные порты на сетевом экране, используемые компонентами Open Single Management Platform

Порт	Протокол	Назначение порта
8060	TCP	Передача на клиентские устройства опубликованных инсталляционных пакетов.
8061	TCP	Передача на клиентские устройства опубликованных инсталляционных пакетов.
13111	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN.
15111	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN.
17111	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN.
5432	TCP	Взаимодействие с СУБД (PostgreSQL). Этот порт используется только, если вы выполняете демонстрационное развертывание и устанавливаете СУБД на целевом устройстве внутри кластера Kubernetes.

В таблице ниже указаны порты, которые необходимо открыть для работы кластера Kubernetes и компонентов инфраструктуры. Эти порты невозможно изменить.

Если вы используете сетевой экран или сетевой экран UFW на целевых устройствах, KDT автоматически откроет требуемые порты на сетевых экранах. Или вы можете вручную открыть перечисленные порты перед развертыванием Open Single Management Platform.

Порты, используемые кластером Kubernetes и компонентами инфраструктуры

Порт	Протокол	Узел
80	TCP	Первичный узел
443	TCP	Первичный узел
10250	TCP	Первичный узел
9443	TCP	Первичный узел
6443	TCP	Первичный узел
8132	TCP	Первичный узел
5000	TCP	Первичный узел
80	TCP	Рабочий узел
443	TCP	Рабочий узел
179	TCP	Рабочий узел
10250	TCP	Рабочий узел
10255	TCP	Рабочий узел
9443	TCP	Рабочий узел
6443	TCP	Рабочий узел

9500	TCP	Рабочий узел
9501	TCP	Рабочий узел
9502	TCP	Рабочий узел
9503	TCP	Рабочий узел
8500	TCP	Рабочий узел
8501	TCP	Рабочий узел
3260	TCP	Рабочий узел
8000	TCP	Рабочий узел
8002	TCP	Рабочий узел
2049	TCP	Рабочий узел
3370	TCP	Рабочий узел
179	UDP	Рабочий узел
51820	UDP	Рабочий узел
51821	UDP	Рабочий узел

Для корректной работы сервисов KUMA, не входящих в кластер Kubernetes, вам нужно открыть порты, указанные в таблице ниже. В таблице ниже показаны значения сетевых портов по умолчанию. Эти порты автоматически открываются во время установки KUMA.

Порты, используемые для взаимодействия с внешними сервисами KUMA

Порт	Протокол	Направление	Назначение подключения
8123	HTTPS	От службы хранилища к узлу кластера ClickHouse.	Запись и получение нормализованных событий в кластере ClickHouse.
9009	HTTPS	Между репликами кластера ClickHouse.	Внутренняя связь между репликами кластера ClickHouse для передачи данных кластера.
2181	TCP	От узлов кластера ClickHouse к службе координации репликации ClickHouse keeper.	Получение и запись метаданных репликации репликами серверов ClickHouse.
2182	TCP	От одного сервиса координации репликации ClickHouse keeper к другому.	Внутренняя связь между службами координации репликации для достижения кворума.
8001	TCP	От Victoria Metrics к серверу ClickHouse.	Получение метрик работы сервера ClickHouse.
9000	TCP	От клиента ClickHouse к узлу кластера ClickHouse.	Запись и получение данных в кластере ClickHouse.

Если вы создаете дополнительный сервис KUMA (коллектор, коррелятор или хранилище) на сервере, вам необходимо вручную открыть порт, соответствующий созданному сервису на сервере. Вы можете использовать порт TCP 7221 или другой порт, используемый для установки службы.

Если используются стандартные примеры служб, при развертывании Open Single Management Platform автоматически открываются следующие порты:

- 7230 TCP
- 7231 TCP
- 7232 TCP
- 7233 TCP
- 7234 TCP
- 7235 TCP
- 5140 TCP

- 5140 UDP
- 5141 TCP
- 5144 UDP

Подготовительные работы и развертывание

В этом разделе описано, как подготовить инфраструктуру к развертыванию Open Single Management Platform, настроить параметры установки, необходимые для развертывания на нескольких узлах или развертывания на одном узле, а также как использовать мастер настройки для создания конфигурационного файла.

Вы узнаете, как установить Open Single Management Platform по схеме развертывания на нескольких узлах и развертывания на одном узле. Также в этом разделе содержится информация о том, как развернуть несколько кластеров Kubernetes с экземплярами Open Single Management Platform и переключаться между ними с помощью KDT.

Развертывание на нескольких узлах: Подготовка устройства администратора и целевых устройств

Подготовка к развертыванию на нескольких узлах включает настройку устройства администратора и целевых устройств. После подготовки устройств и указания конфигурационного файла вы сможете развернуть Open Single Management Platform на целевых устройствах с использованием KDT.

Подготовка устройства администратора

Предварительно вам нужно подготовить устройство, которое будет выполнять роль устройства администратора, с которого будет запускаться KDT. Это устройство может быть включено или не включено в кластер Kubernetes, созданный с помощью KDT во время развертывания. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Open Single Management Platform. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Open Single Management Platform.

Чтобы подготовить устройство администратора:

1. Убедитесь, что оборудование и программное обеспечение на устройстве администратора соответствуют требованиям для KDT.
2. Выделите не менее 10 ГБ свободного места в папке временных файлов (`/tmp`) для KDT. Если у вас недостаточно свободного места в этой папке, выполните следующую команду, чтобы указать путь к другой директории:

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. Установите пакет для Docker версии 23 или выше, а затем выполните действия после установки, чтобы настроить устройство администрирования для правильной работы с Docker.

Не устанавливайте неофициальные версии пакета Docker из хранилищ операционных систем

4. Для устройства администратора, которое будет включено в кластер, выполните дополнительные подготовительные шаги:

   a. Поскольку устройство будет действовать как устройство администратора и целевое устройство, убедитесь, что оно соответствует требованиям для развертывания на нескольких узлах.

   b. Убедитесь, что на устройстве администратора поддерживается технология cgroup v2.

      Технология cgroup v2 поддерживается для версии ядра Linux 2.6.24 и выше.

   c. Установите пакет uidmap на устройстве администратора.

      Убедитесь, что файлы /etc/subgid и /etc/subuid содержат учетную запись пользователя, под которой будет запущен KDT. Для этого вы можете выполнить следующую команду:

      ```
      getsubids USER
      ```

      Если эта команда не возвращает результат, вам нужно вручную добавить учетную запись пользователя в файлы /etc/subgid и /etc/subuid в следующем формате:

      ```
      <username>:<min_subid>:<range_length>
      ```

      где

      - `<username>` – имя пользователя учетной записи, под которым будет запущен KDT.
      - `<min_subid>` – минимальное значение subuid.
      - `<range_length>` – количество subuid, выделенных для пользователя `<username>`.

Подготовка целевых устройств

Целевые устройства – это физические или виртуальные машины, которые используются для развертывания Open Single Management Platform и которые включены в кластер Kubernetes. Компоненты Open Single Management Platform работают на этих устройствах.

Одно из целевых устройств может быть использовано в качестве устройства администратора. В этом случае вам необходимо подготовить это устройство в качестве устройства администратора, как описано в предыдущей процедуре, а затем выполнить подготовку для целевого устройства.

Минимальная конфигурация кластера для развертывания на нескольких узлах включает четыре узла:

- Один первичный узел

  Первичный узел предназначен для управления кластером, хранения метаданных и распределения рабочей нагрузки.

- Три рабочих узла

  Рабочие узлы предназначены для выполнения рабочей нагрузки компонентов Open Single Management Platform.

  Для оптимального распределения нагрузки между узлами рекомендуется использовать узлы с примерно одинаковой производительностью.

Вы можете установить СУБД внутри кластера Kubernetes при выполнении демонстрационного развертывания Open Single Management Platform. В этом случае выделите дополнительный рабочий узел для установки СУБД. KDT установит СУБД во время развертывания Open Single Management Platform.

Для развертывания на нескольких узлах рекомендуется установить СУБД на отдельный сервер вне кластера.
После развертывания Open Single Management Platform замена СУБД, которая установлена внутри кластера, на СУБД, установленную на отдельном сервере, недоступна. Вам необходимо удалить все компоненты Open Single Management Platform и снова установить Open Single Management Platform. В этом случае данные будут потеряны.

Чтобы подготовить целевые устройства:

1. Убедитесь, что оборудование и программное обеспечение на целевых устройствах соответствуют требованиям для развертывания на нескольких узлах и целевые устройства расположены в одном широковещательном домене.

   Для правильной работы Open Single Management Platform версия ядра Linux должна быть 5.15.0.107 или выше на целевых устройствах с операционной системой семейства Ubuntu.

   Docker не должен быть установлен на целевых устройствах, кроме целевого устройства, которое будет использоваться в качестве устройства администратора. KDT установит все необходимое программное обеспечение и зависимости во время развертывания.

2. На каждом целевом устройстве установите пакет sudo, если этот пакет еще не установлен. Для операционных систем семейства Debian установите пакет UFW на целевые устройства.

3. На каждом целевом устройстве настройте файл /etc/environment. Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, подключите целевые устройства к интернету.

4. На первичном узле с конфигурацией UFW разрешите IP-переадресацию. В файле `/etc/default/ufw` установите для параметра `DEFAULT_FORWARD_POLICY` значение `ACCEPT`.

5. Предоставьте доступ к хранилищу пакетов. Это хранилище содержит следующие пакеты, необходимые для работы Open Single Management Platform:

   - nfs-common
   - tar
   - iscsi-package
   - wireguard
   - wireguard-tools

   KDT попытается установить эти пакеты во время развертывания из хранилища пакетов. Также эти пакеты можно установить вручную.

6. Для первичного узла убедитесь, что установлен пакет curl.

7. Для рабочих узлов убедитесь, что установлен пакет libnfs версии 12 и выше.

   Пакеты curl и libnfs не устанавливаются во время развертывания из хранилища пакетов с помощью KDT. Вам нужно установить эти пакеты вручную, если они еще не установлены.

8. Зарезервируйте статические IP-адреса для целевых устройств для шлюза кластера Kubernetes и для устройства с СУБД (если СУБД установлена внутри кластера).

   Кластерный шлюз Kubernetes предназначен для подключения компонентов Open Single Management Platform, установленных внутри кластера Kubernetes. IP-адрес шлюза соединения указан в конфигурационном файле.

   Для стандартного использования решения, когда вы устанавливаете СУБД на отдельный сервер, IP-адрес шлюза соединения – это IP-адрес в нотации CIDR, которая содержит маску подсети /32 (например, 192.168.0.0/32).

   Для демонстрационных целей, когда вы устанавливаете СУБД внутри кластера Kubernetes, IP-адрес шлюза является IP-диапазоном (например, 192.168.0.1–192.168.0.2).

   Убедитесь, что целевые устройства, шлюз соединения кластера Kubernetes и устройство с СУБД находятся в одном широковещательном домене.

9. На своем DNS-сервере зарегистрируйте FQDN служб для подключения к службам Open Single Management Platform.

   По умолчанию службы Open Single Management Platform доступны по следующим адресам:

   - <console_host>.<smp_domain> – доступ к интерфейсу Консоли OSMP.
   - <admsrv_host>.<smp_domain> – взаимодействие с Сервером администрирования.
   - <kuma_host>.<smp_domain> – доступ к интерфейсу Консоли KUMA.
   - <api_host>.<smp_domain> – доступ к API Open Single Management Platform.
   - <psql_host>.<smp_domain> – взаимодействие с СУБД (PostgreSQL).

     Где <console_host>, <admsrv_host>, <kuma_host>, <api_host> и <psql_host> являются именами устройств сервисов, <smp_domain> является доменным именем сервиса. Эти параметры являются частями сервисов FQDN, которые вы можете указать в конфигурационном файле.

     Зарегистрируйте FQDN службы <psql_host>.<smp_domain>, если вы установили СУБД внутри кластера Kubernetes на узле СУБД и вам нужно подключиться к СУБД.

   В зависимости от того, где вы хотите установить СУБД, перечисленные FQDN служб должны быть преобразованы в IP-адрес кластера Kubernetes следующим образом:

   - СУБД на отдельном сервере (стандартное использование).

     В этом случае IP-адрес шлюза соединения – это адрес служб Open Single Management Platform (без учета IP-адреса СУБД). Например, если указан IP-адрес шлюза соединения 192.168.0.0/32, FQDN службы должны быть разрешены следующим образом:

     - <console_host>.<smp_domain> – 192.168.0.0/32
     - <admsrv_host>.<smp_domain> – 192.168.0.0/32
     - <kuma_host>.<smp_domain> – 192.168.0.0/32
     - <api_host>.<smp_domain> – 192.168.0.0/32

   - СУБД внутри кластера Kubernetes (демонстрационное развертывание).

В этом случае IP-адрес шлюза соединения представляет собой IP-диапазон. Первый IP-адрес диапазона – это адрес служб Open Single Management Platform (без учета IP-адреса СУБД). Второй IP-адрес диапазона – IP-адрес СУБД. Например, если указан IP-диапазон шлюза соединения 192.168.0.1–192.168.0.2, FQDN служб должны быть разрешены следующим образом:

- <console_host>.<smp_domain> – 192.168.0.1
- <admsrv_host>.<smp_domain> – 192.168.0.1
- <kuma_host>.<smp_domain> – 192.168.0.1
- <api_host>.<smp_domain> – 192.168.0.1
- <psql_host>.<smp_domain> – 192.168.0.2

10. На целевых устройствах создайте учетные записи, которые будут использоваться для развертывания Open Single Management Platform.

    Эти учетные записи используются для SSH-соединения и должны иметь возможность повышать привилегии (sudo) без ввода пароля. Для этого добавьте созданные учетные записи пользователей в файл `/etc/sudoers`.

11. Настройте SSH-подключение между устройством администратора и целевыми устройствами:

    a. На устройстве администратора сгенерируйте SSH-ключи с помощью утилиты ssh-keygen без парольной фразой.

    b. Скопируйте открытый ключ на каждое целевое устройство (например, в папку `/home/<имя_пользователя>/.ssh`) с помощью утилиты ssh-copy-id.

    Если вы используете целевое устройство в качестве устройства администратора, вам нужно скопировать на него открытый ключ.

12. Для корректной работы компонентов Open Single Management Platform обеспечьте сетевой доступ между целевыми устройствами и при необходимости откройте требуемые порты на сетевом экране устройства администратора и целевых устройств.

13. Настройте синхронизацию времени по протоколу Network Time Protocol (NTP) на устройстве администратора и целевых устройствах.

14. При необходимости подготовьте пользовательские сертификаты для работы с публичными службами Open Single Management Platform.

    Вы можете использовать один промежуточный сертификат, выданный на основе корневого сертификата организации или конечных сертификатов для каждой службы. Подготовленные пользовательские сертификаты будут использоваться вместо самоподписанных сертификатов.

Развертывание на одном узле: Подготовка устройства администратора и целевых устройств

Подготовка к развертыванию на одном узле включает настройку устройства администратора и целевых устройств. В конфигурации с одним узлом кластер Kubernetes и компоненты Open Single Management Platform устанавливаются на одном целевом устройстве. После подготовки целевого устройства и указания конфигурационного файла, вы сможете развернуть Open Single Management Platform на целевом устройстве с использованием KDT.

Подготовка устройства администратора

Предварительно вам нужно подготовить устройство, которое будет выполнять роль устройства администратора, с которого будет запускаться KDT. Это устройство может быть включено или не включено в кластер Kubernetes, созданный с помощью KDT во время развертывания. Если устройство администратора не включено в кластер, оно будет использоваться только для развертывания и управления кластером Kubernetes и Open Single Management Platform. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Open Single Management Platform. В этом случае будет использовано только одно устройство для развертывания и работы решения.

Чтобы подготовить устройство администратора:

1. Убедитесь, что оборудование и программное обеспечение на устройстве администратора соответствуют требованиям для KDT.

2. Выделите не менее 10 ГБ свободного места в папке временных файлов (`/tmp`) для KDT. Если у вас недостаточно свободного места в этой папке, выполните следующую команду, чтобы указать путь к другой директории:

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. Установите пакет для Docker версии 23 или выше, а затем выполните действия после установки, чтобы настроить устройство администрирования для правильной работы с Docker.

   Не устанавливайте неофициальные версии пакета Docker из хранилищ операционных систем

4. Для устройства администратора, которое будет включено в кластер, выполните дополнительные подготовительные шаги:

   a. Так как устройство будет действовать как устройство администратора и целевое устройство, убедитесь, что оно соответствует требованиям для развертывания на одном узле.

   b. Убедитесь, что на устройстве администратора поддерживается технология cgroup v2.

      Технология cgroup v2 поддерживается для версии ядра Linux 2.6.24 и выше.

   c. Установите пакет uidmap на устройстве администратора.

      Убедитесь, что файлы /etc/subgid и /etc/subuid содержат учетную запись пользователя, под которой будет запущен KDT. Для этого вы можете выполнить следующую команду:

      ```
      getsubids USER
      ```

      Если эта команда не возвращает результат, вам нужно вручную добавить учетную запись пользователя в файлы /etc/subgid и /etc/subuid в следующем формате:

      ```
      <username>:<min_subid>:<range_length>
      ```

      где

      - `<username>` – имя пользователя учетной записи, под которым будет запущен KDT.
      - `<min_subid>` – минимальное значение subuid.
      - `<range_length>` – количество subuid, выделенных для пользователя `<username>`.

Подготовка целевого устройства

Целевое устройство – это физическая или виртуальная машина, которая используются для развертывания Open Single Management Platform и которая включена в кластер Kubernetes. Целевое устройство управляет кластером Kubernetes, хранит метаданные, а также на этом устройстве работают компоненты Open Single Management Platform. Минимальная конфигурация кластера для развертывания с одним узлом включает одно целевое устройство, которое действует как первичный и рабочий узлы. На этом первичном рабочем узле установлен кластер Kubernetes и компоненты Open Single Management Platform.

Для стандартного использования вам нужно установить СУБД вручную на целевом устройстве перед развертыванием. В этом случае СУБД будет установлена на целевом устройстве, но не будет включена в кластер Kubernetes. Для демонстрационных целей вы можете установить СУБД внутри кластера с помощью KDT во время развертывания.

Если вы хотите запустить развертывание Open Single Management Platform с целевого устройства, вам нужно подготовить это устройство в качестве устройства администратора, как описано в предыдущей процедуре, а затем выполнить подготовку для целевого устройства.

Чтобы подготовить целевое устройство:

1. Убедитесь, что оборудование и программное обеспечение на целевом устройстве соответствуют требованиям для развертывание на одном узле.

   Для правильной работы Open Single Management Platform версия ядра Linux должна быть 5.15.0.107 или выше на целевом устройстве с операционной системой семейства Ubuntu.

   Не устанавливайте Docker на целевом устройстве, если целевое устройство не будет использоваться в качестве устройства администратора. KDT установит все необходимое программное обеспечение и зависимости во время развертывания.

2. Установите пакет sudo, если этот пакет еще не установлен. Для операционных систем семейства Debian установите пакет UFW.

3. Настройте файл /etc/environment. Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, вам также нужно подключить целевое устройство к интернету.

4. На первичном рабочем узле с конфигурацией UFW разрешите IP-переадресацию. В файле `/etc/default/ufw` установите для параметра `DEFAULT_FORWARD_POLICY` значение `ACCEPT`.

5. Предоставьте доступ к хранилищу пакетов. Это хранилище содержит следующие пакеты, необходимые для работы Open Single Management Platform:

   - nfs-common
   - tar
   - iscsi-package
   - wireguard
   - wireguard-tools

   KDT попытается установить эти пакеты во время развертывания из хранилища пакетов. Также эти пакеты можно установить вручную.

6. Убедитесь, что пакеты curl и libnfs установлены на первичном рабочем узле.

   Пакеты curl и libnfs не устанавливаются во время развертывания из хранилища пакетов с помощью KDT. Вам нужно установить эти пакеты вручную, если они еще не установлены. Используется пакет libnfs версии 12 и выше.

7. Зарезервируйте статические IP-адреса для целевых устройств и шлюза кластера Kubernetes.

   Кластерный шлюз Kubernetes предназначен для подключения компонентов Open Single Management Platform, установленных внутри кластера Kubernetes.

   Для стандартного использования решения, когда вы устанавливаете СУБД на целевое устройство вне кластера, IP-адрес шлюза соединения – это IP-адрес в нотации CIDR, которая содержит маску подсети /32 (например, 192.168.0.0/32).

   Для демонстрационных целей, когда вы устанавливаете СУБД внутри кластера Kubernetes, IP-адрес шлюза является IP-диапазоном (например, 192.168.0.1–192.168.0.2).

   Убедитесь, что целевое устройство и шлюз соединения кластера Kubernetes находятся в одном широковещательном домене.

8. На своем DNS-сервере зарегистрируйте FQDN служб для подключения к службам Open Single Management Platform.

   По умолчанию службы Open Single Management Platform доступны по следующим адресам:

   - <console_host>.<smp_domain> – доступ к интерфейсу Консоли OSMP.
   - <admsrv_host>.<smp_domain> – взаимодействие с Сервером администрирования.
   - <kuma_host>.<smp_domain> – доступ к интерфейсу Консоли KUMA.
   - <api_host>.<smp_domain> – доступ к API Open Single Management Platform.
   - <psql_host>.<smp_domain> – взаимодействие с СУБД (PostgreSQL).

     Где <console_host>, <admsrv_host>, <kuma_host>, <api_host> и <psql_host> являются именами устройств сервисов, <smp_domain> является доменным именем сервиса. Эти параметры являются частями сервисов FQDN, которые вы можете указать в конфигурационном файле.

     Зарегистрируйте FQDN службы <psql_host>.<smp_domain>, если вы установили СУБД внутри кластера Kubernetes на узле СУБД и вам нужно подключиться к СУБД.

   В зависимости от того, где вы хотите установить СУБД, перечисленные FQDN служб должны быть преобразованы в IP-адрес кластера Kubernetes следующим образом:

   - СУБД на целевом устройстве вне кластера Kubernetes (стандартное использование)

     В этом случае IP-адрес шлюза соединения – это адрес служб Open Single Management Platform (без учета IP-адреса СУБД). Например, если указан IP-адрес шлюза соединения 192.168.0.0/32, FQDN службы должны быть разрешены следующим образом:

     - <console_host>.<smp_domain> – 192.168.0.0/32
     - <admsrv_host>.<smp_domain> – 192.168.0.0/32
     - <kuma_host>.<smp_domain> – 192.168.0.0/32
     - <api_host>.<smp_domain> – 192.168.0.0/32
   - СУБД внутри кластера Kubernetes (демонстрационное развертывание).

В этом случае IP-адрес шлюза соединения представляет собой IP-диапазон. Первый IP-адрес диапазона – это адрес служб Open Single Management Platform (без учета IP-адреса СУБД). Второй IP-адрес диапазона – IP-адрес СУБД. Например, если указан IP-диапазон шлюза соединения 192.168.0.1–192.168.0.2, FQDN служб должны быть разрешены следующим образом:

- <console_host>.<smp_domain> – 192.168.0.1
- <admsrv_host>.<smp_domain> – 192.168.0.1
- <kuma_host>.<smp_domain> – 192.168.0.1
- <api_host>.<smp_domain> – 192.168.0.1
- <psql_host>.<smp_domain> – 192.168.0.2

9. Создайте учетные записи пользователей, которые будут использоваться для развертывания Open Single Management Platform.

   Эти учетные записи используются для SSH-соединения и должны иметь возможность повышать привилегии (sudo) без ввода пароля. Для этого добавьте созданные учетные записи пользователей в файл `/etc/sudoers`.

10. Настройте SSH-подключение между устройством администратора и целевыми устройствами:

    a. На устройстве администратора сгенерируйте SSH-ключи с помощью утилиты ssh-keygen без парольной фразой.

    b. Скопируйте открытый ключ на целевое устройство (например, в директорию `/home/<имя_пользователя>/.ssh`) с помощью утилиты ssh-copy-id.

    Если вы используете целевое устройство в качестве устройства администратора, вам нужно скопировать на него открытый ключ.

11. Для корректной работы компонентов Open Single Management Platform откройте требуемые порты на сетевом экране устройства администратора и целевых устройств.

12. Настройте синхронизацию времени по протоколу Network Time Protocol (NTP) на устройстве администратора и целевых устройствах.

13. При необходимости подготовьте пользовательские сертификаты для работы с публичными службами Open Single Management Platform.

    Вы можете использовать один промежуточный сертификат, выданный на основе корневого сертификата организации или конечных сертификатов для каждой службы. Подготовленные пользовательские сертификаты будут использоваться вместо самоподписанных сертификатов.

Подготовка устройств к установке сервисов KUMA

Сервисы KUMA (коллекторы, коррелляторы и хранилища) устанавливаются на целевые устройства KUMA, расположенные вне кластера Kubernetes.

Доступ к сервисам KUMA выполняется с использованием FQDN целевых устройств KUMA. Устройство администратора должно иметь доступ к целевым устройствам KUMA по своим FQDN.

Чтобы подготовить целевые устройства KUMA к установке сервисов KUMA:

1. Убедитесь, что выполнены требования к оборудованию, программному обеспечению и установке.

2. Укажите имена устройств.

   Вам нужно указать FQDN, например: kuma1.example.com.

   Не рекомендуется изменять имя устройства KUMA после установки. Это сделает невозможным проверку подлинности сертификатов и нарушит сетевое взаимодействие между компонентами приложения.

3. Выполните следующие команды:

   ```
   hostname -f
   hostnamectl status
   ```

   Сравните результат команды `hostname -f` и значение поля `Static hostname` в выводе команды `hostnamectl status`. Эти значения должны совпадать с FQDN устройства.

4. Настройте SSH-подключение между устройством администратора и целевыми устройствами KUMA:

   Используйте SSH-ключи, созданные для целевых устройств. Скопируйте открытый ключ на целевые устройства KUMA с помощью утилиты ssh-copy-id.

5. Зарегистрируйте целевые устройства KUMA в зоне DNS вашей организации, чтобы разрешить преобразование имен устройств в IP-адреса.

6. Убедитесь, что на всех целевых устройствах KUMA настроена синхронизация времени по протоколу Network Time Protocol (NTP).

Устройство готово к установке сервисов KUMA.

Установка системы управления базами данных

Open Single Management Platform поддерживает системы управления базами данных (СУБД) PostgreSQL или Postgres Pro. Полный список поддерживаемых СУБД см. в разделе Аппаратные и программные требования.

Для каждого из следующих компонентов Open Single Management Platform требуется база данных:

- Сервер администрирования
- Платформа автоматизации
- Incident Response Platform (IRP)
- Identity and Access Manager (IAM)

Каждый компонент должен использовать отдельную базу данных в одном экземпляре СУБД. Рекомендуется устанавливать экземпляр СУБД вне кластера Kubernetes.

Для установки СУБД KDT требует наличия привилегированной учетной записи СУБД с правами на создание баз данных и других учетных записей СУБД. KDT использует эту привилегированную учетную запись СУБД для создания баз данных и других учетных записей СУБД, необходимых для работы компонентов Open Single Management Platform.

Сведения о том, как установить выбранную СУБД, см. в документации к ней.

После установки СУБД необходимо настроить параметры сервера СУБД для оптимизации работы СУБД с Open Single Management Platform.

Настройка сервера PostgreSQL или Postgres Pro для работы с Open Single Management Platform

Open Single Management Platform поддерживает системы управления базами данных (СУБД) PostgreSQL или Postgres Pro. Полный список поддерживаемых СУБД см. в разделе Аппаратные и программные требования. Рассмотрите возможность настроить параметры сервера СУБД для оптимизации работы СУБД с Сервером администрирования.

Путь по умолчанию к конфигурационному файлу: `/etc/postgresql/<ВЕРСИЯ>/main/postgresql.conf`

Рекомендуемые параметры для работы СУБД PostgreSQL и Postgres Pro с Сервером администрирования:

- `shared_buffers` = 25% от объема оперативной памяти устройства, на котором установлена СУБД

  Если оперативной памяти меньше 1 ГБ, то оставьте значение по умолчанию.

- `max_stack_depth` = Если СУБД установлена на устройстве Linux: максимальный размер стека (выполните команду `ulimit -s`, чтобы получить это значение в КБ) минус 1 МБ

  Если СУБД установлена на устройстве Windows, оставьте значение по умолчанию 2 МБ.

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `max_connections = 220`

  Это минимально рекомендованное значение, вы можете указать большее.

- `max_parallel_workers_per_gather = 0`

- `maintenance_work_mem = 128MB`

Примените конфигурацию или перезапустите службу после обновления файла postgresql.conf. Дополнительную информацию см. в документации PostgreSQL.

Если вы используете Postgres Pro 15.7 или Postgres Pro 15.7.1, выключите параметр `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Подробную информацию о параметрах сервера PostgreSQL и Postgres Pro, а также о том, как указать эти параметры, см. в соответствующей документации по СУБД.

Подготовка файла инвентаря KUMA

Файл инвентаря KUMA – это файл в формате YAML, который содержит параметры установки для развертывания сервисов KUMA, не включенных в кластер Kubernetes. Путь к файлу инвентаря KUMA включен в конфигурационный файл, который используется Kaspersky Deployment Toolkit для развертывания Open Single Management Platform.

Шаблоны файла инвентаря KUMA находятся в дистрибутиве. Если вы хотите установить сервисы KUMA (хранилище, коллектор и коррелятор) на одном устройстве, используйте файл single.inventory.yaml. Чтобы установить сервисы на нескольких устройствах в сетевой инфраструктуре, используйте файл distributed.inventory.yaml.

Рекомендуется создать резервную копию файла инвентаря KUMA, который вы использовали для установки сервисов KUMA. Вы можете использовать его для удаления KUMA.

Чтобы подготовить файл инвентаря KUMA,

откройте шаблон файла инвентаря KUMA, расположенный в дистрибутиве и измените переменные в файле инвентаря.

Файл инвентаря KUMA содержит следующие блоки:

- `all` block

  Блок `all` содержит переменные, которые применяются ко всем устройствам, указанным в файле инвентаря. Переменные находятся в разделе `vars`.

- `kuma` block

  Блок `kuma` содержит переменные, которые применяются к устройствам, на которых будут установлены сервисы KUMA. Эти устройства перечислены в блоке `kuma` в разделе `children`. Переменные находятся в разделе `vars`.

В следующей таблице перечислены возможные переменные, их описания, возможные значения и блоки файла инвентаря KUMA, в которых могут быть расположены эти переменные.

Список возможных переменных в разделе vars

Переменная	Описание	Возможные значения	Блок
Переменные, расположенные в разделе `vars` в блоках `all` и `kuma`			
`ansible_connection`	Метод, используемый для подключения к устройствам с сервисами KUMA.	• `ssh` – подключение к целевым устройствам по SSH установлено. • `local` – подключение к целевым устройствам не установлено. Чтобы обеспечить правильную установку сервисов KUMA, в блоке `all` установите для переменной `ansible_connection` значение `local`. В блоке `kuma` вам нужно указать переменную `ansible_connection` и установить для `ansible_connection` значение `ssh`, чтобы обеспечить подключение к устройствам, на которых установлены сервисы KUMA с помощью SSH.	• `all` • `kuma`
`ansible_user`	Имя пользователя, используемое для подключения к устройствам с сервисами KUMA и для установки внешних сервисов KUMA.	Если пользователь root заблокирован на целевых устройствах, укажите имя пользователя, у которого есть право устанавливать SSH-подключения и повышать привилегии с помощью su или sudo. Чтобы обеспечить правильную установку сервисов KUMA, в блоке `all` установите для переменной `ansible_user` значение `nonroot`. В блоке `kuma` вам нужно изменить переменную `ansible_user` и указать для переменной `ansible_user` имя пользователя учетной записи, которая может подключаться к удаленным устройствам через SSH, чтобы подготовить их к установке сервисов KUMA.	• `all` • `kuma`
`deploy_example_services`	Используемая переменная указывает на создание	• `false` – службы не требуются. Значение по умолчанию для шаблона файла инвентаря KUMA.	`all`

	предопределенных сервисов во время установки.	Установите для переменной `deploy_example_services` значение `false` для стандартного развертывания сервисов KUMA. • `true` – сервисы должны быть созданы во время установки. Установите для переменной `deploy_example_services` значение `true` только для демонстрационного развертывания сервисов KUMA.	
`ansible_become`	Переменная, указывает на необходимость повышения прав учетной записи пользователя, которая используется для установки компонентов KUMA.	• `false` – если значение `ansible_user` – `root`. • `true` – если значение `ansible_user` – не `root`.	`kuma`
`ansible_become_method`	Метод, используемый для повышения привилегий учетной записи пользователя, которая используется для установки компонентов KUMA.	`su` или `sudo`, если значение `ansible_user` не `root`.	`kuma`
Переменные, расположенные в дочернем разделе блока `kuma`			
`kuma_utils`	Группа устройств, на которых хранятся служебные файлы и утилиты KUMA. Устройство может быть включено в группу `kuma_utils` и в группы `kuma_collector`, `kuma_correlator` или `kuma_storage` одновременно. Группа `kuma_utils` может содержать несколько устройств. Во время развертывания Open Single Management Platform на устройствах, входящих в `kuma_utils`, в директорию `/opt/kaspersky/kuma/utils/` копируются следующие файлы: • kuma – исполняемый файл, с которым устанавливаются сервисы KUMA. • kuma.exe – это исполняемый файл, с помощью которого агенты KUMA устанавливаются на устройства с операционной системой Windows. • LEGAL_NOTICES – файл с информацией о стороннем коде. • maxpatrol-tool, kuma-ptvm.tar.gz – это утилиты для интеграции с MaxPatrol. • ootb-content –это архив с готовыми ресурсами для сервисов KUMA.	Группа устройств содержит переменную `ansible_host`, которая указывает уникальное полное доменное имя устройства и IP-адрес.	`kuma`
`kuma_collector`	Группа устройств коллекторов KUMA. Эта группа может содержать несколько устройств.	Группа устройств коллекторов KUMA содержит переменную `ansible_host`, которая указывает уникальное имя устройства FQDN и IP-адрес.	`kuma`
`kuma_correlator`	Группа устройств корреляторов KUMA. Эта группа может содержать несколько устройств.	Группа устройств корреляторов KUMA содержит переменную `ansible_host`, которая указывает уникальное имя устройства FQDN и IP-адрес.	`kuma`
`kuma_storage`	Группа устройств хранилищ KUMA. Эта группа может содержать несколько устройств.	Группа устройств хранилищ KUMA содержит переменную `ansible_host`, которая указывает уникальное имя устройства FQDN и IP-адрес.	`kuma`

		В этой группе вы также можете указать структуру хранилища, если вы устанавливаете примеры сервисов во время демонстрационного развертывания (`deploy_example_services: true`). Для стандартного развертывания (`deploy_example_services: false`) укажите структуру хранилища в интерфейсе Консоли KUMA.	

Пример шаблона файла инвентаря KUMA для установки сервисов KUMA на отдельном устройстве (файл single.inventory.yaml)

```
all:
  vars:
    deploy_example_services: false
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma.example.com:
         ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma.example.com:
         ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma.example.com:
         ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma.example.com:
         ansible_host: 0.0.0.0
         shard: 1
         replica: 1
         keeper: 1
```

Пример шаблона файла инвентаря KUMA для установки сервисов KUMA на нескольких устройствах (файл distributed.inventory.yaml)

```
all:
  vars:
    deploy_example_services: false
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma-utils.example.com:
        ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
        ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
        ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-1.example.com:
         ansible_host: 0.0.0.0
         shard: 1
         replica: 1
         keeper: 1
        kuma-storage-2.example.com:
         ansible_host: 0.0.0.0
         shard: 1
         replica: 2
         keeper: 2
        kuma-storage-3.example.com:
         ansible_host: 0.0.0.0
         shard: 2
         replica: 1
         keeper: 3
        kuma-storage-4.example.com:
         ansible_host: 0.0.0.0
         shard: 2
         replica: 2
```

Распределенное развертывание: Указание параметров установки

Конфигурационный файл – это файл в формате YAML, содержащий набор параметров установки компонентов Open Single Management Platform.

Параметры установки, указанные в таблицах ниже, необходимы для развертывания на нескольких узлах Open Single Management Platform. Чтобы развернуть Open Single Management Platform на отдельном узле, используйте конфигурационный файл, содержащий параметры установки, характерные для развертывания на одном узле.

Шаблон конфигурационного файла (multinode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT. Вы можете заполнить шаблон конфигурационного файла вручную либо с помощью мастера настройки: укажите параметры установки, необходимые для развертывания Open Single Management Platform и сгенерируйте конфигурационный файл.

Не все перечисленные ниже параметры включены в шаблон конфигурационного файла. Этот шаблон содержит только те параметры, которые должны быть указаны пользователю перед развертыванием Open Single Management Platform. Остальные параметры имеют значения по умолчанию и не включены в шаблон. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения.

Для корректной работы KDT с конфигурационным файлом добавьте пустую строку в конце файла.

Раздел `nodes` конфигурационного файла содержит параметры установки для каждого целевого устройства кластера Kubernetes Эти параметры перечислены в таблице ниже.

Раздел узлов

Имя параметра	Обязательная	Описание
`desc`	Да	Название узла.
`type`	Да	Тип узла. Возможные значения параметра: • `primary` • `worker`
`host`	Да	IP-адрес узла. Все узлы должны быть включены в одну подсеть.
`kind`	Нет	Тип узла, определяющий компонент Open Single Management Platform, который будет установлен на этом узле. Возможные значения параметра: • `admsrv` – значение узла, на котором будет установлен Сервер администрирования. • `ncircc` – значение узла, на котором будет установлен компонент для взаимодействия с НКЦКИ. Значение параметра `ncircc` используется, только если для параметра `ncircc_nodeselector` установлено значение `true`. • `db` – значение узла, на котором будет установлена СУБД. Параметр используется, если вы хотите установить СУБД на узел внутри кластера (не для стандартного использования решения, только для демонстрационных целей). Для корректной работы Open Single Management Platform рекомендуется выбрать узлы, на которых будет работать Сервер администрирования и компонент для взаимодействия с НКЦКИ. Также вы можете выбрать узел, на который хотите установить СУБД. Укажите соответствующие значения параметра `kind` для этих узлов. Не указывайте этот параметр для других узлов.
`user`	Да	Имя пользователя учетной записи, созданной на целевом устройстве и используемой для подключения к узлу с помощью KDT.
`key`	Да	Путь к закрытой части SSH-ключа находится на устройстве администратора и используется для подключения к узлу KDT.

Остальные параметры установки перечислены в разделе `parameters` конфигурационного файла и описаны в таблице ниже.

Раздел параметров

Имя параметра	Обязательная	Описание
`psql_dsn`	Да	Строка подключения для доступа к СУБД, которая установлена и настроена на отдельном сервере. Укажите этот параметр следующим образом: `psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`.

		`dbms_username` – имя пользователя привилегированной внутренней учетной записи СУБД. Этой учетной записи предоставлены права на создание баз данных и других учетных записей СУБД. С использованием этой привилегированной учетной записи СУБД во время развертывания будут созданы базы данных и другие учетные записи СУБД, необходимые для работы компонентов Open Single Management Platform. `password` – пароль привилегированной внутренней учетной записи СУБД. `fqdn:port` – полное имя домена и порт подключения отдельного сервера, на котором установлена СУБД. Если задан параметр `psql_dsn`, компоненты Open Single Management Platform используют СУБД, расположенную по указанному FQDN. В противном случае компоненты Open Single Management Platform используют СУБД внутри кластера. Для стандартного использования решения установите СУБД на отдельный сервер вне кластера. После развертывания Open Single Management Platform замена СУБД, которая установлена внутри кластера, на СУБД, установленную на отдельном сервере, недоступна.
`nwc-language`	Да	Язык интерфейса Консоли OSMP, указанный по умолчанию. После установки вы можете изменить язык Консоли OSMP. Возможные значения параметра: • `enUS` • `ruRu`
`ip_address`	Да	Зарезервированный статический IP-адрес шлюза кластера Kubernetes. Шлюз соединения должен быть включен в ту же подсеть, что и все узлы кластера. Для стандартного использования решения, когда вы устанавливаете СУБД на отдельный сервер, укажите IP-адрес шлюза соединения как IP-адрес в нотации CIDR, которая содержит маску подсети /32. Для демонстрационных целей, когда вы устанавливаете СУБД внутри кластера, установите IP-адрес шлюза в IP-диапазоне в формате `0.0.0.0-0.0.0.0`, где первый IP-адрес – это IP-адрес шлюза, а второй IP-адрес – IP-адрес СУБД.
`ssh_pk`	Да	Путь к приватной части SSH-ключа, которая находится на устройстве администратора и используется для подключения к узлам кластеров и узлам с сервисам KUMA (коллекторам, коррелляторам и хранилищам) с помощью утилиты KDT.
`admin_password`	Да	Параметр `admin_password` задает пароль Open Single Management Platform, который будет создан утилитой KDT при установке. Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора. Пароль должен соответствовать следующим правилам: • Пароль пользователя не может содержать менее 8 или более 16 символов. • Пароль должен содержать символы как минимум трех групп списка ниже: • верхний регистр (A–Z); • нижний регистр (a-z); • числа (0–9); • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • Пароль не должен содержать пробелов, символов Юникода или комбинации ".@". Когда вы указываете значение параметра `admin_password` вручную (не с помощью мастера настройки), убедитесь, что это значение соответствует требованиям стандарта YAML для значений в строках: • Значение параметра, содержащего специальные символы, должно быть заключено в одинарные кавычки. • Любая одинарная кавычка ' внутри значения параметра должна быть удвоена, чтобы избежать этой одинарной кавычки. Пример: пароль учетной записи пользователя `Any_pass%1234'5678"90` для параметра `admin_password` должен быть указан как `'Any_pass%1234''5678"90'`.
`low_resources`	Нет	Параметр, указывающий, что Open Single Management Platform установлен на целевом устройстве с ограниченными вычислительными ресурсами.

		Для развертывания на нескольких узлах установите для параметра `low_resources` значение `false`. По умолчанию указано значение `false`. Возможные значения параметра: • `true` – установка с ограниченными вычислительными ресурсами (для развертывания на одном узле). • `false` – стандартная установка.
`core_disk_request`	Да	Параметр, который указывает объем дискового пространства для работы Ядра KUMA. Этот параметр используется, только если для параметра `low_resources` установлено значение `false`. Если для параметра `low_resources` установлено значение `true`, параметр `core_disk_request` игнорируется и выделяется 4 ГБ дискового пространства для работы Ядра KUMA. Если вы не укажете параметр `core_disk_request`, а для параметра `low_resources` установлено значение `false`, для работы Ядра KUMA будет выделен объем дискового пространства по умолчанию. Объем дискового пространства по умолчанию равен 512 ГБ.
`inventory`	Да	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Файл инвентаря содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes.
`host_inventory`	Нет	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Этот файл содержит параметры установки, используемые для частичного добавления или удаления устройств с сервисами KUMA. Если вы выполняете первоначальное развертывание Open Single Management Platform или запускаете пользовательское действие, для которого требуется конфигурационный файл, оставьте значение параметра по умолчанию (`/dev/null`).
`license`	Да	Путь к лицензионному ключу Ядра KUMA.

`iam-nwc_host`
`flow_host`
`hydra_host`
`login_host`
`admsrv_host`
`console_host`
`api_host`
`kuma_host`
`psql_host`
`monitoring_host`
`gateway_host`
	Да	Имя устройства, которое используется в FQDN публичных служб Open Single Management Platform. Имя устройства службы и доменное имя (значение параметра `smp_domain`) являются частью FQDN-службы.
		Значения параметров по умолчанию:
		• `iam-nwc_host="console"`
		• `flow_host="console"`
		• `hydra_host="console"`
		• `login_host="console"`
		• `admsrv_host="admsrv"`
		• `console_host="console"`
		• `api_host="api"`
		• `kuma_host="kuma"`
		• `psql_host="psql"`
		• `monitoring_host="monitoring"`
		• `gateway_host="console"`

`smp_domain`	Да	Имя домена, которое используется в FQDN публичных служб Open Single Management Platform. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `osmp_console`, а значение переменной `smp_domain` равно `smp.local`, тогда FQDN службы, предоставляющей доступ к Консоли OSMP, принимает значение `osmp_console.smp.local`.
`pki_host_list`	Да	Список имен устройств публичных служб Open Single Management Platform, для которых требуется сформировать самоподписанный или пользовательский сертификат.
`intermediate_enabled`	Нет	Параметр, который указывает, использовать ли пользовательский промежуточный сертификат вместо самоподписанных сертификатов для публичных служб Open Single Management Platform. По умолчанию указано значение `true`. Возможные значения параметра: • `true` – использовать пользовательский промежуточный сертификат.

		• `false` – использовать самоподписанные сертификаты.
`intermediate_bundle`	Нет	Путь к пользовательскому промежуточному сертификату, которые используются для работы с общедоступными службами Open Single Management Platform. Укажите этот параметр, если для параметра `intermediate_enabled` указано значение `true`.

`admsrv_bundle`
`api_bundle`
`console_bundle`
`psql_bundle`
	Нет	Пути к пользовательским конечным сертификатам, которые используются для работы с публичными службами Open Single Management Platform: `<admsrv_host>.<smp_domain>`, `<api_host>.<smp_domain>`, `<console_host>.<smp_domain>`, `<psql_host>.<smp_domain>`. Укажите параметр `psql_bundle`, если вы выполняете развертывание в демонстрационных целях и устанавливаете СУБД внутри кластера Kubernetes на узле СУБД.
		Если вы хотите указать конечные пользовательские сертификаты, установите для параметра `intermediate_enabled` значение `false` и не указывайте параметр `intermediate_bundle`.

`encrypt_secret` `sign_secret`	Да	Имена секретных файлов, которые хранятся в кластере Kubernetes. Эти имена содержат имя домена, которое должно соответствовать значению параметра `smp_domain`.
`ksc_state_size`	Да	Объем свободного места на диске, выделенный для хранения данных Сервера администрирования (обновлений, инсталляционных пакетов и других внутренних служебных данных). Измеряется в гигабайтах, указывается как "<объем>Gi". Требуемый объем свободного места на диске зависит от количества управляемых устройств и других параметров и может быть рассчитан. Минимальное рекомендуемое значение – 10 ГБ.
`ksc_backup_size`	Да	Объем свободного дискового пространства, выделяемого для хранения резервных копии данных Сервера администрирования. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 10 ГБ.
`prometheus_size`	Да	Объем свободного дискового пространства, выделенного для хранения метрик. Измеряется в гигабайтах, указывается как "<объем>GB". Минимальное рекомендуемое значение – 5 ГБ.
`loki_size`	Да	Объем свободного дискового пространства, выделенного для хранения журналов событий OSMP. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.
`loki_retention_period`	Да	Период хранения журналов событий OSMP, по истечении которого журналы событий автоматически удаляются. Значение по умолчанию указано 72 часа (в конфигурационном файле установите значение параметра – "<time in hours>h". Например, "72h").
`file_storage_cp`	Нет	Количество свободного дискового пространства, выделенного для хранения данных компонента для работы с действиями по реагированию. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.
`psql_tls_off`	Нет	Параметр, указывающий, следует ли шифровать трафик между компонентами Open Single Management Platform и СУБД по протоколу TLS. По умолчанию указано значение `true`. Возможные значения параметра: • `true` – не шифровать трафик (если СУБД будет установлена внутри кластера). • `false` – шифровать трафик.
`psql_trusted_cas`	Нет	Путь к PEM-файлу, который может содержать TLS-сертификат сервера СУБД или корневой сертификат, из которого может быть выдан сертификат TLS-сервера. Укажите параметр `psql_trusted_cas`, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра `psql_tls_off` указано значение `false`).
`psql_client_certificate`	Нет	Путь к PEM-файлу, содержащему сертификат и закрытый ключ компонента Open Single Management Platform. Этот сертификат используется для установления TLS-соединения между компонентами Open Single Management Platform и СУБД. Укажите параметр `psql_client_certificate`, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра `psql_tls_off` указано значение `false`).
`proxy_enabled`	Нет	Параметр, указывающий использовать ли прокси-сервер для подключения компонентов Open Single Management Platform к интернету. Если устройство, на котором установлен Open Single Management Platform, имеет доступ в интернет, вы также можете предоставить доступ в интернет для работы компонентов Open Single Management Platform (например, Сервера администрирования) и для определенных интеграций как с решениями "Лаборатории Касперского", так и со сторонними производителями. Для

		установки прокси-соединения также необходимо указать параметры прокси-сервера в свойствах Сервера администрирования. По умолчанию указано значение `false`. Возможные значения параметра: • `true` – использовать прокси-сервер. • `false` – не использовать прокси-сервер.
`proxy_addresses`	Нет	IP-адрес прокси-сервера. Если прокси-сервер использует несколько IP-адресов, укажите эти адреса через пробел (например, "`0.0.0.0 0.0.0.1 0.0.0.2`"). Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`proxy_port`	Нет	Номер порта, через который будет установлено прокси-подключение. Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`ncircc_nodeselector`	Нет	Параметр, указывающий на то, что вам необходимо установить компонент для взаимодействия с НКЦКИ на конкретном узле кластера. По умолчанию указано значение `false`. Возможные значения параметра: • `true` – компонент для взаимодействия с НКЦКИ будет установлен на узле, для которого параметр `kind` имеет значение `ncricc`. • `false` – компонент для взаимодействия с НКЦКИ не будет установлен.
`feature_gost_status`	Нет	Параметр, который указывает, использовать ли рабочий процесс, созданный на основании ГОСТ Р 59712-2022, для управления инцидентами. Значение по умолчанию `false`. Возможные значения параметра: • `true` – рабочий процесс по ГОСТ используется. • `false` – рабочий процесс по ГОСТ не используется.
`ansible_extra_flags`	Нет	Уровень детальности журнала событий развертывания Ядра KUMA и сервисов KUMA, которое выполняется KDT. Возможные значения параметра: • `-v` • `-vv` • `-vvv` • `-vvvv` По мере увеличения количества букв "v" в флаге, журналы событий становятся более детальными. Если этот параметр не указан в конфигурационном файле, сохраняются стандартные журналы событий установки компонентов.

Пример конфигурационного файла развертывания Open Single Management Platform на нескольких узлах

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary1
    type: primary
    host: 1.1.1.1
    access:
      ssh:
        user: root
        key: /root/.ssh/id_rsa
  - desc: cdt-w1
    type: worker
    host: 1.1.1.1
    access:
      ssh:
        user: root
        key: /root/.ssh/id_rsa
  - desc: cdt-w2
    type: worker
    host: 1.1.1.1
    access:
      ssh:
        user: root
        key: /root/.ssh/id_rsa
  - desc: cdt-w3
    type: worker
    host: 1.1.1.1
    kind: admsrv
    access:
      ssh:
        user: root
        key: /root/.ssh/id_rsa
parameters:
  - name: psql_dsn
    source:
      value: "postgres://postgres:password@dbms.example.com:1234"
  - name: ip_address
    source:
      value: 1.1.1.1/32
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  - name: admin_password
    source:
      value: "password"
  - name: core_disk_request
    source:
      value: 20Gi
  - name: inventory
    source:
      value: "/root/osmp/inventory.yaml"
  - name: host_inventory
    source:
      value: "/dev/null"
  - name: license
    source:
```

```
    value: "/root/osmp/license.key"
  - name: smp_domain
    source:
      value: "smp.local"
  - name: pki_fqdn_list
    source:
      value: "admsrv api console kuma psql monitoring"
```

Развертывание на одном узле: Указание параметров установки

Конфигурационный файл, используемый для развертывания Open Single Management Platform на одном узле, содержит параметры установки, необходимые как для распределенного, так и для развертывания на одном узле. Также этот конфигурационный файл содержит параметры, специфичные только для развертывания на одном узле (`vault_replicas`, `vault_ha_mode`, `vault_standalone` и `default_class_replica_count`).

Шаблон конфигурационного файла (singlenode.smp_param.yaml.template) находится в дистрибутиве в архиве с утилитой KDT. Вы можете заполнить шаблон конфигурационного файла вручную либо с помощью мастера настройки: укажите параметры установки, необходимые для развертывания Open Single Management Platform и сгенерируйте конфигурационный файл.

Не все перечисленные ниже параметры включены в шаблон конфигурационного файла. Этот шаблон содержит только те параметры, которые должны быть указаны пользователю перед развертыванием Open Single Management Platform. Остальные параметры имеют значения по умолчанию и не включены в шаблон. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения.

> Для корректной работы KDT с конфигурационным файлом добавьте пустую строку в конце файла.

Раздел `nodes` конфигурационного файла содержит параметры целевого устройства, которые перечислены в таблице ниже.

Раздел узлов

Имя параметра	Обязательная	Описание
`desc`	Да	Название узла.
`type`	Да	Тип узла. Возможные значения параметра: • `primary` • `worker` • `primary-worker` Для целевого устройства для параметра `type` задайте значение `primary-worker`, чтобы включить **развертывание на одном узле**. В этом случае целевое устройство будет действовать как первичный и рабочий узлы.
`host`	Да	IP-адрес узла. Все узлы должны быть включены в одну подсеть.
`kind`	Нет	Тип узла, определяющий компонент Open Single Management Platform, который будет установлен на этом узле. Если для параметра `kind` узла задано значение `admsrv`, на этом узле будет установлен Сервер администрирования. Если вы выполняете демонстрационное развертывание и хотите установить СУБД на узле внутри кластера, установите для параметра `kind` значение `db` для соответствующего узла. Для других узлов этот параметр можно оставить пустым. Возможные значения параметра: • `admsrv`

		• `db` Не указывайте параметр `kind` при развертывании Open Single Management Platform на одном узле.
`user`	Да	Имя пользователя учетной записи, созданной на целевом устройстве и используемой для подключения к узлу с помощью KDT.
`key`	Да	Путь к закрытой части SSH-ключа находится на устройстве администратора и используется для подключения к узлу KDT.

Остальные параметры установки перечислены в разделе `parameters` конфигурационного файла и описаны в таблице ниже.

Раздел параметров

Имя параметра	Обязательная	Описание
`psql_dsn`	Да	Строка подключения для доступа к СУБД, которая установлена и настроена вне кластера Kubernetes. Укажите этот параметр следующим образом: `psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`. `dbms_username` – имя пользователя привилегированной внутренней учетной записи СУБД. Этой учетной записи предоставлены права на создание баз данных и других учетных записей СУБД. С использованием этой привилегированной учетной записи СУБД во время развертывания будут созданы базы данных и другие учетные записи СУБД, необходимые для работы компонентов Open Single Management Platform. `password` – пароль привилегированной внутренней учетной записи СУБД. `fqdn:port` – полное имя домена и порт подключения целевого устройства, на котором установлена СУБД. Если задан параметр `psql_dsn`, компоненты Open Single Management Platform используют СУБД, расположенную по указанному FQDN. В противном случае компоненты Open Single Management Platform используют СУБД внутри кластера. Для стандартного использования решения, установите СУБД на целевое устройство вне кластера. После развертывания Open Single Management Platform замена СУБД, которая установлена внутри кластера, на СУБД, установленную на отдельном сервере, недоступна.
`nwc-language`	Да	Язык интерфейса Консоли OSMP, указанный по умолчанию. После установки вы можете изменить язык Консоли OSMP. Возможные значения параметра: • `enUS` • `ruRu`
`ip_address`	Да	Зарезервированный статический IP-адрес шлюза кластера Kubernetes. Шлюз соединения должен быть включен в ту же подсеть, что и все узлы кластера. Для стандартного использования решения, когда вы устанавливаете СУБД на отдельный сервер, IP-адрес шлюза соединения должен содержать маску подсети /32. Для демонстрационных целей, когда вы устанавливаете СУБД внутри кластера, установите IP-адрес шлюза в IP-диапазоне в формате `0.0.0.0-0.0.0.0`, где первый IP-адрес – это IP-адрес шлюза, а второй IP-адрес – IP-адрес СУБД.
`ssh_pk`	Да	Путь к приватной части SSH-ключа, которая находится на устройстве администратора и используется для подключения к узлам кластеров и узлам с сервисам KUMA (коллекторам, корреляторам и хранилищам) с помощью утилиты KDT.
`admin_password`	Да	Параметр `admin_password` задает пароль Open Single Management Platform, который будет создан утилитой KDT при установке. Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора. Пароль должен соответствовать следующим правилам: • Пароль пользователя не может содержать менее 8 или более 256 символов. • Пароль должен содержать символы как минимум трех групп списка ниже: • верхний регистр (A–Z);

		• нижний регистр (a-z); • числа (0–9); • специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • Пароль не должен содержать пробелов, символов Юникода или комбинации ".@".  Когда вы указываете значение параметра `admin_password` вручную (не с помощью мастера настройки), убедитесь, что это значение соответствует требованиям стандарта YAML для значений в строках: • Значение параметра, содержащего специальные символы, должно быть заключено в одинарные кавычки. • Любая одинарная кавычка ' внутри значения параметра должна быть удвоена, чтобы избежать этой одинарной кавычки. Пример: пароль учетной записи пользователя `Any_pass%1234'5678"90` для параметра `admin_password` должен быть указан как `'Any_pass%1234''5678"90'`.
`low_resources`	Да	Параметр, который указывает на то, что Open Single Management Platform установлен на целевом устройстве с ограниченными вычислительными ресурсами. Возможные значения параметра: • `true` – установка с ограниченными вычислительными ресурсами (для развертывания на одном узле). • `false` – стандартная установка. Для **развертывания на одном узле** установите для параметра `low_resources` установлено значение `true`, чтобы компоненты Open Single Management Platform требовали меньше ресурсов памяти и процессора. Если вы включите этот параметр, для установки Ядра KUMA на целевом устройстве будет выделено 4 ГБ свободного дискового пространства.
`vault_replicas`	Да	Количество реплик секретного хранилища в кластере Kubernetes. Для **развертывания на одном узле** установите для параметра `vault_replicas` значение `1`.
`vault_ha_mode`	Да	Параметр, который указывает следует ли запускать хранилище секретов в режиме High Availability (HA). Возможные значения параметра: • `true` • `false` Для **развертывания на одном узле** установите для параметра `vault_ha_mode` значение `false`.
`vault_standalone`	Да	Параметр, который указывает, следует ли запускать хранилище секретов в автономном режиме. Возможные значения параметра: • `true` • `false` Для **развертывания на одном узле** установите для параметра `vault_standalone` значение `true`.
`core_disk_request`	Да	Параметр, который указывает объем дискового пространства для работы Ядра KUMA. Этот параметр используется, только если для параметра `low_resources` установлено значение `false`. Если для параметра `low_resources` установлено значение `true`, параметр `core_disk_request` игнорируется и выделяется 4 ГБ дискового пространства для работы Ядра KUMA. Если вы не укажете параметр `core_disk_request`, а для параметра `lowResources` установлено значение `false`, для работы Ядра KUMA будет выделен объем дискового пространства по умолчанию. Объем дискового пространства по умолчанию равен 512 ГБ.
`inventory`	Да	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Файл инвентаря содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes.
`host_inventory`	Нет	Путь к файлу инвентаря KUMA, находящемуся на устройстве администратора. Этот

		файл содержит параметры установки, используемые для частичного добавления или удаления устройств с сервисами KUMA. Если вы выполняете первоначальное развертывание Open Single Management Platform или запускаете пользовательское действие, для которого требуется конфигурационный файл, оставьте значение параметра по умолчанию (`/dev/null`).
`license`	Да	Путь к лицензионному ключу Ядра KUMA.

`iam-nwc_host`
`flow_host`
`hydra_host`
`login_host`
`admsrv_host`
`console_host`
`api_host`
`kuma_host`
`psql_host`
`monitoring_host`
`gateway_host`
	Да	Имя устройства, которое используется в FQDN публичных служб Open Single Management Platform. Имя устройства службы и доменное имя (значение параметра `smp_domain`) являются частью FQDN-службы.
		Значения параметров по умолчанию:
		• `iam-nwc_host—"console"`
		• `flow_host—"console"`
		• `hydra_host—"console"`
		• `login_host—"console"`
		• `admsrv_host—"admsrv"`
		• `console_host—"console"`
		• `api_host—"api"`
		• `kuma_host—"kuma"`
		• `psql_host—"psql"`
		• `monitoring_host—"monitoring"`
		• `gateway_host—"console"`

`smp_domain`	Да	Имя домена, которое используется в FQDN публичных служб Open Single Management Platform. Имя устройства службы и доменное имя являются частью FQDN-службы. Например, если значение переменной `console_host` равно `console`, а значение переменной `smp_domain` равно `smp.local`, тогда полное имя службы, предоставляющей доступ к Консоли OSMP, принимает значение `console.smp.local`.
`pki_host_list`	Да	Список имен устройств публичных служб Open Single Management Platform, для которых требуется сформировать самоподписанный или пользовательский сертификат.
`intermediate_enabled`	Нет	Параметр, который указывает, использовать ли пользовательский промежуточный сертификат вместо самоподписанных сертификатов для публичных служб Open Single Management Platform. По умолчанию указано значение `true`. Возможные значения параметра: • `true` – использовать пользовательский промежуточный сертификат. • `false` – использовать самоподписанные сертификаты.
`intermediate_bundle`	Нет	Путь к пользовательскому промежуточному сертификату, которые используются для работы с общедоступными службами Open Single Management Platform. Укажите этот параметр, если для параметра `intermediate_enabled` указано значение `true`.

`admsrv_bundle`
`api_bundle`
`console_bundle`
`psql_bundle`
	Нет	Пути к пользовательским конечным сертификатам, которые используются для работы с соответствующими публичными службами Open Single Management Platform: `<admsrv_host>.<smp_domain>`, `<api_host>.<smp_domain>`, `<console_host>.<smp_domain>` и `<psql_host>.<smp_domain>`. Укажите параметр `psql_bundle`, если вы выполняете развертывание в демонстрационных целях и устанавливаете СУБД внутри кластера Kubernetes на узле СУБД.
		Если вы хотите указать конечные пользовательские сертификаты, установите для параметра `intermediate_enabled` значение `false` и не указывайте параметр `intermediate_bundle`.

`encrypt_secret` `sign_secret`	Да	Имена секретных файлов, которые хранятся в кластере Kubernetes. Эти имена содержат имя домена, которое должно соответствовать значению параметра `smp_domain`.

`ksc_state_size`	Да	Объем свободного места на диске, выделенный для хранения данных Сервера администрирования (обновлений, инсталляционных пакетов и других внутренних служебных данных).
`default_class_replica_count`	Да	Количество дисковых томов, на которых хранятся служебные данные компонентов Open Single Management Platform и KDT. По умолчанию указано значение `3`. Для **развертывания на одном узле** установите для параметра `default_class_replica_count` значение `1`.
`prometheus_size`	Да	Объем свободного дискового пространства, выделенного для хранения метрик. Минимальное рекомендуемое значение – 5 ГБ.
`grafana_admin_user`	Нет	Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
`grafana_admin_password`	Нет	Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
`grafana_admin_user`	Нет	Имя учетной записи пользователя, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
`grafana_admin_password`	Нет	Пароль от учетной записи, используемой для просмотра метрик OSMP с помощью инструмента Grafana.
`loki_size`	Да	Объем свободного дискового пространства, выделенного для хранения журналов событий OSMP. Минимальное рекомендуемое значение – 20 ГБ.
`loki_retention_period`	Да	Период хранения журналов событий OSMP, по истечении которого журналы событий автоматически удаляются. Значение по умолчанию указано 72 часа (в конфигурационном файле установите значение параметра – "<time in hours>h". Например, "72h").
`file_storage_cp`	Нет	Количество свободного дискового пространства, выделенного для хранения данных компонента для работы с действиями по реагированию. Измеряется в гигабайтах, указывается как "<объем>Gi". Минимальное рекомендуемое значение – 20 ГБ.
`psql_tls_off`	Нет	Параметр, указывающий, следует ли шифровать трафик между компонентами Open Single Management Platform и СУБД по протоколу TLS. Возможные значения параметра: • `true` – не шифровать трафик (если СУБД будет установлена внутри кластера). • `false` – шифровать трафик.
`psql_trusted_cas`	Нет	Путь к PEM-файлу, который может содержать TLS-сертификат сервера СУБД или корневой сертификат, из которого может быть выдан сертификат TLS-сервера. Укажите параметр `psql_trusted_cas`, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра `psql_tls_off` указано значение `false`).
`psql_client_certificate`	Нет	Путь к PEM-файлу, содержащему сертификат и закрытый ключ компонента Open Single Management Platform. Этот сертификат используется для установления TLS-соединения между компонентами Open Single Management Platform и СУБД. Укажите параметр `psql_client_certificate`, если СУБД будет установлена и настроена на отдельном сервере и если включено шифрование трафика (для параметра `psql_tls_off` указано значение `false`).
`proxy_enabled`	Нет	Параметр, указывающий использовать ли прокси-сервер для подключения компонентов Open Single Management Platform к интернету. Если устройство, на котором установлен Open Single Management Platform, имеет доступ в интернет, вы также можете предоставить доступ в интернет для работы компонентов Open Single Management Platform (например, Сервера администрирования) и для определенных интеграций как с решениями "Лаборатории Касперского", так и со сторонними производителями. Для установки прокси-соединения также необходимо указать параметры прокси-сервера в свойствах Сервера администрирования. По умолчанию указано значение `false`. Возможные значения параметра: • `true` – использовать прокси-сервер. • `false` – не использовать прокси-сервер.
`proxy_addresses`	Нет	IP-адрес прокси-сервера. Если прокси-сервер использует несколько IP-адресов, укажите эти адреса через пробел (например, "`0.0.0.0 0.0.0.1 0.0.0.2`").

		Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`proxy_port`	Нет	Номер порта, через который будет установлено прокси-подключение. Укажите этот параметр, если для параметра `proxy_enabled` указано значение `true`.
`feature_gost_status`	Нет	Параметр, который указывает использовать ли рабочий процесс, созданный на основании ГОСТ Р 59712-2022, для управления инцидентами. Значение по умолчанию `false`. Возможные значения параметра: • `true` – рабочий процесс по ГОСТ используется. • `false` – рабочий процесс по ГОСТ не используется.
`trace_level`	Нет	Уровень трассировки. По умолчанию указано значение `0`. Возможные значения параметра: 0–5.
`ansible_extra_flags`	Нет	Уровень детальности журнала событий развертывания Ядра KUMA и сервисов KUMA, которое выполняется KDT. Возможные значения параметра: • `-v` • `-vv` • `-vvv` • `-vvvv` По мере увеличения количества букв "v" в флаге, журналы событий становятся более детальными. Если этот параметр не указан в конфигурационном файле, сохраняются стандартные журналы событий установки компонентов.

Пример конфигурационного файла для развертывания Open Single Management Platform на одном узле

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-1
    type: primary-worker
    host: 1.1.1.1
    proxy:
    access:
      ssh:
        user: root
        key: /root/.ssh/id_rsa
parameters:
  - name: psql_dsn
    source:
      value: "postgres://postgres:password@dbms.example.com:1234"
  - name: ip_address
    source:
      value: 1.1.1.1/32
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  - name: admin_password
    source:
      value: "password"
  - name: low_resources
    source:
      value: "true"
  - name: default_class_replica_count
    source:
      value: "1"
  - name: vault_replicas
    source:
      value: "1"
  - name: vault_ha_mode
    source:
      value: "false"
  - name: vault_standalone
    source:
      value: "true"
  - name: inventory
    source:
      value: "/root/osmp/inventory.yaml"
  - name: host_inventory
    source:
      value: "/dev/null"
  - name: license
    source:
      value: "/root/osmp/license.key"
  - name: smp_domain
    source:
      value: "smp.local"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma psql monitoring"
```

Указание параметров установки с помощью мастера настройки

Для развертывания на нескольких узлах и развертывания на одном узле Open Single Management Platform необходимо подготовить конфигурационный файл, содержащий параметры установки компонентов Open Single Management Platform. Мастер настройки позволяет указать параметры установки, необходимые для развертывания Open Single Management Platform и сформировать итоговый конфигурационный файл. Необязательные параметры установки имеют значения по умолчанию, и их не следует указывать в мастере настройки. Вы можете вручную добавить эти параметры в конфигурационный файл, чтобы перезаписать их значения по умолчанию.

Предварительные требования

Перед указанием параметров установки с помощью мастера настройки необходимо установить систему управления базами данных на отдельном сервере, расположенном вне кластера Kubernetes, выполнить все подготовительные действия, необходимые для администратора, целевых устройств (в зависимости от развертывания на нескольких узлах или развертывания на одном узле) и устройств KUMA.

Process.

Чтобы указать параметры установки с помощью мастера настройки:

1. На устройстве администратора, на котором расположена утилита KDT, запустите мастер настройки с помощью следующей команды:

   `./kdt wizard -k <путь_к_транспортному_архиву> -o <путь_к_конфигурационному_файлу>`

   где

   - `<path_to_transport_archive>` – путь к транспортному архиву.
   - `<path_to_configuration_file>` – путь, по которому вы хотите сохранить конфигурационный файл и имя конфигурационного файла.

   Мастер настройки предложит вам указать параметры установки. Список параметров установки, характерных для развертывания на нескольких узлах и развертывания на одном узле, различается.

   Если у вас нет прав на запись в указанной папке или в этой папке находится файл с таким же именем, возникает ошибка и мастер завершает работу.

2. Введите IPv4-адрес первичного узла (или первичного рабочего узла, если вы будете выполнять развертывание с одним узлом). Это значение соответствует параметру `host` конфигурационного файла.

3. Введите имя пользователя учетной записи, используемой для подключения к первичному узлу с помощью KDT (параметр `user` конфигурационного файла).

4. Введите путь к закрытой части SSH-ключа, который находится на устройстве администратора и используется для подключения к первичному узлу KDT (параметр `key` конфигурационного файла).

5. Введите количество рабочих узлов.

   Возможные значения:

   - 0 – развертывание на одном узле.

- 3 или более – развертывание на нескольких узлах.

Этот шаг определяет вариант установки Open Single Management Platform. Если вы хотите выполнить развертывание на одном узлом, следующие параметры, характерные для этого варианта развертывания, примут значения по умолчанию:

- `type—primary-worker`
- `low_resources – true`
- `vault_replicas—1`
- `vault_ha_mode—false`
- `vault_standalone—true`
- `default_class_replica_count – 1`

6. Для каждого рабочего узла введите IPv4-адрес (параметр `host` конфигурационного файла).

   Обратите внимание, что первичный и рабочий узлы должны быть включены в одну подсеть.

   Для развертывания на нескольких узлах для параметра `kind` первого рабочего узла по умолчанию установлено значение `admsrv`. Это означает, что Сервер администрирования будет установлен на первом рабочем узле. Для развертывания на одном узле параметр `kind` не указывается для первичного рабочего узла.

7. Для каждого рабочего узла введите имя пользователя, используемое для подключения к рабочему узлу с помощью KDT (параметр `user` конфигурационного файла).

8. Для каждого рабочего узла введите путь к закрытой части SSH-ключа, который используется для подключения к рабочему узлу с помощью KDT (параметр `key` конфигурационного файла).

9. Введите строку подключения для доступа к СУБД, которая установлена и настроена на отдельном сервере (параметр `psql_dsn` конфигурационного файла).

   Укажите этот параметр следующим образом: `postgres://<dbms_username>:<password>@<fqdn>:<port>`.

   > Мастер задает параметры установки только для варианта развертывания с установленной СУБД на отдельном сервере, расположенном вне кластера Kubernetes.

10. Введите IP-адрес шлюза кластера Kubernetes (параметр `ip_address` конфигурационного файла).

    Шлюз соединения должен быть включен в ту же подсеть, что и все узлы кластера. IP-адрес шлюза подключения должен содержать маску подсети /32.

11. Введите пароль учетной записи Open Single Management Platform, которая будет создана KDT при установке (параметр `admin_password` конфигурационного файла).

    Имя пользователя по умолчанию для этой учетной записи – "admin". Этой учетной записи пользователя назначена роль Главного администратора.

12. Введите путь к файлу инвентаря KUMA, расположенному на устройстве администратора (параметр `inventory` конфигурационного файла).

    Файл инвентаря KUMA содержит параметры установки для развертывания сервисов KUMA, не входящих в кластер Kubernetes.

13. Введите путь к файлу с Лицензионным соглашением Ядра KUMA (параметр `license` конфигурационного файла).

14. Введите имя домена, которое используется в FQDN публичных служб Open Single Management Platform (параметр `smp_domain` конфигурационного файла).

15. Укажите путь к пользовательским сертификатам, которые используются для работы с публичными службами Open Single Management Platform (параметр `intermediate_bundle` конфигурационного файла).

    Если вы хотите использовать самоподписанные сертификаты, нажмите на клавишу **Enter**, чтобы пропустить этот шаг.

16. Введите **t**, чтобы использовать рабочий процесс, созданный на основании ГОСТ Р 59712-2022, для управления инцидентами (параметр `feature_gost_status` в конфигурационном файле).

17. Проверьте указанные параметры, которые отображаются в нумерованном списке.

    Чтобы изменить параметр, введите номер параметра и укажите новое значение параметра. В противном случае нажмите на клавишу **Enter**, чтобы продолжить.

18. Нажмите **Y**, чтобы сохранить новый конфигурационный файл с указанными параметрами, или **N**, чтобы остановить мастер настройки без сохранения.

Конфигурационный файл с указанными параметрами сохраняется в формате YAML.

Остальные параметры установки включены в конфигурационный файл со значениями по умолчанию. Вы можете изменить конфигурационный файл вручную перед развертыванием Open Single Management Platform.

Установка Open Single Management Platform

Разверните Open Single Management Platform с помощью KDT. KDT автоматически разворачивает кластер Kubernetes, в котором установлены компоненты Open Single Management Platform и другие компоненты инфраструктуры. Шаги установки Open Single Management Platform не зависят от выбранного варианта развертывания.

Если вам нужно установить несколько кластеров Kubernetes с экземплярами Open Single Management Platform, вы можете использовать необходимое количество контекстов.

Чтобы установить Open Single Management Platform:

1. Распакуйте загруженный дистрибутив с KDT на устройство администратора.

2. Ознакомьтесь с Лицензионным соглашением KDT, находящимся в дистрибутиве с компонентами Open Single Management Platform.

   Когда вы начинаете использовать KDT, вы принимаете условия Лицензионного соглашения KDT.

   Вы можете ознакомиться с Лицензионным соглашением KDT после установки Open Single Management Platform. Файл находятся в директории `/home/kdt/` пользователя, который запускает установку Open Single Management Platform.

3. Во время установки KDT загружает недостающие пакеты из хранилищ операционной системы. Перед установкой Open Single Management Platform, выполните следующую команду на целевых устройствах, чтобы убедиться, что кеш apt/yum актуален.

```
apt update
```

4. На устройстве администратора выполните следующие команды, чтобы начать развертывание Open Single Management Platform с помощью KDT. Укажите путь к транспортному архиву с компонентами Open Single Management Platform и путь к конфигурационному файлу, который вы заполнили ранее (наборы параметров установки для развертывания на нескольких узлах и развертывания на одном узле различаются).

   ```
   chmod +x kdt
   ./kdt apply -k <путь_к_транспортному_архиву> -i <путь_к_конфигурационному_файлу>
   ```

   Вы можете установить OSMP без запроса на ознакомление с условиями Лицензионного соглашения и Политикой конфиденциальности OSMP, если вы используете флаг `--accept-eula`. В этом случае вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности OSMP перед установкой приложения. Файлы находятся в дистрибутиве с компонентами Open Single Management Platform.

   Если вы хотите прочитать и принять условия Лицензионного соглашения и Политики конфиденциальности во время развертывания, не используйте флаг `--accept-eula`.

5. Если вы не использовали флаг `--accept-eula` на предыдущем шаге, прочтите Лицензионное соглашение и Политику конфиденциальности OSMP. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

      Введите `n`, если вы не принимаете условия Лицензионного соглашения.

   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

      Введите `n`, если вы не принимаете условия Политики конфиденциальности.

      > Чтобы использовать Open Single Management Platform, вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности.

   После того как вы примете Лицензионное соглашение и Политику конфиденциальности, KDT развернет компоненты Open Single Management Platform в кластере Kubernetes на целевых устройствах.

   > При развертывании Open Single Management Platform на главном Сервере администрирования создается пользователь. Чтобы начать настройку Консоли OSMP, этому пользователю назначаются следующие роли: XDR-роль Главного администратора в корневом тенанте и роль Главного администратора в Kaspersky Security Center.

6. Просмотрите журналы событий установки компонента Bootstrap в директории с утилитой KDT и при необходимости получите диагностическую информацию о компонентах Open Single Management Platform.

7. Войдите в Консоль OSMP и в Консоль KUMA.

   Адрес Консоли OSMP по умолчанию – `https://<console_host>.<smp_domain>:443`.

   Адрес Консоли KUMA по умолчанию – `https://<kuma_host>.<smp_domain>:443`.

   Адреса состоят из значений параметров `console_host`, `kuma_host` и `smp_domain`, указанных в конфигурационном файле.

Open Single Management Platform развернут на целевых устройствах. Установите сервисы KUMA, чтобы начать работу с решением.

Настройка доступа в интернет целевых устройств

Если инфраструктура вашей организации использует прокси-сервер для доступа в интернет, а также вам необходимо подключить целевые устройства к интернету, вам нужно добавить IP-адрес каждого целевого устройства в переменную `no_proxy` в файле /etc/environment перед развертыванием Open Single Management Platform. Это позволяет установить прямое подключение целевых устройств к интернету и правильно развернуть Open Single Management Platform.

Чтобы настроить доступ в интернет целевых устройств:

1. На целевом устройстве откройте файл /etc/environment с помощью текстового редактора. Например, следующая команда открывает файл с помощью текстового редактора GNU nano:

   ```
   sudo nano /etc/environment
   ```

2. В файл /etc/environment добавьте IP-адрес целевого устройства в переменную `no_proxy` через запятую без пробела.

   Например, переменную `no_proxy` можно изначально указать следующим образом:

   ```
   no_proxy=localhost,127.0.0.1
   ```

   Вы можете добавить IP-адрес целевого устройства (192.168.0.1) в переменную `no_proxy`:

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.1
   ```

   Также вы можете указать подсеть, в которую входят целевые устройства (в нотации CIDR):

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.0/24
   ```

3. Сохраните файл /etc/environment.

После добавления IP-адресов в файл /etc/environment к каждому целевому устройстве вы можете продолжить подготовку целевых устройств и дальнейшее развертывание Open Single Management Platform.

Синхронизация времени на машинах

Чтобы настроить синхронизацию времени на машинах:

1. Выполните следующую команду, чтобы установить chrony:

   ```
   sudo apt install chrony
   ```

2. Настройте системное время для синхронизации с NTP-сервером:

   a. Убедитесь, что у виртуальной машины есть доступ в интернет.

   Если доступ есть, переходите к шагу b.

   Если доступа в интернет нет, измените файл `/etc/chrony.conf`. Замените `2.pool.ntp.org` именем или IP-адресом внутреннего NTP-сервера вашей организации.

   b. Запустите службу синхронизации системного времени, выполнив следующую команду:

   ```
   sudo systemctl enable --now chronyd
   ```

c. Подождите несколько секунд и выполните следующую команду:

```
sudo timedatectl | grep 'System clock synchronized'
```

Если системное время синхронизировано правильно, в выводе будет строка `System clock synchronized: yes`.

Синхронизация настроена.

Установка сервисов KUMA

Сервисы – это основные компоненты KUMA, которые помогают системе управлять событиями. Сервисы позволяют получать события из источников событий и в дальнейшем приводить их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа.

Типы сервисов:

- Хранилища используются для хранения событий.
- Коллекторы используются для получения событий и преобразования их в формат KUMA.
- Корреляторы используются для анализа событий и поиска определенных закономерностей.
- Агенты используются для получения событий на удаленных устройствах и пересылки их коллекторам KUMA.

Устанавливать сервисы KUMA можно только после развертывания Open Single Management Platform. При развертывании Open Single Management Platform подготавливается необходимая инфраструктура: на подготовленных устройствах создаются служебные каталоги, в которые добавляются файлы, необходимые для установки службы. Рекомендуется устанавливать сервисы в следующем порядке: хранилище, коллекторы, корреляторы и агенты.

Чтобы установить и настроить сервисы KUMA:

1. Войдите в консоль KUMA.

   Вы можете использовать один из следующих способов:

   - В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.
   - В браузере перейдите по адресу `https://<kuma_host>.<smp_domain>:443`.

     Адреса Консоли KUMA состоят из значений параметров `kuma_host` и `smp_domain`, указанных в конфигурационном файле.

2. В консоли KUMA создайте набор ресурсов для каждого сервиса KUMA (хранилищ, коллекторов и корреляторов), который вы хотите установить на подготовленных устройствах в сетевой инфраструктуре.
3. Создайте сервисы для хранилищ, коллекторов и корреляторов в Консоли KUMA.
4. Получите идентификаторы сервисов для привязки созданных наборов ресурсов и сервисов KUMA:

   a. В главном меню Консоли KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Выберите требуемый сервис KUMA и нажмите на кнопку **Копировать идентификатор**.

5. На подготовленных устройствах в сетевой инфраструктуре выполните соответствующие команды для установки сервисов KUMA. Используйте идентификаторы сервисов, которые были получены ранее:

- Команда установки хранилища:

  ```
  sudo /opt/kaspersky/kuma/kuma storage --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --install
  ```

- Команда установки для коллектора:

  ```
  sudo /opt/kaspersky/kuma/kuma collector --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --api.port <port used for communication with the collector>
  ```

- Команда установки коррелятора:

  ```
  sudo /opt/kaspersky/kuma/kuma correlator --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --api.port <port used for communication with the correlator> --install
  ```

По умолчанию полное доменное имя Ядра KUMA – `<kuma_console>.<smp_domain>`.

Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию номер порта – 7210.

Откройте порты, соответствующие установленному коллектору и коррелятору на сервере (TCP 7221 и другие порты, используемые для установки сервисов в качестве значения параметра `--api.port <порт>`).

6. Во время установки сервисов KUMA прочтите Лицензионное соглашение KUMA. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   - Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.
   - Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать сервисы KUMA, вам нужно принять условия Лицензионного соглашения.

   Вы можете прочитать Лицензионное соглашение KUMA после установки сервисов KUMA одним из следующих способов:

   - На устройствах, входящих в группу `kuma_utils` в файле инвентаря KUMA, откройте файл LICENSE, расположенный в папке `/opt/kaspersky/kuma/utils`.
   - На устройствах, входящих в другие группы (`kuma_storage`, `kuma_collector` или `kuma_correlator`) в файле инвентаря KUMA, откройте файл LICENSE, расположенный в папке `/opt/kaspersky/kuma`.
   - Выполните следующую команду:

     ```
     /opt/kaspersky/kuma/kuma license --show
     ```

   После того как вы примете Лицензионное соглашение, сервисы KUMA будут установлены на подготовленных машинах в сетевой инфраструктуре.

7. При необходимости убедитесь, что коллектор и коррелятор готовы к получению событий.

8. При необходимости установите агенты в сетевую инфраструктуру KUMA.

   Файлы, необходимые для установки агента, находятся в папке `/opt/kaspersky/kuma/utils`.

Необходимые для работы Open Single Management Platform сервисы KUMA установлены.

Развертывание нескольких кластеров Kubernetes и экземпляров Open Single Management Platform

KDT позволяет развернуть несколько кластеров Kubernetes с экземплярами Open Single Management Platform и переключаться между ними с помощью контекстов. *Контекст* – это набор параметров доступа, которые определяют кластер Kubernetes, с которым пользователь может выбрать взаимодействие. Контекст также включает данные для подключения к кластеру с помощью KDT.

Предварительные требования

Перед созданием контекстов и установкой кластеров Kubernetes с экземплярами Open Single Management Platform необходимо выполнить следующие действия:

1. Подготовить устройство администратора и целевые устройства.

   Для установки нескольких кластеров и экземпляров Open Single Management Platform вам нужно подготовить одно устройство администрирования для всех кластеров и отдельные наборы целевых устройств для каждого кластера. Компоненты Kubernetes не следует устанавливать на целевые устройства.

2. Подготовить устройства к установке сервисов KUMA.

   Для установки сервисов KUMA вам нужно подготовить отдельные наборы устройств для каждого экземпляра Open Single Management Platform.

3. Подготовить файл инвентаря KUMA.

   Для установки сервисов KUMA вам нужно подготовить отдельные файлы инвентаря для каждого экземпляра Open Single Management Platform.

4. Подготовить конфигурационный файл.

   Для установки нескольких кластеров и экземпляров Open Single Management Platform вам нужно подготовить конфигурационные файлы для каждого экземпляра Open Single Management Platform. В этих конфигурационных файлах укажите соответствующие устройства администратора и целевые устройства, а также другие параметры, специфичные для конкретного кластера и экземпляра Open Single Management Platform.

Процесс

Чтобы создать контекст с кластером Kubernetes и экземпляром Open Single Management Platform:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя контекста:

   ```
   ./kdt ctx <имя_контекста> --create
   ```

   Контекст с указанным именем создан.

2. Установка кластера Kubernetes и Open Single Management Platform.

Кластер с экземпляром Open Single Management Platform развернут в контексте. Создание контекста завершено.

Вы можете повторить эту процедуру, чтобы создать необходимое количество контекстов с установленными кластерами и экземплярами Open Single Management Platform.

Вам нужно развернуть кластер Kubernetes и экземпляр Open Single Management Platform после создания контекста, чтобы завершить создание контекста. Если вы не выполните развертывание в контексте, а затем создадите другой контекст, первый контекст будет удален.

Вы можете просмотреть список созданных контекстов с помощью следующей команды:

```
./kdt ctx
```

Если вы хотите переключиться на требуемый контекст, выполните следующую команду и укажите имя контекста:

```
./kdt ctx <имя_контекста>
```

После выбора контекста KDT подключается к соответствующему кластеру Kubernetes. Теперь вы можете работать с этим кластером и экземпляром Open Single Management Platform. К выбранному кластеру применяются команды KDT.

При удалении компонентов Open Single Management Platform, установленных в кластере Kubernetes, и самого кластера с помощью KDT, соответствующие контексты также удаляются. Другие контексты и их кластеры с экземплярами Open Single Management Platform не удаляются.

Вход в Open Single Management Platform

Чтобы войти в Open Single Management Platform, вам нужно знать веб-адрес Консоли Open Single Management Platform. В вашем браузере JavaScript должен быть включен.

Чтобы войти в Консоль Open Single Management Platform:

1. В браузере перейдите по адресу `https://<console_host>.<smp_domain>:443`.

   Адрес Консоли Open Single Management Platform состоит из значений параметров `console_host` и `smp_domain`, указанных в конфигурационном файле.

   Отобразится страница входа в приложение.

2. Выполните одно из следующих действий:

   - Чтобы войти в Консоль Open Single Management Platform Console с использованием доменной учетной записи пользователя, введите имя пользователя и пароль доменного пользователя.

     Вы можете ввести имя доменного пользователя в одном из следующих форматов:

     - `Username@dns.domain`
     - NTDOMAIN\`Username`

Прежде чем войти в систему с доменной учетной записью пользователя, опросите контроллеры домена, чтобы получить список пользователей домена.

- Введите имя пользователя и пароль внутреннего пользователя.
- Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер:

  a. Нажмите на кнопку **Показать параметры виртуального Сервера**.

  b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера.

  c. Введите имя пользователя и пароль внутреннего или доменного пользователя, имеющего права на виртуальном Сервере администрирования.

3. Нажмите на кнопку **Войти**.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз.

Open Single Management Platform позволяет работать с интерфейсами Консоли Open Single Management Platform и Консоли KUMA.

Если вы войдете в одну из консолей, а затем откроете другую консоль на другой вкладке того же окна браузера, вы войдете в другую консоль без повторного ввода учетных данных. В этом случае, когда вы выходите из одной консоли, сеанс также заканчивается для другой консоли.

Если вы используете разные окна браузера или разные устройства для входа в Консоль Open Single Management Platform Console и Консоль KUMA, вам необходимо повторно ввести учетные данные. В этом случае, когда вы выходите из одной консоли в окне браузера или устройства, на котором она открыта, сеанс продолжается в окне или устройстве, на котором открыта другая консоль.

Чтобы выйти из Open Single Management Platform Console:

в главном меню перейдите в параметры своей учетной записи и выберите **Выход**.

Приложение Open Single Management Platform Console закрыто и отображается страница входа в приложение.

Обслуживание Open Single Management Platform

В этом разделе описано обновление, удаление и переустановка компонентов Open Single Management Platform с помощью KDT. Также в разделе приведены инструкции по остановке узлов кластера Kubernetes, обновлению пользовательских сертификатов для публичных сервисов Open Single Management Platform, получению текущей версии конфигурационного файла и выполнению других действий с компонентами Open Single Management Platform с помощью KDT.

Обновление компонентов Open Single Management Platform

KDT позволяет обновлять компоненты Open Single Management Platform (включая веб-плагины управления). В дистрибутив включены новые версии компонентов Open Single Management Platform.

Установка компонентов более ранней версии не поддерживается.

Чтобы обновить компоненты Open Single Management Platform:

1. Загрузите дистрибутив с новыми версиями компонентов Open Single Management Platform.
2. При необходимости экспортируйте текущую версию конфигурационного файла на устройство администратора.

   Вам не нужно экспортировать конфигурационный файл, если параметры установки не добавлены или не изменены.
3. Обновите компоненты Open Single Management Platform:

   - Выполните следующую команду для стандартного обновления компонентов Open Single Management Platform:

     `./kdt apply -k <путь_к_обновлениям_XDR-архива> -i <путь_к_конфигурационному_файлу>`

   - Если версия установленного компонента Open Single Management Platform совпадает с версией компонента в дистрибутиве, обновление этого компонента пропускается. Выполните следующую команду, чтобы принудительно обновить этот компонент с помощью флага `force`:

     ```
     ./kdt apply --force -k <путь_к_обновлениям_XDR-архива> -i
     <путь_к_конфигурационному_файлу>
     ```
4. Если дистрибутив содержит новую версию компонента Bootstrap, выполните следующую команду, чтобы обновить кластер Kubernetes:

   ```
   ./kdt apply -k <путь_к_обновлениям_XDR-архива> -i <путь_к_конфигурационному_файлу> --
   force-bootstrap
   ```

   В описанных выше командах необходимо указать путь к архиву с обновлениями компонентов и путь к текущему конфигурационному файлу. Вы не можете указывать путь к конфигурационному файлу в команде, если параметры установки не добавлены или не изменены.
5. Прочтите Лицензионное соглашение и Политику конфиденциальности компонента Open Single Management Platform, если появится новая версия Лицензионного соглашения и Политики конфиденциальности. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

      Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать компонент Open Single Management Platform, вам нужно принять условия Лицензионного соглашения.

   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

      Введите `n`, если вы не принимаете условия Политики конфиденциальности.

Чтобы обновить компонент Open Single Management Platform, вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности.

После того как вы примете Лицензионное соглашение и Политику конфиденциальности, KDT обновит компоненты Open Single Management Platform.

Вы можете ознакомиться с Лицензионным соглашением и Политикой конфиденциальности компонента Open Single Management Platform после обновления. Файлы находятся в директории `/home/kdt/` пользователя, который запускает установку Open Single Management Platform.

Контроль версий конфигурационного файла

При работе с Open Single Management Platform вам может потребоваться изменить параметры, которые были указаны в конфигурационном файле перед развертыванием Open Single Management Platform. Например, чтобы изменить объем дискового пространства, используемого для хранения данных Сервера администрирования, нужно изменить параметр `ksc_state_size`. Текущая версия конфигурационного файла с измененным параметром `ksc_state_size` обновляется в кластере Kubernetes.

Если вы попытаетесь использовать предыдущую версию конфигурационного файла в пользовательском действии KDT, для которого требуется конфигурационный файл, возникнет конфликт. Чтобы избежать конфликтов, вам нужно использовать только текущую версию конфигурационного файла, экспортированного из кластера Kubernetes.

Чтобы экспортировать текущую версию конфигурационного файла,

На устройстве администратора, на котором расположена утилита KDT, запустите следующее пользовательское действие и укажите путь к конфигурационному файлу и его имя:

```
./kdt export-config --filename <path_to_configuration_file.yaml>
```

Текущая версия конфигурационного файла сохраняется в указанной папке с указанным именем.

Вы можете использовать экспортированный конфигурационный файл, например, при обновлении компонентов Open Single Management Platform или добавлении плагинов управления для приложениями "Лаборатории Касперского".

Вам не нужно экспортировать конфигурационный файл, если параметры установки не добавлены или не изменены.

Удаление Open Single Management Platform

KDT позволяет вам удалить все компоненты Open Single Management Platform установленные в кластере Kubernetes, сам кластер, сервисы KUMA, установленные вне кластера, и другие артефакты, созданные во время развертывания или работы решения.

Чтобы удалить компоненты Open Single Management Platform и связанные с ними данные:

1. На устройстве администратора выполните следующую команду:

```
./kdt remove --all
```

Эта команда удаляет следующие объекты и артефакты:

- Все компоненты Open Single Management Platform, установленные в кластере Kubernetes, и сам кластер.
- Учетную запись пользователя Open Single Management Platform, которая была создана с помощью KDT во время развертывания.
- Базу данных, расположенную на отдельном сервере или внутри кластера, схемы СУБД и учетные записи СУБД, созданные с помощью KDT во время развертывания.
- Сервисы KUMA, установленные вне кластера на устройствах, которые указаны в файле инвентаря.
- Содержимое следующих директорий на целевых устройствах:
  - `/var/spool/ksc/logs`
  - `/var/spool/ksc/backup`
  - `/var/spool/ksc/`
  - `/var/lib/k0s`
  - `/run/k0s`
  - `/etc/k0s/`
  - `/etc/containerd/`
  - `/var/lib/containerd/`
  - `/run/containerd/`
- Журналы событий, полученные во время установки и работы компонентов Open Single Management Platform.
- Данные, относящиеся к компонентам Open Single Management Platform на устройстве администратора.

Если устройство администратора не имеет сетевого доступа к целевому устройству, удаление компонентов прерывается. Вы можете восстановить доступ к сети и перезапустить удаление Open Single Management Platform. Также вы можете удалить компоненты Open Single Management Platform с целевых устройств вручную.

> Если вы используете несколько кластеров Kubernetes, управляемых контекстами, эта команда удаляет только текущий контекст Kubernetes, соответствующий кластер и компоненты Open Single Management Platform, установленные в кластере. Другие контексты и их кластеры с экземплярами Open Single Management Platform не удаляются.

2. Закройте порты, используемые Open Single Management Platform, которые были открыты при развертывании, если это необходимо. Эти порты не закрываются автоматически.
3. При необходимости удалите пакеты операционной системы, которые были автоматически установлены во время развертывания. Эти пакеты не удаляются автоматически.

4. Удалите KDT и содержимое директорий `/home/<user>/kdt` и `/home/<user>/.kdt`.

Компоненты Open Single Management Platform, база данных и связанные с ними данные будут удалены, а порты, используемые Open Single Management Platform, закрыты.

Установленные на управляемых устройствах приложения "Лаборатории Касперского" невозможно удалить с помощью команды `./kdt remove`. Подробнее об удалении приложений "Лаборатории Касперского" см. в документации к ним.

После удаления Open Single Management Platform, целевые устройства не перезагружаются автоматически. При необходимости вы можете перезагрузить эти устройства вручную.

Удаление компонентов Open Single Management Platform вручную

Если устройство администратора не имеет сетевого доступа к целевому устройству, удаление компонентов Open Single Management Platform с помощью KDT прерывается. Вы можете восстановить доступ к сети и перезапустить удаление решения. Также вы можете удалить компоненты Open Single Management Platform с целевых устройств вручную.

Чтобы удалить компоненты Open Single Management Platform с целевых устройств вручную:

1. На целевом устройстве выполните следующую команду, чтобы остановить службу k0s:

   ```
   /usr/local/bin/k0s stop
   ```

2. Выполните следующую команду, чтобы сбросить узлы кластера в исходное состояние:

   ```
   /usr/local/bin/k0s reset
   ```

3. Удалите содержимое следующих папок:

   - Обязательные папки:
     - `/etc/k0s/`
     - `/var/lib/k0s/`
     - `/usr/libexec/k0s/`
     - `/usr/local/bin/` (удалите только файл `k0s`)
   - Необязательные папки:
     - `/var/lib/containerd/`
     - `/var/cache/k0s/`
     - `/var/cache/kubelet/`
     - `/var/cache/containerd/`

Вы можете удалить папки `/var/lib/containerd/` и `/var/cache/containerd/`, если служба containerd используется только для работы Open Single Management Platform. Иначе ваши данные, содержащиеся в папках `/var/lib/containerd/` и `/var/cache/containerd/`, могут быть потеряны.

Содержимое папок `/var/cache/k0s/`, `/var/cache/kubelet/` и `/var/cache/containerd/` автоматически удаляется после перезапуска целевого устройства. Вам не нужно удалять содержимое этих папок вручную.

4. Перезагрузите все целевые устройства.

Компоненты Open Single Management Platform удалены с целевых устройств.

Переустановка Open Single Management Platform после неудачной установки

Во время установки Open Single Management Platform на устройстве администратора KDT отображает журнал событий установки, в котором видно, правильно ли установлены компоненты Open Single Management Platform.

После установки Open Single Management Platform вы можете запустить следующую команду, чтобы просмотреть список всех установленных компонентов:

```
./kdt status
```

Отображается список установленных компонентов. Правильно установленные компоненты имеют статус `Успешно`. Если не удалось установить компонент, этот компонент будет иметь статус `Сбой`.

Чтобы просмотреть полный журнал событий установки некорректно установленного компонента Open Single Management Platform, выполните следующую команду:

```
./kdt status -l <название_компонента>
```

Также можно вывести всю диагностическую информацию о компонентах Open Single Management Platform с помощью следующей команды:

```
./kdt logs get --to-archive
```

Вы можете использовать полученные журналы событий для устранения неполадок самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Чтобы переустановить неправильно установленные компоненты Open Single Management Platform,

- Если вы не изменяли конфигурационный файл, выполните следующую команду и укажите тот же транспортный архив, который использовался при установке Open Single Management Platform:

  ```
  ./kdt apply -k <путь_к_транспортному_архиву>
  ```

- Если вам нужно изменить параметры установки, экспортируйте конфигурационный файл, измените его, а затем выполните следующую команду с транспортным архивом и обновленным конфигурационным файлом:

  ```
  ./kdt apply -k <путь_к_транспортному_архиву> -i <путь_к_конфигурационному_файлу>
  ```

KDT переустанавливает только неправильно установленные компоненты Open Single Management Platform.

Остановка узлов кластера Kubernetes

Вам может потребоваться остановить весь кластер Kubernetes или временно отключить один из узлов кластера для обслуживания.

В виртуальной среде не выключайте виртуальные машины, на которых размещены активные узлы кластера Kubernetes.

Чтобы остановить многоузловой кластер Kubernetes (схема развертывания на нескольких узлах):

1. Войдите на рабочий узел и инициируйте плавное завершение работы. Повторите этот процесс для всех рабочих узлов.
2. Войдите на первичный узел и инициируйте плавное завершение работы.

Чтобы остановить кластер Kubernetes с одним узлом (схема развертывания на одном узле):

Войдите на первичный узел и инициируйте плавное завершение работы.

Использование сертификатов для публичных служб Open Single Management Platform

Для работы с публичными службами Open Single Management Platform вы можете использовать самоподписанные или пользовательские сертификаты. По умолчанию Open Single Management Platform использует самоподписанные сертификаты.

Сертификаты необходимы для следующих публичных служб Open Single Management Platform:

- <console_host>.<smp_domain> – доступ к интерфейсу Консоли OSMP.
- <admsrv_host>.<smp_domain> – взаимодействие с Сервером администрирования.
- <api_host>.<smp_domain> – доступ к API Open Single Management Platform.

FQDN публичных служб Open Single Management Platform состоят из имен устройств и доменного имени, указанных в конфигурационном файле. Список адресов публичных служб Open Single Management Platform, для которых при развертывании определяются самоподписанные или пользовательские сертификаты, указывается в параметре установки pki_fqdn_list.

Пользовательский сертификат должен быть указан как файл в формате PEM, содержащий полную цепочку сертификатов (или только один сертификат) и незашифрованный закрытый ключ.

Вы можете указать промежуточный сертификат из инфраструктуры закрытых ключей (PKI) вашей организации. Пользовательские сертификаты для публичных служб Open Single Management Platform выдаются из этого пользовательского промежуточного сертификата. Также вы можете указать конечные сертификаты для каждой публичной службы. Если конечные сертификаты указаны только для части публичных служб, то для остальных публичных служб выдаются самоподписанные сертификаты.

Для публичных служб <console_host>.<smp_domain> и api.<smp_domain> пользовательские сертификаты можно указать только перед развертыванием в конфигурационном файле. Чтобы использовать пользовательский промежуточный сертификат, укажите параметры установки `intermediate_bundle` и `intermediate_enabled`.

Если вы хотите использовать конечные пользовательские сертификаты для работы с публичными службами Open Single Management Platform, укажите соответствующие параметры установки `console_bundle`, `admsrv_bundle` и `api_bundle`. Установите для параметра `intermediate_enabled` значение `false` и не указывайте параметр `intermediate_bundle`.

Для службы <admsrv_host>.<smp_domain> вы можете заменить выданный самоподписанный сертификат Сервера администрирования пользовательским сертификатом с помощью утилиты klsetsrvcert.

Автоматический перевыпуск сертификатов не поддерживается. Примите во внимание срок действия сертификата и обновите сертификат, когда срок его действия истечет.

Чтобы обновить пользовательские сертификаты:

1. На устройство администратора экспортируйте текущую версию конфигурационного файла.
2. В экспортированном конфигурационном файле укажите путь к новому пользовательскому промежуточному сертификату в параметре установки `intermediate_bundle`. Если вы используете конечные пользовательские сертификаты для каждой публичной службы, укажите параметры установки `console_bundle`, `admsrv_bundle` и `api_bundle`.
3. Выполните следующую команду и укажите путь к измененному конфигурационному файлу:

   ```
   ./kdt apply -i <path_to_configuration_file>
   ```

   Пользовательские сертификаты обновлены.

Расчет и изменение дискового пространства для хранения данных Сервера администрирования

Данные Сервера администрирования включают в себя следующие объекты:

- Информация об активах (устройствах).
- Информация о событиях, зарегистрированных на Сервере администрирования для выбранного клиентского устройства.
- Информация о домене, в котором находятся активы.
- Данные компонента Контроль приложений.
- Обновления. В папке общего доступа требуется дополнительно не менее 4 ГБ для хранения обновлений.
- Инсталляционные пакеты. При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется количество места, равное суммарному размеру устанавливаемых имеющихся инсталляционных пакетов.
- Задачи удаленной установки. При наличии на Сервере администрирования задач удаленной установки на диске дополнительно потребуется количество места на диске, равное суммарному размеру устанавливаемых инсталляционных пакетов.

Расчет минимального дискового пространства для хранения данных Сервера администрирования

Минимальный объем дискового пространства, необходимый для хранения данных Сервера администрирования, можно приблизительно оценить по формуле:

```
(724 * C + 0.15 * E + 0.17 * A + U), КБ
```

где

- "C" – количество активов (устройств).
- "E" – количество сохраняемых событий.
- "A" – суммарное количество объектов домена:
  - учетных записей устройств;
  - учетные записи пользователей;
  - учетных записей групп безопасности;
  - организационных подразделений.
- U – размер обновлений (не менее 4 ГБ).

Если опрос домена выключен, то "A" следует считать равным нулю.

Формула рассчитывает объем дискового пространства, необходимый для хранения типичных данных с управляемых устройств, и типичный размер обновлений. В формулу не входит объем дискового пространства, занятого данными, которые не зависят от количества управляемых устройств для компонента Контроль приложений, инсталляционных пакетов и задач удаленной установки.

Изменение дискового пространства для хранения данных Сервера администрирования

Объем свободного дискового пространства, выделяемого для хранения данных Сервера администрирования, указывается в конфигурационном файле перед развертыванием Open Single Management Platform (параметр `ksc_state_size`). Примите во внимание минимальное дисковое пространство, рассчитанное по формуле.

Чтобы проверить объем дискового пространства, используемого для хранения данных Сервера администрирования после установки Open Single Management Platform, выполните следующие действия:

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke ksc --action getPvSize
```

Отображается объем необходимого свободного места на диске в гигабайтах.

Чтобы изменить объем дискового пространства для хранения данных Сервера администрирования после установки Open Single Management Platform:

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите необходимое свободное место на диске в гигабайтах (например, "50Gi"):

```
./kdt invoke ksc --action setPvSize --param ksc_state_size="<new_disk_space_amount>Gi"
```

Объем свободного дискового пространства, выделяемого для хранения данных Сервера администрирования, изменен.

Ротация секретов

KDT позволяет выполнять ротацию секретов, которые используются для подключения к кластеру Kubernetes, компонентам инфраструктуры Open Single Management Platform и СУБД. Период ротации этих секретов можно указать в соответствии с требованиями информационной безопасности вашей организации. Секреты находятся на устройстве администратора.

Секреты, которые используются для подключения к кластеру Kubernetes, включают клиентский сертификат и закрытый ключ. Секреты доступа к Реестру и СУБД включают соответствующие DSN.

Чтобы выполнить ротацию секретов для подключения к кластеру Kubernetes вручную,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke bootstrap --action RotateK0sConfig
```

Новые секреты подключения к кластеру Kubernetes сгенерированы.

При обновлении Bootstrap секреты подключения к кластеру Kubernetes обновляются автоматически.

Чтобы выполнить ротацию секретов для подключения к Реестру вручную,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke bootstrap --action RotateRegistryCreds
```

Новые секреты для подключения к Реестру сгенерированы.

Добавление устройств для установки дополнительных сервисов KUMA

Если вам нужно расширить хранилище или добавить коллекторы и корреляторы для увеличения потока событий, вы можете добавить дополнительные устройства для установки сервисов KUMA.

Вам нужно указать параметры дополнительных устройств в файле expand.inventory.yml. Этот файл находится в дистрибутиве с транспортным архивом, KDT, конфигурационным файлом и другими файлами. В файле expand.inventory.yml можно указать сразу несколько дополнительных устройств для коллекторов, корреляторов и хранилищ. Убедитесь, что соблюдены аппаратные и программные требования, а также требования к установке на выбранных устройствах.

Чтобы подготовить необходимую инфраструктуру на устройствах, указанных в файле expand.inventory.yml, необходимо создать служебные каталоги, в которые будут добавлены файлы, необходимые для установки службы. Чтобы подготовить инфраструктуру, выполните следующую команду и укажите файл expand.inventory.yml:

```
./kdt invoke kuma --action addHosts --param hostInventory=<путь_к_файлу_инвентаря>
```

На устройствах, указанных в файле expand.inventory.yml, служебные каталоги, в которые добавляются файлы, необходимые для установки службы.

Пример дополнительного файла инвентаря KUMA для установки сервисов KUMA (файл expand.inventory.yml)

```
all:
  vars:
    deploy_example_services: false
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
    kuma_collector:
      hosts:
        kuma1.example.com:
         ansible_host: 0.0.0.0
        kuma2.example.com:
         ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma3.example.com:
         ansible_host: 0.0.0.0
        kuma4.example.com:
         ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma5.example.com:
         ansible_host: 0.0.0.0
        kuma6.example.com:
         ansible_host: 0.0.0.0
```

Добавление дополнительного хранилища, коллектора или коррелятора

Вы можете добавить к существующей инфраструктуре дополнительное хранилище кластера, коллектор или коррелятор. Если вы хотите добавить несколько сервисов, рекомендуется устанавливать их в следующем порядке: хранилища, коллекторы и корреляторы.

Чтобы добавить дополнительное хранилище кластера, коллектор или коррелятор:

1. Войдите в Консоль KUMA.

   Вы можете использовать один из следующих способов:

   - В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.

- В браузере перейдите по адресу `https://<kuma_host>.<smp_domain>:443`.

  Адрес Консоли KUMA состоит из значений параметров `kuma_host` и `smp_domain`, указанных в конфигурационном файле.

2. В Консоли KUMA создайте набор ресурсов для каждого сервиса KUMA (хранилищ, коллекторов и коррелляторов), который вы хотите установить на подготовленных устройствах.

3. Создайте сервисы для хранилищ, коллекторов и коррелляторов в Консоли KUMA.

4. Получите идентификаторы сервисов для привязки созданных наборов ресурсов и сервисов KUMA:

   a. В главном меню Консоли KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Выберите требуемый сервис KUMA и нажмите на кнопку **Копировать идентификатор**.

5. Установите сервисы KUMA на каждое подготовленное устройство, указанное в разделах kuma_storage, kuma_collector и kuma_correlator файла инвентаря expand.inventory.yml. На каждом устройстве в команде установки укажите идентификатор сервиса, соответствующий устройству. Выполните соответствующие команды, чтобы установить сервисы KUMA:

   - Команда установки хранилища:

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --install
     ```

   - Команда установки для коллектора:

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --api.port <port used for communication with the installed component>
     ```

   - Команда установки коррелятора:

     ```
     sudo /opt/kaspersky/kuma/kuma correlator --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --api.port <port used for communication with the installed component> --install
     ```

     Команды установки коллектора и коррелятора автоматически создаются на вкладке **Проверка** в мастере установки. Порт, используемый для связи, автоматически добавляется в команду. Используйте сгенерированные команды для установки коллектора и коррелятора на устройства. Это позволит убедиться, что порты для связи с сервисами, которые указаны в команде, доступны.

   FQDN Ядра KUMA – это <kuma_host>.<smp_domain>.

   Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию номер порта – 7210.

Дополнительные сервисы KUMA установлены.

Добавление устройств в существующее хранилище

Вы можете расширить существующее хранилище (хранилище кластера), добавив устройства в качестве новых узлов хранилища кластера.

Чтобы добавить устройства в существующее хранилище:

1. Войдите в Консоль KUMA.

   Вы можете использовать один из следующих способов:

- В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.
- В браузере перейдите по адресу `https://<kuma_host>.<smp_domain>:443`.

  Адрес Консоли KUMA состоит из значений параметров `kuma_host` и `smp_domain`, указанных в конфигурационном файле.

2. Добавьте узлы в хранилище кластера. Для этого измените параметры существующего хранилища кластера:

   a. В разделе **Ресурсы** → **Хранилища** выберите существующее хранилище и откройте хранилище для изменения.

   b. В разделе **Узлы кластера ClickHouse** нажмите на **Добавить узлы** и в полях для нового узла укажите роли. Укажите соответствующие доменные имена устройств из раздела kuma_storage файла expand.inventory.yml, а затем укажите роли для новых узлов.

   c. Сохраните изменения.

   Поскольку вы добавляете сервера в существующий кластер хранения, создавать отдельное хранилище уже не нужно.

3. Создайте службы хранилища для каждого добавленного узла хранилища кластера в Консоли KUMA и привяжите службы к хранилище кластера.

4. Получите идентификаторы службы хранилища для каждого подготовленного устройства для установки служб KUMA:

   a. В главном меню Консоли KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Выберите требуемый сервис KUMA и нажмите на кнопку **Копировать идентификатор**.

5. Установите сервис хранилища на каждое подготовленное устройство, указанное в разделе kuma_storage файла инвентаря expand.inventory.yml. На каждом устройстве в команде установки укажите идентификатор сервиса, соответствующий устройству. Выполните следующую команду, чтобы установить сервис хранилища:

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --install
   ```

   FQDN Ядра KUMA – это <kuma_host>.<smp_domain>.

   Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию номер порта – 7210.

Дополнительные устройства добавлены в хранилище кластера.

Укажите добавленные устройства в файле инвентаря distributed.inventory.yml, чтобы в нем были актуальные сведения на случай обновления компонентов KUMA.

Замена устройства, использующего хранилище KUMA

Чтобы заменить устройство, использующее хранилище KUMA, на другое:

1. Заполните файл expand.inventory.yml, указав параметры устройства, которое вы хотите заменить.

2. Выполните следующую команду, указав файл expand.inventory.yml для удаления устройства:

   ```
   ./kdt invoke kuma --action removeHosts --param hostInventory=<путь_к_файлу_инвентаря>
   ```

3. Заполните файл expand.inventory.yml, указав параметры нового устройства, которым вы хотите заменить предыдущее, и выполните следующую команду:

   ```
   ./kdt invoke kuma --action addHosts --param hostInventory=<путь_к_файлу_инвентаря>
   ```

4. Выполните шаги 2–6 инструкции по добавлению устройств для сервисов KUMA, чтобы добавить устройство с хранилищем KUMA.

Устройство с хранилищем KUMA заменено на другое.

Если ваша конфигурация хранилища включает в себя шард, содержащий две реплики, и вы заменили второе устройство реплики на новое, выполнив действия, описанные выше, то при установке новой реплики вы можете получить сообщение об ошибке. В этом случае новая реплика работать не будет.

Чтобы исправить ошибку при добавлении реплики шарда:

1. На другом устройстве с репликой того же шарда, которому принадлежит неправильно добавленная реплика, запустите клиент ClickHouse с помощью команды:

   ```
   /opt/kaspersky/kuma/clickhouse/bin/client.sh
   ```

   Если это устройство недоступно, запустите клиент на любом другом устройстве с репликой, включенной в то же хранилище кластера.

2. Запустите команду, чтобы удалить данные об устройстве, которое вы хотите заменить.

   - Если доступно устройство с репликой того же шарда, которому принадлежит неправильно добавленная реплика, выполните следующую команду:

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM TABLE
     kuma.events_local_v2
     ```

   - Если вы используете другой узел хранилища кластера с репликой, выполните следующую команду:

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM ZKPATH
     '/clickhouse/tables/kuma/<shard number of read-only node>/kuma/events_local_v2
     ```

3. Выполните следующую команду, чтобы восстановить работу добавленного устройства с репликой:

   ```
   SYSTEM RESTORE REPLICA kuma.events_local_v2
   ```

Работоспособность добавленного устройства с репликой восстановлена.

Настройка модели статусов инцидентов

Поддерживаются две модели статусов инцидентов:

a. Стандартная:

- **Новый**

Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *В обработке* или *Закрыт*. Когда вы меняете статус *Новый* на *В обработке*, инцидент назначается вам автоматически. Когда вы меняете статус *Новый* на *Закрыт* и у инцидента нет исполнителя, он автоматически назначается вам.

- **В обработке**

  Этот статус означает, что аналитик начал работу над инцидентом или возобновил работу, изменив статус *Отложен*. Когда вы устанавливаете статус *В обработке*, инцидент назначается вам автоматически. Изменить статус *В обработке* можно на любой другой.

- **Отложен**

  Этот статус означает, что аналитик приостановил работу над инцидентом. Обычно вы меняете статус *Отложен* на *В обработке*, когда работа возобновляется, но также можно изменить статус *Отложен* на другие статусы.

- **Закрыт**

  Вы закрываете инциденты, когда не требуется никакой дополнительной работы над инцидентом. Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

  При закрытии инцидента, связанные обнаружения также получают статус *Закрыто* и наследуют решение инцидента. Если у инцидента нет исполнителя, закрытый инцидент автоматически назначается вам. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

  Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый инцидент в работу, измените его статус следующим образом: *Закрыт* → *Новый* → *В обработке*.

b. Совместимая с ГОСТ:

- **Новый**

  Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *Анализ*. Когда вы меняете статус *Новый* на *Анализ*, инцидент назначается вам автоматически.

- **Анализ**

  Этот статус означает, что аналитик начал работу над инцидентом и проводит первичный анализ и определение вовлеченных в инцидент элементов информационной инфраструктуры.

  Вы можете изменить статус инцидента на *Локализация* или *Выполнен*.

- **Локализация**

Этот статус означает, что выполняется меры по предотвращению дальнейшего распространения инцидента.

Вы можете изменить статус инцидента на *Последствия* или *Выполнен*.

- **Последствия**

  Этот статус означает, что выполняется выявление последствий инцидента на вовлеченные в него элементы информационной инфраструктуры.

  Вы можете изменить статус инцидента на *Ликвидация* или *Выполнен*.

- **Ликвидация**

  Этот статус означает, что выполняется устранение последствий инцидента.

  Вы можете изменить статус инцидента на *Выполнен*.

- **Выполнен**

  Этот статус означает, что проводится оценка полноты выполненных действий на этапах *Анализ*, *Локализация*, *Последствия* и *Ликвидация*.

  Вы можете изменить статус инцидента на *Закрыт*, *Анализ*, *Локализация*, *Последствия*, *Ликвидация*.

- **Закрыт**

  Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

  При закрытии инцидента, связанные обнаружения также получают статус *Закрыт* и наследуют решение инцидента. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

Чтобы сменить модель статусов на совместимую с ГОСТ:

1. В файле docker/compose/osmp.yaml укажите значение переменной окружения OSMP_WORKFLOW_ID.

   OSMP_WORKFLOW_ID: "gost"

2. В файле /plugins/irp/.env укажите значение переменной FEATURE_GOST_STATUS.

   FEATURE_GOST_STATUS=true

Статусы инцидентов не конвертируются при смене модели статуса. Не рекомендуется менять модель статусов, если у вас есть активные инциденты.

Перенос данных в Open Single Management Platform

В этом разделе описан перенос данных в Open Single Management Platform из Kaspersky Security Center Windows.

О переносе данных из Kaspersky Security Center Windows

Следуя этому сценарию, вы можете передать структуру группы администрирования, включая управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Open Single Management Platform.

Ограничения:

- Перенос данных возможен только с Kaspersky Security Center 14.2 Windows в Open Single Management Platform, начиная с версии 1.0.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.

Этапы

Сценарий переноса данных состоит из следующих этапов:

1. **Выберите способ переноса данных**

   Вы переносите данные в Open Single Management Platform с помощью мастера переноса данных. Шаги мастера переноса данных зависят от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Open Single Management Platform в иерархию:

   - Перенос данных с использованием иерархии Серверов администрирования

     Выберите этот вариант, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Open Single Management Platform. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Консоли OSMP. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого перед началом переноса данных создайте иерархию.

   - Перенос данных с помощью файла экспорта (ZIP-архив)

     Выберите этот вариант, если Серверы администрирования Kaspersky Security Center Windows и Open Single Management Platform не организованы в иерархию. Вы управляете процессом переноса данных с помощью двух экземпляров консоли, одного экземпляра Kaspersky Security Center Windows и другого Консоли OSMP. В этом случае вы используете файл экспорта, который вы создали и загрузили при экспорте из Kaspersky Security Center Windows, и импортируете этот файл в Open Single Management Platform.

2. **Экспорт данных из Kaspersky Security Center Windows**

   Откройте Kaspersky Security Center Windows и запустите мастер переноса данных.

3. **Импорт данных в Open Single Management Platform**

   Продолжите работу мастера передачи данных, чтобы импортировать экспортированные данные в Open Single Management Platform.

Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не выстроены в иерархию, вы продолжите работу мастера передачи данных после перехода на Open Single Management Platform.

4. **Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Open Single Management Platform вручную (необязательный шаг)**

   Также можно перенести объекты и параметры, которые вы не можете передать с помощью мастера переноса данных. Например, вы можете дополнительно сделать следующее:

   - Настроить глобальные задачи Сервера администрирования.
   - Настроить параметры политики Агента администрирования.
   - Создать инсталляционные пакеты приложений.
   - Создать виртуальные Серверы администрирования.
   - Назначить и настроить точки распространения.
   - Создать правила перемещения устройств.
   - Настроить правила автоматического назначения тегов устройствам.
   - Создать категории приложений.

5. **Переместить импортированные управляемые устройства под управление Open Single Management Platform**

   Для завершения переноса данных переместите импортированные управляемые устройства под управление Open Single Management Platform. Вы можете воспользоваться одним из следующих способов:

   - С помощью групповой задачи Kaspersky Security Center

     Используйте задачу Смена Сервера администрирования, чтобы сменить Сервер администрирования на другой для определенных клиентских устройств.

   - С помощью утилиты klmover.

     Используйте утилиту klmover и укажите параметры подключения для нового Сервера администрирования.

   - С помощью установки или переустановки Агента администрирования на управляемые устройства.

     Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. Используя инсталляционный пакет, установите Агент администрирования на импортированные управляемые устройства с помощью задачи удаленной установки.

     Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.

6. **Обновите Агент администрирования до последней версии.**

   Рекомендуется обновить Агент администрирования до той же версии, что и Консоль OSMP.

7. **Убедитесь, что управляемые устройства отображаются на новом Сервере администрирования.**

   На Сервере администрирования Open Single Management Platform откройте список управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**) и проверьте значения в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**.

Другие способы переноса данных

Помимо мастера переноса данных, вы также можете переносить определенные задачи и политики:

- Экспортируйте задачи из Kaspersky Security Center Windows, а затем импортируйте задачи в Open Single Management Platform.
- Экспортируйте политики из Kaspersky Security Center Windows, а затем импортируйте политики в Open Single Management Platform. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

Экспорт групповых объектов из Kaspersky Security Center Windows

Для переноса структуры группы администрирования, которая включает управляемые устройства и другие объекты группы из Kaspersky Security Center для Windows в Open Single Management Platform, необходимо, чтобы вы сначала выбрали данные для экспорта и создали файл экспорта. Файл экспорта содержит информацию обо всех групповых объектах, которые вы хотите перенести. Файл экспорта будет использован для последующего импорта в Open Single Management Platform.

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых приложений.
- Глобальные задачи.
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

Перед тем, как начать экспорт, ознакомьтесь с общей информацией о переносе данных в Open Single Management Platform. Выберите способ переноса данных: с использованием или без использования иерархии Серверов администрирования Kaspersky Security Center Windows и Open Single Management Platform.

Чтобы экспортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Open Single Management Platform в иерархию, выполните одно из следующих действий:
   - Если Серверы организованы в иерархию, откройте Консоль OSMP и переключитесь на Сервер Kaspersky Security Center Windows.
   - Если Серверы не организованы в иерархию, откройте Консоль OSMP, подключенную к Kaspersky Security Center Windows.
2. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.
3. Выберите **Перенос данных в Kaspersky Security Center Linux или Open Single Management Platform**, чтобы запустить мастер, и следуйте его шагам.

4. Выберите группу или подгруппу администрирования, которую вы хотите экспортировать. Обратите внимание, что в выбранной группе или подгруппе администрирования должно быть не более 10 000 устройств.

5. Выберите управляемые приложения, задачи и политики которых будут экспортированы. Выбирайте только те приложения, которые поддерживаются Open Single Management Platform. Объекты неподдерживаемых приложений все равно будут экспортированы, но не будут работать.

6. Используйте ссылки слева, чтобы выбрать глобальные задачи, выбранные устройства и отчеты для экспорта. Ссылка **Группировать объекты** позволяет исключить из экспорта роли пользователей, внутренних пользователей и группы безопасности, а также пользовательские категории приложений.

Файл экспорта (ZIP-архив) создан. В зависимости от того, выполняете ли вы перенос данных с поддержкой иерархии Сервера администрирования, файл экспорта сохраняется следующим образом:

- Если Серверы организованы в иерархию, файл экспорта сохраняется во временной папке на Сервере OSMP.

- Если Серверы не организованы в иерархию, файл экспорта загружается на ваше устройство.

При переносе данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически после успешного экспорта. При переносе данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Open Single Management Platform.

Импорт файла экспорта в Open Single Management Platform

Чтобы перенести информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Windows, вам необходимо импортировать ее в Open Single Management Platform.

Чтобы импортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Open Single Management Platform в иерархию, выполните одно из следующих действий:

   - Если Серверы организованы в иерархию, переходите к следующему шагу мастера переноса данных после завершения экспорта. Импорт начнется автоматически после успешного экспорта в этом мастере (см. шаг 2 этой инструкции).

   - Если Серверы не организованы в иерархию:

     a. Откройте Консоль OSMP.

     b. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

     c. Выберите файл экспорта (ZIP-архив), который вы создали и загрузили при экспорте из Kaspersky Security Center Windows. Начнется загрузка файла экспорта.

2. После успешной загрузки файла экспорта вы можете продолжить импорт. Если вы хотите указать другой файл для экспорта, перейдите по ссылке **Изменить** и выберите нужный файл.

3. Отображается вся иерархия групп администрирования Open Single Management Platform.

Установите флажок рядом с целевой группой администрирования, в которой необходимо восстановить объекты экспортированной группы администрирования (управляемые устройства, политики, задачи и другие объекты группы).

4. Начнется импорт объектов группы. Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта нельзя. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓) и импорт завершится.

5. Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

> Если в перенесенной задаче указаны данные учетной записи, под которой она запускается, вам нужно открыть задачу и ввести пароль еще раз после завершения импорта.

Если импорт завершился с ошибкой, вы можете выполнить одно из следующих действий:

- Для переноса данных с поддержкой иерархии Сервера администрирования вы можете импортировать файл экспорта еще раз.
- Для переноса данных без поддержки иерархии Сервера администрирования вы можете запустить мастер переноса данных, чтобы выбрать другой файл экспорта, а затем импортировать его снова.

Вы можете проверить, были ли объекты группы, входящие в область экспорта, успешно импортированы в Open Single Management Platform. Для этого перейдите в раздел **Активы (Устройства)** и убедитесь, что импортированные объекты отображаются в соответствующих подразделах.

Обратите внимание, что импортированные управляемые устройства отображаются в подразделе **Управляемые устройства**, но они не видны в сети и на них не установлен и не запущен Агент администрирования (значение *Нет* в столбцах **Видимо в сети**, **Агент администрирования установлен**, **Агент администрирования запущен**).

Для завершения переноса данных вам необходимо переключить управляемые устройства под управление Open Single Management Platform.

Переключение управляемых устройств под управление Open Single Management Platform

После успешного импорта информации об управляемых устройствах, объектах и их параметрах в Open Single Management Platform для завершения переноса данных вам необходимо переключить управляемые устройства под управление Open Single Management Platform.

Вы можете переместить управляемые устройства под управление Open Single Management Platform одним из следующих способов:

- Используя утилиту klmover.
- Используя задачу *Смена Сервера* администрирования.
- Установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки.

Чтобы переключить управляемые устройства под управление Open Single Management Platform, установив Агент администрирования:

1. Удалите Агент администрирования на импортированных управляемых устройствах, которые будут переключены под управление Open Single Management Platform.

2. Переключитесь на Сервер администрирования Kaspersky Security Center Windows.

3. Перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты** и откройте свойства существующего инсталляционного пакета Агента администрирования.

   Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый.

   Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.

4. На вкладке **Параметры** выберите раздел **Подключение**. Укажите параметры подключения Сервера администрирования Open Single Management Platform.

5. Создайте задачу удаленной установки для импортированных управляемых устройств, а затем укажите перенастроенный инсталляционный пакет Агента администрирования.

   Вы можете установить Агент администрирования с помощью Сервера администрирования Kaspersky Security Center Windows или с помощью устройства под управлением Windows, которое выполняет роль точки распространения. Если вы используете Сервер администрирования, включите параметр **Средствами операционной системы с помощью Сервера администрирования**. Если вы используете точку распространения, включите параметр **Средствами операционной системы с помощью точек распространения**.

6. Запустите задачу удаленной установки приложения.

После успешного завершения задачи удаленной установки перейдите на Сервер администрирования Open Single Management Platform и убедитесь, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Агент администрирования запущен**).

О переносе данных из KUMA

Этот раздел содержит информацию о переносе данных с автономной версии KUMA в Open Single Management Platform. Обратите внимание, что представленный сценарий относится к ситуации, когда вы выполняете первоначальную установку Open Single Management Platform вместе с переносом данных существующей автономной версии KUMA. Если у вас уже есть развернутый экземпляр Open Single Management Platform, вы не сможете выполнить перенос данных автономной версии KUMA с соответствующими данными по этому сценарию.

> Вам нужно перенести данные из KUMA 3.0.3. Если вы используете более раннюю версию, вам необходимо обновить ее до версии 3.0.3, а затем выполнить перенос данных в Open Single Management Platform.

Вы можете выполнить перенос данных для следующих типов автономного развертывания KUMA:

- Установка на одном сервере.
- Распределенная установка.

- Распределенная установка в высоко доступной конфигурации.

Перенос данных содержит два этапа:

1. Перенос данных автономной версии KUMA в Open Single Management Platform.
2. Запуск приложения переноса для переноса данных.

После завершения обоих этапов переданные данные и сервисы становятся доступными. Все сервисы автономной версии KUMA настроены для работы в составе Open Single Management Platform. Также перезапускаются перенесенные сервисы.

Что переносится

- Каталог /opt/kaspersky/kuma/core/data.
- Файл ключа шифрования /opt/kaspersky/kuma/core/encryption/key.
- Базовая резервная копия MongoDB.
- Иерархия Серверов администрирования Kaspersky Security Center.

  Серверы администрирования, которые переносятся на Open Single Management Platform, привязываются к его корневым Серверам администрирования.
- Тенанты.

  Перенесенные тенанты зарегистрированы в Open Single Management Platform и становятся дочерними для корневого тенанта. Каждый тенант входит в группу администрирования Open Single Management Platform.

  Чтобы выполнить перенос данных Серверов администрирования Kaspersky Security Center, доменных пользователей и их ролей, создайте конфигурационный файл, а затем задайте в нем необходимые параметры.
- Привязка тенантов к Серверам администрирования Kaspersky Security Center.

  Подчиненный Сервер администрирования Kaspersky Security Center зарегистрирован в соответствующей службе в параметрах тенанта Kaspersky Security Center.

  Связь между тенантом и Сервером администрирования остается такой же, как и в KUMA.

  Вы можете привязывать тенанты только к физическим Серверам администрирования. Привязка тенантов к виртуальным Серверам администрирования недоступна.
- Пользователи домена.

  Для каждого домена, с которым настроена интеграция KUMA, и для пользователей которым назначены роли в тенантах KUMA, необходимо выполнить опрос контроллера домена с помощью Сервера администрирования.
- Роли.

  После завершения опроса контроллера домена и завершения переноса данных пользователей домена, этим пользователям назначаются XDR-роли в Open Single Management Platform и право на подключение к Kaspersky Security Center.

  Если перенесенные пользователи имели назначенные роли на подчиненном Сервере администрирования Kaspersky Security Center, вам нужно назначить пользователям такие же роли в группе администрирования его корневого Сервера администрирования.

Если вы вручную назначили XDR-роли и/или роли Kaspersky Security Center пользователям перед запуском мигратора, по завершении переноса данных пользователям будут назначены новые XDR-роли в тенанте, указанном в конфигурационном файле, а назначенные вручную XDR-роли будут удалены. Роли Kaspersky Security Center не перезаписываются.

- Интеграция с Kaspersky Security Center.
- Интеграция с LDAP и сторонними системами остается доступной.
- События.
- Активы.
- Ресурсы.
- Активные сервисы.

Что не переносится

- Алерты и инциденты недоступны в Open Single Management Platform после переноса данных. Если вы хотите иметь под рукой исходные алерты и инциденты, рекомендуется восстановить резервную копию данных KUMA на отдельном устройстве. Таким образом, вы сможете выполнить ретроспективное сканирование.
- Панели мониторинга не переносятся и остаются доступными в автономной версии KUMA в режиме для чтения, вы не сможете перейти к соответствующим алертам.

  Интеграция с Active Directory (AD) и службами Active Directory Federation Services (ADFS).

Перенос данных автономной версии KUMA в Open Single Management Platform

Чтобы выполнить перенос данных из автономной версии KUMA в Open Single Management Platform, выполните следующие этапы.

Подготовка

Перед выполнением переноса данных выполните предварительные шаги:

1. Скопируйте CA сертификат из автономного Ядра KUMA на устройство администратора.
2. Создайте токен и храните его в надежном месте. Позже вам нужно будет указать новый токен в файле smp_param.
3. Подготовьте резервную копию данных для автономной версии KUMA и храните резервную копию в надежном месте. В случае возникновения чрезвычайных обстоятельств вы сможете восстановить автономный экземпляр KUMA и повторить перенос данных заново. Иначе в случае сбоя Ядро KUMA может быть повреждено и вы не сможете выполнить перенос данных.

   Также рекомендуется следить за временем при подготовке резервной копии данных и обращать внимание на размер резервной копии. Позже вам может потребоваться настроить соответствующие значения для времени ожидания и свободного места на томе хранилища в файле smp_param.

4. Подготовьте устройства для установки Open Single Management Platform: убедитесь, что требуемые порты открыты, CA сертификат скопирован из Ядра KUMA на устройство администратора, токен сгенерирован, у вас есть root-доступ по SSH к целевым устройствам автономного KUMA и доступ с рабочих узловOpen Single Management Platform к TCP-порту 7223 развернутой автономной версии KUMA.

5. Подготовьте файл инвентаря. В файле инвентаря перечислите все устройства, которые вы используете для сервисов в автономной версии KUMA. Устройства должны совпадать в обоих файлах инвентаря. При необходимости вы можете получить необходимую информацию об устройствах в KUMA в разделе **Ресурсы** → **Активные сервисы**. Обратите внимание, что для всех устройств необходимо указывать FQDN и IP-адрес.

6. Подготовьте smp_param файл. Убедитесь, что вы установили следующие параметры:

   a. Установите флаг переноса данных в значение true.

   ```
   - name: migration
   source:
   value: "true"
   ```

   b. Укажите путь к CA сертификату, который вы скопировали из автономного KUMA на устройство администратора.

   ```
   - name: coreSourceCA
   source:
   path: "<полный путь к CA сертификату>"
   ```

   c. Укажите FQDN для автономной версии Ядра KUMA.

   ```
   - name: coreSourceFQDN
   source:
   значение: "<FQDN для автономного Ядра KUMA>"
   ```

   d. Укажите токен.

   ```
   - name: coreSourceToken
   source:
   value: <token>
   ```

   e. Укажите Helm timeout.

   По умолчанию параметр `helmTimeout` равен 5 минутам. Если копирование резервной копии данных занимает больше времени, чем указанное время ожидания, может возникнуть ошибка. В результате ресурсы KUMA могут стать недоступными. Чтобы избежать такого сценария, учитывайте время при подготовке резервной копии и соответствующим образом корректируйте значение времени ожидания. В следующем примере время ожидания составляет 50 минут.

   ```
   - name: helmTimeout
   source:
   value: "50m0s"
   ```

   f. Укажите пользовательские параметры объема хранилища.

   Если вы планируете импортировать большую базу MongoDB, убедитесь, что для параметра `LowResource` установлено значение `false`.

   ```
   - name: lowResources
   source:
   value: 'false'
   ```

Также укажите необходимый размер тома в соответствии с размером подготовленной резервной копии. Значение размера по умолчанию – 512 ГБ, что может быть слишком большим значением для вашего развертывания. Измените значение при необходимости, и укажите требуемые значения. В следующем примере объем Ядра KUMA составляет 50 ГБ:

```
- name: coreDiskRequest
source:
value: 50Gi
```

Перенос данных

Запустите утилиту KDT, используя подготовленный файл smp_param, как и при первоначальной установке.

После завершения переноса данных все сервисы будут доступны в Консоли KUMA в разделе **Ресурсы** → **Активные службы**.

Устранение неисправностей

Если не удалось выполнить перенос данных, выполните следующие действия:

1. Перейдите в папку, в которой находится утилита KDT, и выполните следующую команду, чтобы проверить файл журнала событий:

   ```
   ./kdt status -l kuma
   ```

   Если вы увидите, что перенос данных завершился неудачно при установке сервисов, для которых будут отсутствовать записи журнала событий, другие шаги этой процедуры не помогут, рекомендуется обратиться в Службу технической поддержки.

2. Проверьте параметры в файле smp_param. Убедитесь, что требуемые порты открыты и целевые устройства доступны, а также что установлено соответствующее значение для параметра helmTimeout. При необходимости экспортируйте файл smp_param и измените значения:

   ./kdt ec > /root/ksmp/smp_param1.yaml

3. Запустите инструмент KDT с измененным файлом smp_param:

   ```
   ./kdt apply --force -k <KUMA as a part of XDR archive>.tar -i
   /root/ksmp/smp_param1.yaml
   ```

Запуск приложения переноса для переноса данных

После завершения переноса данных с автономной версии KUMA вам необходимо запустить приложение переноса для переноса данных.

Вы можете получить приложение для переноса данных от Службы технической поддержки.

Чтобы перенести Серверы администрирования Kaspersky Security Center, доменных пользователей и назначенные роли:

1. Запустите установку приложения переноса KUMA в командной строке.

   ```
   kdt apply --force -k kuma-migrator_<версия>.tar --accept-eula
   ```

2. Получите данные для переноса, выполнив следующую команду:

```
kdt invoke kuma-migrator --action fetch
```

3. Скопируйте результат выборки данных и создайте конфигурационный файл в формате YAML.

4. Откройте конфигурационный файл и вставьте результат выборки данных.

   При необходимости вы можете удалить Серверы администрирования Kaspersky Security Center или пользователей, перенос которых не требуется.

5. Для Серверов администрирования Kaspersky Security Center укажите информацию в следующих полях:

   - `Login`.
   - `Password`.
   - `URL`. Вам нужно указать полный путь, добавив *https://*.
   - `Thumbprint_sha1_encoded`. Вам нужно указать SHA1-отпечаток сертификата Сервера администрирования Kaspersky Security Center.

     Вы можете получить сертификат Сервера администрирования в Консоли OSMP. Для этого в главном меню нажмите на значок параметров ( ) рядом с названием требуемого Сервера администрирования, а затем на вкладке **Общие** нажмите на ссылку **Просмотреть сертификат Сервера администрирования**, чтобы загрузить сертификат.
   - `Insecure_skip_verify`.

     По умолчанию для этого параметра выбрано значение `false`. В этом случае сертификат Сервера администрирования проверяется при выполнении переноса данных. Если вы хотите выключить проверку сертификата, укажите в этом поле значение `true`.

     > Не рекомендуется выключать проверку сертификата.

6. Выполните соответствующие команды для переноса данных.

   Если вы хотите перенести все данные, выполните следующую команду:

   ```
   kdt invoke kuma-migrator --action migrate-all --param migrationConfigFilePath=<имя конфигурационного файла>.yaml
   ```

   Если вы хотите перенести только Серверы администрирования Kaspersky Security Center, выполните следующую команду:

   ```
   kdt invoke kuma-migrator --action migrate-ksc-servers --param migrationConfigFilePath=<имя конфигурационного файла>.yaml
   ```

   Если вы хотите перенести только пользователей, выполните следующую команду:

   ```
   kdt invoke kuma-migrator --action migrate-users --param migrationConfigFilePath=<имя конфигурационного файла>.yaml
   ```

Интеграция с другими решениями

Интеграция с другими решениями позволяет расширить функциональность Open Single Management Platform.

Open Single Management Platform поддерживает интеграцию со следующими решениями "Лаборатории Касперского" и решениями сторонних производителей:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal
- Kaspersky Anti-Targeted Attack Platform / Kaspersky Endpoint Detection and Response
- Active Directory
- UserGate
- Ideco NGFW
- Ideco UTM
- Redmine
- Check Point NGFW
- Sophos Firewall
- Континент 4
- СКДПУ НТ

Open Single Management Platform также поддерживает более 100 источников событий. Полный список поддерживаемых источников событий см. в разделе Поддерживаемые источники событий.

Параметры интеграции можно указать для тенанта любого уровня. Параметры родительской интеграции копируются в дочерний тенант. Вы можете изменять скопированные дочерние параметры интеграции, так как дочерние и родительские параметры не связаны, а изменения в дочерних параметрах не влияют на параметры родительского тенанта.

> Для общего тенанта не нужно настраивать параметры интеграции.

Если вам нужно отключить интеграцию, вы можете сделать это вручную в разделе **Параметры** → **Тенанты**.

> Интеграция с решением "Лаборатории Касперского" автоматически удаляется при удалении тенанта, для которого была указана интеграция. Задержка при удалении данных составляет до 24 часов. Восстановление параметров интеграции недоступно.

Интеграция с Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (далее также KASAP) – это платформа для онлайн-обучения, которая позволяет пользователям изучать правила информационной безопасности и связанные с ними угрозы в повседневной работе, а также практиковаться на реальных примерах.

После настройки интеграции вы можете выполнять следующие задачи в Open Single Management Platform:

- Назначать учебные курсы пользователям, связанными с алертами и инцидентами.
- Изменять группы обучения пользователей.
- Просматривать информацию о курсах, пройденных пользователями, и полученных ими сертификатах.

KASAP считается интегрированным с Open Single Management Platform после настройки интеграции между KASAP и KUMA.

Перед настройкой интеграции между KASAP и KUMA необходимо создать токен авторизации и получить URL для API-запросов в KASAP.

Создание токена в KASAP и получение URL для API-запросов

Создание токена

Чтобы авторизовать запросы API-запросы от KUMA к KASAP, запросы должны быть подписаны токеном, созданным в KASAP.

Создать токен может только администратор организации.

Чтобы создать токен:

1. Войдите в веб-интерфейс KASAP.
2. В разделе **Панель мониторинга** выберите раздел **Импорт и синхронизация** и откройте вкладку **OpenAPI**.
3. Нажмите на кнопку **Новый токен**.
4. В открывшемся окне выберите права токена, доступные при интеграции:
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
5. Нажмите на кнопку **Сгенерировать токен**.

   Сгенерированный токен отображается на экране.
6. Скопируйте токен и сохраните его любым удобным способом. Этот токен необходим для настройки интеграции между KASAP и KUMA.

Токен не хранится в системе KASAP в открытом виде. После закрытия окна **Создать токен** токен недоступен для просмотра. Если вы закроете окно без копирования токена, вам нужно будет нажать на кнопку **Перевыпустить токен**, чтобы система сгенерировала новый токен.

Выданный токен действителен 12 месяцев.

Получение URL для запросов API-запросов

Веб-адрес используется для взаимодействия с KASAP через OpenAPI. Вам нужно указать этот веб-адрес при настройке интеграции между KASAP и KUMA.

Чтобы получить URL, используемый в KASAP для запросов API:

1. Войдите в веб-интерфейс KASAP.
2. В разделе **Панель мониторинга** выберите раздел **Импорт и синхронизация** и откройте вкладку **OpenAPI**.
3. В поле **OpenAPI URL** скопируйте веб-адрес и сохраните его любым удобным способом.

Интеграция с Kaspersky Threat Intelligence Portal

Вам нужно настроить интеграцию с Kaspersky Threat Intelligence Portal (далее также Kaspersky TIP), чтобы получать информацию о репутации наблюдаемых объектов.

Перед настройкой параметров вам необходимо создать токен авторизации для API-запросов на Kaspersky TIP или Kaspersky OpenTIP.

Чтобы настроить интеграцию Open Single Management Platform и Kaspersky TIP:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры** и перейдите в раздел **Kaspersky TIP**.

   Вы можете изменить значения в разделе **Kaspersky TIP**, если вам назначена одна из следующих ролей XDR: Главный администратор, Администратор тенанта или Администратор SOC.

4. Если на шаге 2 вы выбрали корневой тенант, вы можете включить переключатель **Прокси-сервер**, чтобы использовать прокси-сервер для взаимодействия с Kaspersky TIP.

   Прокси-сервер настраивается в свойствах корневого Сервера администрирования.

5. В поле **TTL кеш** укажите срок хранения кеша и единицы измерения: дни или часы.

   По умолчанию установлено 7 дней. Если вы не укажете никакого значения, срок хранения кеша неограничен.

Вы устанавливаете период хранения кеша для всех подключений.

6. Включите переключатель **Интеграция** для одного из следующих сервисов:

   - **Kaspersky TIP (общий доступ)**

     После добавления токена авторизации вы сможете получить информацию от Kaspersky TIP о следующих типах объектов, перечисленных на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента: домен, веб-адрес, IP-адрес, хеш MD5 или SHA256. Информация обновляется в столбце **Обогащение**. При запросе данных расходуется квота данных.

   - **Kaspersky TIP (премиум-доступ)**

     После добавления токена авторизации вы сможете выполнять следующие действия:

     - Получать подробную информацию от Kaspersky TIP о следующих типах наблюдаемых объектов, перечисленных на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента: домен, веб-адрес, IP-адрес, хеш MD5 или SHA256. Информация обновляется в столбце **Обогащение**. При запросе данных расходуется квота данных.

     - Получать подробную информацию от Kaspersky TIP о следующих типах наблюдаемых объектов, перечисленных на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента: домен, веб-адрес, IP-адрес, хеш MD5 или SHA256. Информация обновляется в столбце **Обновление статуса**. При запросе данных квота не расходуется.

7. Нажмите на кнопку **Добавить токен**.

8. В открывшемся окне введите нужные данные токена авторизации и нажмите на кнопку **Добавить**.

   Подробнее о формировании токена авторизации для API-запросов см. в справке Kaspersky TIP или Kaspersky OpenTIP.

   После добавления токена вы можете заменить его, нажав на кнопку **Заменить** и введя новый токен в открывшемся окне. Это может быть необходимо, если срок действия токена истек.

9. Нажмите на кнопку **Сохранить**.

Интеграция с KATA/KEDR

Kaspersky Endpoint Detection and Response (далее также KEDR) – это функциональный блок Kaspersky Anti Targeted Attack Platform (далее также KATA), который защищает активы в локальной сети организации (LAN).

Вы можете настроить интеграцию Open Single Management Platform и KATA/KEDR для управления действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response. Команды для выполнения операций принимаются сервером Kaspersky Endpoint Detection and Response, который затем передает эти команды Kaspersky Endpoint Agent, установленному на активах.

Чтобы настроить интеграцию Open Single Management Platform и KATA/KEDR:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры** и перейдите в раздел **KATA/KEDR**.

   Вы можете изменить значения в разделе **KATA/KEDR**, если вам назначена одна из следующих ролей XDR: Главный администратор, Администратор тенанта или Администратор SOC.

4. Включите переключатель **Интеграция KATA**.

5. Нажмите на кнопку **Добавить соединение** и в открывшемся окне выполните следующие действия:

   a. В поле **IP-адрес или имя устройства** введите одно из следующих значений:

   - hostname
   - IPv4
   - IPv6

   b. В поле **Порт** укажите номер порта.

   c. Нажмите на кнопку **Сохранить**.

   Окно закрыто.

   Если подключение не добавлено, отобразится сообщение об ошибке.

   Если подключение добавлено успешно, на экране отображается соответствующее сообщение. XDR ID, сертификат и закрытый ключ генерируются и отображаются в соответствующих полях. При необходимости вы можете сгенерировать новый сертификат и закрытый ключ, нажав на кнопку **Сгенерировать**.

   Чтобы убедиться, что соединение установлено, нажмите на кнопку **Проверить подключение**. Результат отображается в параметре **Статус подключения**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   После добавления соединения вы можете изменить или удалить его, нажав на соответствующие значки. Вы также можете добавить другое подключение, выполнив шаги 1–6.

Если вы хотите получать информацию об алертах Kaspersky Endpoint Detection and Response, вам нужно настроить интеграцию между компонентом KUMA и KATA/KEDR.

Настройка пользовательской интеграции

Вы можете выполнять действия по реагированию на алерты и инциденты через внешние системы, запуская сторонние скрипты на удаленных клиентских устройствах. Чтобы использовать эту функциональность, вам необходимо настроить окружение и интеграцию Open Single Management Platform со службой запуска скриптов.

Чтобы настроить окружение для запуска сторонних пользовательских скриптов, необходимо:

- Выбрать устройство, на котором запускается сторонний пользовательский скрипт.
- Настроить интеграцию Open Single Management Platform со службой запуска скриптов.

- Создать плейбук, который будет использоваться для запуска скрипта.

Клиент предоставляет доступ к пользовательским скриптам сторонних производителей и обновляет скрипты.

Чтобы настроить интеграцию Open Single Management Platform со службой запуска скриптов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры** и в разделе **Пользовательская интеграция**:

   - Включите переключатель **Пользовательская интеграция**.
   - В разделе **Проверка удаленного устройства** включите переключатель **Проверить подключение устройства** и заполните поле **Открытый ключ**, чтобы включить проверку клиентского устройства в Open Single Management Platform.
   - В разделе **Подключение к удаленному устройству** выполните следующие действия:
     - Заполните поля **IP-адрес или имя устройства** и **Порты**.
     - Выберите **Тип SSH-авторизации**, который будет использоваться для установки безопасного соединения с удаленным устройством:
       - **Имя пользователя и пароль**. Если вы выберете этот тип аутентификации, на следующем шаге вам потребуется ввести имя пользователя и пароль.
       - **SSH-ключ**. Если вы выберете этот тип аутентификации, на следующем шаге вам потребуется ввести имя пользователя и SSH-ключ.
     - Нажмите на кнопку **Добавить данные**.

4. В открывшемся окне введите нужные данные и нажмите на кнопку **Сохранить**.

   Если вы хотите изменить сохраненные данные, нажмите на кнопку **Заменить**, введите новые данные в открывшемся окне и сохраните изменения.

   Чтобы убедиться, что соединение установлено, нажмите на кнопку **Проверить подключение**. Результат отображается в параметре **Статус подключения**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Интеграция Open Single Management Platform со службой запуска скриптов настроена. Вы можете выполнять действия по реагированию на удаленных устройствах, запустив плейбуки.

Взаимодействие с НКЦКИ

Open Single Management Platform позволяет вам взаимодействовать с Национальным координационным центром по компьютерным инцидентам (далее НКЦКИ). Субъект ГосСОПКА, который использует Open Single Management Platform, может передавать данные о компьютерных инцидентах, обнаруженных компьютерных атаках и уязвимостях, используя экспорт инцидентов в НКЦКИ. Благодаря обмену информацией об инцидентах, реагирование на компьютерные инциденты, которые происходят на субъектах критической информационной инфраструктуры Российской Федерации, может стать более оперативным.

В Open Single Management Platform в рамках взаимодействия с НКЦКИ можно выполнять следующие действия:

- экспортировать в НКЦКИ инциденты;
- просматривать изменения в параметрах экспортированных инцидентов, сделанные в НКЦКИ.

Условия взаимодействия с НКЦКИ

Для взаимодействия с НКЦКИ должны выполняться следующие условия:

- Лицензия приложения включает модуль ГосСОПКА.
- Настроена интеграция с НКЦКИ.
- Пользователю, который работает с инцидентами НКЦКИ должна быть присвоена одна из следующих предопределенных ролей:
  - Главный администратор.
  - Администратор тенанта.
  - Работа с НКЦКИ.

Этапы взаимодействия с НКЦКИ

В Open Single Management Platform процесс подготовки и обработки инцидентов НКЦКИ состоит из следующих этапов:

1. **Создание инцидента и проверка его на соответствие требованиям НКЦКИ**

   Вы можете создать инцидент НКЦКИ на основе инцидента XDR. Перед отправкой данных в НКЦКИ убедитесь, что категория инцидента соответствует требованиям НКЦКИ.

2. **Экспорт инцидента в НКЦКИ**

   При успешном экспорте инцидента в НКЦКИ, статус инцидента принимает значение *Отправлен в НКЦКИ*.

   В НКЦКИ полученному инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ**.

   Статус инцидента и некоторые параметры инцидента могут обновляться на стороне НКЦКИ. Если сотрудники НКЦКИ внесли изменения, значения параметров инцидента НКЦКИ обновляются. Данные между Open Single Management Platform и НКЦКИ синхронизируются каждые 5–10 минут. Если в НКЦКИ предоставлены все необходимые данные, инциденту присваивается статус *Проверка НКЦКИ*.

3. **Завершение обработки инцидента**

Когда сотрудники НКЦКИ обработают инцидент, в НКЦКИ ему будет присвоен статус *Принято решение*. В Open Single Management Platform этот статус отображается в заголовке окна со сведениями об инциденте НКЦКИ.

При получении статуса *Отправлен в архив* взаимодействие с НКЦКИ по инциденту через Open Single Management Platform становится невозможным. При этом закрытые инциденты можно найти в таблице инцидентов НКЦКИ и просмотреть сведения о них.

Настройка интеграции с НКЦКИ

Вы можете создать подключение к НКЦКИ. Это позволит вам экспортировать в него инциденты, зарегистрированные в Open Single Management Platform.

Чтобы настроить интеграцию с НКЦКИ:

1. В главном меню перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть доступ на чтение.

2. Нажмите на имя требуемого тенанта.

   Откроется окно свойств тенанта. Если у вас есть только право доступа на чтение к этому тенанту, свойства будут доступны только для чтения. Если у вас есть право доступа на запись, вы можете настроить свойства тенанта.

3. В окне свойств тенанта выберите вкладку **Параметры** и в разделе **Сторонние интеграции** выберите **НКЦКИ**.

4. Включите опцию **Интеграция с НКЦКИ**.

5. В поле **URL** введите URL, по которому доступен НКЦКИ. Например: `https://example.cert.gov.ru/api/v2/`.

6. В поле **API-токен** нажмите на кнопку **Добавить токен** и задайте API-токен вручную.

7. В поле **Организация** укажите название вашей компании. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

8. В раскрывающемся списке **Функция затронутой системы** выберите сферу, в которой работает ваша организация. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

   Доступные сферы деятельности компании

- Атомная энергетика.
- Банковская сфера и иные сферы финансового рынка.
- Горнодобывающая промышленность.
- Государственная/муниципальная власть.
- Здравоохранение.
- Металлургическая промышленность.
- Наука.
- Оборонная промышленность.
- Образование.
- Ракетно-космическая промышленность.
- Связь.
- СМИ.
- Топливно-энергетический комплекс.
- Транспорт.
- Химическая промышленность.
- Иная.

9. В раскрывающемся списке **Расположение** выберите геокод, соответствующий субъекту Российской Федерации, в котором располагается ваша компания. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

   Список геокодов Российской Федерации

Список геокодов Российской Федерации

Субъект РФ	Геокод
Адыгея	RU-AD
Алтайский край	RU-ALT
Амурская область	RU-AMU
Архангельская область	RU-ARK
Астраханская область	RU-AST
Башкортостан	RU-BA
Белгородская область	RU-BEL
Брянская область	RU-BRY
Бурятия	RU-BU
Владимирская область	RU-VLA
Волгоградская область	RU-VGG
Вологодская область	RU-VLG
Воронежская область	RU-VOR
Дагестан	RU-DA
Еврейская автономная область	RU-YEV
Забайкальский край	RU-ZAB
Ивановская область	RU-IVA
Ингушетия	RU-IN
Иркутская область	RU-IRK
Кабардино-Балкария	RU-KB
Калининградская область	RU-KGD
Калмыкия	RU-KL
Калужская область	RU-KLU
Камчатский край	RU-KAM
Карачаево-Черкессия	RU-KC
Карелия	RU-KR
Кемеровская область	RU-KEM
Кировская область	RU-KIR
Костромская область	RU-KOS
Краснодарский край	RU-KDA
Красноярский край	RU-KYA
Курганская область	RU-KGN
Курская область	RU-KRS
Ленинградская область	RU-LEN
Липецкая область	RU-LIP
Магаданская область	RU-MAG
Марий Эл	RU-ME
Мордовия	RU-MO
Москва	RU-MOW

Московская область	RU-MOS
Мурманская область	RU-MUR
Ненецкий автономный округ	RU-NEN
Нижегородская область	RU-NIZ
Новгородская область	RU-NGR
Новосибирская область	RU-NVS
Омская область	RU-OMS
Оренбургская область	RU-ORE
Орловская область	RU-ORL
Пензенская область	RU-PNZ
Пермский край	RU-PER
Приморский край	RU-PRI
Псковская область	RU-PSK
Республика Алтай	RU-AL
Республика Коми	RU-KO
Республика Саха	RU-SA
Ростовская область	RU-ROS
Рязанская область	RU-RYA
Самарская область	RU-SAM
Санкт-Петербург	RU-SPE
Саратовская область	RU-SAR
Сахалинская область	RU-SAK
Свердловская область	RU-SVE
Северная Осетия	RU-SE
Смоленская область	RU-SMO
Ставропольский край	RU-STA
Тамбовская область	RU-TAM
Татарстан	RU-TA
Тверская область	RU-TVE
Томская область	RU-TOM
Тульская область	RU-TUL
Тыва	RU-TY
Тюменская область	RU-TYU
Удмуртия	RU-UD
Ульяновская область	RU-ULY
Хабаровский край	RU-KHA
Хакасия	RU-KK
Ханты-Мансийский автономный округ – Югра	RU-KHM
Челябинская область	RU-CHE
Чечня	RU-CE
Чувашия	RU-CU
Чукотский автономный округ	RU-CHU

Ямало-Ненецкий автономный округ	RU-YAN
Ярославская область	RU-YAR

10. Включите параметр **Использовать прокси-сервер**, чтобы подключаться к НКЦКИ через прокси-сервер.

    Нажмите на ссылку **Параметры**, чтобы задать настройки прокси-сервера. Откроется окно свойств Сервера администрирования, в котором вы можете выполнить настройку.

11. Вы можете указать следующие параметры об операторе персональных данных в соответствующих полях:

    - **Наименование**
    - **ИНН**
    - **Адрес**
    - **Адрес электронной почты**

    Вы также можете убедиться, что соединение с НКЦКИ установлено, нажав на кнопку **Проверить подключение**. Статус проверки отобразится в поле **Статус подключения**.

12. Нажмите на кнопку **Сохранить** для завершения настройки интеграции.

Open Single Management Platform интегрирован с НКЦКИ. Теперь вы можете экспортировать в него инциденты.

Чтобы выключить интеграцию с НКЦКИ:

1. В главном меню перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть доступ на чтение.

2. Нажмите на имя требуемого тенанта.

   Откроется окно свойств тенанта. Если у вас есть только право доступа на чтение к этому тенанту, свойства будут доступны только для чтения. Если у вас есть право доступа на запись, вы можете настроить свойства тенанта.

3. В окне свойств тенанта выберите вкладку **Параметры** и в разделе **Сторонние интеграции** выберите **НКЦКИ**.

4. Выключите параметр **Интеграция с НКЦКИ**.

5. Нажмите на кнопку **Сохранить**.

Интеграция Open Single Management Platform с НКЦКИ выключена.

Просмотр таблицы инцидентов НКЦКИ

Таблица инцидентов НКЦКИ содержит информацию обо всех созданных инцидентах НКЦКИ.

Чтобы просмотреть таблицу инцидентов НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.

2. При необходимости отфильтруйте тенанты. По умолчанию фильтр тенантов выключен и в таблице инцидентов отображаются инциденты, относящиеся ко всем тенантам, к которым у вас есть права доступа. Чтобы применить фильтр для тенантов:

   a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

      Откроется список тенантов.

   b. Установите флажки рядом с требуемыми тенантами.

      В таблице инцидентов отображаются только инциденты, обнаруженные на активах, принадлежащих выбранным тенантам.

3. Выберите вкладку **Инциденты НКЦКИ**.

   Откроется таблица с инцидентами НКЦКИ. Таблица содержит следующие столбцы:

   - **Короткий идентификатор** – уникальный идентификатор инцидента НКЦКИ.
   - **Тенант** – имя тенанта, в котором был обнаружен инцидент.
   - **Обнаружен** – дата и время обнаружения инцидента.
   - **Завершен** – дата и время закрытия инцидента.
   - **Статус** – текущий статус инцидента НКЦКИ, экспортированного в НКЦКИ.
   - **Категория** – категория инцидента НКЦКИ.
   - **Тип** – тип инцидента НКЦКИ.

4. Вы можете группировать и фильтровать данные таблицы с инцидентами НКЦКИ. Для этого нажмите на значок параметров ( ) или на значок фильтрации ( ) в правом верхнем углу таблицы и настройте параметры отображения инцидентов.

   По умолчанию таблица инцидентов НКЦКИ отфильтрована по столбцу **Статус**: инциденты со статусом *Отправлен в архив* и *Принято решение* не отображаются.

Просмотр сведений об инциденте НКЦКИ

В окне со сведениями об инциденте НКЦКИ вы можете просматривать всю информацию, относящуюся к инциденту, включая его свойства.

Чтобы просмотреть сведения об инциденте НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Выберите вкладку **Инциденты НКЦКИ**.
3. В открывшейся таблице нажмите на идентификатор инцидента.

Откроется окно со сведениями об инциденте НКЦКИ.

В заголовке окна указан краткий уникальный идентификатор инцидента и статус, присвоенный инциденту в НКЦКИ. Если инцидент еще не был экспортирован в НКЦКИ, он имеет статус *Черновик*. Некоторые параметры инцидента НКЦКИ доступны для редактирования, остальные параметры наследуются от инцидента XDR и не редактируются.

При необходимости вы можете обновить информацию в окне со сведениями об инциденте, нажав на значок рядом с заголовком окна.

С помощью панели инструментов в верхней части окна вы можете выполнять следующие действия:

- редактировать инцидент НКЦКИ;
- удалять инцидент НКЦКИ;
- экспортировать инцидент НКЦКИ.

Окно сведений об инциденте НКЦКИ содержит разделы, описанные ниже.

Сводная информация

В этом разделе вы можете просматривать и при необходимости редактировать следующую общую информацию об инциденте НКЦКИ:

- **Короткий идентификатор** – уникальный идентификатор инцидента НКЦКИ.
- **Тенант** – имя тенанта, в котором был обнаружен инцидент.
- **Обнаружено** – дата и время обнаружения инцидента.
- **Завершено** – дата и время закрытия инцидента. Этот параметр доступен для редактирования.
- **Описание** – краткое описание инцидента. Этот параметр доступен для редактирования.
- **Категория** – категория инцидента НКЦКИ. Этот параметр доступен для редактирования.
- **Тип** – тип инцидента НКЦКИ. Этот параметр доступен для редактирования.
- **Утечка персональных данных** – уведомление об утечке персональных данных. Этот параметр доступен для редактирования.

  Параметр отображается, если при редактировании категории инцидента вы выбрали **Уведомление о компьютерном инциденте**, а затем выбрали один из следующих типов:

  - **Заражение ВПО**
  - **Компрометация учетной записи**
  - **Несанкционированное разглашение информации**
  - **Успешная эксплуатация уязвимости**
  - **Событие не связано с компьютерной атакой**

Доступные поля

Уведомление об утечке персональных данных – включите этот переключатель в случае утечки персональных данных, после чего раздел **Утечка персональных данных** станет доступным.

Оператор персональных данных – наименование оператора персональных данных. Поле отображается, если настроена интеграция с НКЦКИ.

ИНН – ИНН оператора персональных данных. Поле отображается, если настроена интеграция с НКЦКИ.

Адрес – адрес оператора персональных данных. Поле отображается, если настроена интеграция с НКЦКИ.

Адрес электронной почты – адрес электронной почты оператора персональных данных для отправки информации об уведомлении. Поле отображается, если настроена интеграция с НКЦКИ.

Причины, повлекшие нарушение прав субъектов персональных данных – укажите причины, повлекшие нарушение прав субъектов персональных данных.

Характеристики персональных данных – укажите характеристики персональных данных.

Предполагаемый вред, нанесенный правам субъектов персональных данных – укажите, какой вред нанесен правам субъектов персональных данных.

Принятые меры по устранению последствий инцидента.

Дополнительные сведения.

Информация о результатах внутреннего расследования инцидента.

- **Название компании** – наименование главной организации, в которой произошел инцидент.
- **TLP** – маркер протокола Traffic Light, который определяет уровень конфиденциальности информации, содержащейся в сведениях об инциденте НКЦКИ. Этот параметр доступен для редактирования.

  Возможные значения маркера

  - **WHITE** – раскрытие не ограничено.
  - **GREEN** – раскрытие только для сообщества.
  - **AMBER** – раскрытие только для организаций.
  - **RED** – раскрытие только для круга лиц.

- **Состояние действия** – статус реагирования на инцидент. Этот параметр доступен для редактирования.

  Возможные значения статуса

Значения статуса по умолчанию заполняются по таблице соответствий приведенной ниже.

Список статусов инцидентов XDR и соответствующих статусов реагирования

Статус инцидента XDR	Статус реагирования инцидента НКЦКИ
Новый, В процессе, Отложен	Проводятся мероприятия по реагированию
Закрыт как: истинноположительный результат	Меры приняты
Закрыт как: • ложное срабатывание; • низкоприоритетный; • объединен.	Инцидент не подтвержден

- **Инцидент XDR** – инцидент XDR, на основе которого был создан инцидент НКЦКИ.
- **Затронутая система имеет подключение к интернету** – наличие доступа в интернет в системе, где произошел инцидент. Этот параметр доступен для редактирования.

  Если система, где произошел инцидент, имеет доступ в интернет, то становится доступна вкладка, где можно заполнить технические сведения об атакованном ресурсе (раздел **Технические сведения об атакованном ресурсе**) и вредоносной системе (раздел **Технические сведения о вредоносной системе**).
- **Требуется помощь** – необходимость получения помощи от сотрудников НКЦКИ. Этот параметр доступен для редактирования.
- **Имя затронутой системы** – название атакованной системы. Этот параметр доступен для редактирования.
- **Категория затронутой системы** – категория значимости объекта критической информационной инфраструктуры (далее КИИ). Этот параметр доступен для редактирования.

  Список категорий значимости

  Объекты КИИ имеют следующие категории значимости:

  - объект КИИ первой категории значимости;
  - объект КИИ второй категории значимости;
  - объект КИИ третьей категории значимости;
  - объект КИИ без категории значимости;
  - информационный ресурс не является объектом КИИ.
- **Функция затронутой системы** – сфера деятельности организации, в которой функционирует атакованная система.

  Доступные сферы деятельности компании

- Атомная энергетика.
- Банковская сфера и иные сферы финансового рынка.
- Горнодобывающая промышленность.
- Государственная/муниципальная власть.
- Здравоохранение.
- Металлургическая промышленность.
- Наука.
- Оборонная промышленность.
- Образование.
- Ракетно-космическая промышленность.
- Связь.
- СМИ.
- Топливно-энергетический комплекс.
- Транспорт.
- Химическая промышленность.
- Иная.

- **Расположение** – геокод, соответствующий субъекту Российской Федерации, в котором располагается организации.

  Список геокодов Российской Федерации

Список геокодов Российской Федерации

Субъект РФ	Геокод
Адыгея	RU-AD
Алтайский край	RU-ALT
Амурская область	RU-AMU
Архангельская область	RU-ARK
Астраханская область	RU-AST
Башкортостан	RU-BA
Белгородская область	RU-BEL
Брянская область	RU-BRY
Бурятия	RU-BU
Владимирская область	RU-VLA
Волгоградская область	RU-VGG
Вологодская область	RU-VLG
Воронежская область	RU-VOR
Дагестан	RU-DA
Еврейская автономная область	RU-YEV
Забайкальский край	RU-ZAB
Ивановская область	RU-IVA
Ингушетия	RU-IN
Иркутская область	RU-IRK
Кабардино-Балкария	RU-KB
Калининградская область	RU-KGD
Калмыкия	RU-KL
Калужская область	RU-KLU
Камчатский край	RU-KAM
Карачаево-Черкессия	RU-KC
Карелия	RU-KR
Кемеровская область	RU-KEM
Кировская область	RU-KIR
Костромская область	RU-KOS
Краснодарский край	RU-KDA
Красноярский край	RU-KYA
Курганская область	RU-KGN
Курская область	RU-KRS
Ленинградская область	RU-LEN
Липецкая область	RU-LIP
Магаданская область	RU-MAG
Марий Эл	RU-ME
Мордовия	RU-MO
Москва	RU-MOW

Московская область	RU-MOS
Мурманская область	RU-MUR
Ненецкий автономный округ	RU-NEN
Нижегородская область	RU-NIZ
Новгородская область	RU-NGR
Новосибирская область	RU-NVS
Омская область	RU-OMS
Оренбургская область	RU-ORE
Орловская область	RU-ORL
Пензенская область	RU-PNZ
Пермский край	RU-PER
Приморский край	RU-PRI
Псковская область	RU-PSK
Республика Алтай	RU-AL
Республика Коми	RU-KO
Республика Саха	RU-SA
Ростовская область	RU-ROS
Рязанская область	RU-RYA
Самарская область	RU-SAM
Санкт-Петербург	RU-SPE
Саратовская область	RU-SAR
Сахалинская область	RU-SAK
Свердловская область	RU-SVE
Северная Осетия	RU-SE
Смоленская область	RU-SMO
Ставропольский край	RU-STA
Тамбовская область	RU-TAM
Татарстан	RU-TA
Тверская область	RU-TVE
Томская область	RU-TOM
Тульская область	RU-TUL
Тыва	RU-TY
Тюменская область	RU-TYU
Удмуртия	RU-UD
Ульяновская область	RU-ULY
Хабаровский край	RU-KHA
Хакасия	RU-KK
Ханты-Мансийский автономный округ – Югра	RU-KHM
Челябинская область	RU-CHE
Чечня	RU-CE
Чувашия	RU-CU
Чукотский автономный округ	RU-CHU

Ямало-Ненецкий автономный округ	RU-YAN
Ярославская область	RU-YAR

- **Средство обнаружения** – приложение, с помощью которого был зарегистрирован инцидент. Этот параметр доступен для редактирования.

- **Город** – город, в котором расположен объект КИИ, на котором произошел инцидент, атака или обнаружена уязвимость. Этот параметр доступен для редактирования.

- **Влияние на доступность** – влияние инцидента на доступность атакованной системы.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Влияние на целостность** – влияние инцидента на целостность атакованной системы.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Влияние на конфиденциальность** – влияние инцидента на конфиденциальность атакованной системы.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Другое влияние** – описание других последствий компьютерного инцидента или компьютерной атаки.

  Параметр доступен для таких категорий инцидента НКЦКИ как *Уведомление о компьютерном инциденте* и *Уведомление о компьютерной атаке*. Значение статуса определяется параметром **Уровень важности** родительского инцидента XDR.

- **Категория приложений** – наименование и версия уязвимого приложения. Параметр доступен для категории инцидента НКЦКИ *Уведомление о наличии уязвимости*.

- **Технические сведения об атакованном ресурсе** – технические сведения о системе, где произошел инцидент, атака или обнаружена уязвимость. Этот параметр доступен для редактирования.

  Список параметров атакованного ресурса

При наличии доступа в интернет в системе, где произошел инцидент, становится доступна вкладка, где можно заполнить технические сведения об атакованном ресурсе. Параметры раздела доступны к заполнению в зависимости от категории и типа инцидента НКЦКИ (см. таблицу ниже).

Параметры раздела **Технические сведения об атакованном ресурсе**

Название и описание параметра	Категория	Тип
IPv4-адрес IPv4-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
	Уведомление о наличии уязвимости	Уязвимый ресурс
IPv6-адрес IPv6-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
	Уведомление о наличии уязвимости	Уязвимый ресурс
Имя домена	Уведомление о компьютерном	• Заражение ВПО

Доменное имя контролируемого ресурса	инциденте	• Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации
	Уведомление о наличии уязвимости	Уязвимый ресурс
URI-адрес URI-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
	Уведомление о наличии уязвимости	Уязвимый ресурс
Электронная почта Адрес электронной почты атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Компрометация учетной записи • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости

		• Социальная инженерия
Атакуемый сетевой сервис Имя и порт/протокол атакованной сетевой службы	Уведомление о компьютерном инциденте	• Заражение ВПО • Замедление работы ресурса в результате DDoS-атаки • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
	Уведомление о наличии уязвимости	Уязвимый ресурс
AS-Path до атакованной автономной системы (ASN)	Уведомление о компьютерном инциденте	Захват сетевого трафика

- **Технические сведения о вредоносной системе** – технические сведения о вредоносной системе, вследствие атаки которой произошел инцидент. Этот параметр доступен для редактирования.

  Список параметров вредоносной системы

При наличии доступа в интернет в системе, где произошел инцидент, становится доступна вкладка, где можно заполнить технические сведения о вредоносной системе. Параметры раздела доступны к заполнению в зависимости от категории и типа инцидента НКЦКИ (см. таблицу ниже).

Параметры раздела **Технические сведения о вредоносной системе**

Название и описание параметра	Категория	Тип
IPv4-адрес IPv4-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
IPv6-адрес IPv6-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации

		• Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
Имя домена Доменное имя контролируемого ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга • Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
URI-адрес URI-адрес атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Использование контролируемого ресурса для фишинга • Несанкционированное изменение информации

		• Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Социальная инженерия
Функции – тип активности Предлагается к заполнению, если заполнено одно из полей **IPv4-адрес**, **IPv6-адрес**, **Имя домена** или **URI-адрес**. Возможные значения: • **Центр управления ВПО**. • **Элемент инфраструктуры ВПО**. • **Источник распространения ВПО**. • **Тип не определен**.	—	—
Электронная почта Адрес электронной почты атакованного ресурса	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Несанкционированное разглашение информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Социальная инженерия
Хеш вредоносного ПО Хеш-сумма вредоносного модуля	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО
	Уведомление о компьютерной атаке	• Попытки внедрения ВПО
Используемые уязвимости Описание используемых уязвимостей	Уведомление о компьютерном инциденте	• Заражение ВПО • Вовлечение контролируемого ресурса в инфраструктуру ВПО • Замедление работы ресурса в результате DDoS-атаки • Использование контролируемого ресурса для фишинга

		• Компрометация учетной записи • Несанкционированное изменение информации • Несанкционированное разглашение информации • Публикация на ресурсе запрещенной законодательством РФ информации • Рассылка спам-сообщений с контролируемого ресурса • Успешная эксплуатация уязвимости
	Уведомление о компьютерной атаке	• DDoS-атака • Неудачные попытки авторизации • Попытки внедрения ВПО • Попытки эксплуатации уязвимости • Публикация мошеннической информации • Сетевое сканирование • Социальная инженерия
Номер автономной системы (ASN) Номер подставной автономной системы (ASN)	Уведомление о компьютерном инциденте	Захват сетевого трафика
Наименование AS Наименование подставной автономной системы	Уведомление о компьютерном инциденте	Захват сетевого трафика
Наименование LIR Наименование локального интернет-регистратора	Уведомление о компьютерном инциденте	Захват сетевого трафика

Интеграция с НКЦКИ

В этом разделе вы можете просматривать следующую информацию об инциденте, который был экспортирован в НКЦКИ:

- **UUID** – уникальный идентификатор карточки уведомления в НКЦКИ.
- **Регистрационный номер** – регистрационный номер уведомления в НКЦКИ.
- **Зарегистрировано** – дата и время регистрации инцидента в НКЦКИ.
- **Время обновления** – дата последнего обновления инцидента в НКЦКИ.

История

В этом разделе вы можете просматривать следующую информацию об истории изменений инцидента НКЦКИ:

- **Время** – дата и время изменения инцидента.

- **Пользователь** – имя пользователя, который изменил инцидент.
- **Подробнее** – информация об изменении инцидента.

Создание инцидента НКЦКИ

Вы можете создать инцидент НКЦКИ только на основе существующего инцидента XDR.

Чтобы создать инцидент НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Нажмите на инцидент XDR, на основе которого вы хотите создать инцидент для отправки в НКЦКИ. Инцидент XDR может иметь любой статус.

   Откроется окно со сведениями об инциденте XDR.
3. В панели управления в верхней части окна нажмите **Создать инцидент НКЦКИ**.

   Откроется окно создание инцидента НКЦКИ.
4. Заполните следующие поля:
   - **Категория** – категория инцидента НКЦКИ.
   - **Тип** – тип инцидента НКЦКИ.
5. При необходимости в поле **Активы** вы можете выбрать или добавить активы, вовлеченные в инцидент НКЦКИ. В таблице активов у таких устройств в столбце **Имеет признаки** стоит значение "атакующий" или "жертва".

   Данные о выбранных атакованных устройствах и вредоносных системах будут отображаться в окне со сведениями об инциденте НКЦКИ в разделах инцидента **Технические сведения об атакованном ресурсе** и **Технические сведения о вредоносной системе**.

Инцидент НКЦКИ создан. После этого в инцидент XDR добавляется ссылка на созданный инцидент НКЦКИ, а в инциденте НКЦКИ – ссылка на инцидент XDR. Вы можете просмотреть сведения об инциденте, отредактировать их и экспортировать инцидент в НКЦКИ.

Передача инцидентов в НКЦКИ

Чтобы экспортировать инцидент в НКЦКИ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Выберите вкладку **Инциденты НКЦКИ**.
3. В открывшейся таблице нажмите на идентификатор инцидента НКЦКИ, который вы хотите экспортировать.

   Откроется окно со сведениями об инциденте.

   Если в списке инцидентов НКЦКИ отсутствует инцидент, который необходимо экспортировать, вы можете создать инцидент НКЦКИ.

4. При необходимости вы можете отредактировать параметры инцидента НКЦКИ перед экспортом. Для этого нажмите на кнопку **Изменить** в панели в верхней части окна инцидента НКЦКИ, заполните необходимые поля и сохраните изменения.

5. Нажмите на кнопку **Отправить в НКЦКИ** в панели в верхней части окна инцидента НКЦКИ.

6. В открывшемся окне подтвердите отправку инцидента в НКЦКИ.

Запрос в НКЦКИ отправлен. Если экспорт выполнен успешно, в НКЦКИ полученному инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ**. При этом значение поля **Статус** меняется на *Отправлен в НКЦКИ*. С этого момента повторная отправка и редактирование инцидента в НКЦКИ в интерфейсе Open Single Management Platform становятся недоступны. Если вам требуется внести изменения в экспортированный инцидент, это следует делать в личном кабинете НКЦКИ.

Допустимые категории и типы инцидентов НКЦКИ

В таблице ниже перечислены категории и типы инцидентов, которые можно экспортировать в НКЦКИ.

Категории и типы инцидентов НКЦКИ

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Замедление работы ресурса в результате DDoS-атаки
	Заражение вредоносным программным обеспечением (далее ВПО)
	Захват сетевого трафика
	Использование контролируемого ресурса для проведения атак
	Компрометация учетной записи
	Несанкционированное изменение информации
	Несанкционированное разглашение информации
	Публикация на ресурсе запрещенной законодательством РФ информации
	Успешная эксплуатация уязвимости
	Событие не связано с компьютерной атакой
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия
Уведомление о наличии уязвимости	Уязвимый ресурс

Статусы инцидента НКЦКИ

Инцидент, экспортированный в НКЦКИ, может иметь статусы, приведенные в таблице ниже.

Статусы инцидента НКЦКИ

Статус инцидента	Описание

НКЦКИ	
Черновик	Статус присваивается в следующих случаях: • экспорт инцидента не выполнялся; • экспорт инцидента был выполнен с ошибкой.
Отправлен в НКЦКИ	Статус присваивается в следующих случаях: • экспорт инцидента был выполнен успешно; • в НКЦКИ еще не был запрошен статус инцидента.
Создан *Создано* *Зарегистрирован* *Проверка НКЦКИ* *Принято решение* *Отправлен в архив*	При успешном экспорте инциденту присваивается один из перечисленных статусов в зависимости от этапа рассмотрения инцидента специалистами НКЦКИ. Статус инцидента запрашивается в НКЦКИ каждые 5 минут после успешной отправки инцидента в НКЦКИ. После получения статуса *Принято решение* или *Отправлен в архив* запрос по инциденту в НКЦКИ больше не выполняется.

Обнаружение угроз

Open Single Management Platform использует алерты и инциденты в качестве рабочих элементов, которые должны обрабатываться аналитиками.

Разделы **Алерты** и **Инциденты** отображаются в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Open Single Management Platform.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Работа с НКЦКИ, Подтверждающий, Наблюдатель.

Работа с алертами

Этот раздел содержит общую информацию об алертах, их свойствах, типичном жизненном цикле и связи с инцидентами. Предоставленные инструкции помогут вам проанализировать таблицу алертов, изменить свойства алертов в соответствии с текущим состоянием жизненного цикла и объединить алерты в инциденты путем связывания или удаления связи алертов.

Раздел **Алерты** отображается в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Open Single Management Platform.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Работа с НКЦКИ, Подтверждающий, Наблюдатель.

Об алертах

Алерт – это событие в ИТ-инфраструктуре организации, которое было отмечено Open Single Management Platform как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуры организации.

Open Single Management Platform формирует алерт, когда EPP-программа (например, Kaspersky Endpoint Security для Windows) обнаруживает в инфраструктуре определенную активность, соответствующую условиям, заданным в правилах обнаружения.

Алерт создается в течение 30 секунд после возникновения события корреляции KUMA.

Также вы можете создать алерт вручную из набора событий.

После детектирования Open Single Management Platform добавляет алерты в таблицу алертов как объекты, которые должны быть обработаны аналитиками. Вы не можете удалить алерты. Их можно только закрыть.

Алерты могут быть назначены только аналитикам, имеющим право читать и изменять алерты и инциденты.

Вы можете управлять алертами как объектами, используя следующие свойства алертов:

- **Статус алерта.**

  Возможные значения: *Новый*, *В обработке*, *Закрыто* или *В инциденте*.

  Статус алерта показывает текущий статус алерта в его жизненном цикле. Вы можете изменить статус по своему усмотрению, за исключением следующих случаев:

  - Вы не можете вернуть закрытые алерты в статус *В обработке*. Закрытые алерты можно вернуть только в статус *Новый*, а затем статус можно изменить на *В обработке*.
  - Вы не можете установить статус *В инциденте* вручную. Алерты получают этот статус, когда они связаны с инцидентом.
  - Вы можете установить статус *Закрыт* только для связанного алерта. Чтобы установить статус *Новый* или *В обработке*, необходимо отменить связь между алертом и инцидентом.

- **Уровень критичности алерта.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Уровень критичности алерта показывает, какое влияние этот алерт может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского". Уровень важности определяется автоматически и не может быть изменен вручную.

- **Ответственный за алерт.**

  Владелец алерта, аналитик, который отвечает за расследование алерта. Вы можете изменить ответственного за алерт в любое время. Невозможно изменить исполнителя закрытых алертов.

Вы можете комбинировать и связывать алерты с более крупными рабочими объектами, называемыми *инцидентами*. Вы можете связать алерты с инцидентами вручную или включить правила для автоматического создания инцидентов и связывания алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему. Когда вы связываете алерт, ни с чем не связанный в текущий момент, с инцидентом, алерт приобретает статус *В инциденте*. Вы можете связать алерт, ни с чем не связанный в текущий момент, с другим инцидентом. В этом *случае* статус алерта сохраняется. Вы можете связать с инцидентом не более 200 алертов.

Каждый алерт содержит *детали алерта*, которые содержат всю информацию, относящуюся к алерту. Вы можете использовать эту информацию для исследования алерта, отслеживания событий, предшествующих алерту, просмотра обнаруженных артефактов, затронутых активов или для привязки алерта к инциденту.

Модель данных алерта

Структура алерта представлена полями, которые содержат значения (см. таблицу ниже). Некоторые поля являются объектами или массивами объектов со своим набором полей (например, поля `Assignee` и `Assets`).

Алерт

Поле	Тип значения	Требуется	Описание
`InternalID`	Строка	Да	Внутренний идентификатор алерта (в формате UUID). Значение поля может совпадать со значением `SourceID`.
`ID`	Целое число	Да	Короткий внутренний идентификатор алерта.
`TenantID`	Строка	Да	Идентификатор тенанта, с которым связан алерт (в формате UUID).
`CreatedAt`	Строка	Да	Дата и время создания алерта (в формате RFC 3339).
`UpdatedAt`	Строка	Да	Дата и время последнего изменения алерта (в формате RFC 3339).
`StatusChangedAt`	Строка	Нет	Дата и время последнего изменения статуса алерта (в формате RFC 3339).
`Severity`	Строка	Да	Критичность алерта. Возможные значения: • `critical` • `high` • `medium` • `low`
`IntegrationID`	Строка	Да	Идентификатор плагина управления приложения "Лаборатории Касперского", интегрированного в OSMP.
`IntegrationCompatibilityVersion`	Строка	Да	Версия плагина управления приложения "Лаборатории Касперского", интегрированного в OSMP.
`SourceID`	Строка	Нет	Уникальный идентификатор алерта в интегрированном компоненте.
`SourceCreatedAt`	Строка	Нет	Дата и время создания алерта в интегрированном компоненте (в формате RFC 3339).
`FirstEventTime`	Строка	Да	Дата и время первого события телеметрии, связанного с алертом (в формате RFC 3339).
`LastEventTime`	Строка	Да	Дата и время последнего события телеметрии, связанного с алертом (в формате RFC 3339).
`DetectSource`	Строка	Нет	Компонент, который обнаруживает и генерирует алерт.
`DetectionTechnologies`	Массив строк	Нет	Технология срабатывания детектирования.
`Status`	Строка	Да	Статус алерта. Возможные значения: • `new` • `inProgress` • `inIncident` • `closed`
`StatusResolution`	Строка	Нет	Решение статуса алерта. Возможные значения: • `truePositive` • `falsePositive` • `lowPriority` • `merged`

`IncidentID`	Строка	Нет	Внутренний идентификатор инцидента, связанного с алертом.
`IncidentLinkType`	Строка	Нет	Способ добавления алерта в инцидент. Возможные значения: • `manual` • `auto`
`Assignee`	Объект `Assignee`	Нет	Оператор, которому назначен алерт.
`MITRETactics`	Массив объектов `MITRETactic`	Нет	Тактики MITRE, связанные со всеми сработавшими IOA-правилами в алерте.
`MITRETechniques`	Массив объектов `MITRETechnique`	Нет	Техники MITRE, связанные со всеми сработавшими IOA-правилами в алерте.
`Observables`	Массив объектов `Observable`	Нет	Наблюдаемые объекты, связанные с алертом.
`Assets`	Массив объектов `Asset`	Нет	Активы, затронутые алертом.
`Rules`	Массив объектов `Rule`	Нет	Сработавшие правила корреляции, на основании которых формируется алерт.
`OriginalEvents`	Массив объектов	Нет	События, на основании которых формируется алерт.
`ExternalRef`	Строка	Да	Ссылка на объект во внешней системе (например, ссылка на инцидент Jira).
`Extra`	Объект	Нет	Данные, связанные с алертом, в формате JSON. Эти данные получены от управляемых приложений "Лаборатории Касперского", когда события преобразуются в алерты. Это поле не используется в интерфейсе.
`AdditionalData`	Объект	Нет	Дополнительная информация об алерте в формате JSON. Эту информацию может заполнить пользователь или плейбук.
`IsCII`	Логический оператор	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры.
`Name`	Строка	Да	Имя алерта.
`Attachments`	Массив объектов `UnkeyedAttachment`	Нет	Вложения, связанные с инцидентом.

Исполнитель

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор учетной записи оператора, которому назначен алерт.
`Name`	Строка	Да	Имя оператора, которому назначен алерт.

MITRETactic

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор тактики MITRE, связанной со всеми сработавшими IOA-правилами в алерте.
`Name`	Строка	Да	Название тактики MITRE, относящейся ко всем сработавшим IOA-правилам в алерте.

MITRETechnique

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор техники MITRE, связанной со всеми сработавшими IOA-правилами в алерте.
`Name`	Строка	Да	Название техники MITRE, относящейся ко всем сработавшим IOA-правилам в алерте.

Наблюдаемый объект

Поле	Тип значения	Требуется	Описание
`Type`	Строка	Да	Тип наблюдаемого объекта. Возможные значения: • `ip` • `md5` • `sha256` • `url` • `domain` • `userName` • `hostName`
`Value`	Строка	Да	Значение наблюдаемого объекта.
`Details`	Строка	Нет	Дополнительная информация о наблюдаемом объекте.

Правило

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор сработавшего правила.
`Name`	Строка	Нет	Имя сработавшего правила.
`Severity`	Строка	Нет	Критичности сработавшего правила. Возможные значения: • `critical` • `high` • `medium` • `low`
`Confidence`	Строка	Нет	Уровень доверия сработавшего правила. Возможные значения: • `high` • `medium` • `low`
`Custom`	Логический оператор	Нет	Индикатор того, что алерт основан на пользовательских правилах.

Актив

Поле	Тип значения	Требуется	Описание
`Type`	Строка	Да	Тип затронутого актива (устройство или учетная запись). Возможные значения: • `host` • `user`
`ID`	Строка	Да	Идентификатор затронутого актива (устройства или учетной записи).
`Name`	Строка	Нет	Имя затронутого устройства, с которым связан алерт (если для параметра `Type` выбрано значение `host`). Имя пользователя затронутой учетной записи, связанной с событиями, на основе которых создается алерт (если для параметра `Type` выбрано значение `user`).
`IsAttacker`	Логический оператор	Нет	Индикатор того, что затронутый актив (устройство или учетная запись) является атакующим.
`IsVictim`	Логический оператор	Нет	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`CIICategory`	Строка	Нет	Категория значимости того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры. Возможные значения: • `notCII` • `ciiWithoutCategory` • `ciiFirstCategory` • `ciiSecondCategory` • `ciiThirdCategory`

UnkeyedAttachment

Поле	Тип значения	Требуется	Описание
`AttachmentID`	Строка	Да	Идентификатор вложения (в формате UUID).
`Name`	Строка	Да	Имя вложения.
`CreatedAt`	Строка	Да	Дата и время создания вложения в формате UTC.
`UpdatedAt`	Строка	Да	Дата и время последнего изменения вложения в формате UTC.
`CreatedBy`	Строка	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`Size`	Целое число	Да	Размер вложения, указанный в байтах.
`Status`	Строка	Да	Статус вложения, который указывает, находится ли загрузка вложения в процессе, завершена или прервана с ошибкой. Возможные значения: • `completed` • `error` • `uploading`
`Description`	Строка	Нет	Описание вложения.
`StatusCode`	Строка	Нет	Текст статуса, который отображается пользователю (например, сообщение об ошибке, которое отображается при неудачной попытке загрузки вложения).

Просмотр таблицы алертов

В таблице алертов представлена информация обо всех алертах, зарегистрированных Open Single Management Platform.

Чтобы просмотреть таблицу алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.

   Отобразится таблица алертов.

2. При необходимости отфильтруйте тенанты. По умолчанию фильтр для тенантов выключен и в таблице алертов отображаются алерты, относящиеся ко всем тенантам, к которым у вас есть права доступа. Чтобы применить фильтр для тенантов:

   a. По ссылке рядом с параметром **Фильтр тенантов** откройте список тенантов.

   b. Установите флажки рядом с требуемыми тенантами.

      В таблице отображаются только алерты, зарегистрированные на выбранных тенантах.

В таблица алертов содержит следующие столбцы:

- **ID алерта** – уникальный идентификатор алерта.
- **Зарегистрировано** – дата и время, когда алерт был добавлен в таблицу алертов.
- **Время обновления** – дата и время последнего изменения в истории алертов.
- **Статус** – текущий статус алерта.
- **Аналитик** – текущий исполнитель алерта.
- **Тенант** – имя тенанта, в котором зарегистрирован алерт.
- **Технология** – технология, зарегистрировавшая алерт.
- **Правила** – IOC- или IOA-правила, сработавшие для регистрации алерта.
- **Затронутые активы** – устройства и пользователи, затронутые алертом.
- **Наблюдаемые объекты** – артефакты обнаружения, например IP-адреса или MD5-хеши файлов.
- **Тип ссылки инцидента** – способ добавления алерта в инцидент, вручную или автоматически.
- **Критичность** – критичность алерта.
- **Статус изменен** – дата и время последнего изменения статуса алерта.
- **Объект КИИ** – наличие хотя бы одного актива, который включен в алерт и является объектом критической информационной инфраструктуры (КИИ).

  Принимает значение **Да**, если затронутый актив – это объект КИИ первой, второй, третьей категории значимости или объект КИИ без категории значимости. Столбец доступен для отображения, если лицензия приложения включает модуль ГосСОПКА.

События, которые содержат объекты КИИ, должны образовывать отдельный алерт. Для этого вам нужно настроить правило агрегациии.

Просмотр деталей алерта

Детали алерта – это страница в интерфейсе, которая содержит всю информацию, относящуюся к алерту, включая свойства алерта.

Чтобы просмотреть детали алерта:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.
2. В таблице алертов нажмите на идентификатор требуемого алерта.

   Отображаются детали алерта.

Панель инструментов в верхней части деталей алерта позволяет выполнять следующие действия:

- Изменять значение поля **Внешняя ссылка**
- Назначить алерт аналитику
- Изменить статус алерта
- Связать алерт с инцидентом
- Отменить связь алерта с инцидентом
- Выбрать плейбук
- Создать инцидент и привязать к нему алерт

Детали алерта состоят из следующих разделов:

- **Сводная информация**

Раздел сводной информации содержит следующие свойства алерта:

- **Аналитик**. Аналитик, которому назначен алерт.
- **Тенант**. Имя тенанта, в котором зарегистрирован алерт.
- **Активы**. Количество учетных записей пользователей и устройств, связанных с алертом.
- **Критичность**. Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**. Уровень критичности алерта показывает, какое влияние этот алерт может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского".
- **Правила**. Правила, которые сработали для регистрации алерта. Вы можете нажать на значок с многоточием рядом с названием правила, чтобы открыть контекстное меню. Используйте это меню, чтобы узнать больше о правиле, найти алерты или инциденты, которые были зарегистрированы этим же правилом, или выполнить поиск событий, инициировавших правило, в разделе **Поиск угроз** за период между первым и последним событием алерта.
- **Зарегистрировано**. Дата и время, когда алерт был добавлен в таблицу алертов.
- **Первое событие**. Дата и время первого события, связанного с алертом.
- **Последнее событие**. Дата и время последнего события, связанного с алертом.
- **Внешняя ссылка**. Ссылка на объект во внешней системе (например, ссылка на инцидент Jira). Вы можете нажать на кнопку **Изменить**, чтобы указать внешнюю ссылку.
- **Связанный с**. Инцидент, к которому привязан алерт.
- **Технологии**. Технология, зарегистрировавшая алерт.
- **Тактика MITRE**. Тактика или несколько тактик, зарегистрированных в алерте. Тактика определена в базе знаний MITRE ATT&CK.
- **Техника MITRE**. Техника или несколько техник, зарегистрированных в алерте. Методы определены в базе знаний MITRE ATT&CK.

- Подробная информация

В разделе **Подробнее** вы можете отслеживать события телеметрии, связанные с алертом.

В таблице событий отображается результат поиска, который вы определяете с помощью SQL-запроса.

Панель инструментов таблицы событий позволяет выполнить следующие действия:

- **Скачать события**. Нажмите на эту кнопку, чтобы загрузить информацию о связанных событиях в файл CSV (в кодировке UTF-8).

- **Поиск в разделе Поиск угроз**. Нажмите на эту кнопку, чтобы открыть раздел **Поиск угроз**. Этот раздел позволяет выполнять поиск по всем событиям, связанным с тенантами, к которым у вас есть доступ, а не только по событиям, связанным с текущим алертом. По умолчанию открытая таблица событий содержит все события, произошедшие в период между первым и последним событием в алерте. Например, вы можете запустить поисковый запрос, чтобы найти все события, в которых было задействовано устройство.

  В разделе **Поиск угроз** вы можете вручную связать события с алертами. Это может быть полезно, если вы выясните, что некоторые события относятся к алерту, но не были связаны с алертом автоматически. Дополнительные сведения см. в инструкциях по связыванию или удалению связи событий с алертами.

  Вы можете вернуться к деталям инцидента, нажав на кнопку **Исследование алерта** или нажав на кнопку **Назад** в вашем браузере.

- **Удалить связь с алертом**. Выберите событие или несколько событий в таблице и нажмите на эту кнопку, чтобы удалить связь выбранных событий с алертом.

- Активы

В разделе **Активы** можно просмотреть устройства и пользователей, затронутых алертом или участвующих в нем.

Таблица активов содержит следующие столбцы:

- **Тип актива**.

  Возможные значения: устройство или пользователь.

- **Имя актива**.

- **Идентификатор актива**.

- **Имеет признаки**.

  Возможные значения: атакующий или атакуемый.

- **Статус авторизации**.

  Этот параметр применяется только к типу актива – устройство. Статус авторизации устройства определяется KICS for Networks. Вы можете изменить статус авторизации, применив соответствующие действия по реагированию к устройству.

- **Сервер администрирования**.

  Сервер администрирования, который управляет устройством.

- **Группа администрирования**.

  Группа администрирования, к которой принадлежит пользователь.

- **Категории**.

  Категории активов, в которые входит актив.

- **Категория КИИ**.

  Информация о том, является ли актив объектом критической информационной инфраструктуры (КИИ). Столбец доступен для отображения, если лицензия приложения включает модуль ГосСОПКА и если вам назначена одна из следующих ролей XDR: Доступ к объектам КИИ, Главный администратор.

  Возможные значения:

  - Объект КИИ первой категории значимости.
  - Объект КИИ второй категории значимости.
  - Объект КИИ третьей категории значимости.
  - Объект КИИ без категории значимости.
  - Информационный ресурс не является объектом КИИ.

Нажав на имя пользователя или устройства, вы можете:

- Выполнить поиск по имени пользователя или идентификатору устройства в разделе **Поиск угроз** за период между первым и последним событием алерта.
- Выполнить поиск по имени пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по имени пользователя или идентификатору устройства в других инцидентах.
- Скопировать имя пользователя или имя устройства в буфер обмена.

Вы также можете нажать на имя устройства, чтобы открыть свойства устройства.

Нажав на идентификатор пользователя или идентификатор устройства, вы можете:

- Выполнить поиск по идентификатору пользователя или идентификатору устройства в разделе **Поиск угроз** за период между первым и последним событием алерта.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других инцидентах.
- Скопировать идентификатор пользователя или идентификатор устройства в буфер обмена.

Вы также можете нажать на идентификатор устройства, чтобы открыть его свойства.

- **Наблюдаемые объекты**

В разделе **Наблюдаемые объекты** вы можете просмотреть наблюдаемые объекты, связанные с алертом. Наблюдаемые объекты могут включать:

- MD5-хеш
- IP-адрес
- URL
- Имя домена
- SHA256
- UserName
- HostName

Нажав на ссылку в столбце **Значение**, вы можете:

- Поиск наблюдаемого значения в разделе **Поиск угроз** за период между первым и последним событием алерта.
- Выполнить поиск по значению наблюдаемого объекта в других алертах.
- Выполнить поиск по значению наблюдаемого объекта в других инцидентах.
- Скопировать значение наблюдаемого объекта в буфер обмена.

Панель инструментов этого раздела содержит следующие кнопки:

- **Запросить статусы Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию о выбранном наблюдаемом объекте в Kaspersky Threat Intelligence Portal (Kaspersky TIP). В результате информация обновляется в столбце **Статус обновления**. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Обогатить данные Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию обо всех перечисленных наблюдаемых объектах из Kaspersky TIP. В результате информация обновляется в столбце **Обогащение**. Используйте ссылку в столбце **Обогащение**, чтобы открыть полученные сведения об обогащении наблюдаемого объекта. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Поместить на карантин**. Используйте эту кнопку, чтобы переместить устройство, на котором находится файл, на карантин. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Добавить правило запрета**. Используйте эту кнопку, чтобы добавить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Удалить правило запрета**. Используйте эту кнопку, чтобы удалить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Прервать процесс**. Используйте эту кнопку, чтобы прервать процессы, связанные с файлом. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.

- **Похожие закрытые алерты**

В разделе **Похожие закрытые алерты** вы можете просмотреть список закрытых алертов, которые имеют те же затронутые артефакты, что и текущий алерт. Затронутые артефакты включают наблюдаемые объекты и затронутые устройства. Похожие закрытые алерты могут помочь вам изучить текущий алерт.

С помощью списка вы можете оценить степень сходства текущего алерта и других алертов. Сходство рассчитывается следующим образом:

Сходство = M / T * 100

Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном алерте, "T" – общее количество артефактов в текущем алерте.

Если сходство составляет 100%, в текущем алерте нет ничего нового по сравнению с аналогичным алертом. Если сходство равно 0%, текущий и аналогичный алерт полностью различаются. Алерты, имеющие сходство 0%, не включаются в список.

Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

При нажатии на идентификатор алерта открываются детали алерта.

Настройка списка похожих закрытых алертов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте алерты, выбрав период, за который были обновлены алерты. По умолчанию список содержит алерты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать алерты в порядке возрастания или убывания.

- **Подобные инциденты**

В разделе **Подобные инциденты** вы можете просмотреть список инцидентов, которые имеют те же затронутые артефакты, что и текущий алерт. Затронутые артефакты включают наблюдаемые объекты и затронутые устройства. Подобные инциденты могут помочь вам решить, может ли текущий алерт быть связан с существующим инцидентом.

С помощью списка вы можете оценить степень сходства текущего алерта и инцидентов. Сходство рассчитывается следующим образом:

Сходство = M / T * 100

Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном инциденте, "T" – общее количество артефактов в текущем алерте.

Если сходство составляет 100%, в текущем алерте нет ничего нового по сравнению с аналогичным инцидентом. Если сходство равно 0%, текущий алерт и схожий инцидент полностью различаются. Инциденты, имеющие сходство 0%, не включаются в список.

Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

При нажатии на идентификатор инцидента открывается подробная информация об инциденте.

Настройка списка похожих инцидентов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте инциденты, выбрав период, за который были обновлены инциденты. По умолчанию список содержит инциденты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать инциденты в порядке возрастания или убывания.

- **Комментарии**

В разделе **Комментарии** вы можете оставлять комментарии, связанные с алертом. Например, вы можете написать комментарий о результатах расследования или при изменении свойств алерта, таких как исполнитель или статус алерта.

Вы можете изменять или удалять свои комментарии. Комментарии других пользователей невозможно изменить или удалить.

Чтобы сохранить комментарий, нажмите на клавишу **`Enter`**. Чтобы начать новую строку, нажмите на клавиши **`Shift + Enter`**. Чтобы изменить или удалить свой комментарий, используйте кнопки в правом верхнем углу.

Для возможности оставлять комментарии требуется право на **Запись** в функциональной области **Алерты и инциденты**.

- **История**

В разделе **Журнал событий алертов** вы можете отслеживать изменения, внесенные в алерт как в объект:

- Изменение статуса алерта.
- Изменение исполнителя алерта.
- Связь алерта с инцидентом.
- Удаление связи между алертом и инцидентом.

В разделе **История реагирований** вы можете просмотреть действия по реагированию, выполненные вручную, а также действия, выполненные в рамках плейбука. Таблица содержит следующие столбцы:

- **Время**. Время возникновения события.
- **Запущено**. Имя пользователя, запустившего действие по реагированию.
- **События**. Описание события.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.
- **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
- **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
  - **В обработке** – действие по реагированию выполняется.
  - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию завершено с предупреждениями.
  - **Ошибка** – действие по реагированию завершено с ошибками.
  - **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.
- **Плейбук**. Имя плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.
- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

Назначение алертов аналитикам

Как объект, алерт может быть назначен аналитику SOC для проверки и возможного расследования. Вы можете изменить исполнителя активного алерта в любое время. Вы не можете изменить исполнителя закрытого алерта.

Алерты могут быть назначены только аналитикам, имеющим право читать и изменять алерты и инциденты.

Чтобы назначить аналитику алерты:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.
2. Установите флажки рядом с алертами, которые вы хотите назначить аналитику.

   Вам нужно выбрать только алерты, обнаруженные в одном тенанте. Иначе кнопка **Назначить** будет неактивна.

   Также вы можете назначить алерт аналитику из деталей алерта. Чтобы открыть детали алерта, перейдите по ссылке с нужным идентификатором алерта.
3. Нажмите на кнопку **Назначить**.
4. В открывшемся окне **Назначить аналитику** начните вводить имя аналитика или электронную почту, а затем выберите аналитика из списка.

   Вы также можете выбрать вариант **Не назначен** для всех алертов, кроме алертов со статусом **Закрыт**.
5. Нажмите на кнопку **Назначить**.

Алерты назначены аналитику.

Изменение статуса алерта

Как объект, алерт имеет статус, который показывает текущий статус алерта в его жизненном цикле.

Вы можете изменять статусы алертов для своих алертов или алертов других аналитиков, только если у вас есть право доступа для чтения и изменения алертов и инцидентов.

Если статус алерта изменен вручную, плейбуки не будут запускаться автоматически. Вы можете запустить плейбук для такого алерта вручную.

Алерт может иметь один из следующих статусов:

- **Новое.**

  Когда Open Single Management Platform регистрирует новый алерт, он имеет статус *Новый*. Вы можете изменить статус инцидента на *В обработке* или *Закрыт*. Когда вы меняете статус *Новый* на *Закрыт* и у алерта нет исполнителя, оно автоматически назначается вам.

- **В обработке.**

  Этот статус означает, что аналитик начал работу над инцидентом или возобновил работу, изменив статус *Отложен*. Когда вы устанавливаете статус *В обработке*, инцидент назначается вам автоматически. Изменить статус *В обработке* можно на любой другой.

- **Закрыто.**

  Истинно положительные алерты должны быть связаны с инцидентами и расследоваться в рамках инцидентов. Когда вы закрываете инцидент, связанные алерты также переходят в статус *Закрыт*. Вы закрываете несвязанный алерт только как ложное срабатывание или как алерт с низким приоритетом. Когда вы закрываете алерт, вам нужно выбрать решение.

  Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый алерт в работу, измените его статус следующим образом: *Закрыт* → *Новый* → *В обработке*.

  Когда вы закрываете алерт, связанное с инцидентом, автоматически удаляется связь с инцидентом. Если алерт, который вы собираетесь закрыть, никому не назначен, он автоматически назначается аналитику, который закрывает алерт.

- **В инциденте.**

  Этот статус означает, что аналитик приостановил работу над инцидентом. Обычно вы меняете статус *Отложен* на *В обработке*, когда работа возобновляется, но также можно изменить статус *Отложен* на другие статусы.

Чтобы изменить статус одного или нескольких алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив алертов, статус которых вы хотите изменить.
   - Перейдите по ссылке с идентификатором алерта, статус которого вы хотите изменить.

     Откроется окно **Детали алерта**.
3. Нажмите на кнопку **Изменить статус**.
4. В панели **Изменить статус** выберите статус, который нужно установить.

   Если вы выбрали статус *Закрыт*, вам нужно выбрать решение.

   Если вы измените статус алерта на *Закрыт* и этот алерт содержит незавершенные плейбуки или действия по реагированию, все связанные плейбуки и действия по реагированию будут прекращены.
5. Нажмите на кнопку **Сохранить**.

Статусы выбранных алертов будут изменены.

Если алерт добавлен на граф расследования, вы также можете изменить статус алерта на графе.

Создание алертов вручную

Вы можете создать алерт вручную из набора событий. Вы можете использовать эту функцию для проверки гипотетического инцидента, который не был обнаружен автоматически.

Если алерт создан вручную, плейбуки не запускаются автоматически. Вы можете запустить плейбук для такого алерта вручную.

Чтобы создать алерт вручную:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Поиск угроз**.
2. Выберите события, для которых вы хотите создать алерт. События должны принадлежать одному тенанту.
3. Нажмите на кнопку **Создать алерт**.

   Откроется окно с созданным алертом. Значение поля **Критичность** соответствует максимальной критичности среди выбранных событий.

Алерты, созданные вручную, имеют пустое значение **Правила** в таблице **Мониторинг и отчеты** → **Алерты**.

Связь алертов с инцидентами

Вы можете связать один или несколько алертов с инцидентом, по следующим причинам:

- Несколько алертов можно интерпретировать как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае алерты в инциденте можно исследовать как отдельную проблему. Вы можете связать с инцидентом до 200 алертов.
- Один алерт может быть связан с инцидентом, если он определен как истинно положительный.

Вы можете связать алерт с инцидентом, если он имеет любой статус отличный от *Закрыт*. Алерт теряет свой текущий статус и приобретает статус *В инциденте* при связывании с инцидентом. Если вы связываете алерты, которые в настоящее время связаны с другими инцидентами, удаляется связь алертов с текущими инцидентами, так как алерт может быть связан только с одним инцидентом.

Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту.

Алерты могут быть связаны с инцидентом вручную или автоматически.

Связывание алертов вручную

Чтобы связать алерты с существующим или новым инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.
2. Установите флажки рядом с событиями, которые требуется связать с инцидентом.
3. Если вы хотите связать алерты с существующим инцидентом:
   a. Нажмите на кнопку **Связать с инцидентом**.
   b. Выберите инцидент, с которым нужно связать алерты.

   Вы также можете нажать на алерт, чтобы отобразить сведения алерта, и нажать на кнопку **Связать с инцидентом** в панели инструментов.
4. Если вы хотите связать алерты с новым инцидентом:
   a. Нажмите на кнопку **Создать инцидент**.
   b. Заполните свойства нового инцидента: имя, исполнитель, приоритет и описание.

   Вы также можете нажать на алерт, чтобы отобразить сведения алерта, и нажать на кнопку **Создать инцидент** в панели инструментов.
5. Нажмите на кнопку **Сохранить**.

Выбранные алерты связаны с существующим или новым инцидентом.

Автоматическая привязка алертов

Если вы хотите, чтобы алерты автоматически связывались с инцидентом, вам нужно настроить правила сегментации.

Удаление связи алертов с инцидентами

Вам может потребоваться удалить связь между алертом и инцидентом, например, если анализ и расследование алертов показали, что алерт не связан с другими алертами в инциденте. При удалении связи алерта с инцидентом Open Single Management Platform выполняет следующие действия:

- Обновляет все данные, связанные с инцидентом, чтобы отразить, что алерт больше не относится к инциденту. Например, вы можете просмотреть изменения в деталях инцидента.
- Сбрасывает статус несвязанных алертов на *Новый*.

Чтобы удалить связь алерта с инцидентом:

1. Откройте детали алерта.
2. Нажмите на кнопку **Удалить связь с инцидентом** в панели инструментов.

   Откроется окно **Удалить связь с алертами**.
3. Если вы хотите сменить исполнителя, выберите **Назначить алерты** и укажите нового исполнителя.

4. Если вы хотите добавить комментарий, укажите его в разделе **Комментарий**. Указанный вами комментарий отображается в столбце **Сведения** в разделе **История**.

Для выбранных алертов удалена связь с инцидентом.

Связывание событий с алертами

Если во время расследования вы обнаружили событие, связанное с исследуемым алертом, вы можете связать это событие с алертом вручную.

Вы можете связать событие с алертом, если он имеет любой статус отличный от **Закрыт**.

Чтобы привязать событие к алерту:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.
2. В списке алертов перейдите по ссылке с идентификатором алерта, с которым вы хотите связать событие.

   Откроется окно **Детали алерта**.
3. Перейдите в раздел **Подробнее** и нажмите на кнопку **Найти в разделе Поиск угроз**.

   Откроется раздел **Поиск угроз**. По умолчанию таблица событий содержит события, связанные с выбранным алертом.

   Таблица событий содержит только события, связанные с тенантами, к которым у вас есть доступ.
4. В верхней части окна откройте первый раскрывающийся список и выберите **Хранилище**.
5. Откройте третий раскрывающийся список и укажите период.

   Вы можете выбрать предопределенные периоды относительно текущей даты и времени и указать необходимый период, используя поля **Начало периода** и **Окончание периода** или выбрав даты в календаре.
6. Нажмите на кнопку **Выполнить запрос**.
7. В обновленном списке событий выберите событие, которое вы хотите связать с алертом и нажмите на **Связать с алертом**.

Выбранные события привязаны к алерту.

Удаление связи событий с алертами

Вам может потребоваться удалить связь между событием и алертом, например, если анализ и расследование событий показали, что событие не связано с алертами.

Чтобы удалить связь события с алертом:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.

2. В списке алертов перейдите по ссылке с идентификатором алерта, для которого вы хотите удалить связь с событием.

   Откроется окно **Детали алерта**.

3. В разделе **Подробнее** выберите события, для которых вы хотите удалить связь, а затем нажмите на кнопку **Удалить связь с алертом**.

Для выбранных событий удалена связь с алертом.

Изменение алертов с использованием плейбуков

Open Single Management Platform позволяет изменять инциденты вручную или с использованием плейбуков. При создании плейбука, вы можете настроить алгоритм плейбука для изменения свойств алерта.

Чтобы изменить алерт с помощью плейбука, вам должна быть присвоена одна из следующих XDR-ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня или Администратор тенанта.

> Вы не можете изменять алерты, которые имеют статус **Закрыт**.

Вы можете изменить следующие свойства алерта с помощью плейбука:

- Исполнитель.
- Статус алерта.
- Комментарий.
- Атрибут ExternalReference.
- Дополнительный атрибут данных.

Примеры выражений, которые вы можете использовать в алгоритме плейбука для изменения свойств алерта:

- **Назначение алерта пользователю**

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignAlert",
 "params": {
 "assignee": {
 "id": "user_ID"
 }
 }
 }
 }
 }
 ]
}
```

Во время изменения исполнителя в алгоритме плейбука отображаются подсказки. Для удобства подсказки содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать исполнителя инцидента, вы можете выполнить поиск соответствующей записи по имени пользователя, и этот идентификатор будет указан в алгоритме.

- Отмена назначения алерта пользователю

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignAlert",
 "params": {
 "assignee": {
 "id": "nobody"
 }
 }
 }
 }
 }
 ]
}
```

- Изменение статуса алерта

Чтобы изменить статус алерта на **В обработке**:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setAlertStatus",
 "params": {
 "status": "inProgress"
 }
 }
 }
 }
 ]
}
```

Чтобы изменить статус алерта на **Закрыт**:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setAlertStatus",
 "params": {
 "status": "closed",
 "statusResolution": "truePositive"
 }
 }
 }
 }
 ]
}
```

Вы также можете указать следующие значения для параметра statusResolution: `falsePositive` и `lowPriority`.

Когда вы изменяете статус алерта в алгоритме плейбука, могут быть отображены следующие подсказки: `new`, `inProgress`, `closed`.

- Добавление комментария к алерту

```
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addCommentToAlert",
 "params": {
 "text": "${ \"New comment for alert with ID: \" + alert.InternalID }"
 }
 }
 }
 }
 ]
}
```

- Изменение атрибута ExternalReference.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setAlertExternalRef",
 "params": {
 "externalRef": "${ \"Appended externalRef for alert with ID: \" + alert.InternalID }",
 "mode": "append"
 }
 }
 }
 }
 ]
}
```

Чтобы заменить текущее значение атрибута ExternalReference в алерте значением из плейбука, укажите значение `replace` для параметра `mode`.

- Изменение Дополнительного атрибута данных.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addAlertAdditionalData",
 "params": {
 "data": "${ {\"customKey_1 (alert.InternalID)\": (\"customValue_1 (\" + alert.InternalID + \")\" )} }",
 "mode": "append"
 }
 }
 }
 }
 ]
}
```

Чтобы заменить текущее значение атрибута AdditionalData в алерте значением из плейбука, укажите значение `replace` для параметра `mode`.

Работа с алертами на графе расследования

На графе расследования вы можете выполнять следующие действия с алертами:

- Добавлять алерт на граф.
- Скрывать алерт с графа.
- Просматривать детали алерта, выбрав соответствующий элемент из контекстного меню узла алерта.
- Изменять статус алерта.
- Просматривать события, связанные с алертом.
- Просматривать активы, связанные с алертом.
- Просматривать наблюдаемые объекты, связанные с алертом.

Добавление алертов на граф расследования

Вы можете добавить алерт на граф расследования одним из следующих способов:

- Из общей таблицы алертов, которая открывается при нажатии на кнопку **Добавить алерт** на графе расследования. Вам нужно установить флажки рядом с алертами, которые вы хотите отобразить на графе расследования, и нажать на кнопку **Показать на графе**.
- Из таблицы похожих алертов.

Чтобы добавить алерты на граф расследования из таблицы похожих алертов:

1. Выполните одно из следующих действий:

- Если на графе расследования у вас есть актив, наблюдаемый объект или правило сегментации, нажмите на его узел, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

- Если на графе расследования у вас есть событие, нажмите на его узел, а затем в контекстном меню выберите пункт **Просмотреть информацию**. В открывшемся окне нажмите на кнопку **Показать на графе** .

- Если на графе расследования у вас есть алерт, нажмите на его узел и в контекстном меню выберите пункт **События**. В таблице событий нажмите на событие, детали которого вы хотите открыть. Если детали события содержат наблюдаемый объект, актив или правило сегментации, нажмите на ссылку в соответствующем поле, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

- На графе расследования нажмите на кнопку **Поиск угроз**, а затем в общей таблице событий нажмите на событие, детали которого вы хотите открыть. Если детали события содержат наблюдаемый объект, актив или правило сегментации, нажмите на ссылку в соответствующем поле, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

Отобразится таблица похожих алертов.

2. Установите флажки рядом с алертами, которые вы хотите отобразить на графе расследования, и нажмите на кнопку **Показать на графе**.

Выбранные алерты будут добавлены на граф расследования.

Скрытие алертов на графе расследования

Вы можете скрыть алерты на графе расследования одним из следующих способов:

- Нажать на узел алерта и в контекстном меню выбрать пункт **Скрыть** .

- С помощью таблицы алертов.

Чтобы скрыть алерты на графе с помощью таблицы алертов:

1. Выполните одно из следующих действий:

   - В панели инструментов в верхней части графа расследования нажмите на кнопку **Добавить алерт**.

   - Если на графе отображаются узлы наблюдаемых объектов, активов или событий, нажмите на узел, для которого вы хотите добавить алерт, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

   Отобразится таблица алертов.

2. Установите флажки рядом с алертами, которые вы хотите скрыть на графе расследования, и нажмите на кнопку **Показать на графе**.

Выбранные алерты и их ссылки будут скрыты на графе расследования. Связанные узлы останутся на графе расследования.

Изменение статуса алерта

Чтобы изменить статус алерта:

1. Нажмите на узел алерта и в контекстном меню выберите пункт **Изменить статус**.
2. В открывшейся панели **Смена статуса**, выберите статус и нажмите на кнопку **Сохранить**.

   Если вы выбрали статус *Закрыт*, вам нужно выбрать решение.

Статусы выбранных алертов будут изменены.

Просмотр событий, связанных с алертом

Чтобы просмотреть события, связанные с алертом, выполните одно из следующих действий:

- Нажмите на цифру рядом с узлом алерта, события которого вы хотите отобразить. Цифра показывает количество событий, связанных с алертом.
- Нажмите на узел алерта, события которого вы хотите отобразить, и в контекстном меню выберите пункт **События**.

Если вы хотите добавить события из таблицы на граф расследования, установите флажки рядом с событиями и нажмите на кнопку **Показать на графе**.

Если вы хотите скрыть события на графе расследования, установите флажки рядом с событиями и нажмите на кнопку **Скрыть на графе**.

Просмотр активов, связанных с алертом

Чтобы просмотреть активы, связанные с алертом, нажмите на узел алерта.

В контекстном меню цифры рядом с элементами **Устройства** и **Пользователи** показывают количество устройств и пользователей, связанных с алертом.

Если вы хотите добавить устройства или пользователей на граф расследования, выберите соответствующий пункт меню.

Просмотр наблюдаемых объектов, связанных с алертом

Чтобы просмотреть наблюдаемые объекты, связанные с алертом, нажмите на узел алерта и в контекстном меню выберите пункт **События**.

В открывшемся меню цифры рядом с элементами показывают количество наблюдаемых объектов, связанных с алертом.

Если вы хотите добавить наблюдаемый объект (например, **Хеш**, **Домен**, **IP-адрес**) на граф расследования, выберите соответствующий пункт меню.

Работа с инцидентами

В этом разделе содержится общая информация об инцидентах, их свойствах, типичном жизненном цикле и связи с алертами. В этом разделе также приведены инструкции по созданию инцидентов, анализу таблицы инцидентов, изменению свойств инцидентов в соответствии с текущим состоянием в жизненном цикле и объединению инцидентов.

Раздел **Инциденты** отображается в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Open Single Management Platform.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Работа с НКЦКИ, Подтверждающий, Наблюдатель.

Об инцидентах

Инцидент – это контейнер обнаружений, который обычно указывает на истинно положительную проблему в ИТ-инфраструктуре организации. Инцидент может содержать один или несколько алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему.

Вы можете создавать инциденты вручную или включить правила автоматического создания инцидентов. После создания инцидента вы можете связать алерты с ним. Вы можете связать с инцидентом до 200 алертов.

После создания инцидентов Open Single Management Platform добавляет их в таблицу инцидентов как объекты, которые должны быть обработаны аналитиками.

Инциденты можно назначить только аналитикам, имеющим право на чтение и изменение алертов и инцидентов.

Вы можете управлять инцидентами как объектами, используя следующие свойства инцидента:

- **Статус инцидента.**

  Статус инцидента показывает текущее состояние инцидента в его жизненном цикле. Вы можете изменить статус по своему усмотрению.

  Поддерживаются две модели статусов инцидентов. Подробности см. в разделе: Изменение статуса инцидента.

- **Уровень важности инцидента.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Уровень важности инцидента показывает, какое влияние этот инцидент может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского". Уровень критичности инцидента соответствует наивысшей степени критичности связанных алертов и не может быть изменена вручную.

- **Приоритет инцидента.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Приоритет инцидентов определяет порядок, в котором инциденты должны расследоваться аналитиками. Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. Вы можете изменить приоритет инцидента вручную.

- **Исполнитель инцидента.**

  Владелец инцидента, аналитик, который отвечает за расследование и обработку инцидента. Вы можете изменить исполнителя инцидента в любое время, если параметр **Статус** не равен **Закрыт**.

Два или более инцидента могут быть интерпретированы как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае вы можете объединить инциденты, чтобы исследовать их как единую проблему.

У каждого инцидента есть *детали инцидента*, которые предоставляют всю информацию, связанную с инцидентом. Вы можете использовать эту информацию для расследования инцидента или объединения инцидентов.

Модель данных инцидента

Структура инцидента представлена полями, которые содержат значения (см. таблицу ниже). Некоторые поля являются объектами или массивами объектов со своим набором полей (например, поля `Assignee` и `Alerts`).

Инцидент

Поле	Тип значения	Требуется	Описание
`InternalID`	Строка	Да	Внутренний идентификатор инцидента (в формате UUID).
`ID`	Целое число	Да	Короткий внутренний идентификатор инцидента.
`TenantID`	Строка	Да	Идентификатор тенанта, с которым связан инцидент (в формате UUID).
`IncidentType`	Объект `IncidentType`	Да	Тип инцидента.
`Name`	Строка	Да	Имя инцидента.
`WorkflowName`	Строка	Да	Имя рабочего процесса инцидента.
`WorkflowUUID`	Строка	Да	Уникальный идентификатор рабочего процесса инцидента в формате UUID.
`Description`	Строка	Нет	Описание инцидента.
`CreatedAt`	Строка	Да	Дата и время создания инцидента (в формате RFC 3339).
`UpdatedAt`	Строка	Да	Дата и время последнего изменения инцидента (в формате RFC 3339).
`StatusChangedAt`	Строка	Нет	Дата и время последнего изменения статуса инцидента (в формате RFC 3339).
`Severity`	Строка	Нет	Критичность инцидента. Возможные значения: • `critical` • `high` • `medium` • `low`
`Priority`	Строка	Да	Приоритет инцидента. Возможные значения:

			• `critical` • `high` • `medium` • `low`
`Assignee`	Объект `Assignee`	Нет	Оператор, которому назначен инцидент.
`FirstEventTime`	Строка	Нет	Дата и время первого события телеметрии алерта, связанного с инцидентом (в формате RFC 3339).
`LastEventTime`	Строка	Нет	Дата и время последнего события телеметрии алерта, связанного с инцидентом (в формате RFC 3339).
`Status`	Строка	Да	Статус инцидента. Возможные значения: • `open` • `inProgress` • `hold` • `closed`
`StatusUUID`	Строка	Да	Идентификатор статуса инцидента (в формате UUID).
`StatusResolution`	Строка	Нет	Решение статуса инцидента. Возможные значения: • `truePositive` • `falsePositive` • `lowPriority` • `merged`
`DetectSources`	Массив строк	Нет	Компоненты, которые обнаруживают и генерируют инцидент.
`DetectionTechnologies`	Массив строк	Нет	Технология срабатывания детектирования.
`Alerts`	Массив объектов `Alert`	Нет	Алерты, включенные в инцидент.
`AdditionalData`	Объект	Нет	Дополнительная информация об алерте в формате JSON. Эту информацию может заполнить пользователь или плейбук.
`ExternalRef`	Строка	Да	Ссылка на объект во внешней системе (например, ссылка на инцидент Jira).
`SignOfCreation`	Строка	Да	Способ создания инцидента.
`IsCII`	Логический оператор	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры.
`Attachments`	Массив объектов `UnkeyedAttachment`	Нет	Вложения, связанные с инцидентом.

IncidentType

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор типа инцидента (в формате UUID).
`Name`	Строка	Да	Имя типа инцидента.
`Description`	Строка	Да	Описание типа инцидента.

Исполнитель

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор учетной записи оператора, которому назначен инцидент.
`Name`	Строка	Да	Имя оператора, которому назначен инцидент.

UnkeyedAttachment

Поле	Тип значения	Требуется	Описание
`AttachmentID`	Строка	Да	Идентификатор вложения (в формате UUID).
`Name`	Строка	Да	Имя вложения.
`CreatedAt`	Строка	Да	Дата и время создания вложения в формате UTC.
`UpdatedAt`	Строка	Да	Дата и время последнего изменения вложения в формате UTC.
`CreatedBy`	Строка	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`Size`	Целое число	Да	Размер вложения, указанный в байтах.
`Status`	Строка	Да	Статус вложения, который указывает, находится ли загрузка вложения в процессе, завершена или прервана с ошибкой. Возможные значения: • `completed` • `error` • `uploading`
`Description`	Строка	Нет	Описание вложения.
`StatusCode`	Строка	Нет	Текст статуса, который отображается пользователю (например, сообщение об ошибке, которое отображается при неудачной попытке загрузки вложения).

Создание инцидентов

Вы можете создавать инциденты вручную или включить правила автоматического создания инцидентов. В этой статье описано, как создавать инциденты вручную.

Чтобы иметь возможность создавать инциденты, у вас должны быть права на чтение и изменение алертов и инцидентов.

Если инцидент создается вручную, плейбуки не запускаются автоматически. Вы можете запустить плейбук для такого инцидента вручную.

Вы можете создавать инциденты с помощью таблицы инцидентов или таблицы алертов.

Создание инцидентов с помощью таблицы инцидентов

Чтобы создать инцидент:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. Нажмите на кнопку **Создать инцидент**.

2. На шаге **Общие параметры** укажите следующие параметры:

   - Имя инцидента.
   - **Тенант**

     Тенант, с которым связан инцидент. Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту. Вы не сможете изменить тенант инцидента позже.

   - **Исполнитель.**

     Владелец инцидента, аналитик, который отвечает за расследование и обработку инцидента. Вы можете изменить исполнителя инцидента в любое время, если параметр **Статус** не равен **Закрыт**.

   - **Приоритет.**

     Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

     Приоритет инцидентов определяет порядок, в котором инциденты должны расследоваться аналитиками. Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. Вы можете изменить приоритет инцидента вручную.

   - **Описание**

     В этом поле вы можете написать описание инцидента. Например, вы можете описать проблему или предоставить результаты расследования связанных алертов. Описание будет добавлено в раздел **Описание** в сведениях об инциденте.

     Поле не является обязательным.

3. Нажмите на кнопку **ОК**.

   Инцидент создан.

Создание инцидентов с помощью таблицы алертов

Вы создаете инцидент, выбирая алерты для связи с новым инцидентом. См. как связать алерты с инцидентами.

Просмотр таблицы инцидентов

В таблице инцидентов представлена информация обо всех созданных инцидентах.

Чтобы просмотреть таблицу инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.

Откроется таблица инцидентов.

2. При необходимости отфильтруйте тенанты. По умолчанию фильтр тенантов выключен и в таблице инцидентов отображаются инциденты, относящиеся ко всем тенантам, к которым у вас есть права доступа. Чтобы применить фильтр для тенантов:

   a. По ссылке рядом с параметром **Фильтр тенантов** откройте список тенантов.

   b. Установите флажки рядом с требуемыми тенантами.

      В таблице инцидентов отобразятся только инциденты, обнаруженные на активах, принадлежащих выбранным тенантам.

Таблица инцидентов содержит следующие столбцы:

- **ID инцидента, имя** – имя и уникальный идентификатор инцидента.
- **Создан** – дата и время создания инцидента.
- **Время обновления** – дата и время последнего изменения в истории инцидента.
- **Продолжительность угрозы** – время между самыми ранними и самыми последними событиями среди всех алертов, связанных с инцидентом.
- **Статус** – текущий статус инцидента.
- **Критичность** – критичность инцидента.
- **Приоритет** – приоритет инцидента.
- **Аналитик** – текущий исполнитель инцидента.
- **Тенант** – имя тенанта, у которого был обнаружен инцидент.
- **Технология** – технологии, зарегистрировавшие алерты, связанные с инцидентом.
- **Затронутые активы** – устройства и пользователи, затронутые инцидентом.
- **Наблюдаемые объекты** – количество обнаруженных артефактов, например IP-адреса или MD5-хеши файлов.
- **Решение** – решение инцидентов со статусом *Закрыт*.
- **Метод создания** – способ создания инцидента, вручную или автоматически.
- **Количество связанных алертов** – количество алертов в инциденте.
- **Правила** – правила, которые сработали для создания инцидента.
- **Количество затронутых активов** – количество устройств и пользователей, затронутых инцидентом или вовлеченных в него.
- **Количество наблюдаемых объектов** – количество наблюдаемых объектов, которые относятся к алертам, связанным с инцидентом.
- **Объект КИИ** – наличие хотя бы одного актива, который включен в инцидент и является объектом критической информационной инфраструктуры (КИИ).

Принимает значение **Да**, если затронутый актив – это объект КИИ первой, второй, третьей категории значимости или объект КИИ без категории значимости. Столбец доступен для отображения, если лицензия приложения включает модуль ГосСОПКА.

Экспорт информации инцидентов

Вы можете экспортировать информацию обо всех инцидентах, которые отображаются в таблице инцидентов в файл JSON. Это может потребоваться, когда вам нужно будет предоставить эту информацию третьим сторонам.

Чтобы экспортировать информацию инцидентов вам нужно иметь одну из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Работа с НКЦКИ, Подтверждающий, Наблюдатель.

Чтобы экспортировать информацию об инцидентах:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.

   Отобразится таблица инцидентов.

2. Если необходимо группировать и фильтровать данные в таблице следующим образом:

   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.
   - Нажмите на значок параметров ( ) и выберите столбцы для отображения в таблице.

   Отобразится таблица отфильтрованных инцидентов.

3. Нажмите на кнопку **Экспортировать**.

4. В открывшемся окне выберите папку, в которую вы хотите сохранить файл JSON, и нажмите на кнопку **Сохранить**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Просмотр сведений об инциденте

Сведения об инциденте – это страница в интерфейсе, которая содержит всю информацию, относящуюся к инциденту, включая свойства инцидента.

Чтобы просмотреть сведения об инциденте:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инцидент**ы.

2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

Откроется окно со сведениями об инциденте.

Панель инструментов в верхней части информации об инциденте позволяет выполнять следующие действия:

- Измените значения полей **Имя**, **Описание** и **Внешняя ссылка**
- Назначить инцидент аналитику
- Изменить статус инцидента
- Изменить приоритет инцидента
- Связать алерты с инцидентом
- Объединить инцидент с другими инцидентами
- Открыть граф расследования
- Выбрать плейбук

Сведения об инциденте содержат следующие разделы:

- **Сводная информация**

Этот раздел содержит следующие свойства инцидента:

- **Тип**. Тип инцидента.
- **Аналитик**. Текущий исполнитель инцидента.
- **Метод создания**. Как был создан инцидент, вручную или автоматически.
- **Имя**. Имя, указанное при создании инцидента. Вы можете нажать на кнопку **Изменить**, чтобы изменить название инцидента.
- **Тенант**. Имя тенанта, у которого был обнаружен инцидент.
- **Связанные тенанты**. Имена тенантов, алерты которых связаны с инцидентом.
- **Активы**. Количество пользователей и устройств, которые были затронуты инцидентом.
- **Зарегистрировано**. Дата и время создания инцидента.
- **Время обновления**. Дата и время последнего изменения в истории инцидента.
- **Первое событие**. Дата и время первого события, связанного с инцидентом. Это самое раннее событие в разделе Детали алерта среди всех алертов, связанных с инцидентом.
- **Последнее событие.** Дата и время последнего события, связанного с инцидентом. Это последнее событие в разделе Детали алерта среди всех алертов, связанных с инцидентом.
- **Описание.** Описание инцидента. Вы можете нажать на кнопку **Изменить**, чтобы добавить описание.
- **Внешняя ссылка.** Ссылка на объект во внешней системе. Вы можете нажать на кнопку **Изменить**, чтобы указать внешнюю ссылку.
- **Приоритет**. Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критический**. Приоритет инцидентов определяет порядок, в котором инциденты могут расследоваться. Инциденты с приоритетом **Критический** являются наиболее важными и могут быть расследованы в первую очередь. Вы можете изменить приоритет, нажав на текущее значение приоритета.
- **Критичность**. Возможные значения: **Низкий**, **Средний** или **Высокий**. Уровень важности инцидента показывает, какое влияние этот инцидент может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского".
- **Правила**. Правила, которые сработали для регистрации связанных алертов. Вы можете нажать на значок с многоточием рядом с названием правила, чтобы открыть контекстное меню. Используйте это меню, чтобы узнать больше о правиле, найти алерты или инциденты, которые были зарегистрированы этим же правилом, или найти события, инициировавшие правило, в разделе **Поиск угроз** за период между первым и последним событием инцидента.
- **Технология**. Список технологий, зарегистрировавших алерты, связанные с инцидентом.
- **Тактика MITRE**. Тактика или несколько тактик, зарегистрированных в алертах, связанных с инцидентом. Тактика определена в базе знаний MITRE ATT&CK.
- **Техника MITRE**. Техника или несколько техник, зарегистрированных в алертах, связанных с инцидентом. Методы определены в базе знаний MITRE ATT&CK.

- **Extra**. Дополнительная информация об инциденте.

- Подробная информация

  В разделе **Подробнее** вы можете отслеживать события телеметрии, связанные с инцидентом.

  Чтобы просмотреть события, связанные с инцидентом, нажмите на кнопку **Поиск угроз**. В открывшейся таблице отобразятся события алерта, связанные с инцидентом.

  Панель инструментов таблицы событий позволяет выполнить следующие действия:

  - Скачать события. Нажмите на кнопку **TSV**, чтобы скачать информацию о связанных событиях из файла TSV.

  - **Удалить связь с инцидентом**. Выберите событие или несколько событий в таблице и нажмите на эту кнопку, чтобы удалить связь выбранных событий с алертом, связанным с инцидентом.

  Вы можете вернуться к деталям инцидента, нажав на кнопку **Исследование инцидента** или на кнопку **Назад** в вашем браузере.

- Подобные инциденты

В разделе **Подобные инциденты** вы можете просмотреть список инцидентов, которые имеют те же затронутые артефакты, что и текущий инцидент. Затронутые артефакты включают как наблюдаемые объекты, так и затронутые устройства алертов, связанных с инцидентом. В списке есть инциденты во всех статусах.

С помощью вы можете оценить степень сходства текущего инцидента и других инцидентов. Сходство рассчитывается следующим образом:

Сходство = M / T * 100

Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном инциденте, "T" – общее количество артефактов в текущем инциденте.

Если сходство составляет 100%, в текущем инциденте нет ничего нового по сравнению с аналогичным инцидентом. Если сходство равно 0%, текущий инцидент и схожий инцидент полностью различаются. Инциденты, имеющие сходство 0%, не включаются в список.

Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

При нажатии на идентификатор инцидента открывается подробная информация об инциденте.

Настройка списка похожих инцидентов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте инциденты, выбрав период, за который были обновлены инциденты. По умолчанию список содержит инциденты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать инциденты в порядке возрастания или убывания.

- **Алерты**

В разделе **Алерты** вы можете просмотреть список алертов, связанных с текущим инцидентом.

Нажав на идентификатор алерта, вы можете открыть детали алерта. Вы также можете использовать кнопки панели инструментов, чтобы удалить связь алерта с инцидентом.

- **Активы**

В разделе **Активы** вы можете просмотреть устройства и пользователей, затронутых или вовлеченных в инцидент.

Таблица активов содержит следующие столбцы:

- **Тип актива.**

  Возможные значения: устройство или пользователь.

- **Имя актива.**

- **Идентификатор актива.**

- **Имеет признаки.**

  Возможные значения: атакующий или атакуемый.

- **Статус авторизации.**

  Этот параметр применяется только к типу актива – устройство. Статус авторизации устройства определяется KICS for Networks. Вы можете изменить статус авторизации, применив соответствующее действие по реагированию к устройству.

- **Сервер администрирования.**

  Сервер администрирования, который управляет устройством.

- **Группа администрирования.**

  Группа администрирования, к которой принадлежит пользователь.

- **Категории.**

  Категории активов, в которые входит актив.

- **Категория КИИ.**

  Информация о том, является ли актив объектом критической информационной инфраструктуры (КИИ). Столбец доступен для отображения, если лицензия приложения включает модуль ГосСОПКА и если вам назначена одна из следующих ролей XDR: Доступ к объектам КИИ, Главный администратор.

  Возможные значения:

  - Объект КИИ первой категории значимости.
  - Объект КИИ второй категории значимости.
  - Объект КИИ третьей категории значимости.
  - Объект КИИ без категории значимости.
  - Информационный ресурс не является объектом КИИ.

Нажав на имя пользователя или устройства, вы можете:

- Выполнить поиск по имени пользователя или идентификатору устройства в разделе **Поиск угроз** за период между первым и последним событием инцидента.
- Выполнить поиск по имени пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по имени пользователя или идентификатору устройства в других инцидентах.
- Скопировать имя пользователя или имя устройства в буфер обмена.

Вы также можете нажать на имя устройства, чтобы открыть свойства устройства.

Нажав на идентификатор пользователя или идентификатор устройства, вы можете:

- Выполнить поиск по идентификатору пользователя или идентификатору устройства в разделе **Поиск угроз** за период между первым и последним событием инцидента.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других инцидентах.
- Скопировать идентификатор пользователя или идентификатор устройства в буфер обмена.

Вы также можете нажать на идентификатор устройства, чтобы открыть его свойства.

- Наблюдаемые объекты

В разделе **Наблюдаемые объекты** вы можете просмотреть наблюдаемые объекты, которые относятся к алертам, связанными с текущим инцидентом. Наблюдаемые объекты могут включать:

- MD5-хеш
- IP-адрес
- URL
- Имя домена
- SHA256
- UserName
- HostName

Нажав на ссылку в столбце **Значение**, вы можете:

- Поиск наблюдаемого значения в разделе **Поиск угроз** за период между первым и последним событием инцидента.
- Выполнить поиск по значению наблюдаемого объекта в Kaspersky Threat Intelligence Portal (открывается в новой вкладке браузера).
- Выполнить поиск по значению наблюдаемого объекта в других алертах.
- Выполнить поиск по значению наблюдаемого объекта в других инцидентах.
- Скопировать значение наблюдаемого объекта в буфер обмена.

Панель инструментов этого раздела содержит следующие кнопки:

- **Запросить статусы Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию о выбранном наблюдаемом объекте в Kaspersky Threat Intelligence Portal (Kaspersky TIP). В результате информация обновляется в столбце **Статус обновления**. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Обогатить данные Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию обо всех перечисленных наблюдаемых объектах из Kaspersky TIP. В результате информация обновляется в столбце **Обогащение**. Используйте ссылку в столбце **Обогащение**, чтобы открыть полученные сведения об обогащении наблюдаемого объекта. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Поместить на карантин**. Используйте эту кнопку, чтобы переместить устройство, на котором находится файл, на карантин. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Добавить правило запрета**. Используйте эту кнопку, чтобы добавить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Удалить правило запрета**. Используйте эту кнопку, чтобы удалить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
- **Прервать процесс**. Используйте эту кнопку, чтобы прервать процессы, связанные с файлом. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.

- История

В разделе **История журнала событий** вы можете отслеживать изменения, внесенные в инцидент как в объект:

- Изменение статуса инцидента.
- Изменение исполнителя инцидента.
- Связь алерта с инцидентом.
- Удаление связи алерта с инцидентом.
- Объединение инцидента с другими инцидентами.

В разделе **История реагирований** вы можете просмотреть действия по реагированию, выполненные вручную, а также действия, выполненные в рамках плейбука. Таблица содержит следующие столбцы:

- **Время**. Время возникновения события.
- **Запущено**. Имя пользователя, запустившего действие по реагированию.
- **События**. Описание события.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.
- **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
- **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
  - **В обработке** – действие по реагированию выполняется.
  - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию завершено с предупреждениями.
  - **Ошибка** – действие по реагированию завершено с ошибками.
  - **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.
- **Плейбук**. Имя плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.

- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

- **Комментарии**

  В разделе **Комментарии** вы можете оставлять комментарии, связанные с инцидентом. Например, вы можете написать комментарий о результатах расследования или при изменении свойств инцидента, таких как исполнитель или статус инцидента.

  Вы можете изменять или удалять свои комментарии. Комментарии других пользователей невозможно изменить или удалить.

  Чтобы сохранить комментарий, нажмите на клавишу **`Enter`**. Чтобы начать новую строку, нажмите на клавиши **`Shift + Enter`**. Чтобы изменить или удалить свой комментарий, используйте кнопки в правом верхнем углу.

  Для возможности оставлять комментарии требуется право на **Запись** в функциональной области **Алерты и инциденты**.

Назначение инцидентов аналитикам

Как объект, инцидент должен быть передан аналитику SOC для проверки и возможного расследования. Вы можете изменить статус инцидента в любое время.

Инциденты можно назначить только аналитикам, имеющим право на чтение и изменение алертов и инцидентов.

Чтобы назначить аналитику инциденты:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Установите флажки рядом с инцидентами, которые требуется назначить аналитику.

   Вам нужно выбрать только инциденты, обнаруженные в одном тенанте. Иначе кнопка **Назначить** будет неактивна.

   Кроме того, вы можете назначить инцидент аналитику из деталей инцидента. Чтобы открыть детали инцидента, нажмите на ссылку с идентификатором инцидента.
3. Нажмите на кнопку **Назначить**.
4. В открывшемся окне **Назначить аналитику** начните вводить имя аналитика или электронную почту, а затем выберите аналитика из списка.

   Вы также можете выбрать вариант **Не назначен**.
5. Нажмите на кнопку **Назначить**.

Инциденты назначены аналитику.

Изменение статуса инцидента

Как объект, инцидент имеет статус, который показывает текущее состояние инцидента в его жизненном цикле.

Вы можете изменять статус для своих инцидентов или инцидентов других аналитиков, только если у вас есть право **Запись** в функциональной области алертов и инцидентов. Для закрытия инцидента требуется право **Закрытие** в функциональной области алертов и инцидентов.

Если статус инцидента изменен вручную, плейбуки не будут запускаться автоматически. Вы можете запустить плейбук для такого инцидента вручную.

Поддерживаются две модели статусов инцидентов:

a. Стандартная:

- **Новый**

  Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *В обработке* или *Закрыт*. Когда вы меняете статус *Новый* на *В обработке*, инцидент назначается вам автоматически. Когда вы меняете статус *Новый* на *Закрыт* и у инцидента нет исполнителя, он автоматически назначается вам.

- **В обработке**

  Этот статус означает, что аналитик начал работу над инцидентом или возобновил работу, изменив статус *Отложен*. Когда вы устанавливаете статус *В обработке*, инцидент назначается вам автоматически. Изменить статус *В обработке* можно на любой другой.

- **Отложен**

  Этот статус означает, что аналитик приостановил работу над инцидентом. Обычно вы меняете статус *Отложен* на *В обработке*, когда работа возобновляется, но также можно изменить статус *Отложен* на другие статусы.

- **Закрыт**

  Вы закрываете инциденты, когда не требуется никакой дополнительной работы над инцидентом. Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

  При закрытии инцидента, связанные обнаружения также получают статус *Закрыто* и наследуют решение инцидента. Если у инцидента нет исполнителя, закрытый инцидент автоматически назначается вам. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

  Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый инцидент в работу, измените его статус следующим образом: *Закрыт* → *Новый* → *В обработке*.

b. Совместимая с ГОСТ:

- **Новый**

  Когда вы создаете инцидент или он создается автоматически, инцидент имеет статус *Новый*. Вы можете изменить статус инцидента на *Анализ*. Когда вы меняете статус *Новый* на *Анализ*, инцидент назначается вам автоматически.

- **Анализ**

  Этот статус означает, что аналитик начал работу над инцидентом и проводит первичный анализ и определение вовлеченных в инцидент элементов информационной инфраструктуры.

  Вы можете изменить статус инцидента на *Локализация* или *Выполнен*.

- **Локализация**

  Этот статус означает, что выполняется меры по предотвращению дальнейшего распространения инцидента.

  Вы можете изменить статус инцидента на *Последствия* или *Выполнен*.

- **Последствия**

  Этот статус означает, что выполняется выявление последствий инцидента на вовлеченные в него элементы информационной инфраструктуры.

  Вы можете изменить статус инцидента на *Ликвидация* или *Выполнен*.

- **Ликвидация**

  Этот статус означает, что выполняется устранение последствий инцидента.

  Вы можете изменить статус инцидента на *Выполнен*.

- **Выполнен**

  Этот статус означает, что проводится оценка полноты выполненных действий на этапах *Анализ*, *Локализация*, *Последствия* и *Ликвидация*.

  Вы можете изменить статус инцидента на *Закрыт*, *Анализ*, *Локализация*, *Последствия*, *Ликвидация*.

- **Закрыт**

Вы можете закрыть инцидент, по которому принято одно из следующих решений:

- Верное срабатывание.
- Ложное срабатывание.
- Низкий приоритет.

При закрытии инцидента, связанные обнаружения также получают статус *Закрыт* и наследуют решение инцидента. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

Чтобы сменить модель статусов на совместимую с ГОСТ:

1. В файле docker/compose/osmp.yaml укажите значение переменной окружения OSMP_WORKFLOW_ID.
   OSMP_WORKFLOW_ID: "gost"
2. В файле /plugins/irp/.env укажите значение переменной FEATURE_GOST_STATUS.
   FEATURE_GOST_STATUS=true

Статусы инцидентов не конвертируются при смене модели статуса. Не рекомендуется менять модель статусов, если у вас есть активные инциденты.

Чтобы изменить статус одного или нескольких инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив инцидентов, которым требуется изменить статус.
   - Перейдите по ссылке с идентификатором инцидента, статус которого вы хотите изменить.
     Откроется окно **Сведения об инциденте**.
3. Нажмите на кнопку **Изменить статус**.
4. В панели **Изменить статус** выберите статус, который нужно установить.
   Если вы выберете статус **Закрыт**, вам нужно выбрать решение и написать короткий комментарий.

   Если вы измените статус инцидента на *Закрыт* и этот инцидент содержит незавершенные плейбуки или действия по реагированию, все связанные плейбуки и действия по реагированию будут прекращены.
5. Оставьте комментарий (необязательно).
6. Нажмите на кнопку **Сохранить**.

Статусы выбранных инцидентов будут изменены.

Изменение приоритета инцидента

Как объект, инцидент имеет приоритет, который определяет порядок, в котором инцидент должен расследоваться аналитиками. Вы можете изменить приоритет инцидента вручную.

Вы можете изменять приоритеты инцидентов для своих инцидентов или инцидентов других аналитиков, только если у вас есть право доступа на чтение и изменение алертов и инцидентов.

Инцидент может иметь один из следующих приоритетов:

- **Низкий.**
- **Средний** (значение по умолчанию).
- **Высокий.**
- **Предельный.**

Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. **Низкий** приоритет обычно означает, что инцидент помещен в очередь. Вы можете определить свои собственные критерии того, какой приоритет должен быть установлен для какого инцидента.

Чтобы изменить приоритет инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив инцидентов, которым требуется изменить приоритет.
   - Нажмите на идентификатор инцидента, чтобы открыть сведения об инциденте, приоритет которого вы хотите изменить.
3. Нажмите на кнопку **Изменить приоритет**.
4. В окне **Изменить приоритет** выберите приоритет, который нужно установить.
5. Нажмите на кнопку **Сохранить**.

   Приоритеты выбранных инцидентов будут изменены.

Объединение инцидентов

Два или более инцидента могут быть интерпретированы как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае вы можете объединить инциденты, чтобы исследовать их как единую проблему.

Когда вы объединяете инциденты, вам нужно выбрать среди них целевой инцидент. После объединения инцидента проблему необходимо исследовать в рамках целевого инцидента. Целевой инцидент должен иметь статус, отличный от статуса *Закрытый*. Остальные инциденты объединяются в целевой и после объединения получают статус *Закрытый* и решение **Объединено**.

Все алерты, связанные с объединенными инцидентами, автоматически связываются с целевым инцидентом. Так как у инцидента не может быть более 200 связанных алертов, приложение считает алерты, связанные с инцидентами, которые вы хотите объединить. Если общее количество связанных алертов превышает 200, выбранные инциденты не могут быть объединены.

Чтобы объединить инциденты из таблицы инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Установите флажки рядом с инцидентами, которые требуется объединить в целевой инцидент. На первом шаге мастера нужно будет выбрать целевой инцидент.
3. Нажмите на кнопку **Объединить инциденты**.

   Откроется мастер **объединения инцидентов**.
4. Выберите целевой инцидент.
5. Нажмите на кнопку **OK**.

Инциденты объединены.

Чтобы объединить инциденты с использованием сведений об инциденте:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. Нажмите на идентификатор инцидента, чтобы открыть сведения об инциденте. Этот инцидент будет объединен с целевым инцидентом. На первом шаге мастера нужно будет выбрать целевой инцидент.
3. Нажмите на кнопку **Объединить инциденты**.

   Откроется мастер **объединения инцидентов**.
4. Выберите целевой инцидент.
5. Нажмите на кнопку **OK**.

Инциденты объединены.

Изменение инцидентов с использованием плейбуков

Open Single Management Platform позволяет изменять инциденты вручную или с использованием плейбуков. При создании плейбука, вы можете настроить алгоритм плейбука для изменения свойств инцидента.

Чтобы изменить инцидент с помощью плейбука, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня или Администратор тенанта.

Вы не можете изменять инциденты, которые имеют статус **Закрыт**.

Вы можете изменить следующие свойства инцидента с помощью плейбука:

- Исполнитель.
- Статус рабочего процесса инцидента.
- Тип инцидента.
- Комментарий.
- Описание.
- Приоритет.
- Атрибут ExternalReference.
- Дополнительный атрибут данных.

Примеры выражений, которые вы можете использовать в алгоритме плейбука для изменения свойств инцидента:

- **Назначение инцидента пользователю.**

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignIncidentToUser",
 "params": {
 "assignee": {
 "id": "user_ID"
 }
 }
 }
 }
 }
 ]
}
```

Во время изменения исполнителя в алгоритме плейбука отображаются подсказки. Для удобства подсказки содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать исполнителя инцидента, вы можете выполнить поиск соответствующей записи по имени пользователя, и этот идентификатор будет указан в алгоритме.

- **Отмена назначения инцидента пользователю**

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignIncidentToUser",
 "params": {
 "assignee": {
 "id": "nobody"
 }
 }
 }
 }
 }
 ]
}
```

- Изменение статуса рабочего процесса инцидента.

Чтобы изменить статус рабочего процесса инцидента на **Открыт**:

```
{
"dslSpecVersion": "1.1.0",
"version": "1",
"actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentStatus",
 "params": {
 "typeId": "af9dd279-fc30-4596-963b-942f79920375",
 "statusId": "4db36105-5223-4078-b72c-e9e9983b0987"
 }
 }
 }
 }
 ]
}
```

Чтобы изменить статус рабочего процесса инцидента на **Закрыт**:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentStatus",
 "params": {
 "statusId": "INCIDENT_STATUS_ID",
 "statusResolution": "truePositive"
 }
 }
 }
 }
 ]
}
```

Вы также можете указать следующие значения для параметра `statusResolution`: `falsePositive` и `lowPriority`.

Чтобы изменить статус рабочего процесса инцидента на пользовательский статус:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentStatus",
 "params": {
 "typeId": "22222222-2222-2222-2222-222222222222",
 "statusId": "11111111-1111-1111-1111-111111111111"
 }
 }
 }
 }
 ]
}
```

Во время изменения статуса рабочего процесса инцидента в алгоритме плейбука отображаются подсказки. Для удобства предложения содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать статус рабочего процесса инцидента, вы можете выполнить поиск соответствующей записи по названию, и этот идентификатор будет указан в алгоритме.

- Изменение типа инцидента.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentType",
 "params": {
 "id": "INCIDENT_TYPE_UUID"
 }
 }
 }
 }
 ]
}
```

Во время изменения типа инцидента в алгоритме плейбука отображаются подсказки. Для удобства предложения содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать тип инцидента, вы можете выполнить поиск соответствующей записи по названию, и этот идентификатор будет указан в алгоритме.

- Добавление комментария к инциденту.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addCommentToIncident",
 "params": {
 "text": "${ \"Новый комментарий к инциденту с идентификатором: \\(incident.ID)\" }"
 }
 }
 }
 }
 ]
}
```

- Изменение описания инцидента.

```
{
"dslSpecVersion": "1.1.0",
"version": "1",
"actionsSpecVersion": "1",
"executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentDescription",
 "params": {
 "description": "${ incident.ID | tostring | \"New comment for incident with ID: \" + . }",
 "mode": "replace"
 }
 }
 }
 }
 ]
}
```

Чтобы дополнить существующее описание, укажите значение `append` для параметра `mode`.

- Изменение приоритета инцидента.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentPriority",
 "params": {
 "priority": "critical"
 }
 }
 }
 }
 ]
}
```

Вы также можете указать следующие значения для параметра `priority`: `high`, `medium`, `low`.

- Изменение атрибута ExternalReference.

```
{
"dslSpecVersion": "1.1.0",
"version": "1",
"actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentExternalRef",
 "params": {
 "externalRef": "${ \"новое значение extReference\" }",
 "mode": "replace"
 }
 }
 }
 }
 ]
}
```

Чтобы дополнить атрибут ExternalReference, укажите значение `append` для параметра `mode`.

- Изменение Дополнительного атрибута данных.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addIncidentAdditionalData",
 "params": {
 "data": "${ {\"customKey\": \"customValue\"} }",
 "mode": "replace"
 }
 }
 }
 }
 ]
}
```

Чтобы дополнить Дополнительный атрибут данных, укажите значение `append` для параметра `mode`.

Граф расследования

Граф расследования – это инструмент визуального анализа, который показывает связь между следующими объектами:

- события;
- алерты;
- инциденты;

- наблюдаемые объекты;
- активы (устройства);
- правила сегментации.

На графе отображается подробная информация об инциденте: соответствующие алерты и их общие свойства.

Чтобы открыть граф расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.
3. Нажмите на кнопку **Посмотреть на графе**.

Для просмотра графа требуется право на **Запись** в функциональной области **Алерты и инциденты**.
Для просмотра на графе сведений об активе, который является объектом КИИ, пользователю необходимо назначить роль **Доступ к объектам КИИ**.
Дополнительную информацию см. в статье Предопределенные роли пользователей.

Вы можете использовать панорамное отображение и масштабирование в правом нижнем углу для навигации по сложному графу.

Взаимодействие с узлами графа

Вы можете использовать панель инструментов вверху, чтобы добавлять алерты и наблюдаемые объекты.

Вы можете нажать и перетащить узлы графа, чтобы переставить их.

Вы можете нажать на узел графа, чтобы открыть контекстное меню.

Общие пункты контекстного меню:

- **Просмотреть информацию**.

  Открывает окно свойств выбранного узла.
- **Копировать**.

  Копирует значение узла в буфер обмена.
- **Скрыть**.

  Удаляет выбранный узел из графа.

Пункты контекстного меню, специфичные для событий:

- **Дерево процессов**.

  Доступно только для определенных типов событий. Создает дерево процессов для события. Индикация события синим цветом указывает на то, что вы можете сгенерировать дерево процессов для этого события.

Пункты контекстного меню, специфичные для алертов:

- **Изменить статус**.

  Вызывает панель **Изменения статуса**, которая позволяет изменить статус алерта.

- **Наблюдаемые объекты**.

  Меню, которое позволяет добавлять общие наблюдаемые объекты в качестве узлов графа.

- **Устройства**.

  Меню, которое позволяет добавлять общие устройства в качестве узлов графа.

Пункты контекстного меню, специфичные для наблюдаемых объектов:

- **Найти похожие события**.

  Вызывает панель **Поиск угроз**, на которой отображаются похожие события.

- **Найти похожие алерты**.

  Вызывает панель **Алерты**, на которой отображаются похожие алерты.

- **Запросить статусы Kaspersky TIP**.

  Позволяет вам получать подробную информацию о выбранном наблюдаемом объекте в Kaspersky Threat Intelligence Portal (Kaspersky TIP). Подробнее см. в разделе Интеграция с Kaspersky Threat Intelligence Portal.

- **Обогатить данные Kaspersky TIP**.

  Используйте эту кнопку, чтобы получить подробную информацию о выбранном наблюдаемом объекте в Kaspersky TIP. Подробнее см. в разделе Интеграция с Kaspersky Threat Intelligence Portal.

Правила сегментации, специфичные для объектов:

- **Просмотреть сведения в KUMA**.

  Открывает Консоль KUMA в новой вкладке браузера, на которой отображаются сведения о правиле.

- **Найти похожие алерты**.

  Вызывает панель **Алерты**, на которой отображаются похожие алерты.

Если вы попытаетесь добавить алерт для другого тенанта, он не будет отображаться на графе расследования.

Вы также можете добавить наблюдаемые объекты, нажав на алерт или событие. Для этого в открывшемся контекстном меню вам нужно выбрать **Наблюдаемые объекты** и нажать на наблюдаемый объект. Объект будет добавлен в граф расследования. При необходимости вы можете удалить объект с графа расследования. Для этого вам нужно нажать на наблюдаемый объект и в открывшемся контекстном меню нажать на кнопку **Скрыть**.

Группировка элементов графа

Граф расследования автоматически группирует алерты с общими параметрами.

Чтобы разгруппировать алерт:

1. Нажмите на элемент графа, соответствующий группе алертов.

   Отобразится таблица со списком алертов.

2. Выберите алерт, который вы хотите отобразить на графе.

3. Нажмите на кнопку **Показать на графе** в панели инструментов таблицы.

   Алерт будет добавлен в виде узла графа.

4. Если вы хотите скрыть алерт, нажмите на кнопку **Скрыть на графе**.

Связывание элементов графа

Граф расследования автоматически создает ссылки для новых элементов, если это применимо. Ссылки можно добавлять вручную.

Чтобы добавить ссылку вручную:

1. Нажмите на кнопку **Связать узлы**.

   Вокруг узлов графа появятся точки соединения.

2. Нажмите на элемент и перетащите его от точки привязки одного узла к точке привязки другого узла.

Ссылки, созданные вручную, имеют цветовую индикацию.

Поиск угроз

Вы можете провести анализ событий для поиска угроз и уязвимостей, которые не были обнаружены автоматически. Для этого вам нужно нажать на кнопку **Поиск угроз** в панели инструментов вверху или открыть контекстное меню узла графа и выбрать пункт **События** или **Найти похожие события**. Откроется панель **Поиск угроз**. Подробнее см. в статье Поиск угроз.

Экспорт графа

При необходимости вы можете сохранить граф в формате SVG. Для этого вам нужно нажать на кнопку **Экспортировать** в панели инструментов вверху.

Правила сегментации

Правила сегментации позволяют автоматически разделять связанные алерты на отдельные инциденты в зависимости от заданных условий.

Вы можете использовать правила сегментации для создания отдельных инцидентов на основе связанных алертов. Например, вы можете объединить несколько алертов с важной отличительной чертой в отдельный инцидент.

Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту.

Когда вы пишете выражение jq при создании правила сегментации, может появиться ошибка о недопустимом выражении, хотя выражение является корректным. Эта ошибка не блокирует создание правила сегментации. Это известная ошибка.

Чтобы создать правило сегментации:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на тенант, для которого вы хотите создать правило сегментации.
3. На вкладке **Параметры** выберите раздел **Правила сегментации**.
4. Нажмите на кнопку **Создать**.

   Откроется окно **Правило сегментации**.
5. Укажите параметры правила сегментации:

   - **Статус**.

     Включите или выключите правило.
   - **Имя правила**.

     Укажите уникальное имя правила. Имя должно содержать от 1 до 255 символов Юникода.
   - **Максимальное количество алертов в инциденте**.

     Максимальное количество алертов в одном инциденте. Если количество алертов превышает указанное значение, создается другой инцидент.
   - **Минимальное количество алертов в инциденте**.

     Минимальное количество алертов в одном инциденте. Если количество алертов не достигает указанного значения, инцидент не создается.
   - **Имя инцидента (шаблон)**.

     Выражение jq, определяющее шаблон наименований инцидентов, созданных в соответствии с этим правилом сегментации.

     Пример: `"Malware Detected with MD5 \(.Observables[] | select(.Type == "md5") | .Value)"`
   - **Интервал поиска**.

     Период, из которого следует выбирать алерты и инциденты.
   - **Описание**.

     Описание правила (необязательный параметр).
   - **Триггер**.

     Выражение jq, определяющее условие включения алертов в инцидент.

     Пример: `.Rules[].Name | . == "R077_02_KSC. Malware detected"`

     Вы также можете добавить условие включения в инцидент только тех алертов, которые содержат объекты КИИ заданных категорий.

     Пример: `any(.Assets[]?.CIICategory; . == "ciiWithoutCategory" or . == "ciiFirstCategory" or . == "ciiSecondCategory" or . == "ciiThirdCategory")`

- **Группы**.

  Выражение jq, определяющее массив строковых идентификаторов, по которым алерты назначаются инцидентам.

  Пример: `[.Observables[] | select(.Type == "md5") | .Value ]`

6. Нажмите на кнопку **Сохранить**.

Правило сегментации сохранится и отобразится в таблице правил. При необходимости вы можете изменить правило, нажав на его имя в таблице.

Правила сегментации располагаются в таблице в порядке убывания приоритета.

Когда алерт создан, он проверяется всеми активными правилами сегментации из таблицы в соответствие с приоритетом правил. После срабатывания первого подходящего правила формируется массив строковых идентификаторов для алерта и начинается поиск инцидента, в который будет включен алерт.

Правило сегментации срабатывает, если выражение jq, которое вы указали в триггере, возвращает `true`.

Невозможно связать алерт с инцидентом, созданным вручную.

Инцидент также имеет массив, который состоит из массивов алертов, связанных с этим инцидентом. Если в массиве алерта, для которого сработало правило сегментации, есть хотя бы один элемент, совпадающий с каким-либо из элементов массива инцидента, то алерт связывается с инцидентом. В результате массив этого алерта добавляется в массив инцидента.

Если есть несколько инцидентов с совпадающими элементами в массиве, алерт соединяется с инцидентом, у которого самое позднее время обновления. Если нет инцидентов с совпадающими элементами в массиве, создается инцидент.

Когда инцидент новый, его массив пустой. Такой инцидент принимает массив алерта, который к нему присоединяется.

Копирование правил сегментации в другой тенант

Вы можете скопировать существующее правило сегментации другому тенанту.

Когда создается дочерний тенант, он автоматически копирует все правила сегментации из родительского тенанта. Изменение правил сегментации в родительском тенанте не влияет на уже созданные дочерние тенанты.

Чтобы скопировать правила сегментации:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на тенант с правилом сегментации, которое вы хотите скопировать.
3. На вкладке **Параметры** выберите раздел **Правила сегментации**.

4. Выберите правила сегментации, которые вы хотите скопировать, и нажмите на кнопку **Копировать в тенант**.

5. Выберите один или несколько целевых тенантов и нажмите на кнопку **Копировать**.

   Если целевой тенант содержит правило сегментации с таким же именем, откроется окно **Перезаписать или переименовать правила сегментации?**. Нажмите кнопку **Перезаписать**, чтобы удалить ранее созданное правило для целевого тенанта и заменить его правилом, которое вы хотите скопировать. Нажмите **Копировать и переименовать**, чтобы сохранить ранее созданное правило и скопировать указанное правило с добавлением `(copy)` к его заголовку.

Управление типами инцидентов

Open Single Management Platform позволяет управлять инцидентами и настраивать процесс обработки инцидентов с помощью типов инцидентов.

Тип инцидента – это набор атрибутов, для которых вы можете настроить различные процессы, например, назначить рабочий процесс для типа инцидента, настроить триггер или алгоритм плейбука.

Вы можете создать тип инцидента или использовать предустановленные типы инцидентов, которые вы можете настроить.

Типы инцидентов могут быть активными или неактивными. Если тип инцидента активен, вы можете выбрать этот тип в окне с подробной информацией об инциденте.

Тип инцидента, отмеченный как тип по умолчанию, автоматически назначается всем новым инцидентам. Вы не можете переключить тип инцидента по умолчанию в неактивный.

Тип инцидента **Общий** установлен как значение по умолчанию. Вы можете изменить этот параметр.

В тенанте вы можете создать только один тип инцидента по умолчанию.

Просмотр таблицы типов инцидентов

Чтобы просмотреть таблицу типов инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Отобразится вкладка **Типы** с таблицей типов инцидентов.

4. Если вы хотите настроить таблицу типов инцидентов, выполните любое из следующих действий:

   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

- Чтобы скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

В таблице типов инцидентов содержится следующая информация:

- **Имя**. Название пользовательских или предустановленных типов инцидентов.

  В таблице содержатся следующие предустановленные типы инцидентов:

  - Общие.

    > По умолчанию этот тип имеет значение **Да** в столбце **По умолчанию**.

  - Получение информации.
  - Компрометация.
  - Несанкционированный доступ.
  - Атака вредоносного ПО.
  - Фишинг.
  - Доступность.
  - Угроза изнутри.
  - Нарушение безопасности данных.
  - Ошибка конфигурации.
  - Атака через цепочку поставок.
  - Атака веб-приложения.
  - Использование уязвимостей.

- **Активный тип**. Если тип инцидента активен, вы можете выбрать этот тип в окне с подробной информацией об инциденте.
- **По умолчанию**. При создании инцидента, ему автоматически присваивается тип по умолчанию. Возможные значения:

  - **True.**
  - **False.**

- **Рабочий процесс**. Рабочий процесс инцидента.
- **Тенант**. Имя тенанта, которому принадлежит тип инцидента.
- **Тип создания**. Способ создания типа инцидента. Возможные значения:

  - **Пользовательский**

- **Предопределенный**

- **Идентификатор**. Уникальный идентификатор пользовательского или предустановленного типа инцидента. По умолчанию этот столбец скрыт.

- **Описание**. Описание типа инцидента. По умолчанию этот столбец скрыт.

При необходимости, вы можете создавать новые типы инцидентов, а также изменять и удалять предустановленные и пользовательские типы инцидентов.

Создание типов инцидентов

Чтобы создать тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Типы**.
4. Нажмите на кнопку **Создать**.

   Откроется окно **Создать тип инцидента**.
5. Если вы хотите, чтобы новый тип инцидента был активным, включите переключатель **Активный тип**.
6. В поле **Имя** введите название нового типа инцидента.
7. Если вы хотите, чтобы всем новым инцидентам по умолчанию назначался этот тип, установите флажок **Сделать по умолчанию**.

   > В тенанте может быть только один инцидент по умолчанию. Это означает, что, если у тенанта уже есть тип инцидента по умолчанию, этот тип больше не будет типом по умолчанию после того, как вы установите этот флажок.
8. В поле **Рабочий процесс** выберите рабочий процесс инцидента.
9. При необходимости в поле **Описание** укажите описание типа инцидента или комментарий.
10. Нажмите на кнопку **Создать**.

    Новый тип инцидента отобразится в таблице типов инцидентов.

Изменение типов инцидентов

При необходимости вы можете изменять типы инцидентов.

Чтобы изменить тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Вкладка **Типы** отображается с таблицей типов инцидентов.

4. Нажмите на имя типа инцидента, который требуется изменить.

   Откроется окно **Изменить тип инцидента**.

5. Внесите изменения и нажмите на кнопку **Сохранить**. Дополнительные сведения о свойствах типов инцидентов, которые вы можете изменить, см. в разделе Создание типов инцидентов.

Свойства типа инцидента изменены и сохранены.

Удаление типов инцидентов

Если вы хотите удалить тип инцидента, который используется в плейбуке, вам нужно удалить этот тип инцидента из триггера плейбука и/или алгоритма, чтобы избежать ошибок.

Удалить тип инцидента невозможно в следующих случаях:

- Тип инцидента установлен по умолчанию в тенанте, где был создан этот тип инцидента.

  При попытке удалить этот тип инцидента, вам будет предложено установить новый тип инцидента по умолчанию. В открывшемся окне вам нужно выбрать тип инцидента из списка.

- Тип инцидента установлен по умолчанию в дочернем тенанте.

- Текущий тенант или дочерний тенант содержит инцидент с типом, который вы хотите удалить.

  Прежде чем удалить такой тип, вам нужно назначить инциденту другой тип.

Чтобы удалить тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Вкладка **Типы** отображается с таблицей типов инцидентов.

4. Выполните одно из следующих действий:

   - Выберите тип инцидента, который вы хотите удалить и нажмите на кнопку **Удалить**.

   - Нажмите на название типа инцидента, который вы хотите удалить, затем в окне **Изменить тип инцидента** нажмите на кнопку **Удалить**.

5. В диалоговом окне нажмите на кнопку **Удалить**.

Тип инцидента будет удален.

Управление типами рабочих процессов

Open Single Management Platform позволяет настраивать гибкий рабочий процесс инцидента. Open Single Management Platform также отображает рабочий процесс в визуальном редакторе.

Процесс обработки инцидента представляет собой набор статусов и переходов, через которые проходит инцидент в течение его жизненного цикла. *Статус* является шагом в процессе обработки инцидента. *Переход* помогает инциденту переходить в различные статусы. Переход – это ссылка, которая позволяет настраивать переходы от одного статуса инцидента к другому и обратно. При необходимости, вы можете использовать переход как однонаправленную ссылку.

Вы можете создать рабочий процесс инцидента или использовать предустановленный рабочий процесс, который можно настроить.

Также можно назначить рабочий процесс типам инцидентов. Это поможет вам управлять жизненным циклом инцидента наиболее удобным образом.

Просмотр таблицы рабочих процессов инцидентов

Чтобы просмотреть таблицу рабочих процессов инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.

Отобразится таблица рабочих процессов инцидентов.

Чтобы настроить таблицу рабочих процессов инцидентов, выполните одно из следующих действий:

- Нажмите на значок фильтрации ( ), укажите критерий фильтрации и примените его в открывшемся меню.
- Чтобы скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

Таблица рабочих процессов инцидентов настроена, и в таблице отображаются нужные вам данные.

В таблице рабочих процессов инцидентов содержится следующая информация:

- **Имя**. Название пользовательских или предустановленных рабочих процессов инцидентов.
- **Связанные типы**. Количество связанных типов инцидентов.
- **Имя тенанта**. Имя тенанта, которому принадлежит рабочий процесс инцидента.
- **Тип создания**. Способ создания рабочего процесса инцидента. Возможные значения:
  - **Пользовательский**.

- **Предопределенный**.

- **Идентификатор рабочего процесса**. Уникальный идентификатор рабочего процесса инцидента. По умолчанию этот столбец скрыт.

- **Описание**. Описание рабочего процесса инцидента. По умолчанию, этот столбец скрыт.

Предустановленные рабочие процессы инцидентов

Open Single Management Platform позволяет управлять инцидентами с помощью предустановленного рабочего процесса инцидента. В таблице рабочих процессов инцидентов, такой рабочий процесс называется **Стандартный**. В столбце **Тип создания** эти рабочие процессы отмечены как **Предопределенный**.

При необходимости, вы можете изменить предустановленный рабочий процесс.

В таблице ниже описаны статусы предустановленного рабочего процесса и причины, по которым инцидентам присваиваются эти статусы.

Статус	Причины
Начальный	• Инцидент создан (вручную или автоматически). • Статус инцидента был изменен на **Начальный** с одного из следующих статусов: **В обработке**, **Отложен** или **Завершен**.
В обработке	Пользователь вручную изменил статус инцидента с **Начальный** или **Отложен** на **В обработке**.
Отложен	Пользователь вручную изменил статус инцидента с **В обработке** на **Отложен**.
Завершен	• Пользователь закрыл инцидент. • Пользователь связал инцидент с другим похожим инцидентом, который еще не был закрыт.

Рабочий процесс по ГОСТ

Open Single Management Platform предоставляет возможность использовать для управления инцидентами рабочий процесс, созданный на основании ГОСТ Р 59712-2022. По умолчанию, в таблице рабочих процессов он имеет название **ГОСТ** и является предустановленным.

При необходимости вы можете изменить рабочий процесс **ГОСТ** под свои нужды.

Рабочий процесс **ГОСТ** состоит из следующих статусов:

- **Новый**. Создание инцидента (ручное или автоматическое).

- **Анализ**. Изучение негативного воздействия на элементы информационной инфраструктуры.

- **Локализация**. Определение элементов информационной инфраструктуры, которые подверглись негативному воздействию.

- **Последствия**. Определение последствий негативного воздействия на элементы информационной инфраструктуры.
- **Ликвидация**. Ликвидация причины, а также последствий негативного воздействия на элементы информационной инфраструктуры.
- **Выполнен**. Последствия негативного воздействия устранены, причины выявлены.
- **Закрыт**. Проверка достаточности выполненных действий по ликвидация причин и последствий негативного воздействия на элементы информационной инфраструктуры.

Создание рабочих процессов инцидентов

Рабочий процесс инцидента позволяет управлять жизненным циклом инцидента.

Чтобы создать рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Нажмите на кнопку **Создать**.

   Откроется окно **Создать рабочий процесс**.

   > По умолчанию каждый рабочий процесс инцидента содержит предустановленные статусы **Начальный** и **Завершен**. Вы не можете удалить или изменить эти статусы.
5. В поле **Имя** введите название нового рабочего процесса.
6. При необходимости в поле **Описание** введите описание рабочего процесса или комментарий.
7. Чтобы добавить новые статусы, в разделе **Рабочий процесс** нажмите **Добавить статус**.
8. В открывшемся окне настройте следующие параметры:

   a. В поле **Название статуса** введите название нового статуса.

   b. В поле **Категория** выберите одну из следующих категорий статуса:

   - **Начальный.**
   - **В обработке.**
   - **Решен.**
   - **Завершен.**

   Обратите внимание, что категория определяет цвет иконки статуса.

c. В поле **Входящий переход** выберите один или несколько входящих статусов.

Если вы хотите настроить переход от всех статусов к входящим статусам, выберите параметр **Разрешить всем статусам переходить на этот**.

d. В поле **Исходящий переход**, выберите один или несколько исходящих статусов.

Если вы хотите настроить переход от исходящих статусов ко всем статусам, выберите параметр **Разрешить этому статусу переходить на все статусы**

e. Нажмите на кнопку **Добавить**.

Визуализированный рабочий процесс отображается в окне **Создать рабочий процесс**

При необходимости повторите шаги 7 и 8, чтобы добавить новые статусы.

9. В окне **Создать рабочий процесс** нажмите на кнопку **Сохранить**.

Новый рабочий процесс инцидента отобразится в таблице.

Изменение рабочих процессов и статусов инцидентов

Вы можете изменить свойства рабочего процесса, а также статусы и переходы рабочего процесса.

Чтобы изменить рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Выберите рабочий процесс, который требуется изменить.

   Откроется окно **Изменить рабочий процесс**.
5. Измените свойства рабочего процесса. Дополнительные сведения о свойствах рабочего процесса, которые вы можете изменить, см. в разделе Создание рабочего процесса инцидентов.

Свойства рабочего процесса изменены и сохранены.

Чтобы изменить статусы рабочего процесса инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Выберите рабочий процесс, который требуется изменить.

   Откроется окно **Изменить рабочий процесс**.

5. Чтобы изменить статусы и переходы рабочего процесса, нажмите на название статуса, который вы хотите изменить.

   Откроется окно **Изменить статус**.

6. Измените параметры статуса и параметры перехода. Дополнительные сведения о параметрах статуса, которые вы можете изменить, см. в разделе Создание рабочего процесса инцидентов.

   При необходимости, вы можете удалить статус, нажав на кнопку **Удалить**.

   > Вы не можете изменить название и категорию следующих предустановленных статусов: **Начальный** и **Завершен**. Вы также не можете удалить эти предустановленные статусы.

   > Вы не можете удалить статус, если он назначен инциденту.

7. Нажмите на кнопку **Сохранить**.

Статусы рабочего процесса изменены и сохранены.

Удаление рабочих процессов инцидентов

> Вы не можете удалить рабочий процесс инцидента, если есть связанные типы инцидентов, которые принадлежат родительскому или дочернему тенанту. В этом случае вам нужно назначить другой рабочий процесс связанным типам инцидентов, а затем попробовать снова удалить рабочий процесс инцидента.

> Если вы хотите удалить рабочий процесс, который используется в плейбуке, перед удалением измените триггер и/или алгоритм плейбука, чтобы избежать ошибок.

Чтобы удалить рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.

4. В списке рабочих процессов выберите рабочий процесс, который вы хотите удалить, и нажмите на кнопку **Удалить.**

5. В диалоговом окне нажмите на кнопку **Удалить**.

Рабочий процесс инцидента удален.

Настройка периода хранения алертов и инцидентов

Open Single Management Platform позволяет вам уменьшать или увеличивать период хранения алертов и инцидентов в зависимости от ваших требований. По умолчанию период хранения алертов и инцидентов составляет 360 дней.

Дочерний тенант копирует период хранения алертов и инцидентов из родительского тенанта. При необходимости вы можете изменить период хранения алертов и инцидентов для дочернего тенанта.

Чтобы настроить период хранения алертов или инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Срок хранения**.
4. Укажите новый период хранения в одном или обоих полях:

   - **Срок хранения алерта (сут)**
   - **Срок хранения инцидента (сут)**

   Минимальное значение – `1`.
5. Нажмите на кнопку **Сохранить**.

Новый период хранения будет настроен.

Независимо от настроенного периода хранения, если истекший алерт связан с неистекшим инцидентом, алерт будет удален только после истечения периода хранения связанного инцидента. Если истекший инцидент имеет неистекшие связанные алерты, инцидент будет удален только после истечения периода хранения связанных алертов.

Просмотр информации об активе

Детали актива – это окно, которое содержит всю информацию, связанную с активом.

Вы можете просмотреть детали актива одним из следующих способов:

- из деталей алерта;
- из деталей инцидента;
- из деталей события (если событие содержит активы).

Чтобы просмотреть сведения об активе:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** и выполните одно из следующих действий:

   - Если вы хотите просмотреть детали активов из деталей алерта, нажмите **Алерты**, а затем в столбце **Идентификатор** нажмите на идентификатор алерта, которое включает актив, детали которого вы

хотите просмотреть. В открывшемся окне выберите вкладку **Активы**.

- Если вы хотите просмотреть детали активов из деталей инцидента, нажмите **Инциденты**, а затем в столбце **Идентификатор** нажмите на идентификатор инцидента, которое включает актив, детали которого вы хотите просмотреть. В открывшемся окне выберите вкладку **Активы**.

- Если вы хотите просмотреть детали активов из деталей события, нажмите **Поиск угроз**, а затем нажмите на событие, которое содержит актив, детали которого вы хотите просмотреть.

2. Нажмите на имя требуемого актива и в раскрывающемся списке выберите **Просмотреть свойства**.

Отображается окно с деталями актива.

Окно с подробной информацией актива содержит следующие разделы:

- **Свойства актива** – информация об активе, например, название актива, идентификатор, тенант, которому принадлежит актив.

  Если действующая лицензия в KUMA включает AI-модуль, отображается поле **AI-оценка** и оценка актива. Это поле показывает степень нетипичной активности актива и может принимать значения в диапазоне от 0 до 1, где 0 – это ожидаемое поведение, 1 – это неожиданное поведение для актива в рамках инфраструктуры.

- **Категории** – информация о категориях, связанных с активом.

- **Пользовательские поля** – поля активов, которые вы создали в Консоли KUMA.

- **Установленное программное обеспечение** – информация о программном обеспечении, установленном на активе.

- **KSC: уязвимости** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

- **Приложения "Лаборатории Касперского"** – информация о приложениях "Лаборатории Касперского", установленных на активе.

- **Состояние защиты устройства** – статус актива, возможны следующие значения: *OK*, *Критический*, *Предупреждение*. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

- **KICS for Networks: свойства актива** – информация об активе. Эта информация импортируется из KICS for Networks.

- **KICS for Networks: уязвимости** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS for Networks.

Вы можете расширить разделы, нажав на значки (>) рядом с их названиями.

Поиск угроз

Страница **Поиск угроз** содержит инструменты, которые помогают анализировать события для поиска угроз и уязвимостей, которые не были обнаружены автоматически. Чтобы создать алерт из набора событий, выберите события и нажмите на кнопку **Создать алерт**.

Вы можете открыть страницу **Поиск угроз** любым из следующих способов:

- В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Поиск угроз**.
- В деталях алерта или инцидента в контекстном меню выберите пункт **Поиск в разделе Поиск угроз**.
- В сведениях об инциденте нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на кнопку **Поиск угроз**.

На странице **Поиск угроз** отображаются события. Вы можете отфильтровать события:

- изменив SQL-запрос;
- изменив период;
- выбрав тенант, которому принадлежат события.

Работа с событиями

Раздел **Поиск угроз** содержит инструменты, которые помогут вам в поиске угроз и уязвимостей путем анализа событий.

Просмотр таблицы событий

В таблице событий представлен обзор всех событий, полученных Ядром KUMA из источников данных. В таблице отображается список событий, отфильтрованных по выполненному SQL-запросу.

Чтобы просмотреть таблицу событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Поиск угроз**.
2. При необходимости отфильтруйте тенанты. По умолчанию фильтр тенантов выключен и в таблице событий отображаются события, относящиеся ко всем тенантам, к которым у вас есть права доступа на **Чтение**. Чтобы применить фильтр для тенантов:

   a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

   Откроется список тенантов.

   b. Установите флажки рядом с требуемыми тенантами.

   В таблице событий отображаются только события, относящиеся к выбранным тенантам.

Отобразится таблица событий. Дополнительные сведения о столбцах таблицы см. в модели данных нормализованного события.

Поиск и фильтрация событий

Для поиска и фильтрации событий измените SQL-запрос в поле поиска и нажмите на кнопку **Выполнить запрос**. Вы можете ввести SQL-запрос вручную или сгенерировать его с помощью конструктора запросов.

В SQL-запросах поддерживается агрегирование и группировка данных.

Вы можете добавить условия фильтрации к уже сформированному SQL-запросу в окне просмотра статистики, в таблице событий и в области сведений о событии.

Чтобы изменить параметры фильтрации из окна Статистика:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Откройте область деталей **Статистика** одним из следующих способов:
   - В правом верхнем углу таблицы событий нажмите на кнопку ••• и в выберите **Статистика**.
   - В таблице событий нажмите на любое значение, а затем в открывшемся контекстном меню выберите пункт **Статистика**.

   В правой части окна откроется область деталей **Статистика**.
3. Откройте раскрывающийся список необходимого параметра и наведите курсор мыши на требуемое значение.
4. Измените параметры фильтрации, выполнив одно из следующих действий:
   - Чтобы включить только события с выбранным значением, нажмите на кнопку +.
   - Чтобы исключить все события с выбранным значением, нажмите на кнопку —.

Чтобы изменить параметры фильтрации в таблице событий:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значение параметра события в таблице событий.
3. В открывшемся меню выберите следующие параметры:
   - Чтобы оставить в таблице только события с выбранным значением, выберите **Искать события с этим значением**.
   - Чтобы исключить из таблицы все события с выбранным значением, выберите **Искать события без этого значения**.

Чтобы изменить параметры фильтрации в области сведений о событий:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Нажмите на соответствующее событие, чтобы открыть панель **сведений о событии**.

3. Измените параметры фильтрации, выполнив одно из следующих действий:

   - Чтобы включить только события с выбранным значением, нажмите на кнопку +.
   - Чтобы исключить все события с выбранным значением, нажмите на кнопку −.

В результате параметры фильтрации и таблица событий обновятся, а новый поисковый запрос отобразится в верхней части экрана.

> Когда вы переключаетесь на конструктор запросов, параметры запроса, введенного вручную в поле поиска, не передаются в конструктор, поэтому вам нужно будет создать запрос заново. Запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строку поиска, пока вы не нажмете на кнопку **Применить** в окне конструктора.

Нажмите на кнопку , чтобы сохранить текущий фильтр.

Создание SQL-запросов вручную

С помощью строки поиска вы можете вручную создавать SQL-запросы любой сложности для фильтрации событий.

Выполнение SQL-запроса влияет на отображаемые столбцы таблицы.

Если SQL-запрос содержит значение *, указанные в запросе столбцы добавляются в таблицу, если они отсутствовали. Удаление отображаемого столбца из последующих запросов не скрывает соответствующий столбец.

Если SQL-запрос не содержит значения *, в таблице отображаются только столбцы для указанных полей, которые соответствуют нормализованной модели данных событий. Столбцы отображаются, даже если для них нет данных.

Чтобы сформировать SQL-запрос вручную:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Введите SQL-запрос в поле ввода.

3. Нажмите на кнопку **Применить запрос**.

   Отобразится таблица событий, соответствующих условиям вашего запроса. При необходимости вы можете отфильтровать события по периоду.

Чтобы отобразить непечатаемые символы в поле запроса SQL, нажмите любую из следующих комбинаций клавиш:

- **Ctrl+*/Command+***
- **Ctrl+Shift+8/Command+Shift+8**

Если вы включите отображение непечатаемых символов в компоненте XDR, другие компоненты (такие как KUMA) не будут автоматически отображать непечатаемые символы, пока вы не перезагрузите вкладки браузера компонентов.

Поддерживаемые функции и операторы

SELECT

Поля событий, которые следует возвращать.

Для **SELECT** в приложении поддержаны следующие функции и операторы:

Функции агрегации: **count**, **avg**, **max**, **min**, **sum**.

Арифметические операторы: **+**, **-**, *****, **/**, **<**, **>**, **=**, **!=**, **>=**, **<=**.

Вы можете комбинировать эти функции и операторы.

Если вы используете в запросе функции агрегации, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, а также получение статистики недоступны.

FROM

Источник данных.

WHERE

Условия фильтрации событий.

- **AND**, **OR**, **NOT**, **=**, **!=**, **>**, **>=**, **<**, **<=**
- **IN**
- **BETWEEN**
- **LIKE**
- **ILIKE**
- **inSubnet**
- **match** (в запросах используется синтаксис регулярных выражений re2, специальные символы необходимо дополнительно экранировать с помощью обратной косой черты "\")

GROUP BY

Поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективное сканирование недоступны.

ORDER BY

Столбцы, по которым следует сортировать возвращаемые данные.

Возможные значения:

- **DESC** – по убыванию.
- **ASC** – по возрастанию.

OFFSET

Пропуск указанного количества строк перед выводом результатов запроса.

LIMIT

Количество отображаемых в таблице строк.

По умолчанию указано значение 250.

При переключении на конструктор параметры запроса, введенного вручную в строке поиска, не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строку поиска, пока вы не нажмете на кнопку Применить в окне конструктора.

Используемые в поисковых запросах псевдонимы не должны содержать пробелов.

Примеры запросов:

- **SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events с типом **Base** и **Audit**, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250**

  Все события таблицы events, для которых в поле **BytesIn** значение полученного трафика находится в диапазоне от 1000 до 2000 байт, отсортированные по столбцу **Timestamp** в порядке возрастания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events, которые в поле **Message** содержат данные, соответствующие заданному шаблону %ssh:% в нижнем регистре, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events для устройств, которые входят в подсеть 00.0.0.0/00, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону ssh.*, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT max(BytesOut) / 1024 FROM `events`**

Максимальный размер исходящего трафика (КБ) за выбранный период времени.

- **SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250**

  Количество событий и номер порта. События сгруппированы по номеру порта и отсортированы по столбцу **Port** в порядке возрастания. Количество отображаемых в таблице строк – 250.

  Столбцу **ID** в таблице событий присвоено имя Count, столбцу **SourcePort** присвоено имя Port.

- **SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250**

  Если вы хотите указать в запросе специальный символ, вам требуется экранировать его, поместив перед ним обратную косую черту (\).

  Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону ssh: 'connection', и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

Формирование SQL-запроса с помощью конструктора

Вы можете сформировать SQL-запрос для фильтрации событий с помощью конструктора запросов.

Выполнение SQL-запроса влияет на отображаемые столбцы таблицы.

Если SQL-запрос содержит значение *, указанные в запросе столбцы добавляются в таблицу, если они отсутствовали. Удаление отображаемого столбца из последующих запросов не скрывает соответствующий столбец.

Если SQL-запрос не содержит значения *, в таблице отображаются только столбцы для указанных полей, которые соответствуют нормализованной модели данных событий. Столбцы отображаются, даже если для них нет данных.

Чтобы сформировать SQL-запрос с помощью конструктора:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Нажмите на кнопку , чтобы открыть конструктор запросов.

   Сформулируйте поисковый запрос, указав данные в следующих блоках параметров:

   - **SELECT**

     Поля событий, которые следует возвращать. По умолчанию выбрано значение *, означающее, что необходимо возвращать все доступные поля события. Чтобы настроить отображаемые поля, выберите нужные поля в раскрывающемся списке. Стоит учитывать, что Select * в запросе увеличивает длительность выполнения запроса, но избавляет от необходимости указывать поля в запросе.

     Выбрав поле события, вы можете в поле справа от раскрывающегося списка указать псевдоним для столбца выводимых данных, а в крайнем правом раскрывающемся списке можно выбрать операцию, которую следует произвести над данными: **count**, **max**, **min**, **avg**, **sum**.

   - **FROM**

     Источник данных. Выберите значение **events**.

   - **WHERE**

     Условия фильтрации событий.

Чтобы добавить условия и группы, нажмите на кнопки **Добавить условие** и **Добавить группу**. Значение оператора **AND** выбирается по умолчанию в группе условий. Нажмите на значение оператора, чтобы изменить его. Доступные значения: **AND**, **OR**, **NOT**.

Чтобы изменить структуру условий и групп условий, используйте значок ⠿ для перетаскивания выражений.

Чтобы добавить условия фильтрации:

a. В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.

b. В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.

c. Введите значение условия. В зависимости от выбранного типа поля может потребоваться ввести значение вручную, выбрав его из раскрывающегося списка или в календаре.

Чтобы удалить условия фильтрации, нажмите на кнопку **X**. Чтобы удалить условия группы, нажмите на кнопку **Удалить группу**.

- **GROUP BY**

  Поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективное сканирование недоступны.

- **ORDER BY**

  Столбцы, по которым следует сортировать возвращаемые данные. В раскрывающемся списке справа можно выбрать порядок: **DESC** – по убыванию, **ASC** – по возрастанию.

- **LIMIT**

  Количество отображаемых в таблице строк.

  По умолчанию указано значение 250.

  Если при фильтрации событий по периоду, указанному пользователем, количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

3. Нажмите на кнопку **Применить**.

   Текущий SQL-запрос будет перезаписан. Сгенерированный SQL-запрос отображается в поле поиска.

   Чтобы сбросить параметры конструктора, нажмите на кнопку **Запрос по умолчанию**.

   Чтобы закрыть конструктор, не перезаписывая существующий запрос, нажмите на кнопку .

4. Нажмите на кнопку **Применить запрос**, чтобы отобразить данные в таблице.

   В таблице отображаются результаты поиска по сформированному SQL-запросу.

При переходе в другой раздел веб-интерфейса сформированный в конструкторе запрос не сохраняется. Если вы повторно вернетесь в раздел События, в конструкторе будет отображаться запрос по умолчанию.

Просмотр сведений о событии

Чтобы открыть сведения о событии, выберите событие в таблице событий в разделе **Поиск угроз** или на странице деталей алерта.

Панель **Информация о событии** отображается в правой части окна веб-интерфейса и содержит список параметров события со значениями. В этой области вы можете:

- Включить выбранное поле в поиск или исключить его из поиска, нажав на + или на − рядом со значением параметра.
- Найти похожие события и добавить или удалить правило запрета, нажав на значения **FileHash** и **DeviceCustomString**.
- При интеграции с Kaspersky CyberTrace и Kaspersky Threat Intelligence Portal вы можете добавить в пользовательские сведения о киберугрозах CyberTrace и отобразить информацию из Threat Lookup, нажав на значения **FileHash** и **DeviceCustomString**.
- Просмотрите параметры службы, зарегистрировавшей событие, нажав на значение **Служба**.

В панели **Информация о событии** вместо идентификатора отображается имя описываемого объекта в значениях следующих параметров. Если вы измените параметры фильтра в панели **Информация о событии**, в SQL-запрос будет добавлен идентификатор объекта, а не его имя:

- TenantID
- SeriviceID
- DeviceAssetID
- SourceAssetID
- DestinationAssetID
- SourceAccountID
- DestinationAccountID

Сохранение и выбор конфигурации фильтра событий

Вы можете сохранить текущую конфигурацию фильтра, включая временной фильтр, конструктор запросов и параметры таблицы событий, для использования в будущем. Сохраненные конфигурации фильтров доступны вам и другим пользователям, имеющим соответствующие права доступа.

Чтобы сохранить текущие параметры фильтра, запроса и периода

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на кнопку рядом с поисковым запросом и выберите пункт **Сохранить текущий фильтр**.

3. В открывшемся окне **Новый фильтр** введите название конфигурации фильтра в поле **Имя**. Имя должно содержать не более 128 символов Юникода.
4. В раскрывающемся списке **Тенант** выберите тенант, для которого нужно сохранить созданный фильтр.
5. Нажмите на кнопку **Сохранить**.

   Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на кнопку рядом с поисковым запросом и выберите нужный фильтр.

Чтобы сохранить текущие параметры фильтра, запроса и параметры таблицы событий

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок шестеренки в панели над таблицей событий.
3. Нажмите на пункт **Сохранить текущий пресет**.
4. В открывшемся окне **Новый пресет** введите название пресета в поле **Имя**. Имя должно содержать не более 128 символов Юникода.
5. В раскрывающемся списке **Тенант** выберите тенант, для которого нужно сохранить созданный пресет.
6. Нажмите на кнопку **Сохранить**.

   Конфигурация пресета сохранена.

Чтобы выбрать ранее сохраненную конфигурацию пресета

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок шестеренки в панели над таблицей событий. Выберите вкладку **Пресеты**.
3. Выберите необходимый пресет.

Чтобы удалить ранее сохраненную конфигурацию фильтра для всех пользователей

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок рядом с поисковым запросом.
3. Нажмите на значок рядом с конфигурацией, которую нужно удалить.
4. Нажмите на кнопку **OK**.

Фильтрация событий по периоду

Вы можете указать период для отображения событий.

Чтобы отфильтровать события по периоду:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Откройте второй раскрывающийся список в верхней части окна.
3. Укажите период. Вы можете выбрать предопределенные периоды относительно текущей даты и времени или указать необходимый период, используя поля **Начало периода** и **Конец периода** или выбрав даты в календаре.
4. Нажмите на кнопку **Применить**.

Экспорт событий

Вы можете экспортировать информацию о событиях в файл TSV. Выборка событий, которые будут экспортированы в файл TSV, зависит от параметров фильтра. Информация экспортируется из столбцов, которые отображаются в таблице событий. Столбцы в экспортируемом файле заполняются доступными данными, даже если они не отображались в таблице событий в разделе **Поиск угроз** из-за особенностей SQL-запроса.

Чтобы экспортировать информацию о событиях:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. В правом верхнем углу таблицы событий нажмите на кнопку ••• и в раскрывающемся списке выберите **Экспортировать в CSV**.

   Новая задача экспорта файла TSV создана в разделе KUMA **Управление задачами**.
3. Войдите в Консоль KUMA и найдите созданную вами задачу в разделе **Управление задачами**.
4. Нажмите на название типа задачи и выберите в раскрывающемся списке пункт **Загрузить**.

   Файл TSV будет загружен с использованием параметров вашего браузера. По умолчанию имя файла event-export-<date>_<time>.tsv.

Файл сохранен в соответствии с параметрами вашего браузера.

Ретроспективное сканирование

Вы можете использовать ретроспективное сканирование (retroscan), чтобы уточнить ресурсы правил корреляции или проанализировать данные истории.

Вы также можете создавать алерты на основе функции ретроспективного сканирования (retroscan).

Чтобы использовать ретроспективное сканирование:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Поиск угроз**.
2. В правом верхнем углу таблицы событий нажмите на кнопку ••• и в выберите **Ретроспективное сканирование**.

   Откроется панель **Ретроспективное сканирование**.
3. В раскрывающемся списке **Коррелятор** выберите пункт Коррелятор, в который будут передаваться выбранные события.
4. В раскрывающемся списке **Правила корреляции** выберите правила корреляции, которые необходимо использовать при обработке событий.
5. Чтобы выполнить действия по реагированию во время обработки событий, включите переключатель **Выполнить действия по реагированию**.
6. Чтобы генерировать алерты во время обработки событий, включите переключатель **Создать алерты**.
7. Нажмите на кнопку **Создать задачу**.

   Задача ретроспективного сканирования создана в разделе KUMA **Управление задачами**.

Получение статистики таблицы событий

Вы можете получить статистику по выбранным событиям, отображаемым в таблице событий. Выбранные события зависят от параметров фильтра.

Чтобы получить статистику:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Выполните одно из следующих действий:
   - В верхнем правом углу таблицы событий выберите **Статистика** из раскрывающегося списка •••.
   - В таблице событий нажмите на любое значение и в контекстном меню выберите пункт **Статистика**.

Отобразится область сведений раздела **Статистика** со списком параметров из текущей выборки событий. Цифры возле каждого параметра означают количество событий с этим параметром в выборке. Если параметр развернут, отображаются пять наиболее часто встречающихся значений. Введите название параметра в **Поля поиска** для фильтрации отображаемых данных.

Окно **Статистика** позволяет изменять фильтр событий.

> При использовании SQL-запросов с группировкой и агрегированием данных для фильтрации событий статистика недоступна.

Реагирование на угрозы

Чтобы выполнить действия по реагированию, просмотреть результат обогащения, которое вы выполнили из плейбука, и запустить плейбуки вручную, вам нужно перейти в раздел **Алерты** или **Инциденты**.

Разделы **Алерты** и **Инциденты** отображаются в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Open Single Management Platform.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Работа с НКЦКИ, Подтверждающий, Наблюдатель.

После выполнения действия по реагированию, вы можете просмотреть историю действий по реагированию.

Действия по реагированию

Действия по реагированию можно запустить одним из следующих способов:

- вручную, как описано в этом разделе;
- в рамках плейбука.

  В этом случае при создании или изменении плейбука вы можете настроить автоматический запуск действия по реагированию или запросить подтверждение пользователя перед запуском в плейбуке. По умолчанию ручное подтверждение действий по реагированию выключено.

Прерывание процессов

Действие по реагированию *Прервать процесс* позволяет удаленно завершать процессы на устройствах. Вы можете выполнить действие по реагированию Прервать процесс для наблюдаемых объектов или активов.

Вы можете запустить действие по реагированию Прервать процесс одним из следующих способов:

- в деталях алерта или инцидента;
- в сведениях об устройстве;
- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действие по реагированию Прервать процесс, вам должна быть присвоена одна из следующих XDR-ролей: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Запуск процесса завершения для наблюдаемых объектов

Чтобы запустить процесс завершения для наблюдаемых объектов:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.

2. В открывшемся окне выберите вкладку **Наблюдаемые объекты**.

3. В списке наблюдаемых объектов выберите один или несколько наблюдаемых объектов, для которых вы хотите прервать процесс. Наблюдаемые объекты могут включать:

   - MD5

   - SHA256

4. Нажмите на кнопку **Прервать процесс**.

5. В открывшейся панели **Прервать процесс** выберите активы, для которых вы хотите прервать процесс.

6. Нажмите на кнопку **Прервать**.

Процесс прерван.

Запуск процесса завершения для активов

Чтобы выполнить действие по реагированию Прервать процесс для активов:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором алерта.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.

2. В открывшемся окне выберите вкладку **Активы**.

3. В списке активов выберите один или несколько нужных устройств.

4. Нажмите на кнопку **Выбрать действие по реагированию**, а затем на кнопку **Прервать процесс**.

5. В открывшейся панели **Прервать процесс** укажите один из следующих параметров:

- **PID**. Идентификатор процесса.

  Для действия по реагированию Прервать процесс по PID с фиксированной областью, если активы действия по реагированию принадлежат одному Серверу администрирования, вы можете запустить это действие по реагированию только для одного актива за раз.

  Для действия по реагированию Прервать процесс PID с изменяемой областью действия это действие по реагированию выполнить невозможно.

- **Хеш** (алгоритм хеширования MD5 или SHA256) и **Путь** к файлу процесса.

6. Нажмите на кнопку **Прервать**.

Процесс прерван.

Запуск процесса завершения из графа расследования

Параметр доступен, если граф расследования построен.

Чтобы выполнить действия Завершить процесс из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на ссылку с нужным идентификатором инцидента.
2. В открывшемся окне **Сведения об инциденте** нажмите на кнопку **Посмотреть на графе**.

   Откроется окно **графа расследования**.
3. Нажмите на имя нужного алерта, а затем нажмите на **Просмотреть информацию**.
4. В открывшемся окне выберите вкладку **Наблюдаемые объекты**.
5. В списке наблюдаемых объектов выберите один или несколько наблюдаемых объектов, для которых вы хотите прервать процесс. Наблюдаемые объекты могут включать:

   - MD5
   - SHA256
6. Нажмите на кнопку **Прервать процесс**.
7. В открывшейся панели **Прервать процесс** выберите активы, для которых вы хотите прервать процесс.
8. Нажмите на кнопку **Прервать**.

Процесс прерван.

Перемещение устройств в другую группу администрирования

В качестве действия по реагированию вы можете переместить устройство в другую группу администрирования Open Single Management Platform. Это может потребоваться, когда анализ алерта или инцидента показывает, что уровень защиты устройства низкий. При перемещении устройства в другую группу администрирования к устройству применяются групповые политики и задачи.

Группа администрирования, в которую вы перемещаете устройство, должна принадлежать тому же тенанту, что и устройство.

Вы можете переместить устройство в другую группу администрирования одним из следующих способов:

- из деталей алерта или инцидента;
- из сведений об устройстве;
- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы переместить устройство в другую группу администрирования, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Перемещение устройства в другую группу администрирования из деталей алерта или инцидента

Чтобы переместить устройство в другую группу администрирования из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется переместить.
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется переместить.
2. В открывшемся окне выберите вкладку **Активы**.
3. Установите флажок рядом с устройством, которое нужно переместить в другую группу администрирования.

   Вы можете выбрать несколько устройств, если они управляются одним Сервером администрирования: главным, подчиненным или виртуальным.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Переместить в группу**.

   В открывшемся окне **Переместить в группу** в правой части экрана отображаются группы администрирования Сервера администрирования, который управляет выбранным устройством.

5. Выберите группу администрирования, в которую вы хотите переместить устройство или устройства, и нажмите на кнопку **Переместить**.

Устройство перемещено в выбранную группу администрирования. Соответствующее сообщение отобразится на экране.

Перемещение устройства в другую группу администрирования из сведений устройства

Чтобы переместить устройство в другую группу администрирования из сведений устройства:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется переместить.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется переместить.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Переместить в группу**.

   В открывшемся окне **Переместить в группу** в правой части экрана отображаются группы администрирования Сервера администрирования, который управляет выбранным устройством.

5. Выберите группу администрирования, в которую вы хотите переместить устройство или устройства, и нажмите на кнопку **Переместить**.

Устройство перемещено в выбранную группу администрирования. Соответствующее сообщение отобразится на экране.

Перемещение устройства в другую группу администрирования из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы переместить устройство в другую группу администрирования из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется переместить.

2. Нажмите на кнопку **Посмотреть на графе**.

3. В открывшемся графе расследования нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Переместить в группу**.

   В открывшемся окне **Переместить в группу** в правой части экрана отображаются группы администрирования Сервера администрирования, который управляет выбранным устройством.

5. Выберите группу администрирования, в которую вы хотите переместить устройство или устройства, и нажмите на кнопку **Переместить**.

Устройство перемещено в выбранную группу администрирования. Соответствующее сообщение отобразится на экране.

Запуск поиска вредоносного ПО

Чтобы предотвратить распространение угрозы на зараженном устройстве, вы можете запустить поиск вредоносного ПО одним из следующих способов:

- из деталей алерта или инцидента;
- из сведений об устройстве;
- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действие по реагированию Поиск вредоносного ПО, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Запуск поиска вредоносного ПО из деталей алерта или инцидента

Чтобы запустить поиск вредоносного ПО на устройстве из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий устройство, которое требуется проверить.
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, содержащий устройство, которое требуется проверить.

2. В открывшемся окне выберите вкладку **Активы**.

3. Установите флажок рядом с устройством, которое нужно проверить.

   При необходимости вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Запустить проверку на вредоносное ПО**.

   В правой части экрана откроется окно **Антивирусная проверка**.

5. Выберите тип поиска вредоносного ПО:

   - **Полная проверка**

     Вы можете включить переключатель **Сетевые диски**, чтобы включить в проверку сетевые устройства. По умолчанию параметр выключен.

     > Полная проверка может замедлить работу устройства из-за повышенной нагрузки на его операционную систему.

   - **Проверка важных областей**

     Если вы выберете этот тип, выполняется проверка памяти ядра, запущенных процессов и загрузочных секторов диска.

   - **Выборочная проверка**

     В поле **Указать путь к файлу** укажите путь к файлу, который вы хотите проверить. Если вы хотите задать несколько путей, нажмите на кнопку **Добавить путь** и укажите путь.

6. Нажмите на кнопку **Проверить**.

Выбранный тип поиска вредоносного ПО запущен.

Запуск поиска вредоносного ПО из сведений об устройстве

Чтобы запустить поиск вредоносного ПО из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий устройство, которое требуется проверить.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, содержащий устройство, которое требуется проверить.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

   При необходимости вы можете нажать на кнопку **Изменить в KUMA**, чтобы изменить параметры устройства в Консоли KUMA.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Запустить проверку на вредоносное ПО**.

   В правой части экрана откроется окно **Антивирусная проверка**.

5. Выберите тип поиска вредоносного ПО. Типы описаны на шаге 5 в разделе *Запуск поиска вредоносного ПО из деталей алерта или инцидента*.

6. Нажмите на кнопку **Проверить**.

Выбранный тип поиска вредоносного ПО запущен.

Поиск вредоносного ПО из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы запустить поиск вредоносного ПО на устройстве из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, содержащий устройство, которое требуется проверить.
2. Нажмите на кнопку **Посмотреть на графе**.
3. В открывшемся графе расследования нажмите на имя устройства, чтобы открыть сведения об устройстве.
4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Запустить проверку на вредоносное ПО**.

   В правой части экрана откроется окно **Антивирусная проверка**.
5. Выберите тип поиска вредоносного ПО. Типы описаны на шаге 5 в разделе *Запуск поиска вредоносного ПО из деталей алерта или инцидента*.
6. Нажмите на кнопку **Проверить**.

Выбранный тип поиска вредоносного ПО запущен.

Если поиск вредоносного ПО завершен успешно, на экране отображается соответствующее сообщение, а в таблице алертов или в таблице инцидентов отображается статус действия **Успешно**. В противном случае отображается сообщение об ошибке, а алерт или инцидент отображается со статусом действия **Ошибка**.

После завершения поиска вредоносного ПО вы можете просмотреть результат.

Просмотр результатов поиска вредоносного ПО

После завершения поиска вредоносного ПО вы можете просмотреть результат одним из следующих способов:

- в деталях алерта или инцидента;
- в истории реагирования;
- в сведениях о плейбуке.

Чтобы просмотреть результат поиска вредоносного ПО:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** и выполните одно из следующих действий:

- Если вы хотите просмотреть результат из деталей алерта или инцидента, перейдите в раздел **Алерты** или **Инциденты** и нажмите на идентификатор алерта или инцидента, для которого был выполнен поиск вредоносного ПО. В открывшемся окне выберите вкладку **История**, а затем на вкладку **История реагирований**, чтобы отобразить список событий.

- Если вы хотите просмотреть результат в истории действий по реагированию, перейдите в раздел **История реагирований**.

- Если вы хотите просмотреть результат поиска вредоносного ПО из плейбука, перейдите в раздел **Плейбуки** и нажмите на название плейбука, для которого был выполнен поиск вредоносного ПО. В открывшемся окне выберите вкладку **История** для просмотра списка событий.

2. В столбце **Статус действия** нажмите на статус события, для которого вы хотите просмотреть результаты поиска вредоносного ПО.

   В открывшемся окне отображается таблица обнаружений. В поле **Сервер администрирования** вы можете выбрать Сервер администрирования, для которого отображается таблица обнаружений.

   Таблица содержит следующие столбцы:

   - **Устройство**. Имя устройства или идентификатор.
   - **Путь**. Путь к файлу.
   - **Хеш**. SHA256.
   - **Название детектируемого объекта**. Название обнаружения, которое произошло на устройстве.
   - **Статус действия**. Результат обработки угрозы.
   - **Пользователь**. Учетная запись пользователя, связанного с обнаружением.

Обновление баз

Чтобы быстро обнаруживать угрозы и поддерживать уровень защиты клиентского устройства в актуальном состоянии, необходимо регулярно обновлять базы и модули приложений на устройстве.

Вы можете обновить базы на устройстве одним из следующих способов:

- из деталей алерта или инцидента;
- из сведений об устройстве;
- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы обновить базы данных на устройстве, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Обновление баз из деталей алерта или инцидента

Чтобы обновить базы данных на устройстве из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, на котором требуется обновить базы данных.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, на котором требуется обновить базы данных.

2. В открывшемся окне выберите вкладку **Активы**.

3. Установите флажок рядом с устройствами, на которых необходимо обновить базы данных.

   При необходимости вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Обновить базы**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Обновление баз данных из сведений об устройстве

Чтобы обновить базы данных на устройстве из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, на котором требуется обновить базы данных.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, на котором требуется обновить базы данных.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Обновить базы**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Обновление баз данных из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы обновить базы данных на устройстве из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, на котором требуется обновить базы данных.
2. Нажмите на кнопку **Посмотреть на графе**.
3. В открывшемся графе расследования нажмите на имя устройства, чтобы открыть сведения об устройстве.
4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Обновить базы**.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Перемещение файлов на карантин

Чтобы предотвратить распространение угрозы, вы можете переместить устройство, на котором находится файл, на карантин одним из следующих способов:

- из деталей алерта или инцидента;
- из свойств устройства;
- из телеметрии события;
- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы переместить устройство, на котором находится файл, на карантин, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Запуск действия по реагированию может занять до 15 минут из-за интервала синхронизации между управляемым устройством и Сервером администрирования.

Реагирование из деталей алерта или инцидента

Чтобы переместить устройство на карантин из деталей алерта или инцидента:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется

переместить.

- В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется переместить.

2. В открывшемся окне выберите вкладку **Активы**.
3. Установите флажок рядом с устройством, которое нужно переместить на карантин.

   При необходимости вы можете выбрать несколько устройств.
4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Поместить на карантин**.
5. В открывшемся окне в правой части экрана укажите следующую информацию в соответствующих полях:

   - Хеш файла.

     Вы можете выбрать **SHA256** или **MD5**.

   - Путь к файлу.
6. Нажмите на кнопку **Переместить**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из сведений об устройстве

Чтобы переместить устройство на карантин из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется переместить.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется переместить.
2. В открывшемся окне выберите вкладку **Активы**.
3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.
4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Поместить на карантин**.
5. В открывшемся окне в правой части экрана укажите следующую информацию в соответствующих полях:

   - Хеш файла.

     Вы можете выбрать **SHA256** или **MD5**.

   - Путь к файлу.
6. Нажмите на кнопку **Переместить**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из телеметрии события

Чтобы переместить устройство на карантин из телеметрии события:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, которое требуется переместить.
2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:
   - Нажмите на название нужного события и выберите устройство.
   - Нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз** и выберите нужное устройство.

   Вы также можете выбрать вкладку **Наблюдаемые объекты**, установить флажок рядом с файлом, который вы хотите переместить на карантин, и нажать на кнопку **Переместить на карантин**.
3. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Поместить на карантин**.
4. В открывшемся окне в правой части экрана укажите следующую информацию в соответствующих полях:
   - Хеш файла.

     Вы можете выбрать **SHA256** или **MD5**.
   - Путь к файлу.
5. Нажмите на кнопку **Переместить**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы переместить устройство на карантин из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, которое требуется переместить.
2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.
3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.
4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Поместить на карантин**.

5. В открывшемся окне в правой части экрана укажите следующую информацию в соответствующих полях:

   - Хеш файла.

     Вы можете выбрать **SHA256** или **MD5**.

   - Путь к файлу.

6. Нажмите на кнопку **Переместить**.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Изменение статуса авторизации устройств

Вы можете изменить статус авторизации устройства, когда анализ алерта или инцидента показывает, что уровень защиты устройства низкий или устройство наносит вред вашей инфраструктуре.

Это действие по реагированию выполняется на устройствах с установленным KICS for Networks.

Вы можете изменить статус авторизации устройства одним из следующих способов:

- из деталей алерта или инцидента;
- из свойств устройства;
- из телеметрии события;
- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы изменить статус авторизации устройства, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Изменение статуса авторизации устройств из деталей алерта или инцидента

Чтобы изменить статус авторизации устройства из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, статус авторизации которого необходимо изменить.
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, статус авторизации которого необходимо изменить.

2. В открывшемся окне выберите вкладку **Активы**.

3. Установите флажок рядом с устройством, статус авторизации которого нужно изменить.

   При необходимости вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Изменить статус авторизации**.

5. В открывшемся окне в правой части экрана выберите новый статус устройства (*авторизован* или *не авторизован*) и нажмите на кнопку **Изменить**.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Изменение статуса авторизации устройств из сведений об устройстве

Чтобы изменить статус авторизации устройства из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, статус авторизации которого необходимо изменить.

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, статус авторизации которого необходимо изменить.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотреть свойства**.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Изменить статус авторизации**.

5. В открывшемся окне в правой части экрана выберите новый статус устройства (*авторизован* или *не авторизован*) и нажмите на кнопку **Изменить**.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Изменение статуса авторизации устройств из телеметрии события

Чтобы изменить статус авторизации устройства из телеметрии события:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, в котором указано устройство, статус авторизации которого необходимо изменить.

2. В открывшемся окне выберите вкладку **Подробнее** и выполните одно из следующих действий:

   - Нажмите на название нужного события и выберите устройство.

   - Нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз** и выберите нужное устройство.

3. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Изменить статус авторизации**.

4. В открывшемся окне в правой части экрана выберите новый статус устройства (*авторизован* или *не авторизован*) и нажмите на кнопку **Изменить**.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Изменение статуса авторизации устройств из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы изменить статус авторизации устройства из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано устройство, статус авторизации которого необходимо изменить.

2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.

3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите **Изменить статус авторизации**.

5. В открывшемся окне в правой части экрана выберите новый статус устройства (*авторизован* или *не авторизован*) и нажмите на кнопку **Изменить**.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выбранный статус авторизации устройства отображается в карточке алерта или инцидента на вкладке **Активы** → столбец **Статус авторизации**.

Просмотр информации о пользователях KASAP и изменении учебных групп

После настройки интеграции между KASAP и KUMA в Консоли OSMP при просмотре данных о пользователях, связанных с алертами или инцидентами, становится доступна следующая информация из KASAP:

- Учебная группа, к которой принадлежит пользователь.
- Учебные курсы, пройденные пользователем.
- Запланированные учебные курсы и их текущий прогресс.

Вы можете просмотреть данные о пользователе KASAP. Для этого вам необходимо открыть данные пользователя одним из следующих способов:

- в деталях алерта или инцидента;

- из события телеметрии (если вы открываете его из деталей алерта);
- в графе расследования.

> Этот параметр доступен, если граф расследования построен.

Чтобы открыть данные пользователя:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, выберите раздел **Алерты** или **Инциденты**.

   Если вы хотите открыть данные пользователя из события телеметрии, выберите раздел **Алерты**.

   Если вы хотите открыть данные пользователя из графа расследования, выберите раздел **Инциденты**.

2. Нажмите на идентификатор нужного алерта или инцидента.
3. В открывшемся окне выполните одно из следующих действий:

   - Если вы хотите открыть сведения о пользователе из события телеметрии, выберите вкладку **Подробнее**, а затем либо нажмите на имя требуемого события и выберите пользователя, либо нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужного пользователя.
   - Если вы хотите открыть данные пользователя из деталей алерта или инцидента, выберите вкладку **Активы** и нажмите на имя нужного пользователя.
   - Если вы хотите открыть данные пользователя из графа расследования, нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на имя нужного пользователя.

   В правой части экрана откроется окно **Информация об учетной записи**.

4. Выберите вкладку **Курсы по кибербезопасности**.

   В окне отображается информация о пользователе KASAP.

Вы можете изменить учебную группу пользователя KASAP одним из следующих способов:

- из деталей алерта или инцидента;
- из события телеметрии (если вы открываете его из деталей алерта);
- из графа расследования.

> Этот параметр доступен, если граф расследования построен.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука. В этом случае, если вы переместите пользователя в группу, для которой не начато обучение, пользователь не сможет начать обучение.

> Чтобы выполнить действие по реагированию, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Чтобы изменить учебную группу пользователя KASAP:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, выберите раздел **Алерты** или **Инциденты**.

   Если вы хотите открыть данные пользователя KASAP из события телеметрии, выберите раздел **Алерты**.

   Если вы хотите изменить учебную группу пользователя KASAP на графе расследования, выберите раздел **Инциденты**.

2. Нажмите на идентификатор нужного алерта или инцидента.

3. В открывшемся окне выполните одно из следующих действий:

   - Если вы хотите выполнить действие по реагированию с помощью события телеметрии, выберите вкладку **Подробнее**, а затем либо нажмите на имя требуемого события и выберите пользователя, либо нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужного пользователя.

   - Если вы хотите выполнить действие по реагированию с помощью данных пользователя, выберите вкладку **Активы** и нажмите на имя пользователя.

   - Если вы хотите выполнить действие по реагированию с помощью графа расследования, нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на имя пользователя.

   В правой части экрана откроется окно **Информация об учетной записи**.

4. В раскрывающемся списке **Назначить KASAP-группу** выберите учебную группу KASAP, которую вы хотите назначить пользователю.

   > Пересчет плана обучения пользователя KASAP может занять до 30 минут. В этот период не рекомендуется менять учебную группу KASAP.

   Пользователь перемещен в выбранную группу KASAP. Администратор KASAP в компании получает уведомление об изменении учебной группы, и учебный план пересчитывается для выбранной учебной группы.

Для получения подробной информации об учебных группах и о том, как начать работу, обратитесь к документации KASAP.

Реагирование с помощью Active Directory

Вы можете интегрировать Open Single Management Platform со службами Active Directory, которые используются в вашей организации. Active Directory считается интегрированной с Open Single Management Platform после настройки интеграции между Active Directory и KUMA.

Процесс настройки интеграции Open Single Management Platform и Active Directory заключается в настройке подключений к LDAP. Вам нужно настроить подключения к LDAP отдельно для каждого тенанта.

В результате, если возникнет алерт или инцидент, вы сможете выполнить действия по реагированию в отношении связанных пользователей этого тенанта.

Вы можете выполнить действие по реагированию с помощью Active Directory одним из следующих способов:

- из деталей алерта или инцидента;

- из события телеметрии (если вы открываете его из деталей алерта);

- из графа расследования.

  Этот параметр доступен, если граф расследования построен.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действие по реагированию с помощью Active Directory, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Чтобы выполнить действие по реагированию с помощью Active Directory:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, выберите раздел **Алерты** или **Инциденты**.

   Если вы хотите выполнить действие по реагированию из телеметрии события, выберите раздел **Алерты**.

   Если вы выполняете действие по реагированию из графа расследования, выберите раздел **Инциденты**.

2. Нажмите на идентификатор нужного алерта или инцидента.

3. В открывшемся окне выполните одно из следующих действий:

   - Если вы хотите выполнить действие по реагированию с помощью деталей алерта или инцидента, выберите вкладку **Активы** и нажмите на имя пользователя.

   - Если вы хотите выполнить действие по реагированию с помощью события телеметрии, выберите вкладку **Подробнее**, а затем либо нажмите на имя требуемого события и выберите пользователя, либо нажмите на кнопку **Поиск угроз**, чтобы перейти в раздел **Поиск угроз**, и выберите нужного пользователя.

   - Если вы хотите выполнить действие по реагированию с помощью графа расследования, нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на имя пользователя.

   В правой части экрана откроется окно **Информация об учетной записи**.

4. В раскрывающемся списке **Реагирование через Active Directory** выберите действие, которое вы хотите выполнить:

   - **Заблокировать учетную запись**

     Если учетная запись пользователя заблокирована как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

   - **Сбросить пароль**

     Если пароль учетной записи пользователя сброшен как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

   - **Добавить пользователя в группу безопасности**

     В открывшемся окне в поле **Группа безопасности DN** укажите полный путь к группе безопасности, в которую вы хотите добавить пользователя. Например, CN = HQ Team, OU = Groups, OU = ExchangeObjects, DC = avp, DC = ru. Нажмите на кнопку **Добавить**. В рамках одной операции можно указать только одну группу.

Если пользователь добавлен в группу безопасности как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

- **Удалить пользователя из группы безопасности**

  В открывшемся окне в поле **Группа безопасности DN** укажите полный путь к группе безопасности, из которой вы хотите удалить пользователя. Например, CN = HQ Team, OU = Groups, OU = ExchangeObjects, DC = avp, DC = ru. Нажмите на кнопку **Удалить**. В рамках одной операции можно указать только одну группу.

  Если пользователь удален из группы безопасности как результат действия по реагированию на соответствующий алерт или инцидент, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Реагирование с помощью KATA/KEDR

После настройки интеграции Open Single Management Platform и Kaspersky Anti Targeted Attack Platform вы можете выполнять действия по реагированию на устройстве или с хешом файла одним из следующих способов:

- из деталей алерта или инцидента;
- в свойствах устройства;
- в сведениях о событии.

  Этот параметр доступен для действия по реагированию Добавить правило запрета.

- из графа расследования.

Вы также можете настроить автоматический запуск действия по реагированию при создании или изменении плейбука.

Чтобы выполнить действия по реагированию с помощью Kaspersky Anti Targeted Attack Platform, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Выполнение действия по реагированию из деталей алерта или инцидента

Чтобы выполнить действия по реагированию из деталей алерта или инцидента:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Установите флажок рядом с требуемым устройством.

   При необходимости вы можете выбрать несколько устройств.

4. В раскрывающемся списке **Выбрать действия по реагированию** выберите действие, которое вы хотите выполнить:

   - **Включить сетевую изоляцию**

     Если вы выберете это действие по реагированию для устройства, на котором уже включена сетевая изоляция, параметры будут перезаписаны новыми значениями.

     После выбора этого действия по реагированию необходимо настроить нужные параметры в окне, открывающемся в правой части экрана.

   - **Выключить сетевую изоляцию**

     Вы можете выбрать это действие по реагированию для устройств, на которых включена сетевая изоляция.

   - **Запустить исполняемый файл**

     Исполняемый файл всегда запускается от имени системы и должен быть доступен на устройстве до начала действия по реагированию.

     После выбора этого действия по реагированию необходимо настроить нужные параметры в окне, открывающемся в правой части экрана.

   - **Добавить правило запрета**

     После выбора этого действия по реагированию необходимо настроить нужные параметры в окне, открывающемся в правой части экрана.

   - **Удалить правило запрета**

     Вы можете выбрать это действие по реагированию для устройств, на которых было применено правило запрета.

   Все перечисленные действия по реагированию доступны на устройствах, использующих Kaspersky Endpoint Agent для Windows или Kaspersky Endpoint Security для Windows в роли компонента Endpoint Agent. На устройствах с Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Linux единственным доступным действием по реагированию является **Запустить исполняемый файл**.

5. В открывшемся окне задайте необходимые параметры действия по реагированию, выбранного на шаге 4:

   - Для сетевой изоляции

1. Укажите период изоляции устройства и единицы измерения.
2. Если вы хотите добавить исключение из правила сетевой изоляции, нажмите на кнопку **Добавить исключение** и заполните следующие поля:
   - **Направление сетевого трафика**.

     Вы можете выбрать одно из значений:

     - **Входящий**

       При выборе этого направления необходимо указать диапазон локальных портов в полях **Начальный порт** и **Конечный порт**.

     - **Исходящий**

       При выборе этого направления необходимо указать диапазон удаленных портов в полях **Начальный порт** и **Конечный порт**.

     - **Входящий/Исходящий**

       При выборе этого направления вы не сможете указать диапазон портов.

   - **IP-адрес актива**.
3. Нажмите на кнопку **Включить**.

   Окно закрыто.

- Для запуска исполняемого файла.

1. Заполните следующие поля:
   - **Путь к исполняемому файлу**
   - **Параметры командной строки**
   - **Рабочая директория**
2. Нажмите на кнопку **Запустить**.

   Окно закрыто.

- Для добавления правила запрета

1. Укажите хеш файла, который вы хотите заблокировать:

   - **SHA256**
   - **MD5**

   Если вы хотите указать более одного хеша, нажмите на кнопку **Добавить хеш**.

2. Нажмите на кнопку **Добавить**.

   Окно закрыто.

- **Для удаления правила запрета**

  1. Выберите правило, которое вы хотите удалить:

     - Если вы хотите удалить все правила запрета, выберите **Удалить все**.
     - Если вы хотите удалить правило запрета по хешу файла, в поле **Хеш файла** укажите хеш файла, который нужно удалить.

       Если вы хотите указать более одного хеша, нажмите на кнопку **Добавить хеш**.

  2. Нажмите на кнопку **Удалить**.

     Окно закрыто.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из сведений об устройстве

Чтобы выполнить действия по реагированию из сведений об устройстве:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.

2. В открывшемся окне выберите вкладку **Активы**.

3. Нажмите на имя требуемого устройства и в раскрывающемся списке выберите **Просмотр свойств**.

4. Выполните те же действия, что описаны в шагах 4–5 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действия по реагированию из сведений о событии

Этот параметр доступен для действия по реагированию Добавить правило запрета.

Чтобы выполнить действия по реагированию из сведений об устройстве:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**. В столбце **Идентификатор** нажмите на идентификатор алерта, содержащий требуемое устройство.
2. В открывшемся окне выберите вкладку **Подробнее** и выберите нужный хеш файла.
3. Нажмите на кнопку **Добавить правило запрета** и выберите устройство, для которого вы хотите добавить правило запрета.

   Вы также можете выбрать вкладку **Наблюдаемые объекты**, установить флажок рядом с хешем файла, который вы хотите заблокировать, и нажать на кнопку **Добавить правило запрета**.

4. Выполните те же действия, что описаны в шагах 4–5 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Выполнение действий по реагированию из графа расследования

Этот параметр доступен, если граф расследования построен.

Чтобы выполнить действие по реагированию из графа расследования:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Инциденты**. В столбце **Идентификатор** нажмите на идентификатор инцидента, в котором указано требуемое устройство.
2. В открывшемся окне нажмите на кнопку **Посмотреть на графе**.

   Откроется окно графа расследования.

3. Нажмите на имя устройства, чтобы открыть сведения об устройстве.
4. Выполните те же действия, что описаны в шагах 4–5 в разделе *Выполнение действий по реагированию из свойств устройства*.

Если действие по реагированию завершено успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Если вы столкнулись с ошибкой при выполнении действий по реагированию, вам нужно убедиться, что имя устройства в Open Single Management Platform такое же, как и в Kaspersky Anti Targeted Attack Platform.

Реагирование с помощью UserGate

UserGate включает в себя функции унифицированных решений по управлению угрозами и предоставляет следующие средства защиты вашей локальной сети:

- Сетевой экран.
- Защита от вторжений и атак.
- Антивирусная проверка трафика.
- Контроль приложений.

Поддерживается версия UserGate UTM API 7.

Вы можете реагировать на алерты и инциденты с помощью UserGate, если вы ранее настроили интеграцию между Open Single Management Platform и службой запуска скриптов, а также создали плейбук, который запустит скрипт для реагирования. Вы можете скачать скрипты, перейдя по этой ссылке.

Загрузить скрипты

Логин и пароль для доступа к UserGate хранятся в скрипте ug.py. В этом скрипте вы можете изменить *конечную точку*, *учетную запись* и *пароль*.

Для запуска скриптов требуется Python 3.10.

Чтобы выполнить действие по реагированию с помощью UserGate, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня.

Вы можете создавать плейбуки, которые будут выполнять следующие действия по реагированию с помощью UserGate:

- Блокировка IP-адресов, URL и доменных имен.

  UserGate заблокирует IP-адреса, URL и доменные имена в результате запуска плейбука.

- Выход пользователей.

  Все пользователи, вошедшие в UserGate, будут отключены в результате запуска плейбука.

Чтобы запустить скрипт для реагирования с помощью UserGate:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделе **Алерты** или **Инциденты** нажмите на идентификатор нужного алерта или инцидента.
2. Нажмите на кнопку **Выбрать плейбук** и в открывшемся окне выберите плейбук, который вы создали для реагирования с помощью UserGate.
3. Нажмите на кнопку **Запуск**.

Выбранный плейбук запустит скрипт для реагирования с помощью UserGate.

Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Результат запуска плейбука доступен в деталях алерта или инцидента на вкладке **История**.

Реагирование с помощью Ideco NGFW

Ideco NGFW – это решение, которое действует как фильтр для интернет-трафика в корпоративных и частных сетях. Он позволяет заблокировать IP-адреса и веб-адреса, обнаруженные Open Single Management Platform, если вы ранее настроили интеграцию Open Single Management Platform и службы запуска скриптов.

Поддерживается Ideco NGFW версии 16.0 и выше.

Логин и пароль для доступа к Ideco NGFW хранятся в скрипте для интеграции с Ideco NGFW. Вы можете скачать скрипт по следующей ссылке:

Загрузить скрипт

Чтобы использовать скрипт:

1. Установите скрипт одним из следующих способов:

   - С помощью pip, например:

     ```
     pip install -r requirements.txt
     ```

   - Из WHL-файла, например:

     ```
     pip install ./dist/kaspersky_xdr_ideco_integration-<version>-py3-none-any.whl
     ```

   - Автономная установка.

     Если у вас нет доступа в интернет, вы можете установить скрипт автономно. В этом случае сделайте следующее:

     a. Загрузите зависимости на устройство с доступом в интернет, выполнив следующую команду:

     ```
     pip download -r requirements.txt
     ```

     b. Переместите загруженные зависимости на устройство, на котором вы будете запускать скрипт.

     c. Установите зависимости с помощью команды:

     ```
     pip install --no-index --find-links <путь_к_папке_с_загруженными_зависимостям> -r requirements.txt
     ```

2. Настройте скрипт одним из следующих способов:

   - С помощью ENV-файла, например:

     ```
     cp .env.sample .env
     nano .env
     ```

   - В теле скрипта (ideco.py) измените параметры в следующих строках:

     ```
     BASE_URL: str = getenv("BASE_URL", "https://your-ip:your-port")
     ```

```
LOGIN: str = getenv("LOGIN", "your-login")
PASSWORD: str = getenv("PASSWORD", "your-password")
IP_DENY_LIMIT: int = int(getenv("IP_DENY_LIMIT", 1000))
```

3. Добавьте правила запрета для IP-адресов, обнаруженных Open Single Management Platform, и для вредоносных веб-адресов.

Чтобы добавить правило сетевого экрана, которое будет блокировать IP-адреса:

1. **Запустите скрипт с помощью команды add_firewall_rule**.

   Команда имеет следующую логику:

   1. Проверяет, существуют ли IP-адреса в списке объектов Ideco NGFW.

      Если они существуют, текущий IP-адрес не добавляется.

      Если они не существуют, добавляется текущий IP-адрес.

   2. Проверяет, существует ли список IP-адресов с именем `XDR`.

      Если список существует, он используется повторно, и к нему добавляются IP-адреса.

      Если он не существует, создается список, в который добавляются IP-адреса.

   3. Проверяет, существует ли правило для сетевого экрана с именем `XDR`.

      Если правило сетевого экрана существует, оно используется повторно и к нему добавляется список IP-адресов из шага 2.

      Если оно не существует, создается правило сетевого экрана, и к нему добавляется список IP-адресов из шага 2.

2. Укажите IP-адреса, которые вы хотите заблокировать.

   По умолчанию максимальное количество IP-адресов – 1000. Вы можете изменить это значение, как описано в шаге 2 *Настройка скрипта*.

   Необходимо добавлять действительные IPv4-адреса через запятую и без пробелов, например:

   ```
   python ideco.py add_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
   ```

   Правило запрета для выбранных адресов добавлено, например:

```
![Adding content filtering rule](./assets/screencasts/ideco_add_firewall_rule.gif)
```

Чтобы добавить правило фильтрации, которое будет блокировать вредоносные веб-адреса:

1. **Запустите скрипт с помощью команды add_content_filter_file command**.

Команда имеет следующую логику:

1. Проверяет, существует ли категория с именем `XDR`.

   Если она существует, веб-адреса добавляются в эту категорию.

   Если она не существует, создается категория, а затем к ней добавляются веб-адреса.

2. Проверяет, существует ли правило фильтрации содержимого с именем `XDR`.

   Если правило фильтрации содержимого существует, к нему добавляется категория из шага 1.

   Если оно не существует, создается правило фильтрации содержимого, а затем к нему добавляется категория из шага 1.

2. Укажите веб-адреса, которые вы хотите заблокировать.

   Веб-адреса должны быть разделены запятыми и иметь префиксы http:// или https://, например:

   ```
   python ideco.py add_content_filter_rule --url "https://url_1.com, http://url_2.com.uk,
   http://qwerty.nl, http://zxc.xc"
   ```

Правило запрета для указанных веб-адресов добавлено, например:

```
![Adding content filtering rule]
(./assets/screencasts/ideco_add_content_filtering_rule.gif)
```

Реагирование с помощью Ideco UTM

Ideco UTM – это решение, обеспечивающее следующие средства защиты вашей корпоративной сети:

- Сетевой экран – фильтрация сетевого трафика для защиты сети от несанкционированного доступа.
- Защита от вторжений и атак – выявление и блокирование подозрительных действий для обеспечения целостности системы.
- Антивирусное сканирование трафика – защита от вредоносных приложений и их действий.
- Контроль приложений – блокирование или ограничение выполнения неавторизованных приложений.
- Веб-фильтрация – ограничение доступа пользователей к сайтам, которые вы считаете нежелательными.

Поддерживается версия Ideco UTM 15.7.35.

Вы можете реагировать на алерты и инциденты с помощью Ideco UTM, если вы ранее настроили интеграцию между Open Single Management Platform и службой запуска скриптов, а также создали плейбук, который запустит скрипт для реагирования. В результате запуска плейбука Ideco UTM блокирует IP-адреса, IP-диапазоны или URL, в зависимости от действия, которое вы указали при создании плейбука.

Чтобы разблокировать IP-адреса, IP-диапазоны или URL, которые вы заблокировали, вам нужно создать и запустить другой плейбук.

Вы можете скачать скрипт, перейдя по этой ссылке:

Загрузить скрипт

Логин и пароль для доступа к Ideco UTM хранятся в конфигурационном файле env.sample. Вам нужно скопировать информацию из этого файла в новый файл ENV, который вы создаете, и указать необходимые параметры в новом файле.

Для запуска скрипта требуется Python 3.10.

Чтобы выполнить действие по реагированию с помощью Ideco UTM, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня или Аналитик 2-го уровня.

Чтобы запустить скрипт для реагирования с помощью Ideco UTM:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделах **Алерты** или **Инциденты** нажмите на идентификатор нужного алерта или инцидента.
2. Нажмите на кнопку **Выбрать плейбук** и в открывшемся окне выберите плейбук, который вы создали для реагирования с помощью Ideco UTM.
3. Нажмите на кнопку **Запуск**.

   Выбранный плейбук запустит скрипт для реагирования с помощью Ideco UTM.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Результат запуска плейбука доступен в деталях алерта или инцидента на вкладке **История**.

Реагирование с помощью Redmine

Redmine – это веб-приложение для управления проектами и отслеживания вопросов. Это приложение позволяет автоматизировать сценарий работы с проблемами в проектах Redmine с помощью скрипта, если вы ранее настроили интеграцию Open Single Management Platform со службой запуска скриптов.

Скачайте скрипт по этой ссылке:

Загрузить скрипт

Чтобы использовать скрипт:

1. Установите скрипт одним из следующих способов:

   - С помощью pip, например:

     ```
     pip install -r requirements.txt
     ```

   - Из WHL-файла, например:

     ```
     pip install ./dist/kaspersky_xdr_redmine_integration-1.0-py3-none-any.whl
     ```

   - Автономная установка.

     Если у вас нет доступа в интернет, вы можете установить скрипт автономно. В этом случае сделайте следующее:

     a. Загрузите зависимости на устройство с доступом в интернет, используя следующую команду:

```
pip download -r requirements.txt
```

b. Переместите загруженные зависимости на устройство, на котором вы будете запускать скрипт.

c. Установите зависимости с помощью следующей команды:

```
pip install --no-index --find-links <путь_к_папке_с_загруженными_зависимостям> -r
requirements.txt
```

2. Настройте скрипт одним из следующих способов:

- С помощью ENV-файла, например:

  ```
  cp .env.sample .env
  nano .env
  ```

- В теле скрипта (redmine.py) измените параметры в следующих строках:

  ```
  REDMINE_URL: str = getenv("REDMINE_URL", "http://<ip_or_hostname>")
  REDMINE_PORT: str = getenv("REDMINE_PORT", "8080")
  REDMINE_API_KEY: str = str(getenv("REDMINE_API_KEY", "<redmine_api_key>"))
  ```

Вы можете использовать скрипт для работы с проблемами в Redmine.

- Если вы хотите создать задачу, выполните следующую команду:

  ```
  python redmine.py create_issue "project-identifier" "Issue subject" --description
  "Issue description text" --priority_id <id: int>
  ```

  Результаты:

  ```
  {"issue_id": 57}
  ```

- Если вы хотите обновить проблему, выполните следующую команду:

  ```
  python redmine.py update_issue <issue_id: int> --subject "Subject text to be updated"
  --description "Description text to be updated" --priority_id <id: int>
  ```

  Результаты:

  ```
  {"status": "issue_updated"}
  ```

- Если вы хотите получить информацию о проблеме, выполните следующую команду:

  ```
  python redmine.py get_issue <issue id: int>
  ```

  Результаты:

  ```
  {
  "subject": "86",
  "description": "18",
  "project_name": "Test project",
  "author_name": "Redmine Admin",
  "status_name": "backlog",
  "priority_name": "high",
  "start_date": "24.07.2023",
  "due_date": null,
  "created_on": "24.07.2023 10:56:15",
  "updated_on": "24.07.2023 17:18:38"
  ```

```
}
```

Реагирование с помощью Check Point NGFW

Check Point NGFW – это решение, которое действует как фильтр для интернет-трафика в корпоративных сетях. Интеграция с Check Point NGFW позволяет блокировать IP-адреса и URL, обнаруженные Open Single Management Platform.

Check Point NGFW включает в себя функции унифицированных решений по управлению угрозами и предоставляет следующие средства защиты корпоративных сетей:

- Сетевой экран – фильтрация сетевого трафика для защиты сети от несанкционированного доступа.
- Защита от вторжений и атак – выявление и блокирование подозрительных действий для обеспечения целостности системы.
- Антивирусное сканирование трафика – защита от вредоносных приложений и их действий.
- Контроль приложений – блокирование или ограничение выполнения неавторизованных приложений.
- Веб-фильтрация – ограничение доступа пользователей к сайтам, которые вы считаете нежелательными.

Поддерживается Check Point NGFW версии R81.20 или выше.

Вы можете реагировать на алерты и инциденты с помощью Check Point NGFW, если вы ранее настроили интеграцию между Open Single Management Platform и службой запуска скриптов, а также создали плейбук, который запустит скрипт для реагирования. Чтобы разблокировать заблокированные IP-адреса или URL, вам нужно создать и запустить другой плейбук.

Для запуска скриптов требуется Python 3.10.

Чтобы выполнить действие по реагированию с помощью Check Point NGFW, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня или Аналитик 2-го уровня.

Вы можете скачать скрипты для реагирования по следующей ссылке:

Загрузить скрипт

Учетная запись и пароль для доступа к Check Point NGFW хранятся в файле `.envSample`.

Чтобы использовать скрипт:

1. Установите скрипт одним из следующих способов:
   - С помощью pip, например:
     ```
     pip install -r requirements.txt
     ```

- Автономная установка.

  Если у вас нет доступа в интернет, вы можете установить скрипт автономно. В этом случае сделайте следующее:

  a. Загрузите зависимости на устройство с доступом в интернет, выполнив следующую команду:

  ```
  pip download -r requirements.txt
  ```

  b. Переместите загруженные зависимости на устройство, на котором вы будете запускать скрипт.

  c. Установите зависимости с помощью команды:

  ```
  pip install --no-index --find-links <путь_к_папке_с_загруженными_зависимостям> -r requirements.txt
  ```

2. Настройте скрипт одним из следующих способов:

   - С помощью ENV-файла, например:

     ```
     cp .env.sample .env
     nano .env
     ```

   - В теле скрипта (main.py) измените параметры в следующих строках:

     ```
     BASE_IP: str = getenv("BASE_IP", "your-ip")
     BASE_PORT: str = getenv("BASE_PORT", "your-port")
     LOGIN: str = getenv("LOGIN", "your-login")
     PASSWORD: str = getenv("PASSWORD", "your-password")
     ```

3. Добавьте правила запрета для IP-адресов, обнаруженных Open Single Management Platform, и для вредоносных веб-адресов.

Чтобы добавить правило сетевого экрана, которое будет блокировать IP-адреса:

1. **Запустите скрипт с помощью команды add_firewall_rule**.

   Команда имеет следующую логику:

   1. Проверяет, существуют ли IP-адреса в списке объектов Check Point NGFW.

      Если они существуют, текущий IP-адрес не добавляется.

      Если они не существуют, добавляется текущий IP-адрес.

   2. Проверяет, существует ли список IP-адресов с именем `XDR`.

      Если список существует, он используется повторно, и к нему добавляются IP-адреса.

      Если он не существует, создается список, в который добавляются IP-адреса.

   3. Проверяет, существует ли правило для сетевого экрана с именем `XDR`.

      Если правило сетевого экрана существует, оно используется повторно и к нему добавляется список IP-адресов из шага 2.

      Если оно не существует, создается правило сетевого экрана, и к нему добавляется список IP-адресов из шага 2.

2. Укажите IP-адреса, которые вы хотите заблокировать.

По умолчанию максимальное количество IP-адресов – 1000. Вы можете изменить это значение, как описано в предыдущей инструкции на шаге 2 *Настройка скрипта*.

Необходимо добавлять действительные IPv4-адреса через запятую и без пробелов, например:

```
python main.py add_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
```

Правило запрета для выбранных адресов добавлено, например:

```
![Adding content filtering rule](./assets/screencasts/main_add_firewall_rule.gif)
```

Чтобы удалить правило сетевого экрана, которое блокирует IP-адреса:

1. **Запустите скрипт с помощью команды delete_firewall_rule**.

   Команда имеет следующую логику:

   1. Проверяет, существуют ли IP-адреса в списке объектов Check Point NGFW.

      Если они существуют, текущий IP-адрес не добавляется.

      Если они не существуют, добавляется текущий IP-адрес.

   2. Проверяет, существует ли список IP-адресов с именем `XDR`.

      Если список существует, он используется повторно, и к нему добавляются IP-адреса.

      Если он не существует, создается список, в который добавляются IP-адреса.

   3. Проверяет, существует ли правило для сетевого экрана с именем `XDR`.

      Если правило сетевого экрана существует, оно используется повторно и к нему добавляется список IP-адресов из шага 2.

      Если оно не существует, создается правило сетевого экрана, и к нему добавляется список IP-адресов из шага 2.

2. Укажите IP-адреса, которые вы хотите заблокировать.

   По умолчанию максимальное количество IP-адресов – 1000. Вы можете изменить это значение, как описано в предыдущей инструкции на шаге 2 *Настройка скрипта*.

   Необходимо добавлять действительные IPv4-адреса через запятую и без пробелов, например:

   ```
   python main.py delete_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
   ```

   Правило запрета для выбранных веб-адресов удалено.

Чтобы добавить правило фильтрации, которое будет блокировать вредоносные веб-адреса:

1. **Запустите скрипт с помощью команды add_content_filter_file command**.

Команда имеет следующую логику:

1. Проверяет, существует ли категория с именем `XDR`.

   Если она существует, веб-адреса добавляются в эту категорию.

   Если она не существует, создается категория, а затем к ней добавляются веб-адреса.

2. Проверяет, существует ли правило фильтрации содержимого с именем `XDR`.

   Если правило фильтрации содержимого существует, к нему добавляется категория из шага 1.

   Если оно не существует, создается правило фильтрации содержимого, а затем к нему добавляется категория из шага 1.

2. Укажите веб-адреса, которые вы хотите заблокировать.

   Веб-адреса должны быть разделены запятыми и иметь префиксы http:// или https://, например:

   ```
   python main.py add_content_filter_rule --url "https://url_1.com, http://url_2.com.uk,
   http://qwerty.nl, http://zxc.xc"
   ```

Правило запрета для указанных веб-адресов добавлено, например:

```
![Adding content filtering rule]
(./assets/screencasts/main_add_content_filtering_rule.gif)
```

Чтобы удалить правило фильтрации, которое блокирует вредоносные веб-адреса:

1. **Запустите скрипт с помощью команды delete_content_filter_file**.

   Команда имеет следующую логику:

   1. Проверяет, существует ли категория с именем `XDR`.

      Если она существует, веб-адреса добавляются в эту категорию.

      Если она не существует, создается категория, а затем к ней добавляются веб-адреса.

   2. Проверяет, существует ли правило фильтрации содержимого с именем `XDR`.

      Если правило фильтрации содержимого существует, к нему добавляется категория из шага 1.

      Если оно не существует, создается правило фильтрации содержимого, а затем к нему добавляется категория из шага 1.

2. Укажите веб-адреса, которые вы хотите заблокировать.

   Веб-адреса должны быть разделены запятыми и иметь префиксы http:// или https://, например:

   ```
   python main.py delete_content_filter_rule --url "https://url_1.com,
   http://url_2.com.uk, http://qwerty.nl, http://zxc.xc"
   ```

Правило запрета для указанных веб-адресов удалено.

Чтобы запустить скрипт для реагирования с помощью Check Point NGFW:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделах **Алерты** или **Инциденты** нажмите на идентификатор нужного алерта или инцидента.

2. Нажмите на кнопку **Выбрать плейбук** и в открывшемся окне выберите плейбук, который вы создали для реагирования с помощью Check Point NGFW.

3. Нажмите на кнопку **Запустить**.

   Выбранный плейбук запустит скрипт для реагирования с помощью Check Point NGFW.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Результат запуска плейбука доступен в деталях алерта или инцидента на вкладке **История**.

Реагирование с помощью Sophos Firewall

Sophos Firewall – это решение, обеспечивающее следующие средства защиты вашей корпоративной сети:

- Сетевой экран – фильтрация сетевого трафика для защиты сети от несанкционированного доступа.
- Защита от вторжений и атак – выявление и блокирование подозрительных действий для обеспечения целостности системы.
- Антивирусное сканирование трафика – защита от вредоносных приложений и их действий.
- Контроль приложений – блокирование или ограничение выполнения неавторизованных приложений.
- Веб-фильтрация – ограничение доступа пользователей к сайтам, которые вы считаете нежелательными.

Поддерживается версия Sophos Firewall 19.5.

Вы можете реагировать на алерты и инциденты с помощью Sophos Firewall, если вы ранее настроили интеграцию между Open Single Management Platform и службой запуска скриптов, а также создали плейбук, который запустит скрипт для реагирования. В результате запуска плейбука Sophos Firewall блокирует IP-адреса, IP-диапазоны или URL, в зависимости от действия, которое вы указали при создании плейбука.

Чтобы разблокировать заблокированные IP-адреса, IP-диапазоны или URL, вам нужно создать и запустить другой плейбук.

Вы можете скачать скрипт, перейдя по этой ссылке:

Загрузить скрипт

Логин и пароль для доступа к Sophos Firewall хранятся в конфигурационном файле env.sample. Вам нужно скопировать информацию из этого файла в новый файл ENV, который вы создадите, и указать необходимые параметры в новом файле.

Для запуска скрипта требуется Python 3.10.

Чтобы выполнить действие по реагированию с помощью Sophos Firewall, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня или Аналитик 2-го уровня.

Чтобы запустить скрипт для реагирования с помощью Sophos Firewall:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделах **Алерты** или **Инциденты** нажмите на идентификатор нужного алерта или инцидента.

2. Нажмите на кнопку **Выбрать плейбук** и в открывшемся окне выберите плейбук, который вы создали для реагирования с помощью Sophos Firewall.

3. Нажмите на кнопку **Запуск**.

   Выбранный плейбук запустит скрипт для реагирования с помощью Sophos Firewall.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Результат запуска плейбука доступен в деталях алерта или инцидента на вкладке **История**.

Реагирование с помощью Континент 4

Континент 4 – это решение, обеспечивающее следующие средства защиты вашей корпоративной сети:

- Сетевой экран – фильтрация сетевого трафика для защиты сети от несанкционированного доступа.
- Защита от вторжений и атак – выявление и блокирование подозрительных действий для обеспечения целостности системы.
- VPN-шлюз – создание безопасных туннелей для передачи данных между сетями вашей организации.
- Контроль доступа – управление доступом пользователей к внутренним и внешним сетевым ресурсам на основе правил и политик безопасности.
- Шифрование данных – использование криптографических алгоритмов для защиты передаваемых данных.

Поддерживается Континент 4 версии 4.1.7.

Вы можете реагировать на алерты и инциденты с помощью Континент 4, если вы ранее настроили интеграцию между Open Single Management Platform и службой запуска скриптов, а также создали плейбук, который запустит скрипт для реагирования.

Вы можете создавать плейбуки, которые будут выполнять следующие действия по реагированию с помощью Континент 4:

- Блокировать IP-адреса и URL.

  Континент 4 заблокирует IP-адреса и URL. Чтобы разблокировать IP-адреса или URL, которые вы заблокировали, вам нужно создать и запустить другой плейбук.

- Блокировать индикаторы компрометации (Indicators of Compromise, далее также IoC).

  Континент 4 заблокирует наблюдаемые объекты, которые вы указали в триггере плейбука.

Вы можете скачать скрипт, перейдя по этой ссылке:

Загрузить скрипт

Логин и пароль для доступа к Континент 4 хранятся в конфигурационном файле env.sample. Вам нужно скопировать информацию из этого файла в новый файл ENV, который вы создаете, и указать необходимые параметры в новом файле.

Для запуска скрипта требуется Python 3.10.

Чтобы выполнить действие по реагированию с помощью Континент 4, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня или Аналитик 2-го уровня.

Чтобы запустить скрипт для реагирования с помощью Континент 4:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделах **Алерты** или **Инциденты** нажмите на идентификатор нужного алерта или инцидента.
2. Нажмите на кнопку **Выбрать плейбук** и в открывшемся окне выберите плейбук, который вы создали для реагирования с помощью Континент 4.
3. Нажмите на кнопку **Запуск**.

   Выбранный плейбук запустит скрипт для реагирования с помощью Континент 4.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Результат запуска плейбука доступен в деталях алерта или инцидента на вкладке **История**.

Реагирование с помощью СКДПУ НТ

СКДПУ НТ – это решение для управления привилегированными учетными записями.

Поддерживается СКДПУ НТ версии 7.0.4.

Вы можете реагировать на алерты и инциденты с помощью СКДПУ НТ, если вы ранее настроили интеграцию между Open Single Management Platform и службой запуска скриптов, а также создали плейбук, который запустит скрипт для реагирования.

Вы можете создавать плейбуки, которые будут выполнять следующие действия по реагированию с помощью СКДПУ НТ:

- Завершение пользовательского сеанса. Плейбук завершит все сеансы пользователя при обнаружении подозрительных действий или нарушении правил безопасности.
- Блокировка учетной записи пользователя. Плейбук заблокирует учетную запись пользователя и ограничит доступ пользователя к системе.
- Отзыв прав пользователя. Пользователь будет удален из привилегированной группы и права пользователя будут отозваны.

Вы можете скачать скрипт, перейдя по этой ссылке:

Загрузить скрипт

Логин и пароль для доступа к СКДПУ НТ хранятся в конфигурационном файле env.sample. Вам нужно скопировать информацию из этого файла в новый файл ENV, который вы создаете, и указать необходимые параметры в новом файле.

Для запуска скрипта требуется Python 3.10.

Чтобы выполнить действие по реагированию с помощью СКДПУ НТ, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня или Аналитик 2-го уровня.

Чтобы запустить скрипт для реагирования с помощью СКДПУ НТ:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделах **Алерты** или **Инциденты** нажмите на идентификатор нужного алерта или инцидента.
2. Нажмите на кнопку **Выбрать плейбук** и в открывшемся окне выберите плейбук, который вы создали для реагирования с помощью СКДПУ НТ.
3. Нажмите на кнопку **Запуск**.

   Выбранный плейбук запустит скрипт для реагирования с помощью СКДПУ НТ.

   Если операция завершена успешно, на экране отображается соответствующее сообщение. Иначе отображается сообщение об ошибке.

Результат запуска плейбука доступен в деталях алерта или инцидента на вкладке **История**.

Просмотр истории реагирования из деталей алерта или инцидента

После выполнения действия по реагированию вы можете просмотреть историю реагирования одним из следующих способов:

- В деталях алерта или инцидента.
- В разделе История реагирования.
- В сведениях о плейбуке.

Чтобы просмотреть историю действий по реагированию из деталей алерта или инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты**.
2. Откройте раздел **Алерты** или **Инциденты** и нажмите на идентификатор алерта или инцидента, для которого было выполнено действие по реагированию.
3. В открывшемся окне выберите вкладку **История** и перейдите на вкладку **История реагирований**.

   Отобразится таблица событий, содержащая следующие столбцы:

   - **Время**. Время возникновения события.
   - **Запущено**. Имя пользователя, запустившего действие по реагированию.
   - **События**. Описание события.

- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.
- **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
- **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
  - **В обработке** – действие по реагированию выполняется.
  - **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию завершено с предупреждениями.
  - **Ошибка** – действие по реагированию завершено с ошибками.
  - **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.
- **Плейбук**. Имя плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.
- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

4. Нажмите на значок параметров ( ) и выберите столбцы для отображения в таблице, если необходимо.
5. При необходимости нажмите на значок фильтра ( ) и в открывшемся окне укажите и примените критерий фильтрации:
   - Добавьте фильтр, нажав на кнопку **Добавить фильтр**.
   - Измените фильтр, выбрав необходимые значения в следующих полях:
     - **Свойство**
     - **Условие**
     - **Значение**
   - Удалите фильтр.
   - Удалите все фильтры, нажав на кнопку **Сбросить все**.

Плейбуки

Open Single Management Platform использует плейбуки, которые позволяют автоматизировать рабочие процессы и сократить время, необходимое для обработки алертов и инцидентов.

Плейбуки реагируют на алерты или инциденты в соответствии с заданным *алгоритмом*. Плейбук запускает алгоритм, включающий в себя последовательность действий по реагированию, которые помогают анализировать и обрабатывать алерты или инциденты. Вы можете запустить плейбук вручную или настроить автоматический запуск нужного плейбука.

Автоматический запуск плейбуков выполняется в соответствии с *триггером*, который вы настраиваете при создании плейбука. Триггер определяет условия, которым должен соответствовать алерт или инцидент для автоматического запуска этого плейбука.

> Область действия одного плейбука ограничена только алертами или только инцидентами.

Обратите внимание, что плейбук может принадлежать только одному тенанту и он автоматически наследуется всеми дочерними тенантами родительского тенанта, включая дочерние тенанты, которые будут добавлены после создания плейбука. Вы можете выключить наследование плейбука дочерними тенантами при создании или изменении плейбука.

В Open Single Management Platform есть два типа плейбуков:

- Предустановленные плейбуки

  Предустановленные плейбуки созданы специалистами "Лаборатории Касперского". Эти плейбуки отмечены префиксом [KL] в названии и не могут быть изменены или удалены.

  По умолчанию предустановленные плейбуки работают в режиме **Обучение**. Дополнительные сведения см. в разделе Предустановленные плейбуки.

- Пользовательские плейбуки

  Вы можете сами создавать и настраивать плейбуки. При создании пользовательского плейбука нужно указать область действия плейбука (алерт или инцидент), триггер для автоматического запуска плейбука и алгоритм реагирования на угрозы. Для получения подробной информации о создании плейбука см. раздел Создание плейбуков.

Режимы работы

Вы можете настроить как автоматический, так и ручной запуск плейбуков. Способ запуска плейбука зависит от выбранного режима работы.

Существуют следующие типы режимов работы:

- **Автоматический**. Плейбук в этом режиме работы автоматически запускается при обнаружении соответствующих алертов или инцидентов.
- **Обучение**. Плейбук в этом режиме работы запрашивает разрешение пользователя на запуск при обнаружении соответствующих алертов или инцидентов.
- **Ручной**. Плейбук в этом режиме работы можно запустить только вручную.

Роли пользователей

Вы предоставляете пользователю права на управление плейбуками, назначая пользователям роли.

В таблице ниже представлены права доступа для управления плейбуками и выполнения действий пользователя.

Роль пользователя	Права пользователей				
	Чтение	Запись	Удалить	Выполнение	Подтверждение действия по реагированию
Главный администратор	✓	✓	✓	✓	✓
Администратор SOC	✓	✓	✓	–	–
Младший аналитик	✓	–	–	✓	–
Аналитик 1-го уровня	✓	–	–	✓	–
Аналитик 2-го уровня	✓	✓	✓	✓	–
Менеджер SOC	✓	–	–	–	–
Подтверждающий	✓	–	–	–	✓
Наблюдатель	✓	–	–	–	–
Администратор тенанта	✓	✓	✓	✓	✓

Просмотр таблицы плейбуков

Таблица плейбуков отображается в разделе **Мониторинг и отчеты** → **Плейбуки**. По умолчанию в таблице отображаются плейбуки, относящиеся ко всем тенантам, к которым у вас есть права доступа.

> В таблице плейбуков отображаются все существующие плейбуки, за исключением плейбуков с режимом работы **Удален**.

Чтобы настроить таблицу плейбуков, выполните одно из следующих действий:

- Примените фильтр для тенантов:

  a. Перейдите по ссылке рядом с параметром **Фильтр тенантов**.

  b. Откроется список тенантов.

  c. Установите флажки рядом с требуемыми тенантами.

- Отфильтруйте данные таблицы плейбуков:

  a. Нажмите на кнопку **Фильтр**.

  b. На вкладке **Фильтры** укажите и примените критерий фильтрации в открывшемся меню.

- Если вы хотите скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

Таблица плейбуков настроена и отображает нужные вам данные.

Таблица плейбуков содержит следующую информацию:

- **Имя**. Название пользовательских или предустановленных плейбуков.

  Предустановленные плейбуки отмечены префиксом [KL] в названии и не могут быть изменены или удалены.

- **Режим работы**. Режим работы плейбука, определяющий способ запуска плейбука. Подробнее о режимах работы см. в разделе Плейбуки.
- **Теги**. Теги, которые назначены плейбуку. Вы можете фильтровать плейбуки, используя назначенные теги.
- **Действия по реагированию**. Действия, запускаемые в плейбуках.
- **Запуски**. Общее количество запусков плейбука.
- **Изменена**. Дата и время последнего изменения плейбука.
- **Создана**. Дата и время создания плейбука.
- **Доступность**. Доступность запуска плейбука. Возможные значения:
  - **Доступно**. Все действия по реагированию в плейбуке доступны пользователю.
  - **Недоступно**. Есть действия по реагированию, которые не могут быть запущены пользователем.
- **Родительский тенант**. Имя тенанта, которому принадлежит плейбук.
- **Описание.** Описание плейбука или комментарий. По умолчанию этот столбец скрыт.
- **Область действия**. Область действия плейбука. Возможные значения: **Алерт** или **Инцидент**. По умолчанию этот столбец скрыт.
- **Создал**. Имя пользователя, который создал плейбук. По умолчанию этот столбец скрыт.
- **Обновлено**. Имя пользователя, который изменил плейбук. По умолчанию этот столбец скрыт.

Создание плейбуков

Вы можете создать плейбук для автоматизации анализа угроз и реагирования на них.

Чтобы создать плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Open Single Management Platform также позволяет создать плейбук, соответствующий вашим потребностям, на основе существующего. Подробную информацию см. в разделе Настройка плейбуков:

Чтобы создать плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.

2. Нажмите на кнопку **Создать плейбук**.

   Откроется окно **Создать плейбук**.

3. В поле **Тенант** выберите родительский тенант и дочерние тенанты, для которых нужно запустить плейбук.

   Все дочерние тенанты выбранного родительского тенанта автоматически унаследуют этот плейбук. Чтобы выключить наследование плейбука, снимите флажок рядом с дочерними тенантами. Наследование плейбука будет выключено для всех дочерних тенантов.

   Если вы выберете дочерний тенант, все родительские тенанты будут выбраны автоматически.

4. В поле **Имя** введите имя плейбука.

   Обратите внимание, что имя плейбука должно быть уникальным и не может быть длиннее 255 символов.

   Имя плейбука не должно содержать следующие специальные символы: <> ".

5. При необходимости в поле **Теги** укажите до 30 тегов. Вы можете фильтровать плейбуки, используя назначенные теги.

   Максимальная длина тега составляет 50 символов.

6. При необходимости в поле **Описание** введите описание плейбука или комментарий.

7. В списке **Область действия** выберите следующие параметры:

   - **Алерт**. Плейбук будет запускаться только для алертов.
   - **Инцидент**. Плейбук будет запускаться только для инцидентов.

8. В списке **Режим работы** выберите следующие параметры:

   - **Автоматический**. Плейбук в этом режиме работы автоматически запускается при обнаружении соответствующих алертов или инцидентов.
   - **Обучение**. Плейбук в этом режиме работы запрашивает разрешение пользователя на запуск при обнаружении соответствующих алертов или инцидентов.
   - **Ручной**. Плейбук в этом режиме работы можно запустить только вручную.

9. В списке **Правила запусков** выберите действие, которое будет выполняться, если два или более экземпляра плейбука запускаются одновременно:

   - **Добавить экземпляры плейбука в очередь**. Новый экземпляр плейбука будет запущен после завершения текущего. По умолчанию выбрано это действие.
   - **Завершить текущее выполнение и запустить новый экземпляр**. Выполнение текущего экземпляра плейбука будет прекращено. После этого запускается новый экземпляр плейбука.
   - **Не запускать новые экземпляры плейбука**. Новый экземпляр плейбука не будет запущен. Выполнение текущего экземпляра плейбука будет продолжено.

Список **правил запуска** отображается только в том случае, если выбран режим работы **Автоматический**.

10. В разделе **Триггер** укажите условие для автоматического запуска плейбука.

    Чтобы описать условие срабатывания триггера, используйте выражения jq. Для получения дополнительной информации о выражениях jq см. Руководство по jq.

    В зависимости от того, какой параметр вы выбрали в списке **Область действия** при создании или изменении плейбука, используется модель данных алерта или модель данных инцидента.

    Например, чтобы отфильтровать алерты или инциденты по уровню критичности, укажите следующее выражение:

    ```
    .Severity == "critical"
    ```

    Вы также можете указать сложные выражения для фильтрации алертов или инцидентов.

    Например, чтобы отфильтровать критические алерты или инциденты по имени правила, укажите следующее выражение:

    ```
    [(.Severity == "critical") and (.Rules[] |.Name | contains("Rule_1"))]
    ```

    где `Rules [] | .Name` это имя сработавшего правила.

    Проверка выражений jq настроена. Если вы укажете неверное выражение в разделе **Триггер**, ошибка будет отмечена красным цветом. Если вы хотите просмотреть подробную информацию, наведите курсор мыши на ошибку.

    Если вы выберете режим работы **Ручной**, раздел **Триггер** будет недоступен.

11. Чтобы просмотреть алерты или инциденты, соответствующие плейбуку триггера, в разделе **Сопоставление триггеров** нажмите на кнопку **Найти**.

    Также можно запросить полный список алертов или инцидентов. Для этого в разделе **Триггер** введите `true` и нажмите на кнопку **Найти**.

    Отобразится полный список алертов или инцидентов.

12. В разделе **Алгоритм** укажите последовательность действий по реагированию на алерты или инциденты в формате JSON. Подробнее см. в разделе Алгоритм плейбука.

    При необходимости можно скопировать алгоритм из другого плейбука. Для этого выполните следующие:

    a. Нажмите на кнопку **Скопировать из другого плейбука**.

       Откроется окно **Скопировать из другого плейбука**.

    b. В списке плейбуков выберите плейбук для копирования алгоритма и нажмите на кнопку **Добавить**.

       Алгоритм выбранного плейбука добавлен в раздел **Алгоритм**.

    Проверка выражений jq и синтаксиса JSON настроена. Если вы укажете неверное выражение в разделе **Алгоритм**, ошибка будет отмечена красным цветом. Если вы хотите просмотреть подробную информацию, наведите курсор мыши на ошибку.

13. По умолчанию плейбук запускается только для новых алертов или инцидентов, соответствующих триггеру.

Если вы хотите запустить новый плейбук для существующих алертов или инцидентов, соответствующих триггеру, установите флажок **Запустите плейбук для всех совпадающих алертов или инцидентов. Обратите внимание, что система может быть перегружена**.

14. Нажмите на кнопку **Создать**.

Плейбук создан и отображается в списке плейбуков.

Изменение плейбуков

Чтобы изменить плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Для предустановленных плейбуков вы можете изменить только режим плейбука и правило запуска. Вы также можете просматривать алерты или инциденты, соответствующие предустановленному сценарию.

Чтобы изменить плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.
2. Выполните одно из следующих действий:
   - Выберите плейбук, который требуется изменить. В открывшемся окне **Сведения о плейбуке** нажмите на кнопку **Изменить**.
   - Выберите плейбук из списка и нажмите на кнопку **Изменить**.

   Откроется окно **Настроить плейбук**.
3. Измените свойства плейбука. Дополнительные сведения о свойствах плейбука, которые вы можете изменить, см. в разделе Создание плейбуков.
4. Если вы измените режим работы **Автоматический** или **Обучение**, в списке **Запущенные экземпляры** выберите действие, которое будет применяться к запуску экземпляров плейбуков:
   - **Завершение экземпляров, которые выполняются или ожидают утверждения**.
   - **Завершение тех экземпляров, которые ожидают подтверждения**.
   - **Выполнить все экземпляры, которые выполняются или ожидают утверждения**.
5. Нажмите на кнопку **Сохранить**.

Свойства плейбука изменены и сохранены.

Настройка плейбуков

Вы можете настроить любой плейбук как вам нужно.

Чтобы настроить плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.
2. Откройте плейбук для изменения, выполнив одно из следующих действий:
   - Выберите плейбук, который требуется настроить. В открывшемся окне сведений о плейбуке нажмите на кнопку **Дублировать и изменить**.
   - Выберите плейбук из списка и нажмите на кнопку **Дублировать и изменить**.

   Откроется окно **Настроить плейбук**.
3. Настройте свойства плейбука в соответствии с вашими требованиями.

   Дополнительные сведения о свойствах плейбука, которые вы можете изменить, см. в разделе Создание плейбуков.

   Если вы хотите настроить параметры алгоритма плейбука, см. раздел Алгоритм плейбука.

   > Имя настраиваемого плейбука должно быть уникальным.
4. Нажмите на кнопку **Сохранить**.

Настраиваемый плейбук будет изменен и сохранен.

Просмотр свойств плейбука

Плейбуки позволяют автоматизировать рабочие процессы и сокращать время, необходимое для обработки алертов и инцидентов.

> Чтобы просматривать плейбуки, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Наблюдатель, Администратор тенанта.

Чтобы просмотреть свойства плейбука:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.
2. В списке плейбуков нажмите на имя плейбука, который вы хотите просмотреть.

   Откроется окно **Свойства плейбука**.
3. Переключайтесь между вкладками, чтобы получить информацию о плейбуке.

Общие

Вкладка **Общие** содержит следующую информацию о плейбуке.

- **Тенант**. Имя тенанта, которому принадлежит плейбук.
- **Теги**. Теги, присвоенные плейбуку.

- **Описание**. Описание плейбука.
- **Область действия**. Область действия плейбука. Возможные значения: **Алерт** или **Инцидент**.
- **Создана**. Дата и время создания плейбука.
- **Изменена**. Дата и время последнего изменения плейбука.
- **Триггер**. Описание алертов или инцидентов, запускающих плейбук. Триггер описывается с помощью jq-выражений.
- **Алгоритм**. Описание действий по реагированию, которые запускаются во время выполнения плейбука. Алгоритм описан с помощью JSON.

Вы можете изменить свойства плейбука, нажав на кнопку **Изменить**.

История

Вкладка **История** содержит таблицу, в которой перечислены все плейбуки или действия по реагированию, запущенные в плейбуке. На этой вкладке вы можете просмотреть историю реагирования и завершить запущенные плейбуки или действия по реагированию, нажав на кнопку **Прервать**. Вы также можете просмотреть историю действий по реагированию в разделе История реагирования или в деталях алерта или инцидента.

Вы можете группировать и фильтровать данные в таблице следующим образом:

- Нажмите на значок параметров ( ) и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

  Отобразится отфильтрованная таблица устройств.

Таблица содержит следующие столбцы:

- **Действия**. Название действия по реагированию.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в алгоритме плейбука.
- **Начало**. Дата и время запуска плейбука или действия по реагированию.
- **Конец**. Дата и время завершения плейбука или действия по реагированию.
- **ID алерта** или **ID инцидента**. Идентификатор, содержащий ссылку на детали алерта или инцидента.
- **Запущено**. Имя пользователя, запустившего плейбук или действие по реагированию.
- **Подтверждающий**. Имя пользователя, подтвердившего запуск плейбука или действия по реагированию.

  По умолчанию этот столбец скрыт. Чтобы отобразить столбец, нажмите на значок параметров ( ) и выберите столбец **Подтверждающий**.
- **Время подтверждения**. Дата и время, когда пользователь подтвердил или отклонил запуск плейбука или действие по реагированию.

  По умолчанию этот столбец скрыт. Чтобы отобразить столбец, нажмите на значок параметров ( ) и выберите столбец **Время подтверждения**.

- **Статус действия**. Статус выполнения плейбука или действия по реагированию. В этом столбце могут отображаться следующие значения:

  - **Ожидание подтверждения** – действие по реагированию или плейбук ожидают подтверждения для запуска.
  - **В обработке** – действие по реагированию или плейбук выполняются.
  - **Успешно** – действие по реагированию или плейбук завершены без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию или плейбук завершены с предупреждениями.
  - **Ошибка** – действие по реагированию или плейбук завершены с ошибками.
  - **Прервано** – действие по реагированию или плейбук завершены, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию или плейбук завершены, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию или плейбук завершены, так как пользователь отклонил запуск.

  Вы можете нажать на **Статус действия**, чтобы открыть окно с результатом запуска плейбуков или действия по реагированию. Идентификатор запуска может быть использован технической поддержкой.

- **Активы**. Количество активов, для которых запускается плейбук или действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.

- **Тип актива**. Тип актива, для которого запускается действие по реагированию или плейбук. Возможные значения: **Устройство** или **Пользователь**.

Журнал изменений

Вкладка **Журнал изменений** содержит историю изменений плейбука, включая время, автора и описание.

Прерывание работы плейбуков

Вы можете принудительно прервать запущенный плейбук. В этом случае незавершенные действия по реагированию будут прерваны. Завершенные действия по реагированию не будут отменены после завершения плейбука.

Чтобы прервать плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Чтобы прервать плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.
2. В открывшемся окне **Сведения о плейбуке** выберите вкладку **История**.

3. В списке запущенных экземпляров плейбука выберите один или несколько экземпляров, которые вы хотите прервать и нажмите на кнопку **Прервать**.

4. В появившемся окне нажмите на кнопку **Прервать**.

Плейбук прерван.

Удаление плейбуков

Предустановленные плейбуки невозможно удалить.

Чтобы удалить пользовательский плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Чтобы удалить пользовательский плейбук:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.

2. Выполните одно из следующих действий:

   - Выберите плейбук, который требуется удалить. В появившемся окне **Сведения о плейбуке** нажмите на кнопку **Удалить**.

   - Выберите плейбук из списка и нажмите на кнопку **Удалить**.

3. В диалоговом окне нажмите на кнопку **Удалить**.

   Плейбук невозможно удалить, если есть запущенные экземпляры плейбука. В этом случае завершите все запущенные экземпляры перед удалением плейбука.

Удаленные плейбуки будут доступны только для просмотра и копирования в разделе **Плейбуки**.

Запуск плейбуков и действий по реагированию

Запуск плейбуков

В зависимости от ваших требований вы можете настроить способ запуска плейбука. При создании плейбука вы можете выбрать один из следующих режимов работы:

- **Автоматический**. Выберите этот режим работы, если вы хотите запускать автоматически плейбуки и действия по реагированию.

  Плейбуки в этом режиме помогают автоматизировать реагирование на угрозы, а также сокращают время, необходимое для анализа алертов и инцидентов.

- **Обучение**. Выберите этот режим работы, если вы хотите проверить, правильно ли настроен плейбук.

Плейбуки в этом режиме не будут запускаться автоматически при обнаружении соответствующего алерта или инцидента. Вместо этого плейбук запрашивает подтверждения пользователя на запуск.

- **Ручной**. Выберите этот режим работы, если вы хотите запускать плейбук только вручную.

  У плейбуков в этом режиме нет триггера, поэтому вы можете запускать такие плейбуки для любого алерта или инцидента, в зависимости от выбранной области действия плейбука. Дополнительные сведения см. в разделе Запуск плейбуков вручную.

Также можно изменить режим работы плейбука. Дополнительные сведения см. в разделе Изменение плейбуков.

Запуск действий по реагированию

Действия по реагированию могут запускаться вручную, автоматически в рамках плейбука или могут быть настроены на запрос подтверждения пользователя перед запуском в плейбуке. По умолчанию ручное подтверждение действия по реагированию выключено.

Дополнительные сведения о настройке ручного подтверждения действия по реагированию, запущенного в плейбуке, см. в разделе Настройка ручного подтверждения плейбуков и ответных действий.

Запуск плейбуков вручную

Open Single Management Platform позволяет вручную запускать любой плейбук, соответствующий алертам или инцидентам, на которые требуется реагировать.

Чтобы запустить плейбук вручную, вам должна быть присвоена одна из следующих ролей: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Вы также можете запустить плейбук для наблюдаемых объектов и активов, если вы указали эти объекты при создании плейбука и при его запуске.

Запуск плейбука для алерта

Чтобы запустить плейбук вручную для алерта:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Алерты**.
2. В таблице алертов нажмите на ссылку с идентификатором, для которого вы хотите запустить плейбук.
3. В открывшемся окне **Детали алерта** нажмите на кнопку **Выбрать плейбук**.

   Откроется окно **Выбрать плейбук**.
4. В списке плейбуков, соответствующих алертов, выберите плейбук, который вы хотите запустить и нажмите на кнопку **Запуск**.

   Если выбранный плейбук уже запущен для этого алерта, в появившемся окне **Мониторинг и отчеты**, выполните одно из следующих действий:

   - Если вы хотите дождаться завершения текущего экземпляра плейбука, нажмите на кнопку **Подождите и запустите**.

Новый экземпляр плейбука будет запущен после завершения текущего.

- Если вы хотите немедленно запустить новый экземпляр плейбука, нажмите на кнопку **Прервать и запустить новый**.

  Текущий экземпляр плейбука будет прерван, а новый будет запущен.

- Если вы хотите отменить запуск нового плейбука, нажмите на кнопку **Закрыть** (×).

Если выбранный плейбук уже имеет статус **Ожидание подтверждения**, после запуска вручную его статус изменится на **В обработке**.

Плейбук запускается для выбранного алерта. После того, как плейбук будет завершен, вы получите уведомление.

Запуск плейбука для инцидента

Чтобы запустить плейбук вручную для инцидента:

1. В главном меню перейдите в раздел **Мониторинг и отчеты** → **Инциденты** и выберите вкладку **XDR-инциденты**.
2. В таблице инцидентов перейдите по ссылке с идентификатором, для которого вы хотите запустить плейбук.
3. В открывшемся окне **Сведения об инциденте** нажмите на кнопку **Выбрать плейбук**.

   Откроется окно **Выбрать плейбук**.
4. В списке плейбуков, соответствующие инциденту, выберите плейбук, который вы хотите запустить и нажмите на кнопку **Запуск**.

   Если выбранный плейбук уже запущен для этого инцидента, в появившемся окне **Мониторинг и отчеты**, выполните одно из следующих действий:

   - Если вы хотите дождаться завершения текущего экземпляра плейбука, нажмите на кнопку **Подождите и запустите**.

     Новый экземпляр плейбука будет запущен после завершения текущего.

   - Если вы хотите немедленно запустить новый экземпляр плейбука, нажмите на кнопку **Прервать и запустить новый**.

     Текущий экземпляр плейбука будет прерван, а новый будет запущен.

   - Если вы хотите отменить запуск нового плейбука, нажмите на кнопку **Закрыть** (×).

Если выбранный плейбук уже имеет статус **Ожидание подтверждения**, после запуска вручную его статус изменится на **В обработке**.

Плейбук будет запущен для выбранного инцидента. После того, как плейбук будет завершен, вы получите уведомление.

Запуск плейбуков для объектов, указанных пользователями

Вы можете указать наблюдаемые объекты и активы, для которых должен выполняться плейбук. Для этого вам нужно создать плейбук со следующими параметрами:

- В списке **Область действия** выбрать **Алерт** или **Инцидент**.
- В списке **Режим работы** выбрать **Ручной**.
- В разделе **Алгоритм** при настройке действия по реагированию использовать выражения jq, чтобы указать объекты (наблюдаемые объект или активы), для которых вы хотите запустить плейбук. Эти объекты будут входными данными для плейбука при его запуске.

Если вы не укажете объекты в алгоритме плейбука и выберете их только перед запуском плейбука, эти объекты будут проигнорированы.

После того как плейбук создан, вы можете запустить его для выбранных объектов.

Для этого вам должна быть присвоена одна из следующих XDR-ролей: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня или Администратор тенанта.

Чтобы запустить плейбук для выбранных объектов:

1. В главном меню перейдите в раздел **Мониторинг и отчеты**, а затем в разделе **Алерты** или **Инциденты** нажмите на идентификатор алерта или инцидента, из которого вы хотите запустить плейбук.
2. В открывшемся окне нажмите на кнопку **Выбрать плейбук**.

   Откроется окно **Выбрать плейбук**.
3. Выберите параметр **Установите флажок Выберите целевые объекты перед запуском плейбуков** и нажмите на кнопку **Запуск**.
4. В открывшемся окне **Целевые объекты** выберите объекты на вкладках **Наблюдаемые объекты** и **Активы**, для которых вы хотите запустить плейбук, и нажмите на кнопку **Применить и запустить**.

   Плейбук будет запущен для выбранного объекта.

Вы можете просмотреть результат плейбука на вкладке **История** в алерте или инциденте, на вкладке плейбука **История** и в разделе История реагирования.

Например, вы пишете скрипт, который вызывается во время действия по реагированию executeCustomScript. При создании плейбука в разделе **Алгоритм** вы пишете действие по реагированию executeCustomScript с входными данными плейбука. Затем вам нужно запустить скрипт для наблюдаемого объекта с типом IP, который вы выбираете при запуске плейбука. Скрипт использует IP-адрес, который вы выбрали в качестве параметра:

```
{

"dslSpecVersion": "1.0.0",

"version": "1",

"responseActionsSpecVersion": "1",

"executionFlow": [
```

```
{

"responseAction": {

"function": {

"type": "executeCustomScript",

"params": {

"commandLine": "./script.py",

"commandLineParameters": "${ \"-ip \" + ([.input.observables[] | select(.type == \"ip\")]
| map(.value) | join(\",\")) }",

"workingDirectory": "/folder/with/script"

}

},

"onError": "stop"

}

},

{

"responseAction": {

"function": {

"type": "updateBases",

"params": {

"wait": false

},

"assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"

}

}

}

]

}
```

Несколько объектов будут входными данными для плейбука, а список IP-адресов, разделенных запятыми, должны быть входными данными для скрипта:

```
{
"input": {
"observables": [
{
"type": "ip",
"value": "127.0.0.1"
},
{
"type": "ip",
"value": "127.0.0.2"
},
{
"type": "md5",
"value": "29f975b01f762f1a6d2fe1b33b8e3e6e"
}
],
"assets":[
{
"AttackerOrVictim": "unknown",
"ID": "c13a6983-0c40-4986-ab30-e85e49f98114",
"InternalID": "6d831b04-00c2-44f4-b9e3-f7a720643fb7",
"KSCServer": "E5DE6B73D962B18E849DC0BF5A2BA72D",
"Name": "VIM-W10-64-01",
"Type": "host"
}
]
}
```

После того как выражения jq выполнят вычисления с операционными данными плейбука, следующая информация передается в качестве параметров командной строки:

```
-ip 127.0.0.1,127.0.0.2
```

Для плейбука, ожидающего входных данных, если вы указали разные типы объектов при создании плейбука и при его запуске или если вы не выбрали параметр **Выбрать целевые объекты перед запуском плейбука**, плейбук завершится с одним из следующих результатов:

- Произойдет ошибка, поскольку плейбук не получил входных данных.
- Действие не будет выполнено, поскольку плейбук содержит условие или цикл, основанный на входных данных.
- Результат будет зависеть от ответа приложения, службы или скрипта, выполняющего действие.

Запуск плейбуков в режиме Обучение

Режим работы **Обучение** позволяет вам проверять, правильно ли настроен плейбук. Это может быть полезно, если вы планируете изменить режим работы плейбука на **Автоматический**.

Все плейбуки в режиме **Обучение** требуют подтверждения запуска пользователем.

> Чтобы запустить плейбук в режиме работы **Обучение**, вам должна быть присвоена одна из следующих ролей: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.

Плейбук в режиме работы **Обучение** не может быть запущен автоматически при регистрации запускающего алерта или инцидента. Вы можете протестировать запуск плейбука в режиме работы **Обучение** одним из следующих способов:

- Создайте алерт или инцидент, соответствующий триггеру плейбука.
- Измените алерт или инцидент, соответствующий триггеру плейбука. Алерт или инцидент должны иметь статус, отличный от **Закрыт**.

Когда одно из вышеуказанных действий выполнено, плейбук запрашивает подтверждение пользователя для запуска. Дополнительные сведения о том, как подтвердить плейбук, см. в разделе Подтверждение плейбуков или действий по реагированию.

Настройка ручного подтверждения действий по реагированию

Open Single Management Platform позволяет настроить подтверждение действия по реагированию, запущенное в пользовательском плейбуке, вручную. По умолчанию ручное подтверждение действия по реагированию выключено.

> Перед настройкой подтверждения вручную убедитесь, что настроены уведомления по электронной почте для тенантов и указан адрес электронной почты подтверждающего.

Рекомендуется настроить ручное подтверждение следующих действий по реагированию: перемещение устройств в другую группу администрирования, перемещение файлов на карантин, включение и выключение сетевой изоляции, реагирование на учетные записи с помощью Active Directory и обогащение данных.

Чтобы настроить подтверждение действия по реагированию вручную:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Плейбуки**.
2. Откройте плейбук для изменения, выполнив одно из следующих действий:
   - Выберите плейбук, который требуется изменить. В открывшемся окне **Сведения о плейбуке** нажмите на кнопку **Изменить**.
   - Выберите плейбук из списка и нажмите на кнопку **Изменить**.

     Если вы выберете более одного плейбука, кнопка **Изменить** будет неактивна.

   Откроется окно **Настроить плейбук**.
3. В разделе **Алгоритм** укажите один из следующих параметров действия по реагированию, для которого вы хотите включить подтверждение вручную:
   - Чтобы включить подтверждение действия по реагированию вручную со временем подтверждения по умолчанию, укажите следующий параметр:

     ```
     "manualApprove": true
     ```

     По умолчанию время подтверждения составляет 60 минут.
   - Чтобы разрешить подтверждение действия по реагированию вручную с настраиваемым временем подтверждения, укажите следующий параметр:

     ```
     "manualApprove": {"timeout": "period"}
     ```

     где `"период"` – регулируемое время подтверждения.

     Вы можете настроить время подтверждения в часах (h) и/или минутах (m), например:

     ```
     "manualApprove": {"timeout": "20h"}
     "manualApprove": {"timeout": "2h30m"}
     ```
   - Чтобы включить ручное подтверждение действия по реагированию с уведомлениями, отправляемыми на адрес электронной почты подтверждающего, укажите следующий параметр:

     ```
     "emailNotifications": {
      "enabled":true
     }
     ```
   - Чтобы включить ручное подтверждение действия по реагированию с уведомлением, которое отправляется на адрес электронной почты подтверждающего по прошествии определенного периода времени, укажите следующий параметр:

```
"manualApprove": {
 "emailNotifications": {
 "enabled": true,
 "delay": "period"
 }
```

где `"период"` – регулируемое время отправления.

Вы можете настроить время отправки в минутах, например:

```
"delay": "20m"
```

4. Нажмите на кнопку **Сохранить**.

Подтверждение действия по реагированию вручную настроено. Уведомления по электронной почте с запросом на подтверждение действия по реагированию будут отправлены на адрес электронной почты, указанный в свойствах учетной записи пользователя.

Вы можете просмотреть запросы на подтверждение действия по реагированию в разделе **Запросы об утверждении**.

Подтверждение плейбуков или действий по реагированию

Все плейбуки в режиме **Обучение** требуют подтверждения пользователя. Вы также можете настроить подтверждение вручную действий по реагированию, запускаемых в плейбуках.

Действия по реагированию для активов, которые являются КИИ-объектами (первой, второй или третьей категории значимости; а также объектами CII без категории значимости), всегда требуют подтверждение пользователя, независимо от параметров подтверждения действия по реагированию в алгоритме плейбука.

Чтобы подтвердить или отклонить плейбук, вам должна быть присвоена одна из следующих ролей: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Администратор тенанта.
Чтобы подтвердить или отклонить запуск действия по реагированию, вам должна быть присвоена из следующих ролей: Главный администратор, Подтверждающий, Администратор тенанта.

Если есть плейбуки или действия по реагированию, ожидающие подтверждения пользователя, в верхней части Консоли Open Single Management Platform отображается уведомление. Кроме того, если для запуска действия по реагированию требуется подтверждение пользователя, на адрес электронной почты отправляется уведомление в течение периода, указанного в алгоритме плейбука.

Просмотр списка плейбуков и действий по реагированию

Чтобы просмотреть список плейбуков и действий по реагированию, ожидающих подтверждения, выполните одно из следующих действий:

- Перейдите по ссылке **Просмотр запросов на утверждение** в верхней части Консоли Open Single Management Platform.

- Перейдите по ссылке в уведомлении, которое было отправлено на ваш адрес электронной почты.

Откроется панель **Запросы об утверждении**, содержащая полный список запросов на подтверждение.

Таблица **Запросы об утверждении** содержит следующие столбцы:

- **Время**. Дата и время, когда плейбук или действие по реагированию запросили подтверждения пользователя.
- **Срок утверждения**. Дата и время, до которых пользователь должен подтвердить или отклонить плейбук или действие по реагированию. Если к этому времени пользователь не подтвердил плейбук или действие по реагированию, запуск отменяется.
- **Плейбук**. Имя пользовательского или предустановленного плейбука, который запрашивает подтверждение пользователя.
- **Действие по реагированию**. Действия, запускаемые в плейбуках.
- **Активы**. Количество активов, для которых запускается плейбук или действие по реагированию. Вы можете просмотреть список активов, для которых требуется подтверждение пользователя, нажав на ссылку с количеством активов.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию или алгоритме плейбука.
- **ID алерта или инцидента**. Идентификатор, содержащий ссылку на детали алерта или инцидента.

Подтверждение и отклонение плейбуков

Чтобы подтвердить или отклонить плейбук:

1. В уведомлении в верхней части Консоли Open Single Management Platform нажмите на ссылку **Просмотр запросов на утверждение**.

   Уведомление со ссылкой **Просмотр запросов на утверждение** отображается только в том случае, если существует плейбук, ожидающий подтверждения пользователя.

2. В открывшейся панели **Запросы об утверждении** выберите один или несколько плейбуков, а затем выполните одно из следующих действий:

   - Чтобы подтвердить запуск плейбука, нажмите на кнопку **Одобрить**.

     После этого плейбук запускается. Статус действия **История реагирований** изменится на **В обработке**

   - Чтобы отклонить запуск плейбука, нажмите на кнопку **Отклонить**.

     После этого запуск плейбука отменен. Статус действия **История реагирований** изменится на **Отклонено**.

3. Нажмите на кнопку **Закрыть** (✕), чтобы закрыть панель **Запросы об утверждении**.

После подтверждения или отклонения плейбуков вы можете просмотреть их статусы в разделе **История реагирований**.

Подтверждение и отклонение действий по реагированию

Чтобы подтвердить или отклонить действия по реагированию:

1. В уведомлении в верхней части Консоли Open Single Management Platform нажмите на ссылку **Просмотр запросов на утверждение**.

   Уведомление со ссылкой **Просмотр запросов на утверждение** отображается только в том случае, если существует действие по реагированию, ожидающее подтверждения пользователя.

   Откроется панель **Запросы об утверждении**.

2. В открывшейся панели **Запросы об утверждении** в столбце **Активы** перейдите по ссылке с количеством активов.

   Откроется панель **Активы для подтверждения**, содержащая полный список активов.

3. Проверьте список активов, для которых требуется подтверждение вручную, а затем выполните одно из следующих действий:

   - Чтобы подтвердить запуск действия по реагированию для активов, выберите один или несколько активов, которые вам нужны, а затем нажмите на кнопку **Одобрить**. После этого запускается действие по реагированию для выбранных активов.

   - Чтобы отклонить запуск действия по реагированию для активов, выберите один или несколько активов, которые вам нужны, а затем нажмите на кнопку **Отклонить**. После этого запуск действия по реагированию для выбранных активов отменяется.

4. Нажмите на кнопку **Закрыть** (×), чтобы закрыть панель **Активы для подтверждения**.

5. Нажмите на кнопку **Закрыть** (×), чтобы закрыть панель **Запросы об утверждении**.

После подтверждения или отклонения действий по реагированию вы можете просмотреть их статусы в разделе **История реагирований**.

Обогащение из плейбуков

После настройки интеграции между Open Single Management Platform и Kaspersky TIP вы можете получить информацию о репутации наблюдаемых объектов, связанных с алертом или инцидентом, из Kaspersky TIP или Kaspersky OpenTIP, а затем дополнить полученные данные.

Вы можете получить информацию только для наблюдаемых объектов следующего типа: домен, URL, IP, MD5, SHA256.

Вы можете настроить автоматическое обогащение данных. Для этого при создании или изменении плейбука в разделе **Алгоритм** необходимо указать следующее:

1. Источник данных.

   Вы можете указать одно из следующих решений:

   - Kaspersky TIP – Kaspersky Threat Intelligence Portal (общий доступ)

- Kaspersky OpenTIP – Kaspersky Threat Intelligence Portal (премиум-доступ)

2. Ограничьте количество данных, возвращаемых Kaspersky TIP или Kaspersky OpenTIP, если это необходимо.

   Вы можете указать одно из следующих значений:

   - Все записи.
   - Топ-100.

     Это значение установлено по умолчанию.

3. Наблюдаемый объект, для которого плейбук запрашивает данные у Kaspersky TIP или Kaspersky OpenTIP.

В алгоритме плейбука вы можете использовать параметры обогащения вывода, отображаемые в полях, которые возвращает Kaspersky TIP.

Вы можете просмотреть результат обогащения для всех наблюдаемых объектов, связанных с алертом или инцидентом, одним из следующих способов:

- в деталях алерта или инцидента;
- в истории реагирования;
- в плейбуке.

Чтобы просмотреть результат обогащения:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** и выполните одно из следующих действий:

   - Если вы хотите просмотреть результат из деталей алерта или инцидента, перейдите в раздел **Алерты** или **Инциденты** и нажмите на идентификатор алерта или инцидента, для которого было выполнено обогащение. В открывшемся окне выберите вкладку **История** и перейдите на вкладку **История реагирования**.
   - Если вы хотите просмотреть результат в истории действий по реагированию, перейдите в раздел **История реагирований**.
   - Если вы хотите просмотреть результаты обогащения из плейбука, перейдите в раздел **Плейбуки** и нажмите на название плейбука, для которого было выполнено обогащение. В открывшемся окне выберите вкладку **История**.

2. В столбце **Статус действия** нажмите на статус плейбука, для которого вы хотите просмотреть результаты обогащения.

Вы также можете получить информацию из Kaspersky TIP и дополнить данные вручную на вкладке **Наблюдаемые объекты** в деталях алерта или инцидента.

Просмотр истории реагирования

Раздел **История реагирований** позволяет просматривать подробную историю реагирования для всех обнаруженных алертов и инцидентов. Обратите внимание, что при удалении алерта или инцидента история реагирования для этого алерта или инцидента не отображается.

Чтобы просмотреть историю действия по реагированию, вам должна быть присвоена: Главный администратор, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Наблюдатель, Администратор тенанта.

Чтобы просмотреть историю реагирования, в главном меню перейдите в раздел **Мониторинг и отчеты** → **История реагирований**. Откроется таблица с историей реагирования на все алерты и инциденты.

Чтобы отфильтровать данные в таблице,

Нажать на кнопку **Фильтр** и на вкладке **Фильтры** указать и применить критерий фильтрации в открывшемся меню.

Таблица содержит следующие столбцы:

- **Действия**. Название действия по реагированию или плейбука.
- **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию или алгоритме плейбука.
- **Начало**. Дата и время запуска плейбука или действия по реагированию.
- **Конец**. Дата и время завершения плейбука или действия по реагированию.
- **ID алерта или инцидента**. Идентификатор, содержащий ссылку на детали алерта или инцидента.
- **Запущено**. Имя пользователя, запустившего плейбук или действие по реагированию.
- **Статус действия**. Статус выполнения плейбука или действия по реагированию. В этом столбце могут отображаться следующие значения:
  - **Ожидание подтверждения** – действие по реагированию или плейбук ожидают подтверждения для запуска.
  - **В обработке** – действие по реагированию или плейбук выполняются.
  - **Успешно** – действие по реагированию или плейбук завершены без ошибок или предупреждений.
  - **Предупреждение** – действие по реагированию или плейбук завершены с предупреждениями.
  - **Ошибка** – действие по реагированию или плейбук завершены с ошибками.
  - **Прервано** – действие по реагированию или плейбук завершены, так как пользователь прервал выполнение.
  - **Истекло время подтверждения** – действие по реагированию или плейбук завершены, так как время подтверждения для запуска истекло.
  - **Отклонено** – действие по реагированию или плейбук завершены, так как пользователь отклонил запуск.

  Вы можете нажать на **Статус действия**, чтобы открыть окно с результатом запуска плейбуков или действия по реагированию. Идентификатор запуска может быть использован технической поддержкой.
- **Активы**. Количество активов, для которых запускается плейбук или действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.

- **Тип актива**. Тип актива, для которого запускается действие по реагированию или плейбук. Возможные значения: **Устройство** или **Пользователь**.

- **Тенант**. Имя тенанта, которому принадлежит плейбук.

Предустановленные плейбуки

Open Single Management Platform предоставляет готовые предустановленные плейбуки, созданные специалистами "Лаборатории Касперского". Предустановленные плейбуки основаны на правилах корреляции KUMA. Дополнительные сведения о правилах корреляции KUMA, включенных в комплект поставки, см. в разделе Правила корреляции.

Вы можете найти предустановленные плейбуки в разделе **Плейбуки**. Такие плейбуки помечаются тегом "Predefined" и префиксом [KL] в названии.

Обратите внимание, что вы не можете изменять параметры предустановленного плейбука, за исключением полей **Режим работы** и **Запущенные экземпляры**. Если вы хотите изменить другие параметры предустановленного плейбука, вам нужно продублировать плейбук, а затем использовать его в качестве шаблона для создания пользовательского плейбука. Подробную информацию см. в разделе Настройка плейбуков:

Перед использованием предустановленных плейбуков в KUMA необходимо выполнить следующие действия:

- Настроить параметры правила обогащения для обогащения событий с выбранным типом **События** в качестве параметра **Тип источника**. Указать значения **VictimUserID** и **AttackerUserID** для параметра **Целевое поле**.

- Настроить обогащение в KUMA, чтобы получить журнал событий Windows.

Предустановленные плейбуки невозможно удалить.

Предустановленные плейбуки принадлежат родительскому тенанту и наследуются всеми дочерними тенантами.

[KL] P001 "Creation of executable files by office applications"

Этот плейбук содержит действие по реагированию Реагирование с помощью KASAP и может использоваться только в качестве шаблона. Если вы хотите запустить плейбук, нажмите на кнопку **Дублировать и изменить**. В открывшемся окне **Настроить плейбук** в разделе **Алгоритм** укажите идентификатор группы KASAP для параметра `groupId`.

Перед использованием плейбука вам нужно настроить обогащение в KUMA, чтобы получить журнал событий Windows.

По умолчанию плейбук запускает действия по реагированию для всех пользователей в алерте. Если вы хотите, чтобы плейбук запускал действия по реагированию только для учетной записи атакуемого, вы можете сделать следующее:

1. В KUMA настройте параметры правила обогащения. Для обогащения событий, для которых выбран тип **События** в качестве параметра **Тип источника** указано значение **VictimUserID** в **Целевое поле**.

2. В разделе плейбука Алгоритм указать `and .IsVictim` в параметре актива как показано ниже:

   `"assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsVictim) | .ID]}"`.

Предустановленный плейбук **[KL]P001 "Creation of executable files by office applications"** позволяет предотвратить использование злоумышленником офисных приложений, например, для выполнения фишинговой атаки, когда пользователь открывает зараженный документ, а затем документ создает исполняемый файл и выполняет его.

Алерт, запускающий плейбук, создается в соответствии с правилом корреляции *Creation of executable files by office applications*. Это правило помогает обнаруживать создание файлов с подозрительными расширениями, такими как скрипты и исполняемые файлы, от имени офисных приложений.

Раздел плейбука **Триггер** содержит следующее выражение:

```
[.OriginalEvents[] | .ExternalID == "R350"] | any
```

Во время выполнения этот плейбук запускает следующие действия по реагированию:

1. Реагирование с помощью Active Directory и сброс паролей как атакующего, так и учетной записи атакуемого.

   Если во время выполнения действия по реагированию возникает ошибка, плейбук прерывается.

2. Реагирование с помощью KASAP и присвоение учетной записи курса информационной безопасности.

   Если во время выполнения действия по реагированию возникает ошибка, выполнение плейбука продолжается.

Раздел плейбука **Алгоритм** содержит следующую последовательность действий по реагированию:

```
{
 "dslSpecVersion": "1.0.0",
 "version": "1",
 "responseActionsSpecVersion": "1",
 "executionFlow": [
 {
 "responseAction": {
 "function": {
 "type": "resetLDAPPassword",
 "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}"
 },
 "onError": "stop"
 }
 },
 {
 "responseAction": {
 "function": {
```

```
 "type": "assignKasapGroup",
 "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}",
 "params": {
 "groupId": "SET KASAP GROUP ID"
 }
 },
 "onError": "continue"
 }
 }
 ]
}
```

[KL] P002 "Windows Event Log was cleared"

По умолчанию этот плейбук работает в режиме **Ручной**. Не рекомендуется переключать этот плейбук в режим работы **Автоматический** или **Обучение**.

Перед использованием плейбука вам нужно выполнить в KUMA следующее:

- Настроить параметры правила обогащения для обогащения событий с **выбранным типом** События **в качестве параметра** Тип источника. Указать значение **AttackerUserID** для параметра **Целевое поле**.
- Настроить обогащение в KUMA, чтобы получить журнал событий Windows.

Предопределенный плейбук **[KL] P002 "Windows Event Log was cleared"** позволяет предотвратить очистку журнала событий Windows атакующим, так как журнал событий содержит данные телеметрии, достаточные для расследования злонамеренных действий атакующего.

Инцидент, запускающий плейбук, содержит один или несколько алертов, созданных в соответствии с правилом корреляции *Windows Event Log was cleared*. Это правило помогает определить, когда журналы событий Windows очищаются или удаляются с помощью утилиты wevutil, пользовательского интерфейса или команд PowerShell. Чтобы включить создание инцидента, вам необходимо настроить правила сегментации.

Раздел плейбука **Триггер** содержит следующее выражение:

```
[.Alerts[] | .OriginalEvents[] | .ExternalID == "R050"] | any
```

Во время выполнения этот плейбук запускает действие по реагированию с помощью Active Directory и блокирует учетную запись атакующего.

Если во время выполнения действия по реагированию возникает ошибка, плейбук прерывается.

Если один или несколько алертов в инциденте генерируются другим правилом корреляции, плейбук не применяется к этим алертам.

Раздел плейбука **Алгоритм** содержит следующую последовательность действий по реагированию:

```
{
 "dslSpecVersion": "1.0.0",
 "version": "1",
 "responseActionsSpecVersion": "1",
```

```
 "executionFlow": [
 {
 "responseAction": {
 "function": {
 "type": "blockLDAPAccount",
 "assets": "${[ incident.Alerts[] | select(.OriginalEvents[] | .ExternalID == \"R050\") |
.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
 },
 "onError": "stop"
 }
 }
 ]
}
```

[KL] P003 "Suspicious child process from wmiprvse.exe"

Перед использованием плейбука вам нужно выполнить в KUMA следующее:

- Настроить параметры правила обогащения для обогащения событий с **выбранным типом** События **в качестве параметра** Тип источника. Указать значение **AttackerUserID** для параметра **Целевое поле**.
- Настроить обогащение в KUMA, чтобы получить журнал событий Windows.

Предопределенный плейбук **[KL] P003 "Suspicious child process from wmiprvse.exe"** позволяет обнаруживать пары родительских и дочерних процессов, которые отклоняются от нормы и должны рассматриваться как подозрительные.

Алерт, который запускает плейбук, создается в соответствии с правилом корреляции *R297_Suspicious child process from wmiprvse.exe*. Это правило помогает обнаружить запуск подозрительных процессов от имени wmiprvse.exe.

Раздел плейбука **Триггер** содержит следующее выражение:

```
[.OriginalEvents[] | .ExternalID == "R297"] | any
```

Во время выполнения этот плейбук запускает следующие действия по реагированию:

1. Действие по реагированию с помощью Active Directory с последующей блокировкой учетной записи атакующего.
2. Прерывание процесса на устройстве, зарегистрированном в алерте.
3. Запускается проверка на наличие вредоносных приложений, а затем выполняется полная проверка устройства, на котором обнаружен алерт.

   По умолчанию сетевые диски не проверяются во избежание перегрузки системы. Если вы хотите проверить сетевые диски, вам нужно продублировать этот плейбук и установить для параметра `allowScanNetworkDrives` значение `true` в разделе **Алгоритм**.

Раздел плейбука **Алгоритм** содержит следующую последовательность действий по реагированию:

```
{
 "dslSpecVersion": "1.0.0",
 "version": "1",
```

```
 "responseActionsSpecVersion": "1",
 "executionFlow": [
 {
 "responseAction": {
 "function": {
 "type": "blockLDAPAccount",
 "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
 },
 "onError": "stop"
 }
 },
 {
 "split": {
 "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and
.DestinationProcessName != \"\")][] | .DestinationProcessName] }",
 "onError": "stop",
 "steps": [
 {
 "responseAction": {
 "function": {
 "type": "killProcess",
 "params": {
 "path": "${ .[0] }"
 },
 "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
 }
 }
 }
 ]
 }
 },
 {
 "responseAction": {
 "function": {
 "type": "avScan",
 "params": {
 "scope": {
 "area": "full",
 "allowScanNetworkDrives": false
 },
 "wait": false
 },
 "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
 },
 "onError": "stop"
 }
 }
 ]
}
```

Если во время выполнения любого действия по реагированию возникает ошибка, плейбук прерывается.

Триггер плейбука

Триггер плейбука – это фильтр, позволяющий выбрать алерты или инциденты, для которых необходимо запустить плейбук. Фильтр (триггер) применяется к каждому объекту (алерту или инциденту) индивидуально и принимает одно значение: `true` или `false`. Триггер состоит из выражений на языке jq, обрабатывающих структурированные данные в формате JSON. Для получения дополнительной информации о выражениях jq см. Руководство по jq.

В Open Single Management Platform используется gojq. Это реализация jq, написанная на языке go, которая имеет следующие отличия от jq:

- Математические функции реализованы более удобным образом.
- В сообщениях об ошибках точно указано место, где нужно исправить ваш запрос.
- Целочисленные вычисления более точные.
- В gojq улучшены функции, которые некорректно работают в jq.

Дополнительные сведения о различиях между gojq и jq см. на сайте GitHub.

Как написать триггер

Вы можете написать триггер в разделе **Триггер** при создании или изменении плейбука.

В зависимости от того, какой параметр вы выбрали в списке **Область действия** при создании или изменении плейбука, используется модель данных алерта или модель данных инцидента.

> Названия параметров в триггере плейбука должны быть такими же, как в модели данных. Обратите внимание, что элементы выражений jq чувствительны к регистру.

> Чтобы избежать перегрузки системы не рекомендуется указывать в триггере данные `OriginalEvents`, `Observables`, `Extra` и `Alerts`.

Когда вы начнете писать триггер, могут отобразится следующие предложения:

- названия функций;
- особые значения;
- поля, которые указаны как идентификаторы объекта в соответствии с моделью данных.

Подходящие значения фильтруются и отображаются в списке предложений, когда вы начинаете писать триггер. Для удобства некоторые предложения содержат строку поиска. Например, если вы хотите указать идентификатор типа инцидента или идентификатор статуса инцидента, вы можете выполнить поиск соответствующей записи по имени и этот идентификатор будет указан в триггере.

> Обратите внимание, что стандартные статусы (*Новый* и *Закрыт*) имеют одинаковые идентификаторы в разных рабочих процессах. Это означает, что триггер будет запускаться для всех инцидентов с указанным идентификатором статуса. Чтобы ограничить количество инцидентов, для которых будет запущен плейбук, в триггере вам нужно указать идентификатор статуса инцидента и тип инцидента.

Язык jq также обеспечивает подсветку синтаксиса и проверку выражений jq. Если в триггере есть недопустимые выражения, вы не можете сохранить плейбук.

При написании триггера используются базовые синтаксические правила.

Чтобы обратиться к свойствам структуры, вам нужно использовать точку "`.`" и указать атрибут, например:

- `.MITRETactics[]` – для просмотра массива тактик MITRE, связанных со всеми сработавшими IOA-правилами в алерте.
- `.MITRETactics[0]` – для просмотра первого элемента из массива тактик MITRE.

Чтобы обратиться к дочерним свойствам, вы можете использовать вертикальную черту (|) или ту же комбинацию без вертикальной черты, например:

- `.Assignee[0].Name` или `Assignee[0] | .Name` – выражение выводит имя пользователя, которому назначен алерт.
- `.MITRETactics[0].ID` или `.MITRETactics[0] | .ID` – выражение выводит идентификатор первой тактики MITRE.

Чтобы получить значение, необходимо использовать следующие операторы: ==, >, <, >=, <=, !=, например:

- `.Assignee[0] | .Name == "user"` – выражение возвращает значение `true`, если алерт назначен пользователю.
- `(.Serverity == "high") and (.DetectSource == "KES")` – выражение возвращает значение `true`, если уровень важности алерта высокий и источником данных является Kaspersky Endpoint Security.
- `[ .DetectionTechnologies[] | . == "IOC" ] | any` – выражение возвращает значение `true`, если срабатывает технология обнаружения IOC.
- `.DetectionTechnologies | length > 1` – выражение возвращает значение `true`, если срабатывает более одной технологии обнаружения.

Для перечисления значений в массиве объектов можно использовать метод `any`, например:

- `[.Assets[] | .Name == "W21H2-X64-3160"] | any` – выражение фильтрует алерты, в которых любой элемент массива `Assets` имеет значение `W21H2-X64-3160` в поле `Name`.
- `[.Observables[] | .Value == "127.0.0.1"] | any` – выражение фильтрует алерты, в которых любой элемент массива `Observables` имеет значение `127.0.0.1` в поле `Value`.
- `[.Assets[].ID]` – для вывода массива идентификаторов.
- `[.Assets[] | select(.AttackerOrVictim=="attacker") | .ID]` – для отображения массива идентификаторов активов, отфильтрованных по полю `AttackerOrVictim`.

Если вы хотите повторно использовать вычисления, укажите переменную с помощью `$`. Например, выражение `event.manual != true as $not_manual | [ .DetectionTechnologies[] | . == "IOC" ] | any and $not_manual` определяет и использует переменную `$not_manual`, которая содержит флаг, показывающий, внесено ли изменение вручную или нет.

Для работы с датами вы можете использовать следующие функции:

- `now` – чтобы получить текущее время Unix в секундах, например, `now == 1690541520.537496`.

- `todate` – чтобы получить текущее время Unix в секундах, например, `now | todate == "2023-07-28T10:47:36Z"`.
- `fromdate` – чтобы преобразовать дату в секунды, например:
  - `.CreatedAt | split(".")[0] + "Z"` – эта команда удаляет миллисекунды и преобразует строку в формат 2023-07-15T07:49:51Z.
  - `(.CreatedAt | split(".")[0] + "Z") | fromdate == 1689407391` – преобразование в секунды завершено.

Jq использует итераторы – интерфейс, который обеспечивает доступ к элементам набора, например к массиву, и позволяет вам перемещаться по ним. Итераторы всегда являются результатом расчета. Разница в количестве элементов, которые содержит итератор. В Open Single Management Platform итератор должен иметь только один элемент. Остальные случаи считаются ошибкой.

Чтобы написать правильный триггер, вам нужно заключить итератор в квадратные скобки (`[...]`). Например, триггер `.DetectionTechnologies[] == "IOC"` вызовет ошибку, так как возвращает итератор с двумя элементами. Правильный триггер должен иметь следующий вид: `[ .DetectionTechnologies == "IOC" ] | any`, где сначала вам нужно использовать `[]`, чтобы обернуть результат сравнения в массив, а затем обработать его с помощью метода `any`, который возвращает значение `true`, если хотя бы один элемент массива `true`. Иначе возвращается `false`.

Когда запускается триггер

Поиск подходящего плейбука начинается при возникновении одного из следующих триггерных событий:

- Новый алерт/инцидент создан.
- Любое поле активного алерта/инцидента изменилось.
- При создании или изменении плейбука пользователь выбрал **Запустите плейбук для всех совпадающих алертов или инцидентов. Обратите внимание, что система может быть перегружена**.

Поддерживаются следующие типы событий изменения алертов:

- Назначение или удаление аналитика.
- Изменение статуса алерта.
- Изменение базовых событий.
- Связывание или удаление связи алерта с инцидентом.
- Изменение значения в поле `ExternalReference`.

Поддерживаются следующие типы событий изменения инцидента:

- Назначение или удаление аналитика.
- Изменение статуса инцидента.
- Изменение базовых событий.
- Связывание или удаление связи алерта с инцидентом.

- Изменение названия инцидента.
- Изменение описания инцидента.
- Изменение приоритета инцидента.
- Изменение значения в поле `ExternalReference`.
- Объединение инцидентов.

Структура алерта/инцидента не содержит данных об изменении алерта/инцидента. Эти данные передаются в дополнительной информации. Если в триггере плейбука вы хотите сослаться на изменения, используйте функцию события без аргументов.

По умолчанию изменения, внесенные вручную в детали алерта или инцидента, игнорируются. Если вы хотите, чтобы плейбук запускался для изменений выполненных вручную, вы должны использовать функцию `event.manual` в триггере, например:

- `event.manual and ([ event.updateOperations[] | . == "alertReopened" ] | any)` – триггер срабатывает, только если алерт повторно открывается вручную.
- `[ event.updateOperations[] | . == "alertLinkedWithIncidentBySystem" ] | any` – триггер срабатывает, только если алерт автоматически связывается с инцидентом.
- `event.manual != null and (([ event.updateOperations[] | . == "alertChangedToNew" ] | any) | not)` – триггер срабатывает, если статус алерта изменяется на любой статус, кроме *Новый*, вручную или автоматически.
- `event == null and .Status == "inIncident"` – триггер работает для всех алертов со статусом *В инциденте*, но только при изменении плейбука, а не алерта.

При необходимости вы можете протестировать примеры jq-выражений, применить фильтры и просмотреть результаты на сервисе Jq playground.

Алгоритм плейбука

Open Single Management Platform позволяет вам реагировать на алерты и инциденты вручную или автоматически с использованием плейбуков. Реагирование на алерты или инциденты может состоять не из одного действия, а из целого набора шагов и параметров. Эти шаги зависят от указанных условий, данных об алерте или инциденте, а также результатов предыдущих действий по реагированию.

Алгоритм плейбука позволяет вам указать последовательность действий по реагированию, необходимые условия и требуемое воздействие на целевые объекты в формате JSON. Шаги алгоритма плейбука выполняются последовательно. Вы можете указать алгоритм плейбука при создании или изменении плейбука.

После запуска, плейбук получает все данные алертов или инцидентов и помещает их в глобальные данные. Плейбук использует следующие данные:

- Глобальные данные.

  Глобальные данные доступны для чтения на любом этапе плейбука. Глобальные данные содержат информацию об алерте или инциденте, для которого был запущен плейбук.

> Вы не можете изменить глобальные данные с помощью плейбука или изменяя данные алерта или инцидента. Глобальные данные остаются неизменными в течение всего времени существования экземпляра плейбука.

- Операционные данные.

  Операционные данные передаются между шагами плейбука. Вы можете управлять операционными данными с помощью выражений jq, которые указаны в параметрах `input` и `output`.

- Локальные данные.

  Локальные данные ограничены определенным шагом. Вы можете управлять локальными данными, используя параметры `input` (создание локальных данных) и `output` (создание операционных данных из локальных данных).

Как написать алгоритм

Алгоритм плейбука описывается в формате JSON и состоит из двух основных частей:

- Общая информация о плейбуке:
  - Название (`name`).
  - Описание (`description`).
  - Источник (`inputType`).
  - Преобразование входных данных плейбука (`input`).
  - Преобразование выходных данных плейбука (`output`).
  - Время ожидания выполнения плейбука (`playbookRunTimeout`).
  - Политики времени ожидания, которые могут быть применены на определенных шагах (`timeouts`).
  - Версия плейбука (`version`).
  - Версия схемы DSL (`dslSpecVersion`).
  - Версия схемы действия по реагированию (`actionsSpecVersion`).
- Шаги выполнения плейбука (`executionFlow`).

Следующие параметры нужны при написании алгоритма:

- `name`
- `inputType`
- `dslSpecVersion`. Требуемое значение: 1.1.0.
- `actionsSpecVersion`
- `version`

- `executionFlow` (хотя бы один шаг выполнения).

  Каждый шаг выполнения имеет свои обязательные поля.

Если вы попытаетесь сохранить плейбук без заполнения обязательных полей, отобразится ошибка.

Алгоритм плейбука чувствителен к регистру. Чтобы использовать данные активов из алерта, вам нужно использовать параметр `Assets` с заглавной буквы. Например: `alert.Assets[]`. Чтобы использовать данные активов во входных данных при запуске плейбука вручную для целевых объектов, не используйте заглавные буквы в параметре `assets`. Например: `.input.assets[]`.

В зависимости от выбранной вами области действия при создании или изменении плейбука вы можете использовать в алгоритме модель данных алерта или модель данных инцидента. Для этого напишите выражения на языке jq со значением `alert` или `incident` (не используйте точку "`.`" в начале значения). Например:

```
"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
```

Вы можете использовать данные алерта или инцидента в выражении jq на любом шаге выполнения. Данные алерта или инцидента доступны только в режиме чтения. Эти данные не изменяются во время работы плейбука. Если данные алерта или инцидента изменились после запуска плейбука, это не повлияет на выполнение плейбука.

Вы также можете использовать выражения jq при использовании данных плейбука в алгоритме. Для получения дополнительной информации о выражениях jq см. Руководство по jq.

Если вы используете кавычки в выражении jq, вам нужно экранировать эти знаки обратными косыми чертами. Например: `"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"`.

Обратные косые черты, которые не используются для экранирования кавычек, также должны быть экранированы другими обратными косыми чертами. Например: `${\"add_firewall_rule --ip_address=\" + ([.input.observables[] | select(.type == \"ip\") | select(.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.).*\") | not) | .value] | join(\",\"))}.`

Если вы хотите запустить плейбук для определенного объекта (наблюдаемые объекты или активы), используйте параметр `.input` в алгоритме. Эти объекты будут входными данными для плейбука при его запуске. Например:

```
"assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
```

Подробнее см. раздел Запуск плейбуков для объектов, указанных пользователями.

Как вызываются подсказки

Если вам нужна подсказка по доступным полям при написании алгоритма, используйте кавычки (`""`). Отобразится список доступных полей.

Чтобы отобразить подсказки по данным алерта или инцидента, напишите в выражении jq параметры `alert` или `incident`, включая точку "`.`" в конце.

Правильная подсказка появляется, если в вышеуказанных выражениях нет ошибок. Иначе список доступных полей может быть некорректным.

Как вызываются подсказки

Вы можете вызывать подсказки при написании алгоритма плейбука. Подсказки содержат строку поиска и помогают вам быстро указать значение поля. Чтобы просмотреть подсказки, используйте кавычки (`""`). Отобразится список подсказок.

Подсказки также позволяют вам выполнять поиск по имени в полях `id` и `statusId`. Когда вы выбираете необходимое значение, имя автоматически изменяется на идентификатор в алгоритме. Подробнее см. Изменение инцидентов с использованием плейбуков и Изменение алертов с использованием плейбуков.

Пример алгоритма плейбука

```
{
 "actionsSpecVersion": "1",
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "playbookRunTimeout": "24h",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "blockLDAPAccount"
 "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
 },
 "onError": "stop"
 }
 },
 {
 "loop": {
 "batchSize": 1,
 "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and .DestinationProcessName
!= \"\")][] | .DestinationProcessName] }",
 "mode": "parallel",
 "onError": "stop",
 "steps": [
 {
 "action": {
 "function": {
 "type": "killProcess",
 "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
 "params": {
 "path": "${ .[0] }"
 }
 }
 }
 }
 ]
 }
 },
 {
 "action": {
 "function": {
 "type": "avScan",
 "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
 "params": {
 "scope": {
 "allowScanNetworkDrives": false,
 "area": "full"
 },
 "wait": false
 }
 },
 "onError": "stop"
 }
 }
 ]
}
```

Параметры плейбука

Идентификатор параметра	Описание
`name`	Имя плейбука. Указывается системой при создании или обновлении плейбука. Если значение задано в алгоритме, оно будет заменено системой.
`description`	Описание плейбука. Указывается системой при создании или обновлении плейбука. Если значение задано в алгоритме, оно будет заменено системой.
`version`	Версия плейбука. Минимальная длина – 1. Этот параметр является обязательным.
`dslSpecVersion`	Версия схемы DSL. Минимальная длина – 1.

	Этот параметр является обязательным.
`responseActionsSpecVersion`	Версия схемы действий по реагированию. Минимальная длина – 1. Этот параметр является обязательным.
`playbookRunTimeout`	Максимальное время выполнения плейбука, включая ожидание в очереди. Максимальное значение – 48 часов (`48h`). Вы можете настроить максимальное время выполнения в часах (ч) и/или минутах (мин), например: По умолчанию указано значение `24h`.
`inputType`	Тип входящего объекта. Возможные значения: `alert` или `incident`. Тип входящего объекта указывается системой при создании или обновлении плейбука. Если значение задано в алгоритме, оно будет заменено системой.
`input`	Выражение jq, которое можно использовать для преобразования или фильтрации входящих данных перед выполнением плейбука.
`output`	Выражение jq, которое можно использовать для изменения вывода плейбука перед выполнением.
`timeouts`	Определения тайм-аута.
`executionFlow`	Шаги выполнения плейбука. Этот параметр является обязательным.

Параметры шага выполнения

Массив элементов шага выполнения описывает логику плейбука. Шаги выполняются в порядке, описанном в плейбуке. Есть несколько типов шагов выполнения:

- ResponseAction
- Split
- Scatter-gather
- Switch
- UpdateData

Параметры ResponseAction

Параметры *Действия по реагированию* вызывают функцию реагирования.

Идентификатор параметра	Описание
`function`	Объект, определяющий действие по реагированию. Дополнительную информацию см. в разделе Параметры ResponseFunction.
`filterProduct`	Этот параметр позволяет фильтровать компоненты для выполнения действия по реагированию. По запросу плагины компонентов фильтруются по разрешенным и ограниченным компонентам. Например, параметр можно указать следующим образом: `"filterProduct": { "allowed": ["Название_приложения"] }`
`output`	Этот параметр позволяет изменить значение, возвращаемое действием по реагированию, с помощью выражения jq и поместить его в данные плейбука (локальные или операционные).
`timeout`	Этот параметр позволяет установить тайм-аут для вызова функциональности реагирования. Вы можете указать имя политики тайм-аута, установленной в плейбуке, или установить значения тайм-аута вручную. Если значение не указано, то используется значение тайм-аута по умолчанию.

`manualApprove`	Этот параметр позволяет настроить подтверждение действия по реагированию вручную. Возможные значения:
	• Логическое значение:
	  • `true` – ручное подтверждение включено с параметрами по умолчанию.
	  • `false` – ручное подтверждение выключено.
	• Объект `ManualApprove`.

`onError`	Этот параметр определяет поведение при возникновении ошибки во время выполнения действия по реагированию. Возможные значения: • `stop` – определяет прерывание плейбука в случае ошибки при выполнении действия по реагированию. • `continue` – определяет, что выполнение плейбука будет продолжено, даже если одно из действий по реагированию завершится с ошибкой. В этом случае плейбук запускает следующее действие по реагированию, указанное в алгоритме. По умолчанию указано значение `stop`. Обратите внимание, что при возникновении системной ошибки выполнение плейбука завершается с ошибкой независимо от указанного значения параметра `onError`.

Политика времени ожидания

Политика времени ожидания шагов выполнения. Система автоматически определяет политику времени ожидания по умолчанию.

Политику времени ожидания по умолчанию можно изменить, используя имя политики по умолчанию. В этом случае новая политика будет автоматически применяться ко всем шагам выполнения.

Идентификатор параметра	Описание
`name`	Имя политики времени ожидания.
`scheduleToCloseTimeout`	Максимальное время выполнения, включая ожидание в очереди и повторные попытки. Параметр указывается в строковом формате Go. Если значение не указано или равно 0, используется значение из поля `playbookRunTimeout`.

Output

Параметр *output* генерирует операционные данные в конце шага, которые затем передаются на следующий шаг. Укажите параметр `output`, если вы хотите использовать результаты текущего шага плейбука на следующем шаге.

Чтобы избежать перегрузки системы, рекомендуется ограничивать данные, помещаемые в данные плейбука (локальные или операционные).

Идентификатор параметра	Описание
`action`	Этот параметр определяет, будут ли данные плейбука (локальные или операционные) перезаписываться или объединяться. Возможные значения: • `merge` – новые данные объединяются с текущими данными. • `overwrite` – текущие данные перезаписываются новыми данными.
`filter`	Этот параметр определяет выражение jq для обработки выходных данных.

Подтвердить вручную

Идентификатор параметра	Описание
`timeout`	Время ожидания подтверждения вручную в минутах. Минимальное значение – 10 минут (`10m`), максимальное – 180 минут (`180m`). По умолчанию это значение равно 60 минут (`60m`).
`emailNotifications`	Этот параметр позволяет настроить отправку уведомлений по электронной почте.

Параметры уведомлений по электронной почте

Идентификатор параметра	Описание
`enabled`	Флаг для включения уведомлений по электронной почте.
`delay`	Этот параметр определяет задержку перед отправкой уведомления по электронной почте. Значение указывается в минутах. Минимальное значение – 5 минут (`5m`), максимальное – 30 минут (`30m`). По умолчанию это значение равно 10 минут (`10m`).

Split

Прежде чем указать параметр `split`, убедитесь, что параметр `aggregate` также указан в алгоритме плейбука.

Параметры *split* используются для разделения массива входящих данных по элементам и для выполнения различных действий с элементами.

Идентификатор параметра	Описание
`input`	Выражение jq для создания массива или ссылки на массив.
`aggregate`	Этот параметр позволяет настроить правила агрегирования с помощью выражения jq.
`output`	Настройка того, как применить выходные данные к текущим данным плейбука. Возможные значения: • Строковая константа: `merge` или `overwrite`. • Объект `Output`.
`mode`	Режим работы Split. Возможные значения: • `parallel` – определяет, что все элементы обрабатываются параллельно. Количество потоков контролируется интерпретатором. • `sequence` – определяет, что все элементы обрабатываются последовательно. По умолчанию значение равно `parallel`.
`batchSize`	Этот параметр позволяет указать количество элементов массива, которые будут обрабатываться в одном цикле или в одном параллельном потоке. Вы можете использовать этот параметр, если функция плагина ограничивает количество входных элементов. Например, если функция плагина может обрабатывать не более 10 элементов в одном цикле, вы можете указать следующее значение параметра: `batchSize = 10`. По умолчанию значение равно `1`.

`onError`	Этот параметр определяет поведение при возникновении ошибки в одной из веток. Возможные значения:
	• `stop` – определяет завершение всех веток, если произошла ошибка. Остальные ветки продолжат работу.
	  • Если `mode=sequence`, после возникновения ошибки в одной ветке все последующие ветки будут остановлены.
	  • Если `mode = parallel`, после возникновения ошибки в одной ветке все ветки будут продолжать работать независимо друг от друга.

	• `continue` – определяет остановку одной из веток, в которой произошла ошибка. Остальные ветки продолжат работу. По умолчанию указано значение `stop`.
`steps`	Массив шагов запуска.

Scatter-gather

Прежде чем указать параметр `scatter-gather`, убедитесь, что параметр `aggregate` также указан в алгоритме плейбука.

Параметры *Scatter-gather* используются для одновременного выполнения нескольких действий с данными. В отличие от Split, параметр Scatter-gather передает одни и те же входные данные в разные ветки выполнения.

Идентификатор параметра	Описание
`input`	Выражение jq для составления массива.
`aggregate`	Этот параметр позволяет настроить правила агрегирования с помощью выражения jq.
`output`	Настройка того, как применить выходные данные к текущим данным плейбука. Возможные значения: • Строковая константа: `merge` или `overwrite`. • Объект `Output`.
`onError`	Этот параметр определяет поведение при возникновении ошибки в одной из веток. Возможные значения: • `stop` – определяет завершение всех веток, если произошла ошибка. Остальные ветки продолжат работу. • `continue` – определяет остановку одной из веток, в которой произошла ошибка. Остальные ветки продолжат работу. По умолчанию указано значение `stop`.
`branches`	Ветки выполнения.

Ветка

Идентификатор параметра	Описание
`name`	Имя ветки, уникальное для Scatter-gather.
`steps`	Массив шагов запуска.

Switch

Шаг, который позволяет выполнить шаг или набор шагов в соответствии с условием. Обратите внимание, что будет выполнено только первое проверенное условие.

Идентификатор параметра	Описание
`conditions`	Массив условий.

Условие

Идентификатор параметра	Описание
`condition`	Выражение jq, содержащие условия выполнения.

`steps`	Шаги выполнения для текущей ветки.

UpdateData

Параметр *UpdateData* можно описать либо как jq-скрипт с логикой изменения состояния, либо как объект `Output`.

Параметры ResponseFunction

Идентификатор параметра	Описание
`responseAction`	Название действия по реагированию.
`params`	Параметр позволяет описать параметры действия по реагированию, которое вы хотите запустить. Вы можете указать параметр как выражение jq или как объект. Параметры действий по реагированию описаны в таблице ниже.
`assets`	Параметр позволяет использовать выражение jq или массив строк, чтобы указать список активов, для которых вы хотите запустить действие по реагированию. Параметр `assets` необходим для действий по реагированию с активами и не применим для действий по реагированию без активов.

Параметры действий по реагированию

Название действия по реагированию	Параметры

`updateBases`	Действием по реагированию является обновление баз. Возможные параметры:
	• `wait`. Возможные значения:
	  • `true`
	  • `false`
	Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`avScan`	Действием по реагированию является поиск вредоносного ПО. Возможные параметры:
	• `wait`. Возможные значения:
	  • `true`
	  • `false`
	• `scope`. Возможные значения:
	  • `full` – выполнить полную проверку устройства, на котором обнаружен алерт.
	  • `critical` – выполнить проверку памяти ядра, запущенных процессов и загрузочных секторов жесткого диска.
	  • `selective` – выполнить проверку указанных файлов. Чтобы указать путь к файлам, используйте параметр `path`.
	• `allowScanNetworkDrives`. Возможные значения:
	  • `true`
	  • `false`
	По умолчанию значение равно `false`.
	Этот параметр доступен только, если вы хотите выполнить полную проверку.
	Обратите внимание, что проверка сетевых дисков может привести к перегрузке системы.

	• `path` – выражение jq или строка с путем к файлам, которые вы хотите проверить. Также вы можете указать несколько путей к файлам. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`moveHostsToAdministrationGroup`	Действием по реагированию является перемещение в группу. Возможные параметры: • `group` – путь к группе администрирования Open Single Management Platform. Например, `HQ/OrgUnit1`. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`quarantineFile`	Действием по реагированию является перемещение на карантин. Возможные параметры: • `path` – путь к файлу, который нужно поместить на карантин. • `md5` – MD5-хеш файла. • `sha256` – SHA256-хеш файла. Вы можете указать параметры действия по реагированию одним из следующих способов: • Укажите полный путь к файлу, который вы хотите поместить на карантин. В этом случае вам не нужно указывать хеш MD5 или хеш SHA256. • Укажите путь к файлу и хеш файла (MD5 или SHA256). Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`killProcess`	Действием по реагированию является прерывание процесса. Возможные параметры: • `pid` – идентификатор процесса. • `path` – путь к файлу, который нужно поместить на карантин. • `md5` – MD5-хеш файла. • `sha256` – SHA256-хеш файла. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`changeAuthorizationStatus`	Действием по реагированию является изменение статуса авторизации. Возможный параметр:
	• `authorized`. Возможные значения:
	  • `true`
	  • `false`
	
	Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.

`netIsolateOn`	Действием по реагированию является включение изоляции сети. Возможные параметры:
	• `isolationTimeoutSec` – период изоляции сети. Вы можете указать этот параметр в часах или днях.
	Минимальное значение в часах – 1 час, максимальное – 9999 часов.
	Минимальное значение в днях – 1 день, максимальное – 416 дней.
	
	Период изоляции сети указывается в секундах.
	
	• `exclusions` – правила исключения. Вы можете указать одно или несколько правил исключения.
	  • `remoteIPV4Address` – сетевой трафик с указанного IPv4-адреса будет исключен из блокировки. Например, `192.168.2.15`.
	  • `remoteIPV6Address` – сетевой трафик с указанного IPv6-адреса будет исключен из блокировки. Например, `2001:0db8:0000:0000:0000:ff00:0042`.
	  • `remotePortRange` – интервал удаленных портов.
	  • `localPortRange` – интервал локальных портов.

	Если `remotePortRange` и `localPortRange` не указаны, правило исключения применяется ко всем портам.
	• `exclusionsConflictBehavior` – определяет поведение в случае конфликта между различными правилами исключения. Возможные параметры:
	  • `replace`
	  • `skip`
	  • `fail`

`netIsolateOff`	Действием по реагированию является выключение изоляции сети. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`executeCommand`	Действием по реагированию является запуск исполняемого файла. Возможные параметры: • `path` – путь к пользовательскому скрипту или исполняемому файлу, который вы хотите запустить. • `workingDirectory` – путь к рабочей директории. • `commandLineParameters` – параметры командной строки, которые вы хотите применить к команде. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`addFilePreventionRules`	Действием по реагированию является добавление правила запрета. Возможные параметры: • `md5` – хеш-массив MD5. • `sha256` – хеш-массив SHA256. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`deleteFilePreventionRules`	Действием по реагированию является удаление правила запрета. Возможные параметры: • `md5` – хеш-массив MD5. • `sha256` – хеш-массив SHA256. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`resetFilePreventionRules`	Действием по реагированию является удаление всех правил запрета. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`assignKasapGroup`	Действием по реагированию является назначение KASAP-группы. Возможные параметры: `groupId` – идентификатор группы KASAP. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`addToLDAPGroup`	Действием по реагированию является добавление пользователя в группу безопасности. Возможные параметры: `groupDN` – отличительное имя (DN) группы LDAP. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`removeFromLDAPGroup`	Действием по реагированию является удаление пользователя из группы безопасности. Возможные параметры: `groupDN` – отличительное имя (DN) группы LDAP. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`blockLDAPAccount`	Действием по реагированию является блокировка учетной записи. Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`resetLDAPPassword`	Действием по реагированию является сброс пароля.

	Чтобы запустить это действие по реагированию, вам необходимо указать параметр `asset` для функции реагирования.
`executeCustomScript`	Действием по реагированию является выполнение пользовательских скриптов. Возможные параметры: • `commandLine` – команда для запуска. • `commandLineParameters` – параметры командной строки, которые вы хотите применить к команде. • `stdIn` – стандартный входной поток. Используйте этот параметр, если для выполнения скрипта требуются дополнительные данные из стандартного ввода. • `workingDirectory` – путь к рабочей директории.

`iocsEnrichment`	Действием по реагированию является обогащение данных. Возможные параметры:
	• `observables` – выражение jq с массивом наблюдаемых объектов, которые вы хотите обогатить.
	• `source` – источник данных. Возможные значения:
	  • `OpenTIP`
	  • `TIP`
	• `fullEnrichment` – определяет количество запрошенных записей. Возможные значения:
	  • `true` – запрашивать все записи из источника.
	  • `false` – запрашивать 100 самых популярных записей из источника.

Изменение инцидентов с использованием плейбуков

Open Single Management Platform позволяет изменять инциденты вручную или с использованием плейбуков. При создании плейбука, вы можете настроить алгоритм плейбука для изменения свойств инцидента.

Чтобы изменить инцидент с помощью плейбука, вам должна быть присвоена одна из следующих ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня или Администратор тенанта.

Вы не можете изменять инциденты, которые имеют статус **Закрыт**.

Вы можете изменить следующие свойства инцидента с помощью плейбука:

- Исполнитель.
- Статус рабочего процесса инцидента.
- Тип инцидента.
- Комментарий.
- Описание.
- Приоритет.
- Атрибут ExternalReference.

- Дополнительный атрибут данных.

Примеры выражений, которые вы можете использовать в алгоритме плейбука для изменения свойств инцидента:

- Назначение инцидента пользователю.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignIncidentToUser",
 "params": {
 "assignee": {
 "id": "user_ID"
 }
 }
 }
 }
 }
 ]
}
```

Во время изменения исполнителя в алгоритме плейбука отображаются подсказки. Для удобства подсказки содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать исполнителя инцидента, вы можете выполнить поиск соответствующей записи по имени пользователя, и этот идентификатор будет указан в алгоритме.

- Отмена назначения инцидента пользователю

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignIncidentToUser",
 "params": {
 "assignee": {
 "id": "nobody"
 }
 }
 }
 }
 }
 ]
}
```

- Изменение статуса рабочего процесса инцидента.

Чтобы изменить статус рабочего процесса инцидента на **Открыт**:

```
{
"dslSpecVersion": "1.1.0",
"version": "1",
"actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentStatus",
 "params": {
 "typeId": "af9dd279-fc30-4596-963b-942f79920375",
 "statusId": "4db36105-5223-4078-b72c-e9e9983b0987"
 }
 }
 }
 }
 ]
}
```

Чтобы изменить статус рабочего процесса инцидента на **Закрыт**:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentStatus",
 "params": {
 "statusId": "INCIDENT_STATUS_ID",
 "statusResolution": "truePositive"
 }
 }
 }
 }
 ]
}
```

Вы также можете указать следующие значения для параметра `statusResolution`: `falsePositive` и `lowPriority`.

Чтобы изменить статус рабочего процесса инцидента на пользовательский статус:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentStatus",
 "params": {
 "typeId": "22222222-2222-2222-2222-222222222222",
 "statusId": "11111111-1111-1111-1111-111111111111"
 }
 }
 }
 }
 ]
}
```

Во время изменения статуса рабочего процесса инцидента в алгоритме плейбука отображаются подсказки. Для удобства предложения содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать статус рабочего процесса инцидента, вы можете выполнить поиск соответствующей записи по названию, и этот идентификатор будет указан в алгоритме.

- Изменение типа инцидента.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentType",
 "params": {
 "id": "INCIDENT_TYPE_UUID"
 }
 }
 }
 }
 ]
}
```

Во время изменения типа инцидента в алгоритме плейбука отображаются подсказки. Для удобства предложения содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать тип инцидента, вы можете выполнить поиск соответствующей записи по названию, и этот идентификатор будет указан в алгоритме.

- Добавление комментария к инциденту.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addCommentToIncident",
 "params": {
 "text": "${ \"Новый комментарий к инциденту с идентификатором: \\(incident.ID)\" }"
 }
 }
 }
 }
 ]
}
```

- Изменение описания инцидента.

```
{
"dslSpecVersion": "1.1.0",
"version": "1",
"actionsSpecVersion": "1",
"executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentDescription",
 "params": {
 "description": "${ incident.ID | tostring | \"New comment for incident with ID: \" + . }",
 "mode": "replace"
 }
 }
 }
 }
 ]
}
```

Чтобы дополнить существующее описание, укажите значение `append` для параметра `mode`.

- Изменение приоритета инцидента.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentPriority",
 "params": {
 "priority": "critical"
 }
 }
 }
 }
 ]
}
```

Вы также можете указать следующие значения для параметра `priority`: `high`, `medium`, `low`.

- Изменение атрибута ExternalReference.

```
{
"dslSpecVersion": "1.1.0",
"version": "1",
"actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setIncidentExternalRef",
 "params": {
 "externalRef": "${ \"новое значение extReference\" }",
 "mode": "replace"
 }
 }
 }
 }
 ]
}
```

Чтобы дополнить атрибут ExternalReference, укажите значение `append` для параметра `mode`.

- Изменение Дополнительного атрибута данных.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addIncidentAdditionalData",
 "params": {
 "data": "${ {\"customKey\": \"customValue\"} }",
 "mode": "replace"
 }
 }
 }
 }
 ]
}
```

Чтобы дополнить Дополнительный атрибут данных, укажите значение `append` для параметра `mode`.

Изменение алертов с использованием плейбуков

Open Single Management Platform позволяет изменять инциденты вручную или с использованием плейбуков. При создании плейбука, вы можете настроить алгоритм плейбука для изменения свойств алерта.

Чтобы изменить алерт с помощью плейбука, вам должна быть присвоена одна из следующих XDR-ролей: Главный администратор, Администратор SOC, Аналитик 1-го уровня, Аналитик 2-го уровня или Администратор тенанта.

Вы не можете изменять алерты, которые имеют статус **Закрыт**.

Вы можете изменить следующие свойства алерта с помощью плейбука:

- Исполнитель.
- Статус алерта.
- Комментарий.
- Атрибут ExternalReference.
- Дополнительный атрибут данных.

Примеры выражений, которые вы можете использовать в алгоритме плейбука для изменения свойств алерта:

- **Назначение алерта пользователю**

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignAlert",
 "params": {
 "assignee": {
 "id": "user_ID"
 }
 }
 }
 }
 }
 ]
}
```

Во время изменения исполнителя в алгоритме плейбука отображаются подсказки. Для удобства подсказки содержат строку поиска, где вы можете выполнить поиск по имени. Если вы хотите указать исполнителя инцидента, вы можете выполнить поиск соответствующей записи по имени пользователя, и этот идентификатор будет указан в алгоритме.

- **Отмена назначения алерта пользователю**

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "assignAlert",
 "params": {
 "assignee": {
 "id": "nobody"
 }
 }
 }
 }
 }
 ]
}
```


- Изменение статуса алерта

Чтобы изменить статус алерта на **В обработке**:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setAlertStatus",
 "params": {
 "status": "inProgress"
 }
 }
 }
 }
 ]
}
```

Чтобы изменить статус алерта на **Закрыт**:

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setAlertStatus",
 "params": {
 "status": "closed",
 "statusResolution": "truePositive"
 }
 }
 }
 }
 ]
}
```

Вы также можете указать следующие значения для параметра statusResolution: `falsePositive` и `lowPriority`.

Когда вы изменяете статус алерта в алгоритме плейбука, могут быть отображены следующие подсказки: `new`, `inProgress`, `closed`.

- Добавление комментария к алерту

```
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addCommentToAlert",
 "params": {
 "text": "${ \"New comment for alert with ID: \" + alert.InternalID }"
 }
 }
 }
 }
 ]
}
```

- Изменение атрибута ExternalReference.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "setAlertExternalRef",
 "params": {
 "externalRef": "${ \"Appended externalRef for alert with ID: \" + alert.InternalID }",
 "mode": "append"
 }
 }
 }
 }
 ]
}
```

Чтобы заменить текущее значение атрибута ExternalReference в алерте значением из плейбука, укажите значение `replace` для параметра `mode`.

- Изменение Дополнительного атрибута данных.

```
{
 "dslSpecVersion": "1.1.0",
 "version": "1",
 "actionsSpecVersion": "1",
 "executionFlow": [
 {
 "action": {
 "function": {
 "type": "addAlertAdditionalData",
 "params": {
 "data": "${ {\"customKey_1 (alert.InternalID)\": (\"customValue_1 (\" + alert.InternalID + \")\" )} }",
 "mode": "append"
 }
 }
 }
 }
 ]
}
```

Чтобы заменить текущее значение атрибута AdditionalData в алерте значением из плейбука, укажите значение `replace` для параметра `mode`.

REST API

В XDR можно обращаться из сторонних решений с помощью API. XDR REST API работает по протоколу HTTP и состоит из набора методов запросов/ответов.

Запросы REST API необходимо отправлять по следующему адресу:

https://api.<XDR FQDN>/xdr/api/v1/<request>

https://api.<XDR FQDN>/xdr/api/v2.1/kuma/<request> (для API, специфичного для KUMA)

Пример:

https://api.example.com/xdr/api/v1/

https://api.example.com/xdr/api/v2.1/kuma/ (для API, специфичного для KUMA)

Создание токена

Чтобы сгенерировать пользовательский API-токен:

1. В главном окне приложения перейдите в раздел **Параметры** → **API-токен**.
2. Нажмите на кнопку **Добавить токен**.
3. В панели **Добавить токен** настройте параметры токена.
   a. Нажмите на **Дата истечения срока действия** и используйте календарь, чтобы указать дату истечения срока действия токена. Если вы хотите выключить автоматическое истечение срока действия токена, установите флажок **Без срока действия**.

      Максимальный срок действия – 365 дней.

      > Рекомендуется включить автоматическое истечение срока действия для токенов, у которых есть доступ к методам POST.

   b. Установите флажки рядом с методами API, к которым вы хотите разрешить доступ.
4. Нажмите на кнопку **Сгенерировать**.
5. Нажмите на кнопку **Копировать и закрыть**.

   > Вы не сможете скопировать токен позже.

Токен создан и скопирован в буфер обмена. Сохраните токен любым удобным способом.

Авторизация запросов API

Каждый запрос API должен включать авторизацию с использованием токенов. Пользователь, чей токен используется для запроса API, должен иметь разрешения на выполнение этого типа запроса.

Каждый запрос должен сопровождаться следующим заголовком:

```
Authorization: Bearer <token>
```

Возможные ошибки

HTTP-код	Описание	Значение поля message
400	Неверный заголовок.	Неверный заголовок авторизации.
403	Токен не существует или пользователь (владелец токена) выключен.	Доступ запрещен.

API-операции

Описание доступных запросов и реагирование.

Просмотр списка алертов

GET /xdr/api/v1/alerts

Возвращает список алертов для указанных тенантов.

Пример:

https://api.example.com/xdr/api/v1/alerts?tenantID=00000000-0000-0000-0000-000000000000&withHistory

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
page	Числовое	Нет	Номер страницы. Начинается с 1. Размер страницы – 100 записей. Если значение не указано или установлено значение меньше 1, используется значение 1.	1
id	Строка	Нет	Идентификатор алерта. Если указано несколько значений, формируется список, к которому применяется логический оператор ИЛИ. Если алерт с указанным идентификатором не найден, это значение идентификатора игнорируется. Если значение идентификатора не указано, возвращаются все алерты для указанных тенантов.	00000000-0000-0000-0000-000000000000
tenantID	Строка	Да	Идентификатор тенанта. Если указано несколько значений, формируется список, к которому применяется логический оператор ИЛИ. Если у пользователя нет права **Чтение** для любого из указанных тенантов, запрос не выполняется.	00000000-0000-0000-0000-000000000000
name	Строка	Нет	Имя алерта. Регистронезависимое регулярное выражение (PCRE).	alert ^My alert$
timestampField	Строка	Нет	Поле данных алерта, используемое для сортировки (в порядке	lastSeen

			убывания) и фильтрации (параметры "от" и "до") списка алертов. По умолчанию указано значение lastSeen.	firstSeen
from	Строка	Нет	Начало периода, используемого для фильтрации списка алертов, в формате RFC3339. Используйте значение timestampField, чтобы указать поле данных алерта.	2021-09-06T00:00:00Z 2021-09-06T00:00:00.000Z 2021-09-06T00:00:00Z+00:00
to	Строка	Нет	Окончание периода, используемого для фильтрации списка алертов, в формате RFC3339. Используйте значение timestampField, чтобы указать поле данных алерта.	2021-09-06T00:00:00Z 2021-09-06T00:00:00.000Z 2021-09-06T00:00:00Z+00:00
status	Строка	Нет	Статус алерта. Если указано несколько значений, формируется список, к которому применяется логический оператор ИЛИ.	new inProgress inIncident closed
withEvents	bool	Нет	Указывает, следует ли включать нормализованные события из KUMA.	/xdr/api/v1/alerts?withEvents /xdr/api/v1/alerts?withEvents=123
withAffected	bool	Нет	Указывает, следует ли включать подробные данные об активах и учетных записях, связанных с алертами.	/xdr/api/v1/alerts?withAffected /xdr/api/v1/alerts?withAffected=123
withHistory	bool	Нет	Указывает, следует ли включать данные об изменениях, внесенных в алерт.	/xdr/api/v1/alerts?withHistory /xdr/api/v1/alerts?withHistory=123

Действие по реагированию

HTTP-код: 200

Формат: JSON

Пример:


```
{
 "Total": 0,
 "Alerts": [
 {
 "ID": 0,
 "InternalID": "881dee1f-380d-4366-a2d8-094e0af4c3f6",
 "TenantID": "string",
 "Assets": [
 {
 "Data": {},
 "ID": "string",
 "IsAttacker": true,
 "IsVictim": true,
 "KSCServer": "string",
 "Name": "string",
 "Type": "host",
 "HostInfo": {
 "ID": "string",
 "TenantID": "string",
 "DisplayName": "string",
 "AssetSource": "string",
 "CreatedAt": 0,
 "IsDeleted": true,
 "IpAddress": [
 "string"
 ],
 "Fqdn": [
 "string"
 ],
 "MacAddress": [
 "string"
 ],
 "DirectCategories": [
```

```
"string"
],
"Weight": "low",
"CiiCategory": "notCII",
"OS": "string",
"OSVersion": "string",
"Sources": [
"ksc"
],
"LastVisible": 0,
"Products": [
{
"ProductVersion": "string",
"ProductName": "string"
}
],
"KSC": {
"GroupID": 0,
"GroupName": "string",
"StatusMask": [
0
],
"StatusID": 0,
"RtProtectionState": 0,
"EncryptionState": 0,
"AntiSpamStatus": 0,
"EmailAvStatus": 0,
"DlpStatus": 0,
"EdrStatus": 0,
"LastAvBasesUpdate": 0,
"LastInfoUpdate": 0,
"LastUpdate": 0,
"LastSystemStart": 0,
"VirtualServerID": 0
},
"KICS": {
"status": "string",
"risks": [
{
"ID": 0,
"Name": "string",
"Category": "string",
"Description": "string",
"DescriptionURL": "string",
"Severity": 0,
"Cvss": 0
}
],
"serverIP": "string",
"connectorID": 0,
"deviceID": 0,
"hardware": {
"Model": "string",
"Version": "string",
"Vendor": "string"
},
"software": {
"Model": "string",
"Version": "string",
"Vendor": "string"
}
}
},
"UserInfo": {
"osmpId": "string",
"tenantID": "string",
"tenantName": "string",
"domain": "string",
"cn": "string",
"displayName": "string",
"distinguishedName": "string",
"mail": "string",
"mailNickname": "string",
"mobile": "string",
"objectSID": "string",
"samAccountName": "string",
"samAccountType": "string",
"telephoneNumber": "string",
"userPrincipalName": "string",
"isArchived": true,
"memberOf": [
"string"
],
"title": "string",
"division": "string",
"department": "string",
"manager": "string",
"location": "string",
"company": "string",
"streetAddress": "string",
"physicalDeliveryOfficeName": "string",
"managedObjects": [
"string"
],
"userAccountControl": "string",
"whenCreated": 0,
"whenChanged": 0,
"accountExpires": 0,
"badPasswordTime": 0
}
}
],
"Assignee": {
"ID": "string",
"Name": "string"
},
"CreatedAt": "2024-01-16T09:55:50.417Z",
"DetectionTechnologies": [
"string"
],
"Extra": {
"additionalProp1": "string",
```

```
  "additionalProp2": "string",
  "additionalProp3": "string"
  },
  "IncidentID": "string",
  "IncidentLinkType": "auto",
  "FirstEventTime": "2024-01-16T09:55:50.417Z",
  "LastEventTime": "2024-01-16T09:55:50.417Z",
  "MITRETactics": [
  {
  "ID": "string"
  }
  ],
  "MITRETechniques": [
  {
  "ID": "string"
  }
  ],
  "Observables": [
  {
  "Details": "string",
  "Type": "ip",
  "Value": "string"
  }
  ],
  "OriginalEvents": [
  {}
  ],
  "Rules": [
  {
  "Confidence": "high",
  "Custom": true,
  "ID": "string",
  "Name": "string",
  "Severity": "critical",
  "Type": "string"
  }
  ],
  "Severity": "critical",
  "SourceCreatedAt": "2024-01-16T09:55:50.417Z",
  "SourceID": "string",
  "ExternalRef": "string",
  "Status": "new",
  "StatusChangedAt": "2024-01-16T09:55:50.417Z",
  "StatusResolution": "truePositive",
  "UpdatedAt": "2024-01-16T09:55:50.417Z"
  "HistoryRecords": [
  {
  "entityID": "string",
  "entityKind": "Alert",
  "tenantID": "string",
  "type": "alertAssigned",
  "createdAt": "2024-03-12T11:10:59.329Z",
  "params": {}
  }
  ]
  }
  ]
}
```


Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Недопустимое значение timestampField.	Недопустимое поле отметки времени.	
400	Недопустимое значение "от".	Не удалось проанализировать.	Переменная.
400	Недопустимое значение.	Не удалось проанализировать.	Переменная.
400	Значение ID не в формате UUID.		
400	Недопустимое значение статуса.	invalid status	
403	Пользователь не имеет необходимых прав в функциональной области **Алерты и инциденты** ни у одного из указанных тенантов.	Доступ запрещен.	
500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Просмотр списка инцидентов

GET /xdr/api/v1/incidents

Возвращает список инцидентов для указанных тенантов.

Пример:

https://api.example.com/xdr/api/v1/incidents?tenantID=00000000-0000-0000-0000-000000000000&withHistory

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
page	Числовое	Нет	Номер страницы. Начинается с 1. Размер страницы – 100 записей. Если значение не указано или установлено значение меньше 1, используется значение 1.	1
id	Строка	Нет	Идентификатор инцидента. Если указано несколько значений, формируется список, к которому применяется логический оператор ИЛИ. Если инцидент с указанным идентификатором не найден, это значение идентификатора игнорируется. Если значение идентификатора не указано, возвращаются все инциденты для указанных тенантов.	00000000-0000-0000-0000-000000000000
tenantID	Строка	Да	Идентификатор тенанта. Если указано несколько значений, формируется список, к которому применяется логический оператор ИЛИ. Если у пользователя нет права **Чтение** для любого из указанных тенантов, запрос не выполняется.	00000000-0000-0000-0000-000000000000
name	Строка	Нет	Имя инцидента в формате Perl Compatible Regular Expression (PCRE). Если имя не указано, возвращаются все инциденты для указанных тенантов.	incident ^My incident$
timestampField	Строка	Нет	Поле данных инцидента, используемое для фильтрации списка инцидентов. Используйте значения "от" и "до", чтобы указать период.	createdAt updatedAt statusChangedAt
from	Строка	Нет	Начало периода, используемого для фильтрации списка инцидентов, в формате RFC3339. Используйте значение timestampField, чтобы указать поле данных инцидента.	2021-09-06T00:00:00Z 2021-09-06T00:00:00.000Z 2021-09-06T00:00:00Z+00:00
to	Строка	Нет	Окончание периода, используемого для фильтрации списка инцидентов, в формате RFC3339. Используйте значение timestampField, чтобы указать поле данных инцидента.	2021-09-06T00:00:00Z 2021-09-06T00:00:00.000Z 2021-09-06T00:00:00Z+00:00
status	Строка	Нет	Статус инцидента. Если указано несколько значений, формируется список, к которому применяется логический оператор ИЛИ.	new inProgress hold closed
withAffected	bool	Нет	Указывает, следует ли включать подробные данные об активах и учетных записях, связанных с инцидентами.	/xdr/api/v1/incidents?withAffected /xdr/api/v1/incidents?withAffected=123
withHistory	bool	Нет	Указывает, следует ли включать данные об изменениях, внесенных в инциденты.	/xdr/api/v1/incidents?withHistory /xdr/api/v1/incidents?withHistory=123

Действие по реагированию

HTTP-код: 200

Формат: JSON

Пример:


```
{
 "Total": 0,
 "Incidents": [
 {
 "ID": 0,
 "InternalID": "881dee1f-380d-4366-a2d8-094e0af4c3f6",
 "TenantID": "string",
 "Name": "string",
 "Assets": [
 {
 "Data": {},
 "ID": "string",
 "IsAttacker": true,
 "IsVictim": true,
 "KSCServer": "string",
 "Name": "string",
 "Type": "host",
 "HostInfo": {
 "ID": "string",
 "TenantID": "string",
 "DisplayName": "string",
 "AssetSource": "string",
 "CreatedAt": 0,
 "IsDeleted": true,
 "IpAddress": [
 "string"
 ],
 "Fqdn": [
 "string"
 ],
 "MacAddress": [
 "string"
 ],
 "DirectCategories": [
 "string"
 ],
 "Weight": "low",
 "CiiCategory": "notCII",
 "OS": "string",
 "OSVersion": "string",
 "Sources": [
 "ksc"
 ],
 "LastVisible": 0,
 "Products": [
 {
 "ProductVersion": "string",
 "ProductName": "string"
 }
 ],
 "KSC": {
 "GroupID": 0,
 "GroupName": "string",
 "StatusMask": [
 0
 ],
 "StatusID": 0,
 "RtProtectionState": 0,
 "EncryptionState": 0,
 "AntiSpamStatus": 0,
 "EmailAvStatus": 0,
 "DlpStatus": 0,
 "EdrStatus": 0,
 "LastAvBasesUpdate": 0,
 "LastInfoUpdate": 0,
 "LastUpdate": 0,
 "LastSystemStart": 0,
 "VirtualServerID": 0
 },
 "KICS": {
 "status": "string",
 "risks": [
 {
 "ID": 0,
 "Name": "string",
 "Category": "string",
 "Description": "string",
 "DescriptionURL": "string",
 "Severity": 0,
 "Cvss": 0
 }
 ],
 "serverIP": "string",
 "connectorID": 0,
 "deviceID": 0,
 "hardware": {
 "Model": "string",
 "Version": "string",
 "Vendor": "string"
```

```
},
"software": {
"Model": "string",
"Version": "string",
"Vendor": "string"
}
}
},
"UserInfo": {
"osmpId": "string",
"tenantID": "string",
"tenantName": "string",
"domain": "string",
"cn": "string",
"displayName": "string",
"distinguishedName": "string",
"mail": "string",
"mailNickname": "string",
"mobile": "string",
"objectSID": "string",
"samAccountName": "string",
"samAccountType": "string",
"telephoneNumber": "string",
"userPrincipalName": "string",
"isArchived": true,
"memberOf": [
"string"
],
"title": "string",
"division": "string",
"department": "string",
"manager": "string",
"location": "string",
"company": "string",
"streetAddress": "string",
"physicalDeliveryOfficeName": "string",
"managedObjects": [
"string"
],
"userAccountControl": "string",
"whenCreated": 0,
"whenChanged": 0,
"accountExpires": 0,
"badPasswordTime": 0
}
}
],
"AlertIDs": [
"string"
],
"Assignee": {
"ID": "string",
"Name": "string"
},
"CreatedAt": "2024-01-16T09:56:29.939Z",
"DetectionTechnologies": [
"string"
],
"FirstEventTime": "2024-01-16T09:56:29.939Z",
"LastEventTime": "2024-01-16T09:56:29.939Z",
"MITRETactics": [
{
"ID": "string"
}
],
"MITRETechniques": [
{
"ID": "string"
}
],
"Observables": [
{
"Details": "string",
"Type": "ip",
"Value": "string"
}
],
"Rules": [
{
"Confidence": "high",
"Custom": true,
"ID": "string",
"Name": "string",
"Severity": "critical",
"Type": "string"
}
],
"Severity": "critical",
"ExternalRef": "string",
"Status": "open",
"StatusChangedAt": "2024-01-16T09:56:29.939Z",
"StatusResolution": "truePositive",
"UpdatedAt": "2024-01-16T09:56:29.939Z",
"Description": "string",
"SignOfCreation": "auto",
"Priority": "low",
"HistoryRecords": [
{
"entityID": "string",
"entityKind": "Alert",
"tenantID": "string",
"type": "alertAssigned",
"createdAt": "2024-03-12T11:11:58.864Z",
"params": {}
}
],
"IncidentType": {
"ID": "string",
"Name": "string"
}
}
```

```
  ]
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Недопустимое значение timestampField.	Недопустимое поле отметки времени.	
400	Недопустимое значение "от".	Не удалось проанализировать.	Переменная.
400	Недопустимое значение.	Не удалось проанализировать.	Переменная.
400	Значение ID не в формате UUID.		
403	Пользователь не имеет необходимых прав в функциональной области **Алерты и инциденты** ни у одного из указанных тенантов.	Доступ запрещен.	
500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Просмотр списка тенантов

GET /xdr/api/v1/tenants

Возвращает список тенантов, для которых пользователь имеет право **Чтение**.

Пример:

https://api.example.com/xdr/api/v1/tenants

Действие по реагированию

HTTP-код: 200

Формат: JSON

Пример:

```
[
 {
 "ID": "string",
 "Name": "string",
 "Description": "string",
 "Removable": true,
 "Subtenants": [
 "string"
 ],
 "IsRoot": true
 }
]
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`

500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Закрытие алертов

POST /xdr/api/v1/alerts/close

Устанавливает значение статуса "Закрыт" для указанного алерта.

Пример:

https://api.example.com/xdr/api/v1/alerts/close

Тело запроса

Формат: JSON

Пример:

```
[
 {
 "ID": "00000000-0000-0000-0000-000000000000",
 "TenantID": "00000000-0000-0000-0000-000000000000",
 "Reason": "falsePositive"
 }
]
```

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
ID	Строка	Да	Идентификатор алерта.	00000000-0000-0000-0000-000000000000
TenantID	Строка	Да	Идентификатор тенанта.	00000000-0000-0000-0000-000000000000
Reason	Строка	Да	Причина закрытия.	falsePositive lowPriority

Действие по реагированию

HTTP-код: 204

Если алерт уже был закрыт с тем же значением причины, код ответа будет также 204.

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Значение идентификатора не указано.	id required	
400	Значение поля Причина не указано.	Требуется причина.	
400	Недопустимое значение поля Причина.	Недопустимая причина.	
403	Пользователь не имеет необходимой роли в функциональной области **Алерты и**	Доступ	

	инциденты ни у одного из указанных тенантов.	запрещен.	
404	Алерт с указанным идентификатором не найден.	Алерт не найден.	
500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Закрытие инцидентов

POST /xdr/api/v1/incidents/close

Устанавливает значение статуса "Закрыто" для указанного инцидента.

Пример:

https://api.example.com/xdr/api/v1/incidents/close

Тело запроса

Формат: JSON

Пример:

```
[
 {
 "ID": "00000000-0000-0000-0000-000000000000",
 "TenantID": "00000000-0000-0000-0000-000000000000",
 "Reason": "falsePositive"
 }
]
```

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
ID	Строка	Да	Идентификатор инцидента.	00000000-0000-0000-0000-000000000000
TenantID	Строка	Да	Идентификатор тенанта.	00000000-0000-0000-0000-000000000000
Reason	Строка	Да	Причина закрытия.	truePositive falsePositive lowPriority

Действие по реагированию

HTTP-код: 204

Если инцидент уже был закрыт с тем же значением причины, код реагирования будет также 204.

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Значение идентификатора не указано.	id required	
400	Значение поля Причина не указано.	Требуется	

		причина.	
400	Недопустимое значение поля Причина.	Недопустимая причина.	
403	Пользователь не имеет необходимой роли в функциональной области **Алерты и инциденты** ни у одного из указанных тенантов.	Доступ запрещен.	
404	Инцидент с указанным идентификатором не найден.	Инцидент не найден.	
500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Загрузка файлов, связанных с алертом или инцидентом

POST /xdr/api/v1/incident/<entityKind>/<entityInternalID>/attachments

Загружает вложения и связывает их с указанным алертом или инцидентом.

Вы можете загружать файлы любого расширения. Допускаются дубликаты имен файлов.

Ограничения:

- Количество файлов не может превышать 100 на один алерт.
- Общий размер файла не может превышать 26,2 МБ на один алерт.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
entityKind	Строка	Да	Указывает, следует ли прикрепить файл, связанный с алертом или инцидентом.	alerts incidents
entityInternalID	Строка	Да	Идентификатор алерта или инцидента.	00000000-0000-0000-0000-000000000000
X-Content-Length	целое число	Да	Длина двоичного объекта.	1024

Действие по реагированию

HTTP-код: 201

Формат: JSON

Если двоичный объект не удалось успешно обработать, метод API все равно добавляет вложение и возвращает код 201. Рекомендуется вручную проверить вложение и при необходимости удалить его.

Просмотр списка файлов, связанных с алертом или инцидентом

GET /xdr/api/v1/incident/<entityKind>/<entityInternalID>/attachments

Читает список вложений, связанных с указанным алертом или инцидентом.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
entityKind	Строка	Да	Указывает, следует ли читать список файлов, прикрепленных к алерту или инциденту.	alerts incidents
entityInternalID	Строка	Да	Идентификатор алерта или инцидента.	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

Возвращает массив объектов Attachment.

Параметры объекта Attachment

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
id	Строка	Да	Идентификатор вложения.	00000000-0000-0000-0000-000000000000
name	Строка	Да	Имя вложения.	report.txt
status	Строка	Да	Статус загрузки.	completed error
size	целое число	Да	Размер файла вложения, в байтах.	1024
description	Строка	Нет	Описание вложения.	

GET /xdr/api/v1/incident/<entityKind>/<entityInternalID>/attachments/<attachmentID>

Возвращает клиенту открытый поток вложения.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
entityKind	Строка	Да	Указывает, следует ли скачивать файл вложения, связанный с алертом или инцидентом.	alerts incidents
entityInternalID	Строка	Да	Идентификатор алерта или инцидента.	00000000-0000-0000-0000-000000000000
attachmentID	Строка	Да	Идентификатор вложения.	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

DELETE /xdr/api/v1/incident/<entityKind>/<entityInternalID>/attachments/<attachmentID>

Удаляет указанное вложение, связанное с алертом или инцидентом.

Фактический объект файла удаляется асинхронно.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
entityKind	Строка	Да	Указывает, следует ли удалить файл вложения, связанный с алертом или инцидентом.	alerts incidents
entityInternalID	Строка	Да	Идентификатор алерта или инцидента.	00000000-0000-0000-0000-000000000000
attachmentID	Строка	Да	Идентификатор вложения.	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 204

Формат: JSON

Просмотр списка активных листов на коррелляторе

GET /xdr/api/v2.1/kuma/activeLists/

Целевой коррелятор должен быть запущен.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
correlatorID	Строка	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response []ActiveListInfo

type ActiveListInfo struct {
    ID      string `json:"id"`
    Name    string `json:"name"`
    Dir     string `json:"dir"`
    Records uint64 `json:"records"`
    WALSize uint64 `json:"walSize"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор сервиса коррелятора	query parameter required	correlatorID
403	Пользователь не имеет необходимой роли в тенанте коррелятора	Доступ запрещен.	-
404	Сервис с указанным идентификатором (correlatorID) не найден	service not found	-
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором	service is not correlator	-
406	Коррелятор не выполнил первый старт	service not paired	-
406	Тенант коррелятора отключен	tenant disabled	-
50x	Не удалось обратиться к API коррелятора	correlator API request failed	Переменная.
500	Не удалось декодировать тело ответа, полученное от коррелятора	correlator response decode failed	Переменная.
500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Импорт записей в активный лист

POST /xdr/api/v2.1/kuma/activeLists/import

Целевой коррелятор должен быть запущен.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
correlatorID	Строка	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000
activeListID	Строка	Если не указан activeListName	Идентификатор активного листа	00000000-0000-0000-0000-000000000000
activeListName	Строка	Если не	Имя активного листа	Attackers

		указан activeListID		
format	Строка	Да	Формат импортируемых записей	CSV, TSV, internal
keyField	Строка	Только для форматов csv и tsv	Имя поля в заголовке csv или tsv файла, которое будет использовано в качестве ключевого поля записи активного листа. Значения этого поля должны быть уникальными	ip
clear	bool	Нет	Очистить активный лист перед выполнением импорта. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются.	/xdr/api/v2.1/kuma/activeLists/import?clear

Тело запроса

Формат	Содержание
CSV	Первая строка – заголовок, где перечислены поля, разделенные запятой. Остальные строки – значения, соответствующие полям в заголовке, разделенные запятой. Количество полей на каждой строке должно быть одинаковым.
TSV	Первая строка – заголовок, где перечислены поля, разделенные TAB. Остальные строки – значения, соответствующие полям в заголовке, разделенные TAB. Количество полей на каждой строке должно быть одинаковым.
internal	Каждая строка содержит один индивидуальный объект JSON. Данные в internal формате можно получить путем экспорта содержимого активного листа из коррелятора в Консоли KUMA.

Действие по реагированию

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор сервиса коррелятора	query parameter required	correlatorID
400	Не указан ни параметр activeListID, ни параметр activeListName	one of query parameters required	activeListID, activeListName
400	Не указан параметр `format`	query parameter required	format
400	Параметр `format` имеет неверное значение	invalid query parameter value	format
400	Параметр `keyField` не задан	query parameter required	keyField
400	Тело запроса имеет нулевую длину	request body required	-
400	CSV или TSV файл не содержит поле, указанное в параметре keyField	correlator API request failed	Переменная.
400	Ошибка парсинга тела запроса	correlator API request failed	Переменная.
403	Пользователь не имеет необходимой роли в тенанте коррелятора	Доступ запрещен.	-
404	Сервис с указанным идентификатором (correlatorID) не найден	service not found	-
404	Активный лист не найден	active list not found	-
406	Сервис с указанным идентификатором (`correlatorID`) не является коррелятором	service is not correlator	-
406	Коррелятор не выполнил первый старт	service not paired	-
406	Тенант коррелятора отключен	tenant disabled	-
406	Поиск активного листа выполнялся по имени (`activeListName`) и было	more than one matching	-

	найдено более одного активного листа	active lists found	
50x	Не удалось обратиться к API коррелятора	correlator API request failed	Переменная.
500	Не удалось декодировать тело ответа, полученное от коррелятора	correlator response decode failed	Переменная.
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Поиск активов

GET /xdr/api/v2.1/kuma/assets/

Информация о программном обеспечении активов не хранится в OSMP и не будет показана в действии по реагированию.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня, Младший аналитик, Доступ к объектам НКЦКИ, Доступ к объектам КИИ, Наблюдатель.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
page	Числовое	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	Строка	Нет	Идентификатор актива. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	Строка	Нет	Идентификатор тенанта актива. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	Строка	Нет	Название актива. Регистронезависимое регулярное выражение (PCRE).	asset ^My asset$
fqdn	Строка	Нет	FQDN актива. Регистронезависимое регулярное выражение (PCRE).	example.com
ip	Строка	Нет	IP-адрес актива. Регистронезависимое регулярное выражение (PCRE).	10.10 ^192.168.1.2$
mac	Строка	Нет	MAC-адрес актива. Регистронезависимое регулярное выражение (PCRE).	^00:0a:95:9d:68:16$

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response []Asset

type Asset struct {
 ID string `json:"id"`
 TenantID string `json:"tenantID"`
 TenantName string `json:"tenantName"`
 Name string `json:"name"`
 FQDN []string `json:"fqdn"`
 IPAddresses []string `json:"ipAddresses"`
 MACAddresses []string `json:"macAddresses"`
 Owner string `json:"owner"`
 OS *OS `json:"os"`
```

```
 Software []Software `json:"software"`
 Vulnerabilities []Vulnerability `json:"vulnerabilities"`
 KICSRisks []*assets.KICSRisk `json:"kicsVulns"`
 KSC *KSCFields `json:"ksc"`
 Created string `json:"created"`
 Updated string `json:"updated"`
 CustomFields []CustomField `json:"customFields"`
}

type KSCFields struct {
 NAgentID string `json:"nAgentID"`
 KSCInstanceID string `json:"kscInstanceID"`
 KSCMasterHostname string `json:"kscMasterHostname"`
 LastVisible string `json:"lastVisible"`
}

type OS struct {
 Name string `json:"name"`
 Version uint64 `json:"version"`
}

type Software struct {
 Name string `json:"name"`
 Version string `json:"version"`
 Vendor string `json:"vendor"`
}

type Vulnerability struct {
 KasperskyID string `json:"kasperskyID"`
 ProductName string `json:"productName"`
 DescriptionURL string `json:"descriptionURL"`
 RecommendedMajorPatch string `json:"recommendedMajorPatch"`
 RecommendedMinorPatch string `json:"recommendedMinorPatch"`
 SeverityStr string `json:"severityStr"`
 Severity uint64 `json:"severity"`
 CVE []string `json:"cve"`
 ExploitExists bool `json:"exploitExists"`
 MalwareExists bool `json:"malwareExists"`
}

type assets.KICSRisk struct {
 ID int64 `json:"id"`
 Name string `json:"name"`
 Category string `json:"category"`
 Description string `json:"description"`
 DescriptionUrl string `json:"descriptionUrl"`
 Severity int `json:"severity"`
 Cvss float64 `json:"cvss"`
}

type CustomField struct {
 ID string `json:"id"`
 Name string `json:"name"`
 Value string `json:"value"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Неверное значение параметра page	invalid query parameter value	page
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Импорт активов

POST /xdr/api/v2.1/kuma/assets/import

Массовое создание или обновление активов.

Если указан FQDN актива, он играет роль уникального идентификатора актива в рамках тенанта. Если имя актива не указано, оно заполняется либо значением FQDN, либо значением первого IP-адреса. Активы, импортированные из Kaspersky Security Center не могут быть обновлены, поэтому в процессе импорта могут возникать конфликты по FQDN, если в тенанте уже существует актив Kaspersky Security Center с таким FQDN. Возникновение такого конфликта препятствует обработке конфликтующего актива, но не препятствует обработке других активов, указанных в теле запроса. Позволяет заполнять пользовательские поля по uuid из настроек assetsCustomFields.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Тело запроса

Формат: JSON

```
type Request struct {
 TenantID string `json:"tenantID"`
    Assets []Asset `json:"assets"`
}

type Asset struct {
 Name string `json:"name"`
 FQDN string `json:"fqdn"`
 IPAddresses []string `json:"ipAddresses"`
 MACAddresses []string `json:"macAddresses"`
 Owner string `json:"owner"`
 OS *OS `json:"os"`
 Software []Software `json:"software"`
 Vulnerabilities []Vulnerability `json:"vulnerabilities"`
 CustomFields []CustomField `json:"customFields"`
}

type OS struct {
 Name string `json:"name"`
 Version uint64 `json:"version"`
}

type Software struct {
 Name string `json:"name"`
 Version string `json:"version"`
 Vendor string `json:"vendor"`
}

type Vulnerability struct {
 KasperskyID string `json:"kasperskyID"`
 ProductName string `json:"productName"`
 DescriptionURL string `json:"descriptionURL"`
 RecommendedMajorPatch string `json:"recommendedMajorPatch"`
 RecommendedMinorPatch string `json:"recommendedMinorPatch"`
 SeverityStr string `json:"severityStr"`
 Severity uint64 `json:"severity"`
 CVE []string `json:"cve"`
 ExploitExists bool `json:"exploitExists"`
 MalwareExists bool `json:"malwareExists"`
}

type CustomFields struct {
 ID string `json:"id"`
 Value string `json:"value"`
}
```

Обязательные поля Request

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
tenantID	Строка	Да	Идентификатор тенанта	00000000-0000-0000-0000-000000000000
assets	[]Asset	Да	Массив импортируемых активов	

Обязательные поля Asset

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
fqdn	Строка	Если не указан ipAddresses	FQDN актива. Рекомендуется указывать именно FQDN, а не просто имя устройства. Приоритетный признак для идентификации актива.	[my-asset-1.example.com] [my-asset-1]
ipAddresses	[]string	Если не указан fqdn	Массив IP-адресов актива. IPv4-адрес или IPv6-адрес. Первый элемент массива используется как второстепенный признак для идентификации актива.	["192.168.1.1", "192.168.2.2"] ["2001:0db8:85a3:0000:0000:8a2e:0370:7334"]

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response struct {
InsertedIDs map[int64]interface{} `json:"insertedIDs"`
UpdatedCount uint64 `json:"updatedCount"`
Errors []ImportError `json:"errors"`
}

type ImportError struct {
Index uint64 `json:"index"`
Message string `json:"message"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор тенанта (tenantID)	tenantID required	-
400	Попытка импорта активов в общий тенант	import into shared tenant not allowed	-
400	В теле запроса не указан ни один актив	at least one asset required	-
400	Не указано ни одно из обязательных полей	one of fields required	asset[<index>]: fqdn, ipAddresses
400	Неверный FQDN	invalid value	asset[<index>].fqdn
400	Неверный IP-адрес	invalid value	asset[<index>].ipAddresses[<index>]
400	Дублируется IP-адрес	duplicated value	asset[<index>].ipAddresses
400	Неверный MAC-адрес	invalid value	asset[<index>].macAddresses[<index>]
400	Дублируется MAC-адрес	duplicated value	asset[<index>].macAddresses
403	Пользователь не имеет необходимой роли в указанном тенанте	access denied	-
404	Указанный тенант не найден	tenant not found	-
406	Указанный тенант выключен	tenant disabled	-
500	Любая другая внутренняя ошибка.	variable	Переменная.

Удаление активов

POST /xdr/api/v2.1/kuma/assets/delete

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Доступ к объектам КИИ, Подтверждающий.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
tenantID	Строка	Да	Идентификатор тенанта	00000000-0000-0000-0000-000000000000
ids	[]string	Если не указаны ни fqdns, ни ipAddresses	Список идентификаторов активов	["00000000-0000-0000-0000-000000000000"]
fqdns	[]string	Если не указаны ни ids, ни ipAddresses	Массив FQDN активов	["my-asset-1.example.com", "my-asset-1"]
ipAddresses	[]string	Если не указаны ни ids, ни fqdns	Массив основных IP-адресов активов	["192.168.1.1", "2001:0db8:85a3:0000:0000:8a2e:0370:7334"]

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response struct {
 DeletedCount uint64 `json:"deletedCount"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор тенанта (tenantID)	tenantID required	-
400	Попытка удаления актива из общего тенанта	delete from shared tenant not allowed	-
400	Не указано ни одно из обязательных полей	one of fields required	ids, fqdns, ipAddresses
400	Указан неверный FQDN	invalid value	fqdns[<index>]
400	Указан неверный IP адрес	invalid value	ipAddresses[<index>]
403	Пользователь не имеет необходимой роли в указанном тенанте	access denied	-
404	Указанный тенант не найден	tenant not found	-
406	Указанный тенант выключен	tenant disabled	-
500	Любая другая внутренняя ошибка.	variable	Переменная.

Поиск событий

POST /xdr/api/v2.1/kuma/events/

Разрешены только поисковые или агрегационные запросы (SELECT).

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня, Младший аналитик, Доступ к объектам НКЦКИ, Доступ к объектам КИИ, Наблюдатель.

Тело запроса

Формат: JSON

Запрос

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
period	Period	Да	Период поиска	
sql	Строка	Да	SQL-запрос	SELECT * FROM events WHERE Type = 3 ORDER BY Timestamp DESC LIMIT 1000 SELECT sum(BytesOut) as TotalBytesSent, SourceAddress FROM events WHERE DeviceVendor = 'netflow' GROUP BY SourceAddress LIMIT 1000 SELECT count(Timestamp) as TotalEvents FROM events LIMIT 1
clusterID	Строка	Нет, если кластер единственный	Идентификатор Storage кластера. Можно найти запросив список сервисов с kind = storage. Идентификатор кластера будет в поле resourceID.	00000000-0000-0000-0000-000000000000
rawTimestamps	bool	Нет	Отображать timestamp'ы в исходном виде - Milliseconds since EPOCH. По умолчанию false.	true false
emptyFields	bool	Нет	Отображать пустые поля нормализованных событий. По умолчанию false.	true false

Period

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
from	Строка	Да	Нижняя граница периода в формате RFC3339. Timestamp >= <from>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)
to	Строка	Да	Верхняя граница периода в формате RFC3339. Timestamp <= <to>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)

Действие по реагированию

HTTP-код: 200

Формат: JSON

Результат выполнения SQL-запроса

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Нижняя граница диапазона не указана	period.from required	-
400	Нижняя граница диапазона указана в неподдерживаемом формате	cannot parse period.from	Переменная.
400	Нижняя граница диапазона равна нулю	period.from cannot be 0	-
400	Верхняя граница диапазона не указана	period.to required	-
400	Верхняя граница диапазона указана в неподдерживаемом формате	cannot parse period.to	Переменная.
400	Верхняя граница диапазона равна нулю	period.to cannot be 0	-
400	Нижняя граница диапазона больше верхней	period.from cannot be greater than period.to	-
400	Неверный SQL-запрос	invalid sql	Переменная.
400	В SQL-запросе фигурирует неверная таблица	the only valid table is `events`	-
400	В SQL-запросе отсутствует LIMIT	sql: LIMIT required	-
400	LIMIT в SQL-запросе превышает максимальный (1000)	sql: maximum LIMIT is 1000	-
404	Storage cluster не найден	cluster not found	-
406	Параметр clusterID не был указан и в KUMA зарегистрировано множество кластеров	multiple clusters found, please provide clusterID	-
500	Нет доступных нод кластера	no nodes available	-
50x	Любая другая внутренняя ошибка.	event search failed	Переменная.

Просмотр информации о кластере

GET /xdr/api/v2.1/kuma/events/clusters/

Доступ: Кластеры главного тенанта доступны всем пользователям.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
page	Числовое	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	Строка	Нет	Идентификатор кластера. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	Строка	Нет	Идентификатор тенанта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	Строка	Нет	Имя кластера. Регистронезависимое регулярное выражение (PCRE).	cluster ^My cluster$

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response []Cluster

type Cluster struct {
 ID string `json:"id"`
 Name string `json:"name"`
 TenantID string `json:"tenantID"`
 TenantName string `json:"tenantName"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Неверное значение параметра page	invalid query parameter value	page
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Просмотр содержимого файла с ресурсами

POST /xdr/api/v2.1/kuma/resources/toc

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
fileID	Строка	Да	Идентификатор файла, полученный в результате выполнения загрузки файла с ресурсами.	00000000-0000-0000-0000-000000000000
password	Строка	Да	Пароль файла с ресурсами.	SomePassword!88

Действие по реагированию

HTTP-код: 200

Формат: JSON

Версия файла, список ресурсов, категорий, папок.

Идентификатор полученных ресурсов необходимо использовать при импорте.

```
type TOCResponse struct {
 Folders []*Folder `json:"folders"`
}

type Folder struct {
 ID string `json:"id"`
 TenantID string `json:"tenantID"`
 TenantName string `json:"tenantName"`
 ExportID string `json:"exportID"`
 Kind string `json:"kind"`
 SubKind string `json:"subKind"`
```

```
 Name string `json:"name"`
 Description string `json:"description"`
 UserID string `json:"userID"`
 ParentID string `json:"parentID"`
 CreatedAt int64 `json:"createdAt"`
 Resources []*Resource `json:"resources"`
}

type Resource struct {
 ID string `json:"id"`
 Kind string `json:"kind"`
 Name string `json:"name"`
 Deps []string `json:"deps"`
}
```

Просмотр информации о предъявителе токена

GET /xdr/api/v2.1/kuma/users/whoami

Действие по реагированию

Реагирование возвращает высшую роль из всех ролей, назначенных пользователю.

HTTP-код: 200

Формат: JSON

```
type Tenant struct {
 ID string `json:"id"`
 Name string `json:"name"`
}

type Role struct {
 ID string `json:"id"`
 Name string `json:"name"`
 Tenants []Tenant `json:"tenants"`
}

type Response struct {
 ID string `json:"id"`
 Name string `json:"name"`
 Login string `json:"login"`
 Email string `json:"email"`
 Roles []Role `json:"roles"`
}
```

Обновление словаря в сервисах

POST /xdr/api/v2.1/kuma/dictionaries/update

Обновить можно только словари в ресурсах словарей типа таблица.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
dictionaryID	Строка	Да	ID словаря, который будет обновлен.	00000000-0000-0000-0000-

				000000000000
needReload	Числовое	Нет	Указывает, обновлять ли параметры сервисов, использующих этот словарь: • 0 – не обновлять параметры сервиса после обновления словаря. • 1 – обновлять параметры сервиса после обновления словаря. Используется, если тип словаря указан словарь. Если указан тип словаря указан "таблица", параметры сервисов, использующих словарь, всегда обновляются.	0 1

Обновление произойдет на всех сервисах, где используется указанный словарь. Если обновление на одном из сервисов заканчивается ошибкой, это не прерывает обновления на других сервисах.

Тело запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
file	CSV-файл	Да	Запрос содержит CSV-файл. Данные существующего словаря заменяются на данные этого файла. Первая строка CSV-файла с названиями столбцов не должна меняться. Если указан тип словаря "таблица", разрешены только столбцы "key" и "value".	key columns,column1,column2 key1,k1col1,k1col2 key2,k2col1,k2col2

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response struct {
 ServicesFailedToUpdate []UpdateError `json:"servicesFailedToUpdate"`
}
type UpdateError struct {
 ID string `json:"id"`
 Err error `json:"err"`
}
```

Возвращает только ошибки для сервисов, на которых словари не были обновлены.

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Неверное тело запроса	request body decode failed	Возникшая ошибка.
400	Нулевое количество строк словаря	request body required	-
400	Не указан ID словаря	invalid value	dictionaryID
400	Некорректное значение строки словаря	invalid value	rows или rows[i]
400	Словарь с указанным ID имеет неверный вид (не таблица)	can only update table dictionary	-
400	Попытка изменить столбцы словаря	columns must not change with update	-
403	Нет доступа к запрашиваемому ресурсу	Доступ запрещен.	-
404	Сервис не найден	service not found	-
404	Словарь не найден	dictionary not found	идентификатор сервиса
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Получение словаря

GET /xdr/api/v2.1/kuma/dictionaries/

Получить можно только словари в ресурсах словарей типа таблица.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
dictionaryID	Строка	Да	ID словаря, который будет получен	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: text/plain; charset=utf-8

Возвращается CSV-файл с данными словаря в теле ответа.

Просмотр пользовательских полей активов

GET /xdr/api/v2.1/kuma/settings/id/:id

Пользователь может просматривать список пользовательских полей, сделанных пользователем KUMA в веб-интерфейсе приложения.

Пользовательское поле представляет из себя контейнер для ввода текста. При необходимости может использоваться значение по умолчанию и маска для проверки корректности вводимого текста в формате https://pkg.go.dev/regexp/syntax. Все символы косой черты в маске необходимо дополнительно экранировать.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня, Подтверждающий, Наблюдатель, Доступ к объектам НКЦКИ, Доступ к объектам КИИ.

Параметры запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
id	Строка	Да	Идентификатор конфигурации пользовательских полей	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Settings struct {
 ID string `json:"id"`
 TenantID string `json:"tenantID"`
 TenantName string `json:"tenantName"`
 Kind string `json:"kind"`
 UpdatedAt int64 `json:"updatedAt"`
 CreatedAt int64 `json:"createdAt"`
 Disabled bool `json:"disabled"`
 CustomFields []*CustomField `json:"customFields"`
}

type CustomField struct {
 ID string `json:"id"`
 Name string `json:"name"`
 Default string `json:"default"`
 Mask string `json:"mask"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
404	Параметры не найдены: неверный идентификатор или параметров нет	Not found in database	null
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Просмотр списка контекстных таблиц в коррелляторе

GET /xdr/api/v2.1/kuma/contextTables/

Целевой коррелятор должен быть запущен.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
correlatorID	Строка	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response []ContextTableInfo

type ContextTableInfo struct {
 ID string `json:"id"`
```

```
  Name string `json:"name"`
  Dir string `json:"dir"`
  Records uint64 `json:"records"`
  WALSize uint64 `json:"walSize"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор сервиса коррелятора.	query parameter required	correlatorID
403	Пользователю не присвоена необходимая роль в тенанте коррелятора.	Доступ запрещен.	-
404	Сервис с указанным идентификатором (correlatorID) не найден.	service not found	-
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором.	service is not correlator	-
406	Коррелятор не выполнил первый старт.	service not paired	-
406	Тенант коррелятора отключен.	tenant disabled	-
50x	Не удалось обратиться к API коррелятора.	correlator API request failed	Переменная.
500	Не удалось декодировать тело ответа, полученное от коррелятора.	correlator response decode failed	Переменная.
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Импорт записей в контекстную таблицу

POST /xdr/api/v2.1/kuma/contextTables/import

Целевой коррелятор должен быть запущен.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
correlatorID	Строка	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000
contextTableID	Строка	Если не указан contextTableName	Идентификатор контекстной таблицы.	00000000-0000-0000-0000-000000000000
contextTableName	Строка	Если не указан contextTableID	Имя контекстной таблицы	Attackers
format	Строка	Да	Формат импортируемых записей	CSV, TSV, internal
clear	bool	Нет	Очистить контекстную таблицу перед выполнением импорта. Если параметр присутствует в URL query, его значение принимается как true. Указанные пользователем значения игнорируются.	/xdr/api/v2.1/contextTables/import?clear

Тело запроса

Формат	Содержание
CSV	Первая строка - заголовок, где перечислены поля, разделенные запятой. Остальные строки - значения, соответствующие полям в заголовке, разделенные запятой. Количество полей на каждой строке должно быть одинаковым и должно соответствовать количеству полей в схеме контекстной таблицы. Значения списочных полей разделяются символом "|". Например, значение списочного поля целочисленного типа - 1|2|3.
TSV	Первая строка - заголовок, где перечислены поля, разделенные TAB. Остальные строки - значения, соответствующие полям в заголовке, разделенные TAB. Количество полей на каждой строке должно быть одинаковым и должно соответствовать количеству полей в схеме контекстной таблицы. Значения списочных полей разделяются символом "|".
internal	Каждая строка содержит один индивидуальный объект JSON. Данные в internal формате можно получить путем экспорта содержимого контекстной таблицы из коррелятора в Консоли KUMA.

Действие по реагированию

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор сервиса коррелятора.	query parameter required	correlatorID
400	Не указан ни параметр contextTableID, ни параметр contextTableName.	one of query parameters required	contextTableID, contextTableName
400	Не указан параметр format.	query parameter required	format
400	Параметр format имеет неверное значение.	invalid query parameter value	format
400	Тело запроса имеет нулевую длину.	request body required	-
400	Ошибка парсинга тела запроса, а том числе соответствие схеме контекстной таблицы наименования полей и типов импортируемой записи.	correlator API request failed	Переменная.
403	Пользователю не присвоена необходимая роль в тенанте коррелятора.	Доступ запрещен.	-
404	Сервис с указанным идентификатором (correlatorID) не найден.	service not found	-
404	Контекстная таблица не найдена.	context table not found	-
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором.	service is not correlator	-
406	Коррелятор не выполнил первый старт.	service not paired	-
406	Тенант коррелятора отключен.	tenant disabled	-
406	Поиск контекстной таблицы выполнялся по имени contextTableName и было найдено более одной контекстной таблицы.	more than one matching context tables found	-
50x	Не удалось обратиться к API коррелятора.	correlator API request failed	Переменная.
500	Ошибка подготовки данных для импорта в сервис коррелятора.	context table process import request failed	Переменная.
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Экспорт записей из контекстной таблицы

GET /xdr/api/v2.1/kuma/contextTables/export

Целевой коррелятор должен быть запущен.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
correlatorID	Строка	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000
contextTableID	Строка	Если не указан contextTableName	Идентификатор контекстной таблицы.	00000000-0000-0000-0000-000000000000
contextTableName	Строка	Если не указан contextTableID	Имя контекстной таблицы	Attackers

Действие по реагированию

HTTP-код: 200

Формат: application/octet-stream

Тело: экспортированные данные контекстной таблицы в формате internal - каждая строка содержит один индивидуальный объект JSON.

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор сервиса коррелятора.	query parameter required	correlatorID
400	Не указан ни параметр contextTableID, ни параметр contextTableName.	one of query parameters required	contextTableID, contextTableName
403	Пользователю не присвоена необходимая роль в тенанте коррелятора.	Доступ запрещен.	-
404	Сервис с указанным идентификатором (correlatorID) не найден.	service not found	-
404	Контекстная таблица не найдена.	context table not found	-
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором.	service is not correlator	-
406	Коррелятор не выполнил первый старт.	service not paired	-
406	Тенант коррелятора отключен.	tenant disabled	-
406	Поиск контекстной таблицы выполнялся по имени contextTableName и было найдено более одной контекстной таблицы.	more than one matching context tables found	-
50x	Не удалось обратиться к API коррелятора.	correlator API request failed	Переменная.
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Поиск пользователей

GET /xdr/api/v2.1/kuma/users/<id>

`id` является идентификатором пользователя.

Доступ: Главный администратор.

Действие по реагированию

HTTP-код: 200

Формат: JSON

Пользователь с его параметрами, роли тенантов и доступные конечные точки.

Пример:


```
{
 "notifications": {
 "alerts": {
 "internal": false,
 "smtp": false
 },
 "disabled": false
 },
 "categories": {
 "pins": null
 },
 "defaultDashboardID": "00000000-0000-0000-0000-000000000000",
 "defaultSearchID": "00000000-0000-0000-0000-000000000000",
 "defaultAlertSearchID": "00000000-0000-0000-0000-000000000000",
 "defaultIncidentSearchID": "00000000-0000-0000-0000-000000000000",
 "defaultEventPresetID": "",
 "showNotPrintable": false,
 "language": "",
 "sharedDashboardTenantIDs": null,
 "tv": {
 "tvMode": false,
 "slideShow": false,
 "timeout": 0,
 "queue": null
 }
}
```


Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор пользователя.	-	
403	Пользователю не присвоена необходимая роль в тенанте коррелятора.	-	-
404	Параметры не найдены: неверный идентификатор или параметров нет	-	-
500	Любые другие внутренние ошибки.	Переменная.	Переменная.

Экспорт активного листа

GET /xdr/api/v2.1/kuma/services/<id>/activeLists/export/<list>

Укажите идентификаторы коррелятора и активного листа, чтобы получить идентификатор для последующего скачивания активного листа.

Значение параметра идентификатора из действия по реагированию используется для загрузки экспортированного активного списка с помощью операции /download.

Доступ: Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
id	Строка	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000
list	Строка	Да	Идентификатор активного листа	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
{
 "id": "00000000-0000-0000-0000-000000000000"
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400			
403	Пользователь не имеет необходимой роли в тенанте коррелятора		

Получение активного листа

GET /xdr/api/v2.1/kuma/services/<id>/activeLists/scan/<list>

Укажите идентификаторы коррелятора и активного листа, чтобы получить записи активного листа.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query): поиск по строке

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
id	Строка	Да	Идентификатор объекта	00000000-0000-0000-0000-000000000000
list	Строка	Да	Идентификатор активного листа	00000000-0000-0000-0000-000000000000
pattern	Строка	Нет	Строка для поиска в ключах и значениях активного	foo

			листа. Если этот параметр указан, параметры `from` и `exclude` игнорируются.	

Параметры запроса (URL Query): поиск по временной метке

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
id	Строка	Да	Идентификатор объекта	00000000-0000-0000-0000-000000000000
list	Строка	Да	Идентификатор активного листа	00000000-0000-0000-0000-000000000000
sort	Строка	Нет	Столбец, который следует использовать в качестве источника временной метки. Используйте символ "-" в начале названия столбца, чтобы указать порядок сортировки по убыванию. Если символ "-" не используется, по умолчанию сортировка происходит по возрастанию. Значения, указанные в параметрах `from` и `exclude`, применяются для фильтрации данных в столбце, который вы указали для сортировки.	expires
from	Строка	Нет	Укажите начало или конец периода в наносекундах. Указанный в столбце параметр `sort` используется, если этот параметр применяется. Начало или конец периода зависит от сортировки исходного столбца. Если сортировка по возрастанию, указывается начало периода. Если сортировка по убыванию, указывается конец периода. Если указан параметр `pattern`, этот параметр игнорируется.	1704067200000000000
exclude	Строка	Нет	Укажите точный момент для исключения в наносекундах. Указанный в столбце параметр `sort` используется, когда этот параметр применяется. Если указан параметр `pattern`, этот параметр игнорируется.	1704067200000000000
limit	Строка	Нет	Укажите общее количество возвращенных записей.	100

Изменение словаря

POST /xdr/api/v2.1/kuma/dictionaries/add_row

Вы можете добавить или изменить существующую строку в словаре на сервисах, где используется этот словарь.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня. Аналитики 1-го уровня могут изменять только те словари, владельцами которых они являются.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
dictionaryID	Строка	Да	Идентификатор словаря, который будет изменен.	00000000-0000-0000-0000-000000000000
rowKey	Строка	Да	Идентификатор строки для добавления, обновления или удаления.	key3
overwriteExist	Числовое	Нет	Указывает, следует ли добавить строку или перезаписать существующую: • 0 – если строка существует, новая строка не добавляется и существующая строка остается без изменений. • 1 – перезаписать существующую строку.	0
needReload	Числовое	Нет	Следует ли перезагрузить сервисы, которые используют указанный словарь: • 0 – не перезагружать сервисы, которые используют указанный словарь. • 1 – перезагрузить сервисы, которые используют указанный словарь. Этот параметр применятся только для словаря с типом: "dictionary".	0

Тело запроса

Запрос содержит массив пар ключ-значение, где ключ – это имя поля строки, значение – это значение поля строки. Ключ и значение имеют тип строки.

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
{
 "servicesFailedToUpdate": [
 {
 "err": "string",
 "id": "string"
 }
 ]
}
```

Возвращает только ошибки для сервисов, на которых словари не были обновлены.

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found
409	conflict
500	internal error

Удаление строк из словаря

POST /xdr/api/v2.1/kuma/dictionaries/delete_row

Вы можете добавить или изменить существующую строку в словаре на сервисах, где используется этот словарь.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня. Аналитики 1-го уровня могут изменять только те словари, владельцами которых они являются.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
dictionaryID	Строка	Да	Идентификатор словаря, который будет изменен.	00000000-0000-0000-0000-000000000000
rowKey	Строка	Да	Идентификатор строки для добавления, обновления или удаления.	key3
needReload	Числовое	Нет	Следует ли перезагрузить сервисы, которые используют указанный словарь: • 0 – не перезагружать сервисы, которые используют указанный словарь. • 1 – перезагрузить сервисы, которые используют указанный словарь. Этот параметр применятся только для словаря с типом: "dictionary".	0

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
{
 "servicesFailedToUpdate": [
 {
 "err": "string",
 "id": "string"
 }
 ]
}
```

Возвращает только ошибки для сервисов, на которых словари не были обновлены.

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden

404	not found
409	conflict
500	internal error

Создание ресурсов

POST /xdr/api/v2.1/kuma/resources/<kind>/create

Передает тип ресурса и его содержимое для создания ресурса.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
kind	Строка	Да	Тип ресурса. Доступные значения: • correlator • storage • activeList • contextTable • correlationRule • enrichmentRule • destination • filter • normalizer • responseRule • search • emailTemplate	correlator

Тело запроса

Формат: JSON

Пример:

```
{
 "tenantID": "00000000-0000-0000-0000-000000000000",
 "kind": "storage",
 "name": "storage_resource_example",
 "description": "Example of storage resource",
 "payload": {
 "id": "",
 "name": "storage_config_example",
 "override": "<merge_tree><parts_to_delay_insert>600</parts_to_delay_insert><parts_to_throw_insert>1100</parts_to_throw_insert></merge_tree>",
 "defaultRetention": 30,
 "defaultColdRetention": 1,
 "auditRetention": 365,
```

```
"auditColdRetention": 0,
"bufferSize": 33554432,
"flushInterval": 5,
"diskBufferDisabled": false,
"diskBufferSizeLimit": 5368709120,
"spaces": [
{
"id": "",
"name": "space_example",
"retention": 0,
"coldRetention": 0,
"filter": {
"id": "",
"name": "filter_example",
"root": {
"group": false,
"or": false,
"not": false,
"conditions": null,
"leftKind": "",
"leftEvent": "",
"leftID": "",
"leftField": "",
"leftKeys": null,
"leftKeyMap": null,
"leftListItemIdx": 0,
"leftTICategory": "",
"leftTIField": "",
"leftShared": false,
"op": "",
"rightKind": "",
"rightEvent": "",
"rightID": "",
"rightField": "",
"rightKeys": null,
"rightKeyMap": null,
"rightListItemIdx": 0,
"rightTICategory": "",
"rightTIField": "",
"rightShared": false,
"constant": null,
"list": null,
"ignoreCase": false,
"checkTypes": false,
"filter": null,
"vulns": null
},
"shared": false,
"currentTab": 0
}
}
],
"nodes": [
{
"fqdn": "kuma.example",
"shard": 1,
"replica": 1,
"keeper": 1
}
],
"disks": [
{
"type": "local",
"name": "disk_1",
"path": "/disk_1_path/",
"endpoint": ""
},
{
"type": "hdfs",
"name": "disk_2",
"endpoint": "hdfs://hdfs1:9000/clickhouse/"
}
],
"writeLocal": false,
"debug": false,
"shared": false
}
}
```


Действие по реагированию

HTTP-код: 200

Формат: JSON

Возвращает содержимое созданного ресурса.

Возможные ошибки

HTTP-код	Описание
400	bad request

403	forbidden
404	not found
409	conflict
500	internal error

Импорт ресурсов

POST /xdr/api/v2.1/kuma/resources/import

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Тело запроса

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
fileID	Строка	Да	Идентификатор файла, полученный в результате выполнения загрузки файла с ресурсами.	00000000-0000-0000-0000-000000000000
password	Строка	Да	Пароль файла с ресурсами.	SomePassword!88
tenantID	Строка	Да	Идентификатор целевого тенанта	00000000-0000-0000-0000-000000000000
actions	map[string]uint8	Да	Маппинг идентификатора ресурса к действию, которое нужно предпринять в отношении него.	0 – не импортировать (используется при разрешении конфликтов) 1 – импортировать (изначально должно быть присвоено каждому ресурсу) 2 – заменить (используется при разрешении конфликтов) `{ "00000000-0000-0000-0000-000000000000": 0, "00000000-0000-0000-0000-000000000001": 1, "00000000-0000-0000-0000-000000000002": 2, }`

Действие по реагированию

HTTP-код	Тело
204	
409	Идентификаторы импортируемых ресурсов, конфликтующих с уже существующими по ID. В этом случае необходимо повторить операцию импорта, указав для данных ресурсов следующие действия: 0 – не импортировать 2 – заменить `type ImportConflictsError struct { HardConflicts []string `json:"conflicts"` }`

Экспорт ресурсов

POST /xdr/api/v2.1/kuma/resources/export

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
ids	[]string	Да	Идентификаторы ресурсов, которые необходимо экспортировать	["00000000-0000-0000-0000-000000000000"]
password	Строка	Да	Пароль файла с экспортированными ресурсами	SomePassword!88
tenantID	Строка	Да	Идентификатор тенанта, которому принадлежат экспортируемые ресурсы	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

Идентификатор файла с экспортированными ресурсами. Следует использовать его в запросе на скачивание файла с ресурсами.

```
type ExportResponse struct {
 FileID string `json:"fileID"`
}
```

Скачивание файла с ресурсами

GET /xdr/api/v2.1/kuma/resources/download/<id>

`id` – идентификатор файла, полученный в результате выполнения запроса на экспорт ресурсов.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Действие по реагированию

HTTP-код: 200

Зашифрованное содержимое файла с ресурсами в бинарном формате.

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Не указан идентификатор файла	route parameter required	id
400	Идентификатор файла не является валидным UUID	id is not a valid UUID	-
403	Пользователь не имеет необходимых ролей ни в одном из тенантов	Доступ запрещен.	-
404	Файл не найден	file not found	-
406	Файл является директорией	not regular file	-
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Загрузка файла с ресурсами

POST /xdr/api/v2.1/kuma/resources/upload

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Тело запроса

Зашифрованное содержимое файла с ресурсами в бинарном формате.

Действие по реагированию

HTTP-код: 200

Формат: JSON

Идентификатор файла. Следует указать его в теле запросов на просмотр содержимого файла и на импорт ресурсов.

```
type Response struct {
 ID string `json:"id"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Размер файла превышает максимально допустимый (64 МБ)	maximum file size is 64 MB	-
403	Пользователь не имеет необходимых ролей ни в одном из тенантов	Доступ запрещен.	-
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Просмотр ресурсов

GET /xdr/api/v2.1/kuma/resources/<kind>/<id>

Передает тип ресурса и его идентификатор, чтобы получить содержимое ресурса.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
kind	Строка	Да	Тип ресурса. Доступные значения: • correlator • storage • activeList • contextTable • correlationRule • enrichmentRule • destination • filter • normalizer • responseRule • search • emailTemplate	correlator
id	Строка	Да	Идентификатор ресурса.	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 200

Формат: JSON

Возвращает содержимое ресурса.

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found

409	conflict
500	internal error

Поиск ресурсов

GET /xdr/api/v2.1/kuma/resources/

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня, Наблюдатель.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
page	Числовое	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	Строка	Нет	Идентификатор ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	Строка	Нет	Идентификатор тенанта ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	Строка	Нет	Имя ресурса. Регистронезависимое регулярное выражение (PCRE).	resource ^My resource$
kind	Строка	Нет	Тип ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	collector, correlator, storage, activeList, aggregationRule, connector, correlati enrichmentRule, destination, filter, normalizer, responseRule, search, agent, pro
userID	Строка	Нет	Идентификатор пользователя. Если параметр указан несколько раз, то формируется список и применяется	00000000-0000-0000-0000-000000000000 me

			логический оператор ИЛИ. Значение me соответствует пользователю, выполняющему запрос.	

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response []Resource

type Resource struct {
 ID string `json:"id"`
 Kind string `json:"kind"`
 Name string `json:"name"`
 Description string `json:"description"`
 TenantID string `json:"tenantID"`
 TenantName string `json:"tenantName"`
 UserID string `json:"userID"`
 UserName string `json:"userName"`
 Created string `json:"created"`
 Updated string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметр kind	invalid kind	<kind>
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Проверка правильности ресурсов

POST /xdr/api/v2.1/kuma/resources/<kind>/validate

Передает тип ресурса и его содержимое для проверки на ошибки.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
kind	Строка	Да	Тип ресурса. Доступные значения: • correlator • storage • activeList • contextTable	correlator

			• correlationRule • enrichmentRule • destination • filter • normalizer • responseRule • search • emailTemplate	

Действие по реагированию

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found
409	conflict
500	internal error

Изменение ресурсов

PUT /xdr/api/v2.1/kuma/resources/<kind>/<id>

Передает тип ресурса, его идентификатор и новое содержимое для изменения ресурса.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня. Аналитики 1-го уровня могут изменять только ресурсы, которые они создали.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
kind	Строка	Да	Тип ресурса. Доступные значения: • correlator • storage • activeList • contextTable • correlationRule	correlator

			• enrichmentRule • destination • filter • normalizer • responseRule • search • emailTemplate	
id	Строка	Да	Идентификатор ресурса.	00000000-0000-0000-0000-000000000000

Тело запроса

Формат: JSON

Пример:


```
{
 "tenantID": "00000000-0000-0000-0000-000000000000",
 "kind": "storage",
 "name": "storage_resource_example",
 "description": "Example of storage resource",
 "payload": {
 "id": "",
 "name": "storage_config_example",
 "override": "<merge_tree><parts_to_delay_insert>600</parts_to_delay_insert><parts_to_throw_insert>1100</parts_to_throw_insert></merge_tree>",
 "defaultRetention": 30,
 "defaultColdRetention": 1,
 "auditRetention": 365,
 "auditColdRetention": 0,
 "bufferSize": 33554432,
 "flushInterval": 5,
 "diskBufferDisabled": false,
 "diskBufferSizeLimit": 5368709120,
 "spaces": [
 {
 "id": "",
 "name": "space_example",
 "retention": 0,
 "coldRetention": 0,
 "filter": {
 "id": "",
 "name": "filter_example",
 "root": {
 "group": false,
 "or": false,
 "not": false,
 "conditions": null,
 "leftKind": "",
 "leftEvent": "",
 "leftID": "",
 "leftField": "",
 "leftKeys": null,
 "leftKeyMap": null,
 "leftListItemIdx": 0,
 "leftTICategory": "",
 "leftTIField": "",
 "leftShared": false,
 "op": "",
 "rightKind": "",
 "rightEvent": "",
 "rightID": "",
 "rightField": "",
 "rightKeys": null,
 "rightKeyMap": null,
 "rightListItemIdx": 0,
 "rightTICategory": "",
 "rightTIField": "",
 "rightShared": false,
 "constant": null,
 "list": null,
 "ignoreCase": false,
 "checkTypes": false,
 "filter": null,
 "vulns": null
 },
 "shared": false,
 "currentTab": 0
 }
 }
 ],
 "nodes": [
 {
 "fqdn": "kuma.example",
 "shard": 1,
 "replica": 1,
```

```
  "keeper": 1
  }
  ],
  "disks": [
  {
  "type": "local",
  "name": "disk_1",
  "path": "/disk_1_path/",
  "endpoint": ""
  },
  {
  "type": "hdfs",
  "name": "disk_2",
  "endpoint": "hdfs://hdfs1:9000/clickhouse/"
  }
  ],
  "writeLocal": false,
  "debug": false,
  "shared": false
  }
 }
```


Действие по реагированию

HTTP-код: 200

Формат: JSON

Возвращает обновленное содержимое ресурса.

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found
409	conflict
500	internal error

Создание сервисов

POST /xdr/api/v2.1/kuma/services/create

Передает идентификатор ресурса для создания сервиса на его основе.

Доступ: Главный администратор, Администратор тенанта.

Тело запроса

Ресурс для создания сервиса.

Пример:


```
{
 "resourceID": "00000000-0000-0000-0000-000000000000"
}
```

Действие по реагированию

HTTP-код: 200

Формат: JSON

Возвращает созданный сервис.

Пример:


```
{
 "id": "00000000-0000-0000-0000-000000000000",
 "tenant_id": "00000000-0000-0000-0000-000000000000",
 "resource_id": "00000000-0000-0000-0000-000000000000",
 "kind": "storage",
 "name": "storage_resource_example",
 "status": "red",
 "created": "2024-09-06T00:00:00.000Z",
 "started": "2024-09-06T00:00:00.000Z"
}
```


Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found
409	conflict
500	internal error

Поиск служб

GET /xdr/api/v2.1/kuma/services/

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Аналитик 1-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
page	Числовое	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	Строка	Нет	Идентификатор сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	Строка	Нет	Идентификатор тенанта сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	Строка	Нет	Имя службы. Регистронезависимое регулярное выражение	service

			(PCRE).	^My service$
kind	Строка	Нет	Тип сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	collector, correlator, storage, agent
fqdn	Строка	Нет	FQDN сервиса. Регистронезависимое регулярное выражение (PCRE).	hostname ^hostname.example.com$
paired	bool	Нет	Выводить только те сервисы, которые выполнили первый запуск. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются.	/xdr/api/v2.1/kuma/services?paired

Действие по реагированию

HTTP-код: 200

Формат: JSON

```
type Response []Service

type Service struct {
 ID string `json:"id"`
 TenantID string `json:"tenantID"`
 TenantName string `json:"tenantName"`
 ResourceID string `json:"resourceID"`
 Kind string `json:"kind"`
 Name string `json:"name"`
 Address string `json:"address"`
 FQDN string `json:"fqdn"`
 Status string `json:"status"`
 Warning string `json:"warning"`
 APIPort string `json:"apiPort"`
 Uptime string `json:"uptime"`
 Version string `json:"version"`
 Created string `json:"created"`
 Updated string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля `message`	Значение поля `details`
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметр kind	invalid kind	<kind>
500	Любая другая внутренняя ошибка.	Переменная.	Переменная.

Перезагрузка сервисов

POST /xdr/api/v2.1/kuma/services/<id>/reload

Передает идентификатор сервиса для обновления его конфигурации.

Доступ: Главный администратор, Администратор тенанта, Аналитик 2-го уровня.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения

id	Строка	Нет	Идентификатор сервиса.	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found
409	conflict
500	internal error

Перезапуск сервисов

POST /xdr/api/v2.1/kuma/services/<id>/reload

Передает идентификатор сервиса, чтобы перезапустить его.

Доступ: Главный администратор, Администратор тенанта.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательное ли поле	Описание	Пример значения
id	Строка	Нет	Идентификатор сервиса.	00000000-0000-0000-0000-000000000000

Действие по реагированию

HTTP-код: 202

Возможные ошибки

HTTP-код	Описание
400	bad request
403	forbidden
404	not found
409	conflict
500	internal error

Управление Kaspersky Unified Monitoring and Analysis Platform

В этом разделе представлена информация о функциях Kaspersky Unified Monitoring and Analysis Platform, связанных с работой и обслуживанием Open Single Management Platform.

О приложении Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform (далее KUMA или "приложение") – это комплексное программное решение, сочетающее в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- поиск по полученным событиям;
- создание уведомлений о выявлении признаков угроз информационной безопасности.

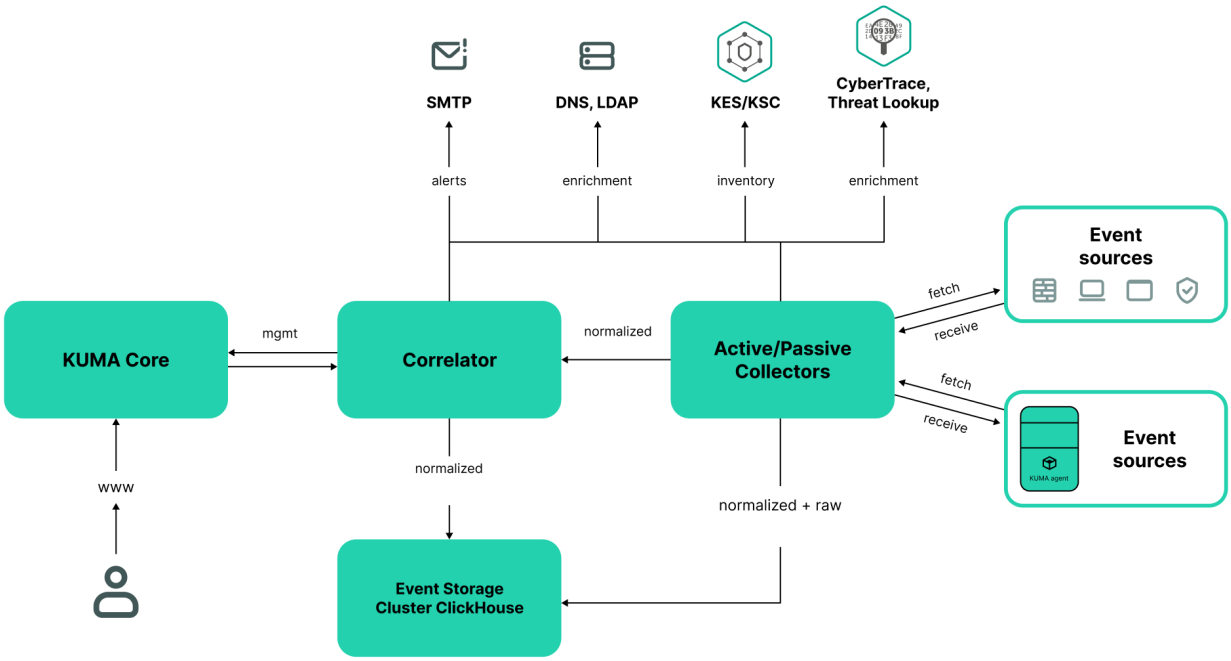
Приложение построено на микросервисной архитектуре. Это означает, что вы можете создавать и настраивать только необходимые микросервисы (далее также "сервисы"), что позволяет использовать KUMA и как систему управления журналами, и как полноценную SIEM-систему. Кроме того, благодаря гибкой маршрутизации потоков данных вы можете использовать сторонние сервисы для дополнительной обработки событий.

Архитектура приложения

Стандартная установка приложения включает следующие компоненты:

- *Ядро*, включающее графический интерфейс для мониторинга и управления настройками компонентов системы.
- Один или несколько *коллекторов*, которые получают сообщения из источников событий и осуществляют их парсинг, нормализацию и, если требуется, фильтрацию и/или агрегацию.
- *Коррелятор*, который анализирует полученные из коллекторов нормализованные события, выполняет необходимые действия с активными листами и создает алерты в соответствии с правилами корреляции.
- *Хранилище*, в котором содержатся нормализованные события и зарегистрированные алерты.

События передаются между компонентами по надежным транспортным протоколам (при желании с шифрованием). Вы можете настроить балансировку нагрузки для ее распределения между экземплярами сервисов, а также включить автоматическое переключение на резервный компонент в случае недоступности основного. Если недоступны все компоненты, события сохраняются в буфере жесткого диска и передаются позже. Размер буфера в файловой системе для временного хранения событий можно менять.



Архитектура KUMA

Ядро

Ядро – это центральный компонент KUMA, на основе которого строятся все прочие сервисы и компоненты. Предоставляемый Ядром графический пользовательский интерфейс консоли предназначен как для повседневного использования операторами и аналитиками, так и для настройки системы в целом.

Ядро позволяет выполнять следующие задачи:

- создавать и настраивать сервисы (или компоненты) приложения, а также интегрировать в систему необходимое программное обеспечение;
- централизованно управлять сервисами и учетными записями пользователей приложения;
- визуально представлять статистические данные о работе приложения;
- расследовать угрозы безопасности на основе полученных событий.

Хранилище

Хранилище KUMA используется для хранения нормализованных событий таким образом, чтобы к ним обеспечивался быстрый и бесперебойный доступ из KUMA с целью извлечения аналитических данных. Скорость и бесперебойность доступа обеспечивается за счет использования технологии ClickHouse. Таким образом *хранилище* – это кластер ClickHouse, связанный с сервисом хранилища KUMA. Кластеры ClickHouse можно дополнять дисками холодного хранения данных.

При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий. Дополнительные сведения см. в документации ClickHouse.

В хранилищах можно создавать *пространства*. Пространства позволяют организовать в кластере структуру данных и, например, хранить события определенного типа вместе.

Коллектор

Коллектор – это компонент приложения, который получает сообщения из источников событий, обрабатывает их и передает в хранилище, коррелятор и/или сторонние сервисы для выявления алертов.

Для каждого коллектора нужно настроить один коннектор и один нормализатор. Вы также можете настроить любое количество дополнительных нормализаторов, фильтров, правил обогащения и правил агрегации. Для того чтобы коллектор мог отправлять нормализованные события в другие сервисы, необходимо добавить точки назначения. Как правило, используются две точки назначения: хранилище и коррелятор.

Алгоритм работы коллектора состоит из следующих этапов:

1. **Получение сообщений из источников событий**

   Для получения сообщений требуется настроить активный или пассивный коннектор. Пассивный коннектор только ожидает события от указанного источника, а активный – инициирует подключение к источнику событий, например к системе управления базами данных.

   Коннекторы различаются по типу. Выбор типа коннектора зависит от транспортного протокола для передачи сообщений. Например, для источника событий, передающего сообщения по протоколу TCP, необходимо установить коннектор типа TCP.

   В приложении доступны следующие типы коннекторов:

   - internal
   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - diode
   - ftp
   - nfs
   - wmi
   - wec
   - snmp

- elastic
- etw

2. **Парсинг и нормализация событий**

   События, полученные коннектором, обрабатываются с помощью нормализатора и правил нормализации, заданных пользователем. Выбор нормализатора зависит от формата сообщений, получаемых из источника события. Например, для источника, отправляющего события в формате CEF, необходимо выбрать нормализатор типа CEF.

   В приложении доступны следующие нормализаторы:

   - JSON
   - CEF
   - Regexp
   - Syslog (как для RFC3164 и RFC5424)
   - CSV
   - Ключ-значение
   - XML
   - NetFlow v5
   - NetFlow v9
   - IPFIX (v10)

3. **Фильтрация нормализованных событий**

   Вы можете настроить фильтры, которые позволят вам выбрать события, соответствующие заданным условиям, для дальнейшей обработки.

4. **Обогащение и преобразование нормализованных событий**

   Правила обогащения позволяют дополнить содержащуюся в событии информацию данными из внутренних и внешних источников. В приложении представлены следующие источники обогащения:

   - константы;
   - cybertrace;
   - словари;
   - dns;
   - события;
   - ldap;
   - шаблоны;
   - данные о часовых поясах;
   - геоданные.

Правила преобразования позволяют преобразовать содержимое поля события в соответствии с заданными условиями. В приложении представлены следующие методы преобразования:

- lower – перевод всех символов в нижний регистр;
- upper – перевод всех символов в верхний регистр;
- regexp – извлечение подстроки с использованием регулярных выражений RE2;
- substring – получение подстроки по заданным номерам начальной и конечной позиции;
- replace – замена текста введенной строкой;
- trim – удаление заданных символов;
- append – добавление символов в конец значения поля;
- prepend – добавление символов в начало значения поля.

5. **Агрегация нормализованных событий**

   Вы можете настроить правила агрегации, чтобы уменьшить количество схожих событий, передаваемых в хранилище и/или коррелятор. Настройка правил агрегации позволит объединить несколько событий в одно событие. Это помогает снизить нагрузку на сервисы, которые отвечают за дальнейшую обработку событий, сэкономить место для хранения данных и сэкономить лицензионную квоту (EPS). Например, можно агрегировать в одно событие все события сетевых подключений, выполненных по одному и тому же протоколу транспортного и прикладного уровней между двумя IP-адресами и полученных в течение заданного интервала.

6. **Передача нормализованных событий**

   После завершения всех этапов обработки событие отправляется в настроенные точки назначения.

Коррелятор

Коррелятор – это компонент приложения, который анализирует нормализованные события. В процессе корреляции может использоваться информация из активных листов и/или словарей.

Полученные в ходе анализа данные применяются для выполнения следующих задач:

- управление содержимым активных листов;
- отправка корреляционных событий в настроенные точки назначения.

Корреляция событий выполняется в реальном времени.

Принцип работы коррелятора основан на сигнатурном анализе событий. Это значит, что каждое событие обрабатывается в соответствии с правилами корреляции, заданными пользователем. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, приложение создает корреляционное событие и отправляет его в Хранилище. Корреляционное событие можно также отправлять на повторный анализ в коррелятор, позволяя таким образом настраивать правила корреляции на срабатывание от предыдущих результатов анализа. Результаты одного правила корреляции могут использоваться другими правилами корреляции.

Вы можете распределять правила корреляции и используемые ими активные листы между корреляторами, разделяя таким образом нагрузку между сервисами. В этом случае коллекторы будут отправлять нормализованные события во все доступные корреляторы.

Алгоритм работы коррелятора состоит из следующих этапов:

1. **Получение события**

   Коррелятор получает нормализованное событие из коллектора или другого сервиса.

2. **Применение правил корреляции**

   Правила корреляции можно настроить на срабатывание на основе одного события или последовательности событий. Если по правилам корреляции не был выявлен алерт, обработка события завершается.

3. **Реагирование на алерт**

   Вы можете задать действия, которые приложение будет выполнять при выявлении алерта. В приложении доступны следующие действия:

   - обогащение события;
   - операции с активными листами;
   - отправка уведомлений;
   - сохранение корреляционного события.

4. **Отправка корреляционного события**

   При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, приложение создает корреляционное событие и отправляет его в хранилище. На этом обработка события коррелятором завершается.

Основные сущности

В этом разделе описаны основные сущности, с которыми работает KUMA.

О событиях

События – это события информационной безопасности, зарегистрированные на контролируемых элементах IT-инфраструктуры организации. Например, события включают попытки входа в систему, взаимодействия с базой данных и многоадресную рассылку информации. Каждое отдельное событие может показаться бессмысленным, но, если рассматривать их вместе, они формируют более широкую картину сетевой активности, которая помогает идентифицировать угрозы безопасности. Это основная функциональность KUMA.

KUMA получает события из журналов и реструктурирует их, приводя данные из разнородных источников к единому формату (этот процесс называется нормализацией). После этого события фильтруются, агрегируются и отправляются в сервис коррелятора для анализа и в сервис хранилища для хранения. Когда KUMA распознает заданное событие или последовательность событий, создаются *корреляционные события*, которые также анализируются и сохраняются. Если событие или последовательность событий указывают на потенциальную угрозу безопасности, KUMA создает алерт. Этот алерт состоит из предупреждения об угрозе и всех связанных данных, которые должен изучить сотрудник службы безопасности.

На протяжении своего жизненного цикла события претерпевают изменения и могут называться по-разному. Так выглядит жизненный цикла типичного события:

Первые шаги выполняются в коллекторе.

1. "Сырое" событие. Исходное сообщение, полученное KUMA от источника событий с помощью коннектора, называется *"сырым" событием*. Это необработанное сообщение, и KUMA пока не может использовать его. Чтобы с таким событием можно было работать, его требуется нормализовать, то есть привести к модели данных KUMA. Это происходит на следующем этапе.

2. Нормализованное событие. Нормализатор преобразует данные "сырого" события так, чтобы они соответствовали модели данных KUMA. После этой трансформации исходное сообщение становится *нормализованным событием* и может быть проанализировано в KUMA. С этого момента KUMA работает только с нормализованными событиями. Необработанные, "сырые" события больше не используются, но их можно сохранить как часть нормализованных событий внутри поля `Raw`.

   В приложении представлены следующие нормализаторы:

   - JSON
   - CEF
   - Regexp
   - Syslog (как для RFC3164 и RFC5424)
   - CSV/TSV
   - Ключ-значение
   - XML
   - Netflow v5, v9, IPFIX (v10), sFlow v5
   - SQL

   После завершения этого этапа нормализованные события можно использовать для анализа.

3. Точка назначения. После обработки события коллектором, оно готово к пересылке в другие сервисы KUMA: в коррелятор и/или хранилище KUMA.

Следующие этапы жизненного цикла события проходят в корреляторе.

Типы событий:

1. Базовое событие. Событие, которое было нормализовано.

2. Агрегированное событие. Чтобы не тратить время и ресурсы на обработку большого количества однотипных сообщений, похожие события можно объединять в одно событие. Такие события ведут себя и обрабатываются так же, как и базовые события, но в дополнение ко всем параметрам родительских событий (событий, которые были объединены) агрегированные события имеют счетчик, показывающий количество родительских событий, которые они представляют. Агрегированные события также хранят время, когда были получены первое и последнее родительские события.

3. Корреляционные события. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, приложение создает *корреляционное событие*. Эти события можно фильтровать, обогащать и агрегировать. Их также можно отправить на хранение или в коррелятор на анализ.

4. Событие аудита. События аудита создаются при выполнении в KUMA определенных действий, связанных с безопасностью. Эти события используются для обеспечения целостности системы. Они автоматически размещаются в отдельном пространстве хранилища и хранятся не менее 365 дней.

5. Событие мониторинга. Такие события используются для отслеживания изменений в количестве данных, поступающих в KUMA.

Об алертах

В KUMA алерты создаются при получении последовательности событий, запускающей правило корреляции. Аналитики KUMA создают правила корреляции для проверки входящих событий на предмет возможных угроз безопасности, поэтому при срабатывании правила корреляции появляется предупреждение о возможной вредоносной активности. Сотрудники службы безопасности, ответственные за защиту данных, должны изучить эти алерты и при необходимости отреагировать на них.

KUMA автоматически присваивает уровень важности каждому алерту. Этот параметр показывает, насколько важны или многочисленны процессы, запустившие правило корреляции. В первую очередь следует обрабатывать алерты с более высоким уровнем важности. Значение уровня важности автоматически обновляется при получении новых корреляционных событий, но сотрудник службы безопасности также может задать его вручную. В этом случае уровень важности алерта больше не обновляется автоматически.

К алертам привязаны относящиеся к ним события, благодаря чему происходит обогащение алертов данными из событий. В KUMA также можно детально анализировать алерты.

На основании алертов можно создать инциденты.

Работа с алертами в KUMA описана в этом разделе.

Об инцидентах

Если характер поступающих в KUMA данных, создаваемых корреляционных событий и обнаружений указывает на возможную атаку или уязвимость, признаки такого происшествия можно объединить в *инцидент*. Это позволяет специалистам службы безопасности анализировать проявления угрозы комплексно и облегчает реагирование.

Инцидентам можно присваивать категории, типы и уровни важности, а также назначать их сотрудникам, ответственным за защиту данных, для обработки.

Инциденты можно экспортировать в НКЦКИ.

О ресурсах

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления связи с заданным веб-адресом или преобразования данных по определенным правилам. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов, на основе которых в свою очередь создаются сервисы KUMA.

О сервисах

Сервисы – это основные компоненты KUMA, с помощью которых осуществляется работа с событиями: получение, обработка, анализ и хранение. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть сервиса создается внутри Консоли KUMA на основе набора ресурсов для сервисов.
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же агента или хранилища могут быть установлены сразу на нескольких устройствах.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Об агентах

Агенты KUMA – это сервисы, которые используются для пересылки необработанных событий с серверов и рабочих станций в точки назначения KUMA.

Типы агентов:

- wmi-агенты – используются для получения данных с удаленных устройств Windows с помощью Windows Management Instrumentation. Устанавливается на активы Windows.
- wec-агенты – используются для получения журналов событий Windows с локального устройства с помощью Windows Event Collector. Устанавливается на активы Windows.
- tcp-агенты – используются для получения данных по протоколу TCP. Устанавливается на активы Linux и Windows.
- udp-агенты – используются для получения данных по протоколу UDP. Устанавливается на активы Linux и Windows.
- nats-агенты – используются для коммуникации через NATS. Устанавливается на активы Linux и Windows.
- kafka-агенты – используются для коммуникации с помощью kafka. Устанавливается на активы Linux и Windows.
- http-агенты – используются для связи по протоколу HTTP. Устанавливается на активы Linux и Windows.
- file-агенты – используются для получения данных из файла. Устанавливается на активы Linux.
- ftp-агенты – используются для получения данных по протоколу File Transfer Protocol. Устанавливается на активы Linux и Windows.
- nfs-агенты – используются для получения данных по протоколу Network File System. Устанавливается на активы Linux и Windows.
- snmp-агенты – используются для получения данных с помощью Simple Network Management Protocol. Устанавливается на активы Linux и Windows.
- diode-агенты – используются вместе с диодами данных для получения событий из изолированных сегментов сети. Устанавливается на активы Linux и Windows.
- etw-агенты используются для получения данных Event Tracing for Windows. Устанавливается на активы Windows.

Об уровне важности

Параметр *Уровень важности* отражает, насколько чувствительны для безопасности происшествия, обнаруженные коррелятором KUMA. Он показывает порядок, в котором следует обрабатывать алерты, а также указывает, требуется ли участие старших специалистов по безопасности.

Коррелятор автоматически назначает уровень важности корреляционным событиям и алертам, руководствуясь настройками правил корреляции. Уровень важности алерта также зависит от активов, связанных с обработанными событиями, так как правила корреляции принимают во внимание уровень важности категории этих активов. Если к алерту или корреляционному событию не привязаны активы с уровнем важности или не привязаны активы вообще, уровень важности такого алерта или корреляционного события приравнивается к уровню важности породившего их правила корреляции. Уровень важности алерта или корреляционного события всегда больше или равен уровню важности породившего их правила корреляции.

Уровень важности алерта можно изменить вручную. Измененный вручную уровень важности перестает автоматически обновляться правилами корреляции.

Возможные значения уровня важности:

- Низкий
- Средний
- Высокий
- Предельный

Руководство администратора

В этой главе представлена информация об установке и настройке SIEM-системы KUMA.

Вход в Консоль KUMA

Чтобы перейти в Консоль KUMA, в Консоли OSMP перейдите в раздел **Параметры** → **KUMA**.

Вы перейдете к Консоли KUMA. Консоль откроется в новой вкладке браузера.

Сервисы KUMA

Сервисы – это основные компоненты KUMA, с помощью которых система осуществляет работу с событиями: сервисы позволяют получить события из источников, чтобы в дальнейшем привести их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть сервиса создается внутри Консоли KUMA на основе набора ресурсов для сервисов.

- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же агента или хранилища могут быть установлены сразу на нескольких устройствах.

  В серверной части сервисы KUMA располагаются в директории `/opt/kaspersky/kuma`.

  При установке KUMA в режиме высокой доступности в кластере устанавливается только Ядро KUMA. Коллекторы, коррелляторы и хранилища размещаются на устройствах вне кластера Kubernetes.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Типы сервисов:

- Хранилища используются для хранения событий.
- Коррелляторы используются для анализа событий и поиска определенных закономерностей.
- Коллекторы используются для получения событий и преобразования их в формат KUMA.
- Агенты используются для получения событий на удаленных устройствах и пересылки их коллекторам KUMA.

В Консоли KUMA сервисы отображаются в разделе **Ресурсы** → **Активные сервисы** в виде таблицы. Таблицу сервисов можно обновлять с помощью кнопки **Обновить** и сортировать по столбцам, нажимая на активные заголовки.

Максимальный размер таблицы не ограничен. Если вы хотите выбрать все сервисы, прокрутите таблицу до конца и установите флажок **Выбрать все**, таким образом все доступные в таблице сервисы будут выбраны.

Столбцы таблицы:

- **Статус** – статус сервиса:
  - Зеленый – сервис работает.
  - Красный – сервис не работает.
  - Желтый – это статус, который применяется ко всем сервисам, кроме агента. Желтый статус означает, что сервис работает, но есть ошибки или алерты от Victoria Metrics. Сообщение об ошибке можно просмотреть, наведя курсор мыши на статус.
  - Фиолетовый – этот статус применяется к работающим сервисам, у которых изменился конфигурационный файл в базе данных и при этом отсутствуют другие ошибки. Если у сервиса некорректный конфигурационный файл и есть ошибки, например от Victoria Metrics, статус сервиса будет желтым.
  - Серый – если в удаленном тенанте был работающий сервис, который продолжает работать, на странице **Активные сервисы** он будет отображаться с серым статусом. Сервисы в сером статусе остаются, чтобы вы могли скопировать идентификатор и удалить сервисы на серверах. Удалить сервисы с серым статусом может только Главный администратор. Когда тенант удаляется, его службы назначаются главному тенанту.
- **Тип** – вид сервиса: **агент**, **коллектор**, **коррелятор**, **хранилище**.

- **Название** – название сервиса. При нажатии на название сервиса открываются его настройки.
- **Версия** – версия сервиса.
- **Тенант** – название тенанта, которому принадлежит сервис.
- **Полное доменное имя** – доменное имя сервера, на котором установлен сервис.
- **IP-адрес** – IP-адрес сервера, на котором установлен сервис.
- **Порт API** – номер порта для внутренних коммуникаций.
- **Время работы** – как долго сервис работает.
- **Создан** – дата и время создания сервиса.

В таблице предусмотрена сортировка данных по возрастанию и убыванию, а также по параметру **Статус**. Вы можете отсортировать активные сервисы, вызвав контекстное меню правой кнопкой мыши и выбрав один или несколько статусов.

С помощью кнопок в верхней части окна **Сервисы** можно выполнить следующие групповые действия:

- Добавить сервис.

  Вы можете создавать новые сервисы на основе существующих наборов ресурсов для сервисов. Мы не рекомендуем создавать сервисы вне основного тенанта без предварительного внимательного планирования межтенантных взаимодействий различных сервисов и пользователей.

- Обновить.

  Вы можете обновить список активных сервисов.

- Обновить параметры.
- Перезапустить.

Для действий с отдельными сервисами воспользуйтесь контекстным меню, которое вы можете вызвать нажатием правой кнопки мыши. Доступны следующие действия:

- Сбросить сертификат.
- Удалить.
- Скачать журнал.

  Если вы хотите получать детализированные данные, настройте в параметрах сервиса режим Отладка.

- Скопировать идентификатор сервиса

  Идентификатор понадобится вам для установки, перезапуска, остановки или удаления сервиса.

- Перейти к событиям.
- Перейти к активным листам.
- Перейти к контекстным таблицам.
- Перейти к партициям.

Чтобы изменить сервис, выберите сервис в разделе **Ресурсы → Активные сервисы**. Откроется окно с набором ресурсов, на основе которых был создан сервис. Вы можете изменить параметры набора ресурсов и сохранить изменения. Чтобы применить сохраненные изменения, перезапустите сервис.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы → Нормализаторы**.

Инструменты сервисов

В этом разделе описываются инструменты по работе с сервисами, доступные в Консоли KUMA в разделе **Ресурсы → Активные сервисы**.

Получение идентификатора сервиса

Идентификатор сервиса используется для связи частей сервиса – расположенных внутри KUMA и установленных в сетевой инфраструктуре – в единый комплекс. Идентификатор присваивается сервису при его создании в KUMA, а затем используется при установке сервиса на сервер.

Чтобы получить идентификатор сервиса:

1. Войдите в Консоль KUMA и откройте раздел **Ресурсы → Активные сервисы**.
2. Установите флажок рядом с сервисом, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

   Идентификатор сервиса помещен в буфер. Его можно использовать, например, для установки службы на сервере.

Остановка, запуск и проверка статуса сервиса

В ходе работы с KUMA может возникнуть необходимость в следующих операциях:

- Временно остановить сервис. Например, в процессе восстановления Ядра из резервной копии или если вы хотите отредактировать параметры сервиса, связанные с операционной системой.
- Запустить сервис.
- Проверить статус сервиса.

В таблице "Команды остановки, запуска и проверки статуса сервиса" представлены команды, которые могут быть полезны во время работы с KUMA.

Команды остановки, запуска и проверки статуса сервиса

Сервис	Остановить сервис	Запустить сервис	Проверить статус сервиса
Ядро	`sudo systemctl stop kuma-core.service`	`sudo systemctl start kuma-core.service`	`sudo systemctl status kuma-core.service`

Сервисы с идентификатором: • collector • correlator • storage	`sudo systemctl stop kuma-<collector/correlator/storage>-<идентификатор сервиса>.service`	`sudo systemctl start kuma-<collector/correlator/storage>-<идентификатор сервиса>.service`	`sudo systemctl status kuma-<collector/correlator/storage<идентификатор сервиса>.service`
Сервисы без идентификатора: • kuma-grafana.service • kuma-mongodb.service • kuma-victoria-metrics.service • kuma-vmalert.service	`sudo systemctl stop kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl start kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl status kuma-<grafana/victoria-metrics/vmalert>.service`
Агенты под управлением ОС Windows	Чтобы остановить сервис агента: 1. В Консоли KUMA скопируйте идентификатор агента. 2. Подключитесь к устройству, на котором необходимо выполнить запуск службы агента KUMA. 3. Запустите PowerShell от имени пользователя с правами администратора. 4. Выполните следующие команды в PowerShell: `Stop-Service -Name "WindowsAgent-<идентификатор агента>"`	Чтобы запустить сервис агента: 1. В Консоли KUMA скопируйте идентификатор агента. 2. Подключитесь к устройству, на котором необходимо выполнить запуск службы агента KUMA. 3. Запустите PowerShell от имени пользователя с правами администратора. 4. Выполните следующие команды в PowerShell: `Start-Service -Name "WindowsAgent-<идентификатор агента>"`	Чтобы просмотреть статус сервиса агента: 1. В ОС Windows перейдите в мен Пуск → Службы и в списке слу откройте двойным щелчком нужный агент KUMA. 2. В открывшемся окне на вкладке General просмотрите статус агента в поле Service status.

Перезапуск сервиса

Чтобы перезапустить сервис:

1. Войдите в Консоль KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом и выберите нужную опцию:
   - **Обновить параметры** – обновить конфигурацию работающего сервиса, не останавливая его. Например, так можно изменить настройки сопоставления полей или параметры точки назначения.
   - **Перезапустить** – остановить сервис и запустить его снова. Эта опция используется для изменения таких параметров, как порт или тип коннектора.

     Особенности перезапуска агентов KUMA:

     - Агент KUMA для Windows может быть перезагружен, как описано выше, только если он запущен на удаленном компьютере. Если сервис на удаленном компьютере неактивен, при попытке перезагрузки из KUMA вы получите сообщение об ошибке. В этом случае следует перезапустить сервис Агент KUMA для Windows на удаленном компьютере с Windows. Чтобы узнать, как перезапустить сервисы Windows, обратитесь к документации, относящейся к версии операционной системы вашего удаленного компьютера с Windows.

- Агент KUMA для Linux при использовании этой опции останавливается. Для запуска агента необходимо выполнить команду, с помощью которой он был запущен.

- **Сбросить сертификат** – удалить сертификаты, используемые сервисом для внутренней связи. Например, эту опцию можно использовать для обновления сертификата Ядра.

  Особенности удаления сертификатов для агентов Windows:

  - Если агент находится в зеленом статусе и вы выбрали **Сбросить сертификат**, KUMA удаляет действующий сертификат и создает новый, агент продолжает работу с новым сертификатом.

  - Если агент находится в красном статусе и вы выбрали **Сбросить сертификат**, KUMA выдаст ошибку о том, что агент не запущен. В папке установки агента %APPDATA%\kaspersky\kuma\<ID агента>\certficates следует вручную удалить файлы internal.cert и internal.key и вручную запустить агент. При запуске агента новый сертификат будет создан автоматически.

  Особенности удаления сертификатов для агентов Linux:

  1. Независимо от статуса агента необходимо применить опцию **Сбросить сертификат** через веб-интерфейс, чтобы удалить сертификат в базах.

  2. В папке установки агента /opt/kaspersky/agent/<ID агента>/certificates следует вручную удалить файлы internal.cert и internal.key.

  3. Поскольку опция **Сбросить сертификат** останавливает агент, для продолжения работы следует вручную запустить агент. При запуске агента новый сертификат будет создан автоматически.

Удаление сервиса

Перед удалением сервиса получите его идентификатор. Идентификатор потребуется, чтобы удалить сервис с сервера.

Чтобы удалить сервис в Консоли KUMA:

1. Войдите в Консоль KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.

2. Установите флажок рядом с нужным сервисом и нажмите **Удалить**.

   Откроется окно подтверждения.

3. Нажмите на кнопку **ОК**.

Сервис удален из KUMA.

Чтобы удалить сервис с сервера, выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage> --id <идентификатор сервиса> --uninstall
Сервис удален с сервера.
```

Окно Разделы

Создав и установив сервис хранилища, вы можете просмотреть его разделы в таблице **Разделы**.

*Чтобы открыть таблицу **Разделы**:*

1. Войдите в Консоль KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным хранилищем и нажмите **Смотреть разделы**.

   Откроется таблица **Разделы**.

Таблица имеет следующие столбцы:

- **Тенант** – название тенанта, которому принадлежат хранимые данные.
- **Создан** – дата создания раздела.
- **Пространство** – название раздела.
- **Размер** – размер раздела.
- **События** – количество хранимых событий.
- **Переход к холодному хранению** – дата, когда данные будут перенесены с кластеров ClickHouse на диски для холодного хранения.
- **Окончание хранения** – дата, когда истекает срок действия раздела. По достижении этого срока раздел и содержащиеся в нем события перестают быть доступны.

Вы можете удалять разделы.

Чтобы удалить раздел:

1. Откройте таблицу **Разделы** (см. выше).
2. Откройте раскрывающийся список ... слева от необходимого раздела.
3. Выберите пункт **Удалить**.

   Откроется окно подтверждения.
4. Нажмите на кнопку **ОК**.

   Раздел удален. Разделы для событий аудита удалить невозможно.

Поиск связанных событий

Вы можете искать события, обработанные определенным коррелятором или коллектором.

Чтобы найти события, относящиеся к корреляторy или коллектору:

1. Войдите в Консоль KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным коррелятором или коллектором и нажмите **Перейти к событиям**.

   Откроется новая вкладка браузера с открытым разделом KUMA **События**.

3. Чтобы найти события, нажмите на значок .

   Отобразится таблица с событиями, отобранными по поисковому выражению `ServiceID = <идентификатор выбранного сервиса>`.

Наборы ресурсов для сервисов

Наборы ресурсов для сервисов – это тип ресурсов, компонент KUMA, представляющий собой комплект настроек, на основе которых создаются и функционируют сервисы KUMA. Наборы ресурсов для сервисов собираются из ресурсов.

Ресурсы, объединяемые в набор ресурсов, должны принадлежать к тому же тенанту, что и создаваемый набор ресурсов. Исключением является общий тенант: принадлежащие ему ресурсы можно использовать в наборах ресурсов других тенантов.

Наборы ресурсов для сервисов отображаются в Консоли KUMA в разделе **Ресурсы** → **<Тип набора ресурсов для сервиса>**. Доступные типы:

- Коллекторы.
- Корреляторы.
- Хранилища.
- Агенты.

При выборе нужного типа открывается таблица с имеющимися наборами ресурсов для сервисов этого типа. Таблица содержит следующие столбцы:

- **Название** – имя набора ресурсов. Может использоваться для поиска и сортировки.
- **Последнее обновление** – дата и время последнего обновления набора ресурсов. Может использоваться для сортировки.
- **Создал** – имя пользователя, создавшего набор ресурсов.
- **Описание** – описание набора ресурсов.

Создание хранилища

Хранилище состоит из двух частей: одна часть создается внутри Консоли KUMA, а вторая устанавливается на серверах сетевой инфраструктуры, предназначенных для хранения событий. Серверная часть хранилища KUMA представляет собой собранные в кластер узлы ClickHouse. Кластеры ClickHouse можно дополнять дисками холодного хранения данных.

Для каждого кластера ClickHouse требуется установить отдельное хранилище.

> Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.

В качестве файловой системы рекомендуется использовать ext4.

Создание хранилища производится в несколько этапов:

1. **Создание набора ресурсов хранилища в Консоли KUMA**
2. **Создание сервиса хранилища в Консоли KUMA**
3. **Установка узлов хранилища в сетевой инфраструктуре**

При создании узлов кластера хранилища убедитесь в сетевой связности системы и откройте используемые компонентами порты.

При изменении параметров хранилища его сервис необходимо перезапустить.

Структура кластера ClickHouse

Кластер ClickHouse – логическая группа устройств, обладающих всеми накопленными нормализованными событиями KUMA. Подразумевает наличие одного или нескольких логических *шардов*.

Шард – логическая группа устройств, обладающих некоторой **частью** всех накопленных в кластере нормализованных событий. Подразумевает наличие одной или нескольких *реплик*. Увеличение количества шардов позволяет:

- Накапливать больше событий за счет увеличения общего количества серверов и дискового пространства.
- Поглощать больший **поток** событий за счет распределения нагрузки, связанной со вставкой новых событий.
- Уменьшить время поиска событий за счет распределения поисковых зон между несколькими устройствами.

Реплика – устройство, являющееся членом логического шарда и обладающее одной копией данных этого шарда. Если реплик несколько – копий тоже несколько (данные реплицируются). Увеличение количества реплик позволяет:

- Повысить отказоустойчивость.
- Распределить общую нагрузку, связанную с поиском данных, между несколькими машинами (однако для этой цели лучше увеличить количество шардов).

Кипер – устройство, участвующее в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одно устройство с этой ролью. Рекомендуемое количество устройств с такой ролью – 3. Число устройств, участвующих в координации репликации, должно быть **нечетным**. Роль *кипера* и *реплики* можно совмещать.

Параметры узлов кластера ClickHouse

Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.

При создании узлов кластера ClickHouse убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Для каждого узла кластера ClickHouse требуется указать следующие параметры:

- Полное доменное имя (FQDN) – уникальный адрес, по которому должен быть доступен узел. Необходимо указывать FQDN целиком, например `kuma-storage.example.com`.
- Идентификаторы шарда, реплики и кипера – комбинация этих параметров определяет положение узла в структуре кластера ClickHouse и его роль.

Роли узлов

Роли узлов зависят от указанных параметров:

- шард, реплика, кипер – узел участвует в накоплении и поиске нормализованных событий KUMA, а также в координации репликации данных на уровне всего кластера.
- шард, реплика – узел участвует в накоплении и поиске нормализованных событий KUMA.
- кипер – узел **не** накапливает нормализованные события, но участвует в координации репликации данных на уровне всего кластера. Выделенные киперы следует указывать в начале списка в разделе **Ресурсы** → **Хранилища** → <Хранилище> → **Основные настройки** → **Узлы кластера ClickHouse**.

Требования к идентификаторам:

- Если в одном кластере создано несколько шардов, идентификаторы шардов должны быть уникальными в рамках этого кластера.
- Если в одном шарде создано несколько реплик, идентификаторы реплик должны быть уникальными в рамках этого шарда.
- Идентификаторы киперов должны быть уникальными в рамках кластера.

Пример идентификаторов узлов кластера ClickHouse:

- шард 1, реплика 1, кипер 1;
- шард 1, реплика 2;
- шард 2, реплика 1;
- шард 2, реплика 2, кипер 3;
- шард 2, реплика 3;
- кипер 2.

Холодное хранение событий

В KUMA можно настроить перенос устаревших данных с кластера ClickHouse на холодное хранение. Для холодного хранения могут использоваться смонтированные в операционной системе локальные диски или распределенная файловая система Hadoop Distributed File System (HDFS). Функция холодного хранения включается, если указан хотя бы один диск холодного хранения. Если диск холодного хранения не настроен и на сервере закончилось место, сервис хранилища остановится. Если есть горячее и холодное хранение и на диске холодного хранения закончилось место, сервис хранилища KUMA остановится. Мы рекомендуем избегать таких ситуаций.

Диски холодного хранения можно добавлять и удалять.

После изменения параметров холодного хранения сервис хранилища необходимо перезапустить. Если сервис не запускается, причина будет указана в журнале хранилища.

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо воссоздать диск с таким же путем (для локальных дисков) или таким же адресом (для HDFS-дисков), а затем удалить его из параметров хранилища.

Правила переноса данных на диски холодного хранения

При задействованном холодном хранении KUMA раз в час проверяет сроки хранения пространств:

- Если срок хранения пространства на кластере ClickHouse истек, данные переносятся на диски холодного хранения. Если диск холодного хранения настроен неверно, данные удаляются.
- Если срок хранения пространства на диске холодного хранения истек, данные удаляются.
- Если диски кластера ClickHouse заполнены на 95%, самые большие партиции автоматически переносятся на диски холодного хранения. Это действие может происходить больше одного раза в час.
- При начале и окончании переноса данных создаются события аудита.

Во время переноса данных сервис хранилища продолжает работать, при этом в Консоли KUMA в разделе **Ресурсы** → **Активные сервисы** для него сохраняется зеленый статус. При наведении указателя мыши на значок статуса отображается сообщение о переносе данных. При удалении холодного диска сервис хранилища отображается в желтом статусе.

Особенности хранения событий и доступа к ним

- При использовании для холодного хранения HDFS-дисков необходимо обеспечить защиту данных одним из следующих способов:
  - Настроить отдельный физический интерфейс в сети VLAN, в котором будут расположены только HDFS-диски и кластер ClickHouse.
  - Настроить правила сегментации сети и фильтрации трафика, исключающие прямой доступ к HDFS-диску или перехват трафика к диску со стороны ClickHouse.

- События, находящиеся в кластере ClickHouse и на дисках холодного хранения, одинаково доступны в консоли KUMA. Например, при поиске событий или при просмотре событий, относящихся к алерту.

- Допускается не хранить события или события аудита на дисках холодного хранения: для этого в параметрах хранилища в поле **Срок холодного хранения** или **Срок холодного хранения событий аудита** необходимо указать `0` (дней).

Особенности использования HDFS-дисков

- Перед подключением HDFS-дисков на них необходимо создать директории для каждого узла кластера ClickHouse в формате `<устройство HDFS-диска>/<идентифика тор шарда>/<идентификатор реплики>`. Например, если кластер состоит из двух узлов, на которых расположены две реплики одного шарда, необходимо создать следующие директории:

  - hdfs://hdfs-example-1:9000/clickhouse/1/1/

  - hdfs://hdfs-example-1:9000/clickhouse/1/2/

  События из узлов кластера ClickHouse будут переноситься в директории, в названии которых указаны идентификаторы их шарда и реплики. Если изменить эти параметры узла и при этом не создать соответствующую директорию на HDFS-диске, события при переносе могут быть потеряны.

- HDFS-диски, добавленные к хранилищу, работают в режиме JBOD. Это означает, что при отказе одного из дисков будет потерян доступ к хранилищу. При использовании HDFS следует учитывать необходимость высокой доступности и настроить RAID, а также хранение данных из разных реплик на различных устройствах.

- Скорость записи событий в HDFS, как правило, ниже скорости записи событий на локальные диски. Скорость доступа к событиям в HDFS, как правило, значительно ниже скорости доступа к событиям на локальных дисках. При использовании одновременно локальных дисков и HDFS-дисков запись будет происходить в них по очереди.

Удаление дисков холодного хранения

Перед физическим отключением дисков холодного хранения необходимо удалить эти диски из параметров хранилища.

Чтобы удалить диск из параметров хранилища:

- В Консоли KUMA перейдите в раздел **Ресурсы** → **Хранилища** и выберите нужное хранилище.

  Откроется хранилище.

- В окне в разделе **Диски холодного хранения** в блоке параметров нужного диска нажмите **Удалить диск**.

  Данные с удаляемого диска автоматически начинают переноситься на другие диски холодного хранения или, если их нет, в кластер ClickHouse. В процессе переноса данных значок статуса хранилища светится желтым цветом. При начале и окончании переноса данных создаются события аудита.

- После завершения переноса событий диск автоматически удаляется из параметров хранилища. Теперь его можно безопасно отключить.

На удаляемых дисках могут оставаться события. Если вы хотите их удалить, вы можете, например, вручную удалить партиции с данными с помощью команды DROP PARTITION.

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо создать диск с таким же путем (для локальных дисков) или таким же адресом (для HDFS-дисков), а затем удалить его из параметров хранилища.

Отключение, архивирование и подключение партиций

Если вы хотите оптимизировать дисковое пространство и ускорить выполнение запросов в KUMA, вы можете отключить в ClickHouse партиции с данными, архивировать партиции или перенести их на носитель. При необходимости вы можете снова подключить необходимые партиции и выполнить обработку данных.

Отключение партиций

Чтобы отключить партиции, выполните следующие шаги:

1. Определите шард, на всех репликах которого вы планируете отключить партицию.
2. Получите идентификатор партиции с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "SELECT partition, name FROM system.parts;" |grep 20231130
   ```

   В приведенном примере в результате выполнения команды будет получен идентификатор партиции от 30 ноября 2023 года.
3. На каждой реплике шарда отключите партицию с помощью следующей команды, указав требуемый идентификатор:

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 DETACH PARTITION ID '<идентификатор партиции>'"
   ```

В результате партиция отключена на всех репликах шарда. Теперь вы можете перенести каталог с данными на носитель или заархивировать партицию.

Архивирование партиций

Чтобы архивировать отключенные партиции:

1. Найдите отключенную партицию в дисковой подсистеме сервера:

   ```
   sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <идентификатор отключенной партиции>\*
   ```
2. Перейдите в каталог detached с отключенной партицией и, находясь в каталоге detached, выполните архивирование:

   ```
   sudo cd <путь к каталогу detached, содержащему отключенную партицию>
   sudo zip -9 -r detached.zip *
   ```

   Например:

   ```
   sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   sudo zip -9 -r detached.zip *
   ```

Архивирование партиции выполнено.

Подключение партиций

Чтобы подключить архивные партиции к KUMA, необходимо выполнить следующие действия:

1. Увеличьте значение параметра **Срок хранения**.

   KUMA удаляет данные на основании даты, указанной в поле Timestamp - когда событие получено, и на основании значения параметра **Срок хранения**, которое вы задали для хранилища.

   Перед тем как выполнять восстановление архивных данных, убедитесь, что значение параметра **Срок хранения** перекрывает дату из поля Timestamp. В противном случае, архивные данные будут удалены в течение 1 часа.

2. Поместите архивную партицию в раздел detached вашего хранилища и распакуйте архив:

   `sudo unzip detached.zip -d <путь к каталогу detached>`

   Например:

   `sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/`

3. Выполните команду подключения партиции:

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<идентификатор партиции>'"
   ```

   `Повторите шаги распаковки архива и подключения партиции на каждой реплике шарда.`

В результате архивная партиция подключена и события снова доступны для поиска.

Создание набора ресурсов для хранилища

Сервис хранилища в Консоли KUMA создается на основе набора ресурсов для хранилища.

Чтобы создать набор ресурсов для хранилища в Консоли KUMA:

1. В Консоли KUMA в разделе **Ресурсы** → **Хранилища** нажмите **Добавить хранилище**.

   Откроется окно **Создание хранилища**.

2. На вкладке **Основные параметры** в поле **Название хранилища** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.

4. В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

5. В поле **Срок хранения** укажите, в течение какого количества дней с момента поступления вы хотите хранить события в кластере ClickHouse. По истечении указанного срока события будут автоматически удалены из кластера ClickHouse. Если настроено холодное хранение событий и срок хранения событий в кластере ClickHouse истек, данные переносятся на диски холодного хранения. Если диск холодного хранения настроен неверно, данные удаляются.

6. В поле **Срок хранения событий аудита** укажите, в течение какого количества дней вы хотите хранить события аудита. Минимальное значение и значение по умолчанию: `365`.

7. При необходимости холодного хранения данных введите сроки хранения событий:

   - **Срок холодного хранения** – количество дней хранения событий. Минимальное значение – `1`.

- **Срок холодного хранения событий аудита** – количество дней хранения событий аудита. Минимальное значение – 0.

8. В раскрывающемся списке **Отладка** укажите, будет ли включено логирование ресурса. Значение по умолчанию: **Выключено** - это означает, что для всех компонентов KUMA в журнале событий регистрируются только ошибки. Если вы хотите получать детализированные данные в журналах, выберите значение **Включено**.

9. При необходимости изменения параметров ClickHouse в поле **Переопределение параметров ClickHouse** вставьте строки с параметрами из XML-файла конфигурации ClickHouse /opt/kaspersky/kuma/clickhouse/cfg/config.xml. Указание корневых элементов <yandex>, </yandex> не требуется. Переданные в поле параметры конфигурации будут использоваться вместо параметров по умолчанию.

   Пример:

   <merge_tree>

   <parts_to_delay_insert>600</parts_to_delay_insert>

   <parts_to_throw_insert>1100</parts_to_throw_insert>

   </merge_tree>

10. При необходимости в разделе **Пространства** добавьте в хранилище пространства, по которым вы хотите распределять хранимые события.

    Пространств может быть несколько. Пространства можно добавить с помощью кнопки **Добавить пространство** и удалить с помощью кнопки **Удалить пространство**.

    Доступные параметры:

    - В поле **Название** укажите название пространства: от 1 до 128 символов в кодировке Unicode.

    - В поле **Срок хранения** укажите количество дней, в течение которых события будут храниться в кластере ClickHouse.

    - При необходимости в поле **Срок холодного хранения** укажите количество дней, в течение которого события должны находиться на холодном хранении. Минимальное значение – `1`.

    - В разделе **Фильтр** можно задать условия определения событий, которые будут помещаться в это пространство. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

      Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

После создания сервиса пространства можно просматривать и удалять в параметрах набора ресурсов хранилища.

Нет необходимости создавать отдельное пространство для событий аудита. События этого типа (Тип=4) автоматически помещаются в отдельную область аудита со сроком хранения не менее 365 дней. Это пространство невозможно изменить или удалить из Консоли KUMA.

11. При необходимости в разделе **Диски холодного хранения** добавьте в хранилище диски, на которые вы хотите переносить события на длительное хранение из кластера ClickHouse.

Дисков может быть несколько. Диски можно добавить с помощью кнопки **Добавить диск** и удалить с помощью кнопки **Удалить диск**.

Доступные параметры:

- В раскрывающемся списке **Тип** выберите тип подключаемого диска:
  - **Локальный** – для дисков, смонтированных в операционной системе как директории.
  - **HDFS** – для дисков распределенной файловой системы Hadoop Distributed File System.
- В поле **Название** укажите название диска. Название должно содержать от 1 до 128 символов в кодировке Unicode.
- Если в качестве типа диска вы выбрали **Локальный**, в поле **Путь** введите абсолютный путь директории смонтированного локального диска. Путь должен начинаться и оканчиваться символом "/".
- Если в качестве типа диска вы выбрали **HDFS**, в поле **Устройство** введите путь к HDFS. Например: `hdfs://hdfs1:9000/clickhouse/`.

12. При необходимости в разделе **Узлы кластера ClickHouse** добавьте в хранилище узлы кластера ClickHouse.

    Узлов может быть несколько. Узлы можно добавить с помощью кнопки **Добавить узел** и удалить с помощью кнопки **Удалить узел**.

    Доступные параметры:

    - В поле **Полное доменное имя** укажите FQDN добавляемого узла. Например, `kuma-storage-cluster1-server1.example.com`.

    - В полях идентификаторов шарда, реплики и кипера укажите роль узла в кластере ClickHouse. Идентификаторы шарда и кипера должны быть уникальными в рамках кластера, идентификатор реплики должен быть уникальным в рамках шарда. Ниже показан пример заполнения раздела **Узлы кластера ClickHouse** для хранилища с выделенными киперами в **распределенной схеме установки**. Вы можете адаптировать пример под свои потребности.

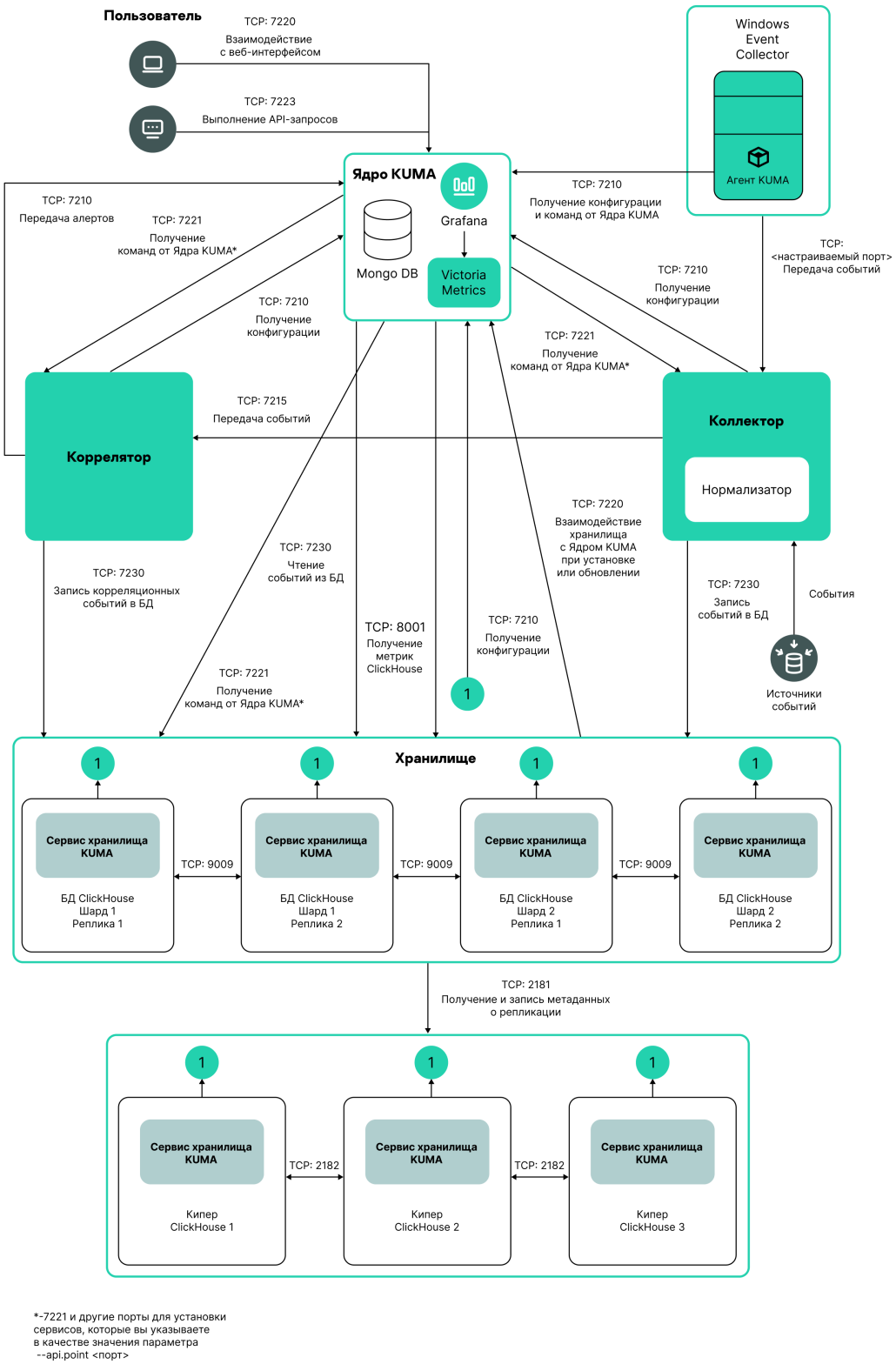


Схема распределенной установки

Пример:

Узлы кластера ClickHouse

Полное доменное имя: kuma-storage-cluster1-server1.example.com

Идентификатор шарда: 0

Идентификатор реплики: 0

Идентификатор кипера: 1

Полное доменное имя: kuma-storage-cluster1server2.example.com
Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 2
Полное доменное имя: kuma-storage-cluster1server3.example.com
Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 3
Полное доменное имя: kuma-storage-cluster1server4.example.com
Идентификатор шарда: 1
Идентификатор реплики: 1
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server5.example.com
Идентификатор шарда: 1
Идентификатор реплики: 2
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server6.example.com
Идентификатор шарда: 2
Идентификатор реплики: 1
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server7.example.com
Идентификатор шарда: 2
Идентификатор реплики: 2
Идентификатор кипера: 0

13. На вкладке **Дополнительные параметры** в поле **Размер буфера** укажите размер буфера в байтах, при достижении которого следует передать события в базу. Значение по умолчанию – 64 МБ. Максимального значения нет. Если на виртуальной машине меньше свободной памяти, чем заданное значение **Размер буфера**, KUMA установит ограничение в 128 МБ.

14. На вкладке **Дополнительные параметры** в поле **Интервал очистки буфера** укажите интервал в секундах, в течение которого KUMA будет ждать заполнения буфера. Если буфер не заполнен, но указанное время прошло, KUMA передает события в базу. Значение по умолчанию – 1 с.

15. На вкладке **Дополнительные параметры** в поле **Размер дискового буфера** укажите значение в байтах. Дисковый буфер используется для временного размещения тех событий, которые не удалось отправить для дальнейшей обработки или хранения. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер. Значение по умолчанию: 10 ГБ.

16. На вкладке **Дополнительные параметры** в раскрывающемся списке **Дисковый буфер** выберите значение, с помощью которого можно **Включить** или **Выключить** использование дискового буфера. По умолчанию дисковый буфер включен.

17. На вкладке **Дополнительные параметры** в раскрывающемся списке **Запись в локальную таблицу базы данных** выберите значение, с помощью которого можно **Включить** или **Выключить** запись. По умолчанию запись отключена.

    В режиме **Включить** запись будет выполняться только на том узле, на котором установлено хранилище. Мы рекомендуем использовать эту функцию только при условии, что у вас настроена балансировка на коллекторе и/или коррелляторе: в коллекторе и/или коррелляторе на шаге **6. Маршрутизация** в разделе **Дополнительные настройки** в поле **Политика выбора URL** установлено значение **По очереди**.

    В режиме **Выключить** данные распределяются по шардам кластера.

Набор ресурсов для хранилища создан и отображается в разделе **Ресурсы** → **Хранилища**. Теперь можно создать сервис хранилища.

Создание сервиса хранилища в Консоли KUMA

Когда набор ресурсов для хранилища создан, можно перейти к созданию сервиса хранилища в KUMA.

Чтобы создать сервис хранилища в Консоли KUMA:

1. В Консоли KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.
2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для хранилища и нажмите **Создать сервис**.

Сервис хранилища создан в Консоли KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы хранилища необходимо установить на каждом узле кластера ClickHouse, используя идентификатор сервиса.

Установка хранилища в сетевой инфраструктуре KUMA

Чтобы создать хранилище:

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Создайте папку /opt/kaspersky/kuma/.
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

   `sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из Консоли KUMA> --install`

   Пример: `sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --id XXXXX --install`

   При развертывании нескольких сервисов KUMA на одном устройстве в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

5. Повторите шаги 1–2 для каждого узла хранилища.

Хранилище установлено.

Создание коррелятора

Коррелятор состоит из двух частей: одна часть создается внутри Консоли KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий.

Действия в Консоли KUMA

Коррелятор создается в Консоли KUMA с помощью мастера установки. Этот мастер объединяет необходимые ресурсы в набор ресурсов для коррелятора. После завершении работы мастера на основе этого набора ресурсов автоматически создается сам сервис.

Чтобы создать коррелятор в Консоли KUMA,

запустите мастер установки коррелятора:

- В Консоли KUMA в разделе **Ресурсы** нажмите **Создать коррелятор**.
- В Консоли KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

В результате выполнения шагов мастера в Консоли KUMA создается сервис коррелятора.

В набор ресурсов для коррелятора объединяются следующие ресурсы:

- правила корреляции;
- правила обогащения (при необходимости);
- правила реагирования (при необходимости);
- точки назначения (как правило, одна: задается отправка событий в хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коррелятора KUMA

При установке коррелятора на сервер, предназначенный для обработки событий, на сервере требуется запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор, автоматически присвоенный сервису в Консоли KUMA, а также используемый для связи порт.

Проверка установки

После создания коррелятора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коррелятора

Чтобы запустить мастер установки коррелятора:

- В Консоли KUMA в разделе **Ресурсы** нажмите **Создать коррелятор**.
- В Консоли KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

Следуйте далее указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

После завершения мастера в Консоли KUMA в разделе Ресурсы → **Корреляторы** создается **набор ресурсов для коррелятора**, а в разделе Ресурсы → **Активные сервисы** добавляется **сервис коррелятора**.

Шаг 1. Общие параметры коррелятора

Это обязательный шаг мастера установки. На этом шаге указываются основные параметры коррелятора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коррелятора:

- В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.
- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать коррелятор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

  Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другой тенант, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и общего тенантов.

- В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлен сервис.
- При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса.
- В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

Основные параметры коррелятора заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Глобальные переменные

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными переменными. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменным можно присвоить какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Чтобы добавить глобальную переменную в корреляторе,

Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

- В окне **Переменная** введите название переменной.

  Требования к наименованию переменных

- Должно быть уникально в рамках коррелятора.
- Имя должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

- В окне **Значение** введите функцию переменной.

  Описание функций переменных.

Глобальная переменная добавлена. К ней можно обращаться из правил корреляции, добавляя перед названием переменной символ $. Переменных может быть несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

Перейдите к следующему шагу мастера установки.

Шаг 3. Корреляция

Это необязательный, но рекомендуемый шаг мастера установки. На вкладке мастера установки **Корреляция** следует выбрать или создать правила корреляции. Эти ресурсы определяют последовательность событий, которые указывают на инциденты, связанные с безопасностью. При обнаружении этих последовательностей коррелятор создает событие корреляции и алерт.

Если вы добавили в коррелятор глобальные переменные, все добавленные правила корреляции могут к ним обращаться.

Добавленные в набор ресурсов для коррелятора правила корреляции отображаются в таблице со следующими столбцами:

- **Правила корреляции** – название ресурса правила корреляции.
- **Тип** – тип правила корреляции: **standard**, **simple**, **operational**. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.
- **Действия** – перечень действий, которые совершит коррелятор при срабатывании правила корреляции. Действия указываются в параметрах правила корреляции. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.

  Доступные значения:

  - **В дальнейшую обработку** – корреляционные события, создаваемые этим правилом корреляции, передается в другие ресурсы коррелятора: в обогащение, в правиле реагирования, а затем в другие сервисы KUMA.
  - **Изменение активного листа** – правило корреляции вносит изменения в активные листы.
  - **В коррелятор** – корреляционное событие отправляется на повторную обработку в то же правило корреляции.
  - **Изменение категории актива** – корреляционное правило изменяет категории активов.
  - **Обогащение событий** – в корреляционном правиле настроено обогащение корреляционных событий.
  - **Не создавать алерт** – когда в результате срабатывания правила корреляции создается корреляционное событие, одновременно с ним НЕ создается алерт. Если вы не хотите создавать алерт

при срабатывании правила корреляции, но все же хотите отправить событие корреляции в хранилище, установите флажки **Выводить** и **Нет алертов**. Если вы установите только флажок **Нет алертов**, событие корреляции не сохраняется в хранилище.

- **Используются общие ресурсы** – правило корреляции или ресурсы, которые задействованы в правиле корреляции, расположены в общем тенанте.

С помощью поля **Поиск** можно искать правила корреляции. Добавленные правила корреляции можно убрать из набора ресурсов, выбрав нужные правила и нажав **Удалить**.

При выборе правила корреляции открывается окно с его параметрами: параметры можно изменить и **Сохранить**. При нажатии в этом окне на кнопку **Удалить**, правило корреляции отвязывается от набора ресурсов.

Используйте кнопки **Вверх** и **Вниз**, чтобы изменить положение выбранных правил корреляции в таблице. Это влияет на последовательность их выполнения при обработке событий. С помощью кнопки **Поднять operational-правила** можно переместить правила корреляции типа **operational** в начало списка правил корреляции.

Чтобы привязать к набору ресурсов для коррелятора существующие правила корреляции:

1. Нажмите **Привязать**.

   Откроется окно выбора ресурсов.

2. Выберите нужные правила корреляции и нажмите **OK**.

Правила корреляции привязаны к набору ресурсов для коррелятора и отображаются в таблице правил.

Чтобы создать в наборе ресурсов для коррелятора новое правило корреляции:

1. Нажмите на кнопку **Добавить**.

   Откроется окно создания правила корреляции.

2. Укажите параметры правила корреляции и нажмите **Сохранить**.

Правило корреляции создано и привязано к набору ресурсов для коррелятора. Оно отображается в таблице правил корреляции, а также в списке ресурсов в разделе **Ресурсы → Правила корреляции**.

Перейдите к следующему шагу мастера установки.

Шаг 4. Обогащение

Это необязательный шаг мастера установки. На вкладке мастера установки **Обогащение** можно выбрать или создать правила обогащения с указанием, какими данными и из каких источников следует дополнить создаваемые коррелятором корреляционные события. Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите на кнопку **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коррелятора.

Чтобы создать в наборе ресурсов новое правило обогащения:

1. Нажмите на кнопку **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено.
     - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа.

     Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива.

   - **dictionary**

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

  Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns;**

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10.

Доступные параметры:

- **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
- **Рабочие процессы** – максимальное количество запросов в один момент времени. По умолчанию указано значение `1`.
- **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Срок жизни кеша** – время жизни значений, хранящихся в кеше. По умолчанию указано значение `60`.
- **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

- cybertrace;

Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
- **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение `30`.
- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - **ip**
  - **url**
  - **hash**

  В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- часовой пояс

Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В набор ресурсов для коррелятора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 5. Действие по реагированию

Это необязательный шаг мастера установки. На вкладке мастера установки **Реагирование** можно выбрать или создать правила реагирования с указанием, какие действия требуется выполнить при срабатывании правил корреляции. Правил реагирования может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки .

Чтобы добавить в набор ресурсов существующее правило реагирования:

1. Нажмите на кнопку **Добавить**.

Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите нужный ресурс.

Правило реагирования добавлено в набор ресурсов для коррелятора.

Чтобы создать в наборе ресурсов новое правило реагирования:

1. Нажмите на кнопку **Добавить**.

Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите **Создать**.

3. В раскрывающемся списке **Тип** выберите тип правила реагирования и заполните относящиеся к нему параметры:

- **Реагирование через KSC** – правила реагирования для автоматического запуска задач на активах Kaspersky Security Center. Например, вы можете настроить автоматический запуск антивирусной проверки или обновление базы данных.

  Автоматический запуск задач выполняется при интеграции KUMA с Kaspersky Security Center. Задачи запускаются только на активах, импортированных из Kaspersky Security Center.

  Параметры реагирования

  - **Задача Kaspersky Security Center** (обязательно) – название задачи Open Single Management Platform, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, "`KUMA antivirus check`".

    Типы задач Open Single Management Platform, которые можно запустить с помощью KUMA:

    - Обновление.
    - Поиск вирусов.

  - **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Open Single Management Platform. Возможные значения:

    - SourceAssetID
    - DestinationAssetID
    - DeviceAssetID

  Для отправки запросов в Open Single Management Platform необходимо убедиться, что Open Single Management Platform доступен по протоколу UDP.

- **Запуск скрипта** – правила реагирования для автоматического запуска скрипта. Например, вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий.

  Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts.

  Пользователю `kuma` этого сервера требуются права на запуск скрипта.

  Параметры реагирования

- **Время ожидания** – количество секунд, которое выждет система, прежде чем запустить скрипт.
- **Название скрипта** (обязательно) – имя файла скрипта.

  Если ресурс реагирования прикреплен к сервису коррелятора, однако в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.
- **Аргументы скрипта** – параметры или значения полей событий, которые необходимо передать скрипту.

  > Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

  Параметры можно обрамлять кавычками (").

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

  Пример: `-n "\"usr\": {{.SourceUserName}}"`

- **Реагирование через KEDR** – правила реагирования для автоматического создания правил запрета, запуска сетевой изоляции или запуска приложения на активах Kaspersky Endpoint Detection and Response и Kaspersky Security Center.

  Автоматические действия по реагированию выполняются при интеграции KUMA с Kaspersky Endpoint Detection and Response.

  Параметры реагирования

- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID
- **Тип задачи** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - Включить сетевую изоляцию.

    При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

    - **Срок действия изоляции** – количество часов, в течение которых будет действовать сетевая изоляция актива. Вы можете указать от 1 до 9999 часов.

      При необходимости вы можете **добавить исключение для сетевой изоляции**.

      Чтобы добавить исключение для сетевой изоляции:

      a. Нажмите на кнопку **Добавить исключение**.

      b. Выберите направление сетевого трафика, которое не должно быть заблокировано:
         - Входящее.
         - Исходящее.
         - Входящее/Исходящее.

      c. В поле **IP актива** введите IP-адрес актива, сетевой трафик которого не должен быть заблокирован.

      d. Если вы выбрали **Входящее** или **Исходящее**, укажите порты подключения в полях **Удаленные порты** и **Локальные порты**.

      e. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить исключение** и повторите действия по заполнению полей **Направление трафика**, **IP актива**, **Удаленные порты** и **Локальные порты**.

      f. Если вы хотите удалить исключение, нажмите на кнопку **Удалить** под нужным вам исключением.

      При добавлении исключений в правило сетей изоляции Kaspersky Endpoint Detection and Response может некорректно отображать значения портов в информации о правиле. Это не влияет на работоспособность приложения. Подробнее о просмотре правила сетевой изоляции см. в *справке Kaspersky Anti Targeted Attack Platform*.
  - Выключить сетевую изоляцию.

- Добавить правило запрета.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Поля события для получения хеш-суммы** – поля событий, из которых KUMA извлекает SHA256- или MD5-хеши файлов, запуск которых требуется запретить.

    Выбранные поля событий, а также значения, выбранные в **Поле события**, требуется добавить в наследуемые поля правила корреляции.

  - **Хеш файла №1** – SHA256- или MD5-хеш файла, который требуется запретить.

  Хотя бы одно из указанных выше полей должно быть заполнено.

- Удалить правило запрета.

- Запустить приложение.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Путь к файлу** – путь к файлу процесса, который вы хотите запустить.
  - **Аргументы командной строки** – параметры, с которыми вы хотите запустить файл.
  - **Текущая директория** – директория, в которой на момент запуска располагается файл.

  При срабатывании правила реагирования для пользователей с ролью Главный администратор в разделе **Диспетчер задач** веб-интерфейса приложения отобразится задача **Запустить приложение**. В столбце **Создал** таблицы задач для этой задачи отображается **Задача по расписанию**. Вы можете просмотреть результат выполнения задачи.

  Все перечисленные операции выполняются на активах с Kaspersky Endpoint Agent для Windows. На активах с Kaspersky Endpoint Agent для Linux выполняется только запуск приложения.

  На программном уровне возможность создания правил запрета и сетевой изоляции для активов с Kaspersky Endpoint Agent для Linux не ограничена. KUMA и Kaspersky Endpoint Detection and Response не уведомляют о неуспешном применении этих правил.

- **Реагирование через KICS for Networks** – правила реагирования для автоматического запуска задач в на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

  Автоматический запуск задач выполняется при интеграции KUMA с KICS for Networks.

  Параметры реагирования

- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID
- **Задача KICS for Networks** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - **Изменить статус актива на Разрешенное**.
  - **Изменить статус актива на Неразрешенное**.

  При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.

- **Реагирование через Active Directory** – правила реагирования для изменения прав пользователей Active Directory. Например, блокировать пользователя.

  Запуск задач выполняется при интеграции с Active Directory.

  Параметры реагирования

  - **Источник идентификатора аккаунта** – поле события, откуда будет взято значение идентификатора учетной записи Active Directory. Возможные значения:
    - SourceAccountID
    - DestinationAccountID
  - **Команда Active Directory** – команда, которая будет применяться к учетной записи при срабатывании правила реагирования. Доступные значения:
    - Добавить учетную запись в группу
    - Удалить учетную запись из группы
    - Сбросить пароль учетной записи
    - Блокировать учетную запись

- В поле **Рабочие процессы** укажите количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

  Поле не является обязательным.

1. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр

или **Создать** новый фильтр.

Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В набор ресурсов для коррелятора добавлено новое правило реагирования.

Перейдите к следующему шагу мастера установки.

Шаг 6. Маршрутизация

Это необязательный шаг мастера установки. На вкладке мастера установки **Маршрутизация** можно выбрать или создать точки назначения, в параметрах которых будут определено, куда следует перенаправлять созданные коррелятором события. Обычно события от коррелятора перенаправляются в хранилище для хранения и для возможности просматривать их позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коррелятора существующую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

- Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
- Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
- Выберите **Другое**, если хотите отправлять события в другие места.

> К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки .

3. Нажмите на кнопку **Сохранить**.

Выбранная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Чтобы добавить в набор ресурсов коррелятора новую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры на вкладке **Основные параметры**:

   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.
   - Выберите **Тип** точки назначения:
     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.
     - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
     - Выберите **nats-jetstream**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.
   - Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

     Для всех типов, кроме **nats-jetstream** и **file**, с помощью кнопки **URL** можно указать несколько адресов отправки.
   - Для типов **nats-jetstream** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать символы в кодировке Unicode. Топик для Kafka имеет ограничение длины в 255 символов.

3. При необходимости укажите параметры на вкладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения:

   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Прокси-сервер** – раскрывающийся список для выбора прокси-сервера.
- **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. По умолчанию указано значение `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Идентификатор кластера** – идентификатор кластера NATS.
- **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  При использовании TLS невозможно указать IP-адрес в качестве URL.
- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:
  - **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.
  - **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.
  - **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Путь** – путь к файлу, если выбран тип точки назначения **file**.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. По умолчанию указано значение `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить

проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

4. Нажмите на кнопку **Сохранить**.

Созданная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 7. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в KUMA создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коррелятора отображается в разделе **Ресурсы** → **Корреляторы**. Его можно использовать для создания новых сервисов коррелятора. При изменении этого набора ресурсов все службы, работающие на основе этого набора ресурсов, начнут использовать новые параметры после перезапуска служб. Для этого вы можете использовать кнопки **Сохранить и перезапустить службы** и **Сохранить и обновить конфигурации служб**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы** → **Активные сервисы**. Службы, созданные с помощью мастера установки, выполняют функции внутри приложения KUMA. Чтобы взаимодействовать с внешними частями сетевой инфраструктуры, вам необходимо установить аналогичные внешние службы на предназначенные для них серверы и активы. Например, внешний сервис коррелятора следует установить на сервере, предназначенном для обработки событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех активах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите на кнопку **Создать и сохранить сервис**.

На вкладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и активы.

Например:

/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты.

2. Закройте мастер, нажав **Сохранить**.

Сервис коррелятора создан в KUMA. Теперь аналогичный сервис необходимо установить на сервере, предназначенном для обработки событий.

Установка коррелятора в сетевой инфраструктуре KUMA

Коррелятор состоит из двух частей: одна часть создается внутри Консоли KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий. В сетевой инфраструктуре устанавливается вторая часть коррелятора.

Чтобы установить коррелятор:

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Создайте папку /opt/kaspersky/kuma/.
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN сервера Ядра KUMA>:
<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется
порт 7210)> --id <идентификатор сервиса, скопированный из Консоли KUMA> --api.port
<порт, используемый для связи с устанавливаемым компонентом> --install
```

Пример: `sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

Команду, с помощью которой можно установить коррелятор на сервере, можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коррелятора, а также порт, который этот коррелятор использует для связи. Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

При развертывании нескольких сервисов KUMA на одном устройстве в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

Коррелятор установлен. С его помощью можно анализировать события на предмет угроз.

Проверка правильности установки коррелятора

Проверить готовность коррелятора к получению событий можно следующим образом:

1. В Консоли KUMA откройте раздел **Ресурсы** → **Активные сервисы**.
2. Убедитесь, что у установленного вами коррелятора зеленый статус.

Если в коррелятор поступают события, удовлетворяющие условиям фильтра правил корреляции, на вкладке событий будут отображаться события с параметрами `DeviceVendor=Kaspersky` и `DeviceProduct=KUMA`. Название сработавшего правила корреляции будет отображаться как название этих корреляционных событий.

Если корреляционные события не найдены

Можно создать более простую версию правила корреляции, чтобы найти возможные ошибки. Используйте **правило корреляции типа** simple и одно действие **Отправить событие на дальнейшую обработку**. Рекомендуется создать фильтр для поиска событий, которые KUMA получает регулярно.

При обновлении, добавлении или удалении правила корреляции необходимо обновить конфигурацию коррелятора.

Когда вы закончите тестирование правил корреляции, нужно удалить все тестовые и временные правила корреляции из KUMA и обновить параметры коррелятора.

Создание коллектора

Коллектор состоит из двух частей: одна часть создается внутри Консоли KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий.

Действия в Консоли KUMA

Коллектор создается в Консоли KUMA с помощью мастера установки. Этот мастер объединяет необходимые ресурсы в набор ресурсов для коллектора. После завершения работы мастера на основе этого набора ресурсов автоматически создается сама служба.

Чтобы создать коллектор в Консоли KUMA,

Запустите мастер установки коллектора:

- В Консоли KUMA в разделе **Ресурсы** нажмите на кнопку **Подключить источник**.
- В Консоли KUMA в разделе **Ресурсы** → **Коллекторы** нажмите на кнопку **Добавить коллектор**.

В результате выполнения шагов мастера в Консоли KUMA создается сервис коллектора.

В набор ресурсов для коллектора объединяются следующие ресурсы:

- коннектор;
- нормализатор (как минимум один);
- фильтры (при необходимости);
- правила агрегации (при необходимости);
- правила обогащения (при необходимости);
- точки назначения (как правило, две: задается отправка событий в коррелятор и хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коллектора KUMA

При установке коллектора на сервер, предназначенный для получения событий, требуется запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор, автоматически присвоенный сервису в Консоли KUMA, а также используемый для связи порт.

Проверка установки

После создания коллектора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коллектора

Коллектор состоит из двух частей: одна часть создается внутри Консоли KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий. В мастере установки создается первая часть коллектора.

Чтобы запустить мастер установки коллектора:

- В Консоли KUMA в разделе **Ресурсы** нажмите на кнопку **Подключить источник**.
- В Консоли KUMA в разделе **Ресурсы** → **Коллекторы** нажмите на кнопку **Добавить коллектор**.

Следуйте далее указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

После завершения мастера в Консоли KUMA в разделе Ресурсы → **Коллекторы** создается **набор ресурсов для коллектора**, а в разделе Ресурсы → **Активные сервисы** добавляется **сервис коллектора**.

Шаг 1. Подключение источников событий

Это обязательный шаг мастера установки. На этом шаге указываются основные параметры коллектора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коллектора:

1. В поле **Название коллектора** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   При создании некоторых типов коллекторов вместе с ними автоматически создаются агенты, имеющие название "agent: <Название коллектора>, auto created". Если такой агент уже создавался ранее и не был удален, то коллектор с названием <Название коллектора> невозможно будет создать. В такой ситуации необходимо или указать другое название коллектора, или удалить ранее созданный агент.

2. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать коллектор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

   Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другой тенант, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и общего тенантов.

3. В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлен сервис.

4. При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса.

   Сообщения об ошибках сервиса коллектора помещаются в журнал, даже если режим отладки выключен. Журнал можно просмотреть на машине, где установлен коллектор, в директории /opt/kaspersky/kuma/collector/<идентификатор коллектора>/log/collector.

5. В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

Основные параметры коллектора будут заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Транспорт

Это обязательный шаг мастера установки. На вкладке мастера установки **Транспорт** следует выбрать или создать коннектор, в параметрах которого будет определено, откуда сервис коллектора должен получать события.

Чтобы добавить в набор ресурсов существующий коннектор,

выберите в раскрывающемся списке **Коннектор** название нужного коннектора.

На вкладке мастера установки **Транспорт** отобразятся параметры выбранного коннектора. Выбранный коннектор можно открыть для редактирования в новой вкладке браузера с помощью кнопки .

Чтобы создать коннектор:

1. Выберите в раскрывающемся списке **Коннектор** пункт **Создать**.

2. В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:

   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - ftp
   - nfs
   - wmi
   - wec
   - snmp

   При использовании типа коннектора **tcp** или **udp** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса активов, с которых были получены события.

   При использовании типа коннектора **wmi** или **wec** будут автоматически созданы агенты для приема событий Windows.

   Рекомендуется использовать кодировку по умолчанию (то есть UTF-8) и применять другие параметры только при получении в полях событий битых символов.

   > Для настройки коллекторов KUMA на прослушивание портов с номерами меньше 1000 сервис нужного коллектора необходимо запускать с правами root. Для этого после установки коллектора в его конфигурационный файл systemd в раздел [Service] требуется дописать строку `AmbientCapabilities=CAP_NET_BIND_SERVICE`.
   > Systemd-файл располагается в директории /usr/lib/systemd/system/kuma-collector-<`идентификатор коллектора`>.service.

   Коннектор добавлен в набор ресурсов коллектора. Созданный коннектор доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

Перейдите к следующему шагу мастера установки.

Шаг 3. Парсинг событий

Это обязательный шаг мастера установки. На вкладке мастера установки **Парсинг событий** следует выбрать или создать нормализатор, в параметрах которого будут определены правила преобразования "сырых" событий в нормализованные. В нормализатор можно добавить несколько правил парсинга событий, реализуя таким образом сложную логику обработки событий. Вы можете протестировать работу нормализатора, используя тестовые события.

При создании нового нормализатора в мастере установки по умолчанию он будет сохранен в наборе ресурсов для коллектора и не сможет быть использован в других коллекторах. С помощью флажка **Сохранить нормализатор** вы можете создать нормализатор в виде отдельного ресурса, в таком случае нормализатор будет доступен для выбора в других коллекторах тенанта.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы → Нормализаторы**.

Добавление нормализатора

Чтобы добавить в набор ресурсов существующий нормализатор:

1. Нажмите на кнопку **Добавить парсинг событий**.

   Откроется окно **Основной парсинг событий** с параметрами нормализатора и активной вкладкой **Схема нормализации**.

2. В раскрывающемся списке **Нормализатор** выберите нужный нормализатор. В раскрывающемся списке доступны нормализаторы, принадлежащие тенанту коллектора и Общему тенанту.

   В окне **Основной парсинг событий** отобразятся параметры выбранного нормализатора.

   Если вы хотите отредактировать параметры нормализатора, в раскрывающемся списке **Нормализатор** нажмите на значок карандаша рядом с названием нужного нормализатора. Откроется окно **Редактирование нормализатора** с темным кружком. Если вы нажмете на темный кружок, откроется окно **Основной парсинг событий** и параметры нормализатора будут доступны для редактирования.

   Если вы хотите настроить параметры дополнительного парсинга, наведите курсор на темный кружок и нажмите на появившийся значок плюса, откроется окно **Дополнительный парсинг событий**. Подробнее о настройке дополнительного парсинга событий см. ниже.

3. Нажмите на кнопку **OK**.

На вкладке мастера установки **Основной парсинг событий** отображается нормализатор в виде темного кружка. Можно нажать на кружок, чтобы открыть параметры нормализатора для просмотра.

Чтобы создать в коллекторе новый нормализатор:

1. На шаге Парсинг событий на вкладке **Схемы парсинга** нажмите на кнопку **Добавить парсинг событий**.

   Откроется окно **Основной парсинг событий** с параметрами нормализатора и активной вкладкой **Схема нормализации**.

2. Если хотите сохранить нормализатор в качестве отдельного ресурса, установите флажок **Сохранить нормализатор** - таким образом сохраненный нормализатор будет доступен для использования в других коллекторах тенанта. По умолчанию флажок снят.

3. Введите в поле **Название** уникальное имя для нормализатора. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требующие заполнения.

   Доступные методы парсинга:

   - **json**

     Этот метод парсинга используется для обработки данных в формате JSON, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла.

     При обработке файлов с иерархически выстроенными данными можно обращаться к полям вложенных объектов, поочередно через точку указывая названия параметров. Например, к параметру `username` из строки `"user":{"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

     Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованы некорректно.

     В сложных схемах нормализации, где используются дополнительные нормализаторы, все вложенные объекты обрабатываются на первом уровне нормализации за исключением случаев, когда условия дополнительной нормализации не заданы и, следовательно, в дополнительный нормализатор передается обрабатываемое событие целиком.

     В качестве разделителя строк могут выступать символы `\n` и `\r\n`. Строки должны быть в кодировке UTF-8.

     Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** выберите в раскрывающемся списке **Использовать сырое событие** значение **Да**.

   - **cef**

     Этот метод парсинга используется для обработки данных в формате CEF.

     При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

   - **regexp**

Этот метод парсинга используется для создания собственных правил обработки данных в формате с использованием регулярных выражений.

В поле блока параметров **Нормализация** добавьте регулярное выражение (синтаксис RE2) с именованными группами захвата. Имя группы и ее значение будут интерпретироваться как поле и значение необработанного события, которое может быть преобразовано в поле события в формате KUMA.

Чтобы добавить правила обработки событий:

1. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например "(?P<name>regexp)". Регулярное выражение, добавленное в параметр **Нормализация**, должно полностью совпадать с событием. Также при разработке регулярного выражения рекомендуется использовать специальные символы, обозначающие начало и конец текста: ^, $.

   Можно добавить несколько регулярных выражений с помощью кнопки **Добавить регулярное выражение**. Если нужно удалить регулярное выражение, нажмите на кнопку .

3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Теперь вы можете выбрать соответствующее поле KUMA в столбце рядом с каждой группой захвата. Если вы назвали группы захвата в соответствии с форматом CEF, вы можете использовать автоматическое сопоставление CEF, установив флажок **Использовать синтаксис CEF для нормализации**.

Правила обработки событий добавлены.

- **syslog**

  Этот метод парсинга используется для обработки данных в формате syslog.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- **csv**

  Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

  При выборе этого метода необходимо в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя допускается использовать любой однобайтовый символ ASCII.

- **kv**

Этот метод парсинга используется для обработки данных в формате ключ-значение.

При выборе этого метода необходимо указать значения в следующих обязательных полях:

- **Разделитель пар** – укажите символ, которые будет служит разделителем пар ключ-значение. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем значений.

- **Разделитель значений** – укажите символ, который будет служить разделителем между ключом и значением. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем пар ключ-значение.

- xml

Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** выберите в раскрывающемся списке **Использовать сырое событие** значение **Да**.

При выборе этого метода в блоке параметров **Атрибуты XML** можно указать ключевые атрибуты, которые следует извлекать из тегов. Если в структуре XML в одном теге есть атрибуты с разными значениями, можно определить нужное значение, указав ключ к нему в столбце **Исходные данные** таблицы **Сопоставление**.

Чтобы добавить ключевые атрибуты XML,

Нажмите на кнопку **Добавить поле** и в появившемся окне укажите путь к нужному атрибуту.

Можно добавить несколько атрибутов. Атрибуты можно удалить по одному с помощью значка с крестиком или все сразу с помощью кнопки **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

Нумерация тегов

Начиная с версии KUMA 2.1.3 доступна **Нумерация тегов**. Опция предназначена для выполнения автоматической нумерации тегов в событиях в формате XML, чтобы можно было распарсить событие с одинаковыми тегами или неименованными тегами, такими как <Data>.

В качестве примера мы используем функцию **Нумерация тегов** для нумерации тегов атрибута EventData [события Microsoft Windows PowerShell event ID 800](#).

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    <System>
        <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-8497-1e730c959516}" EventSourceName="NTDS" />
        <EventID Qualifiers="0000">0000</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>15</Task>
        <Opcode>0</Opcode>
        <Keywords>0x8080000000000000</Keywords>
        <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
        <EventRecordID>55647</EventRecordID>
        <Correlation />
        <Execution ProcessID="1" ThreadID="1" />
        <Channel>service</Channel>
        <Computer>computer</Computer>
        <Security UserID="0000" />
    </System>
    <EventData>
        <Data>583</Data>
        <Data>36</Data>
        <Data>192.168.0.1:5084</Data>
        <Data>level</Data>
        <Data>name,lDAPDisplayName</Data>
        <Data />
        <Data>5545</Data>
        <Data>3</Data>
        <Data>0</Data>
        <Data>0</Data>
        <Data>0</Data>
        <Data>15</Data>
        <Data>none</Data>
    </EventData>
</Event>
```

Чтобы выполнить парсинг таких событий необходимо:

- Настроить нумерацию тегов.

- Настроить мапинг данных для пронумерованных тегов с полями события KUMA.

KUMA 3.0.x поддерживает одновременное использование параметров **XML-атрибутов** и **Нумерация тегов** в одном дополнительном нормализаторе. Если атрибут содержит неименованные теги или одинаковые теги, рекомендуется использовать функцию **Нумерация тегов**. Если атрибут содержит только именованные теги, используйте **Атрибуты XML**. Чтобы использовать эту функциональность в дополнительных нормализаторах, вам нужно последовательно включить параметр "Сохранить исходное событие" в каждом дополнительном нормализаторе на пути, по которому событие следует к целевому дополнительному нормализатору, и в самом целевом дополнительном нормализаторе.

В качестве примера использования этой функции вы можете обратиться к нормализатору MicrosoftProducts, параметр "Сохранить исходное событие" включен последовательно в дополнительных нормализаторах "AD FS" и "424".

Чтобы настроить парсинг событий с тегами, содержащими одинаковое название или теги без названия:

1. Создайте новый нормализатор или откройте существующий нормализатор для редактирования.

2. В окне нормализатора **Основной парсинг событий** в раскрывающемся списке **Метод парсинга** выберите значение xml и в поле **Нумерация тегов** нажмите **Добавить поле**.

   В появившемся поле укажите полный путь к тегу, элементам которого следует присвоить порядковый номер. Например, Event.EventData.Data. Первый номер, который будет присвоен тегу – 0. Если тег пустой, например, <Data />, ему также будет присвоен порядковый номер.

3. Чтобы настроить мапинг данных, в группе параметров **Сопоставление** нажмите **Добавить строку** и выполните следующие действия:

   a. В появившейся строке в поле **Исходные данные** укажите полный путь к тегу и его индекс. Для события Microsoft Windows из примера выше полный путь с индексами будет выглядеть следующим образом:

      - Event.EventData.Data.0
      - Event.EventData.Data.1
      - Event.EventData.Data.2 и так далее

   b. В раскрывающемся списке **Поле KUMA** выберите поле в событии KUMA, в которое попадет значение из пронумерованного тега после выполнения парсинга.

4. Чтобы сохранить изменения:

   - Если вы создали новый нормализатор, нажмите **Сохранить**.
   - Если вы редактировали существующий нормализатор, нажмите **Обновить параметры** в коллекторе, к которому привязан нормализатор.

Настройка парсинга завершена.

- netflow5

Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип netflow5 выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для типа **netflow5** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow9**

  Этот метод парсинга используется для обработки данных в формате NetFlow v9.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип netflow9 выбран для основного парсинга, дополнительная нормализация недоступна.

  В правилах сопоставления по умолчанию для типа **netflow9** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sflow5**

  Этот метод парсинга используется для обработки данных в формате sflow5.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип sflow5 выбран для основного парсинга, дополнительная нормализация недоступна.

- **ipfix**

  Этот метод парсинга используется для обработки данных в формате IPFIX.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип ipfix выбран для основного парсинга, дополнительная нормализация недоступна.

  В правилах сопоставления по умолчанию для типа **ipfix** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sql** – этот метод становится доступным, только при использовании коннектора типа sql

  Нормализатор использует этот метод для обработки данных, полученных с помощью выборки из базы данных.

5. В раскрывающемся списке **Сохранить исходное событие** укажите, надо ли сохранять исходное "сырое" событие во вновь созданном нормализованном событии. Доступные значения:

   - **Не сохранять** – не сохранять исходное событие. Это значение используется по умолчанию.
   - **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке службы. В этом случае каждый раз, когда у события есть непустое поле `Raw`, это означает, что возникла проблема.

     Если поля с названиями `*Address` или `*Date*` не соответствуют правилам нормализации, такие поля игнорируются. При этом не возникает ошибка нормализации и значения полей не попадают в поле `Raw` нормализованного события, даже если был указан параметр **Сохранить исходное событие → При возникновении ошибок**.

   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

6. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля исходного события в нормализованном событии, если для них не были настроены правила сопоставления (см. ниже). Данные сохраняются в поле события `Extra`. Нормализованные события можно искать и фильтровать по данным, хранящимся в поле `Extra`.

   Фильтрация по данным из поля события Extra

   Условия для фильтров по данным из поля события **Extra**:

   - Условие – **Если**.
   - Левый операнд – **поле события**.
   - В поле события вы можете указать одно из следующих значений:
     - Поле **Extra**.
     - Значение из поля Extra в следующем формате:

       `Extra.<название поля>`

       Например, `Extra.app`.

       Значение этого типа указывается вручную.
     - Значение из массива, записанного в поле **Extra**, в следующем формате:

       `Extra.<название поля>.<элемент массива>`

       Например, `Extra.array.0`.

       Нумерация значений в массиве начинается с 0.

       Значение этого типа указывается вручную.

       Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
   - Оператор – =.
   - Правый операнд – **константа**.
   - Значение – значение, по которому требуется фильтровать события.

По умолчанию поля не сохраняются.

7. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

8. В таблице **Сопоставление** настройте сопоставление полей сырого события с полями событий в формате KUMA:

   a. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите преобразовать в поле события KUMA.

   Подробнее о формате полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

   Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку , откроется окно **Преобразование**, в котором при нажатии на кнопку **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

   Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

b. В столбце **Поле KUMA** в раскрывающемся списке выберите требуемое поле события KUMA. Поля можно искать, вводя в поле их названия.

Рекомендации для полей столбцов KUMA

Рекомендуется настроить сопоставление для следующих полей KUMA. Иначе вы не сможете просматривать наблюдаемые объекты в деталях алертов и инцидентов.

Рекомендуемые поля KUMA зависят от типов наблюдаемых объектов:

- Для наблюдаемых объектов типа MD5 и SHA256:
  - FileHash
- Для наблюдаемых объектов типа URL:
  - RequestUrl
- Для наблюдаемых объектов типа IP-адреса:
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress
  - SourceTranslatedAddress
  - SourceAddress
- Для наблюдаемых объектов типа Доменное имя:
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain
  - SourceDnsDomain
  - SourceNtDomain
- Для наблюдаемых объектов типа UserName:
  - DestinationUserName
  - SourceUserName

- Для наблюдаемых объектов типа HostName:
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. Если название поля события KUMA, выбранного на предыдущем шаге, начинается с `DeviceCustom*` и `Flex*`, в поле **Подпись** можно добавить уникальную пользовательскую метку.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

Чтобы KUMA могла выполнить обогащение событий данными про активы, и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам необходимо настроить сопоставление полей для адреса устройства и имени устройства в зависимости от назначения актива. Например, сопоставление для SourceAddress и SourceHostName, или DestinationAddress и DestinationHostName. В результате обогащения в карточке события появится поле SourceAssetID или DestinationAssetID и ссылка, по которой можно будет перейти в карточку актива. Также в результате обогащения сведения об активе будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события KUMA.

Если размер поля события KUMA оказывается меньше длины помещаемого в него значения, значение обрезается до размера поля события.

9. Нажмите на кнопку **OK**.

На вкладке мастера установки **Парсинг событий** отображается нормализатор в виде темного кружка. Если вы хотите открыть параметры нормализатора для просмотра, нажмите на темный кружок. При наведении курсора мыши на кружок отображается знак плюса. Нажмите на него, чтобы добавить правила парсинга событий (см. ниже).

Обогащение нормализованного события дополнительными данными

В только что созданные нормализованные события можно добавлять дополнительные данные, создавая в нормализаторе правила обогащения. Эти правила хранятся в нормализаторе, в котором они были созданы. Правил обогащения может быть несколько.

Чтобы добавить правила обогащения в нормализатор:

1. Выберите основное или дополнительное правило нормализации, а затем в открывшемся окне перейдите на вкладку **Обогащение**.

2. Нажмите на кнопку **Добавить обогащение**.

   Появится блок параметров правила обогащения. Блок параметров можно удалить, нажав на кнопку ✕.

3. В раскрывающемся списке **Тип источника** выберите тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

   Доступные типы источников обогащения:

   - **константа**

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

- В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива.

- dictionary

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- table

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

- В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
- В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра Тип источника данных выбран тип "Событие", а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом "Массив строк", а целевым полем является поле с типом "Строка", значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем "Массив строк" и целевое поле полем "Массив строк", значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

   Этот параметр недоступен для типа источника обогащения **таблица**.

5. Если вы хотите включить детализацию в журнале нормализатора, переведите переключатель **Отладка** в активное положение. По умолчанию детализация отключена.

6. Нажмите на кнопку **OK**.

В нормализатор, в выбранное правило парсинга, добавлены правила обогащения событий дополнительными данными.

Настройка парсинга с привязкой к IP-адресам

Вы можете направить события с нескольких IP-адресов, от источников разных типов в один коллектор, и коллектор применит соответствующие заданные нормализаторы.

Такой способ доступен для коллекторов с коннектором типа UDP, TCP, HTTP. Если в коллекторе на шаге **Транспорт** указан коннектор UDP, TCP, HTTP, на шаге **Парсинг событий** на вкладке **Настройки парсинга** вы можете задать несколько IP-адресов и указать, какой нормализатор следует использовать для событий, поступающих с заданных адресов. Доступны следующие типы нормализаторов: json, cef, regexp, syslog, csv, kv, xml.

Если в коллекторе с настроенными нормализаторами с привязкой к IP-адресам вы измените тип коннектора на какой-либо, кроме UDP, TCP, HTTP, вкладка **Настройки парсинга** исчезнет и на шаге **Парсинг** будет указан только первый нормализатор из указанных прежде. Вкладка исчезает в веб-интерфейсе сразу, изменения будут применены после сохранения ресурса. Если вы хотите вернуться к прежним параметрам, выйдите из мастера установки коллектора без сохранения.

Для нормализаторов типа Syslog и regexp допускается использование цепочки нормализаторов: вы можете задать дополнительные условия нормализации в зависимости от значения поля DeviceProcessName. Отличие от дополнительной нормализации: вы можете указывать общедоступные нормализаторы.

Чтобы настроить парсинг с привязкой к IP-адресам:

1. На шаге **Парсинг событий** перейдите на вкладку **Настройки парсинга**.

2. В поле **IP-адрес(-а)** укажите один или несколько IP-адресов, с которых будут поступать события. Вы можете указать несколько IP-адресов через запятую. Доступный формат: IPv4. Длина списка адресов не ограничена, при этом мы рекомендуем указывать разумное количество адресов для соблюдения баланса нагрузки на коллектор. Поле обязательно для заполнения, если вы хотите применять несколько нормализаторов в одном коллекторе.

   Ограничение: IP-адрес должен быть уникальным для каждой комбинации IP + нормализатор. KUMA выполняет проверку уникальности адресов, если вы укажете один и тот IP-адрес для разных нормализаторов, появится сообщение "Поле должно быть уникальным".

   Если вы планируете отправлять все события в один нормализатор без указания IP-адресов, мы рекомендуем создать отдельный коллектор. Также мы рекомендуем создать отдельный коллектор с одним нормализатором, если вы хотите применить один нормализатор к событиям с большого количества IP-адресов - в таком варианте производительность будет выше.

3. В поле **Нормализатор** создайте или выберите в раскрывающемся списке существующий нормализатор. Стрелка рядом с раскрывающимся списком позволяет выполнить переход на вкладку **Схемы парсинга**.

   Нормализация будет срабатывать если у вас настроен тип коннектора: UDP, TCP, HTTP, при этом для HTTP должен быть указан header источника событий.

   С учетом доступных коннекторов, следующие типы нормализатора доступны для автоматического распознавания источников: json, cef, regexp, syslog, csv, kv, xml.

4. Если вы выбрали тип нормализатора Syslog или regexp, вы можете **Добавить условную нормализацию**. Условная нормализация будет доступна, если в основном нормализаторе настроено **Сопоставление полей** для DeviceProcessName. В группе параметров **Условие** укажите имя процесса в поле DeviceProcessName и создайте или выберите из раскрывающегося списка существующий нормализатор. Вы можете указать несколько комбинаций DeviceProcessName + нормализатор, нормализация будет выполняться до первого совпадения.

Настройка парсинга с привязкой к IP-адресам выполнена.

Создание структуры правил нормализации событий

Для реализации сложной логики обработки событий в нормализатор можно добавить более одного правила парсинга событий. События передаются между правилами парсинга в зависимости от заданных условий. Последовательность создания правил парсинга важна. Событие обрабатывается последовательно, путь к нему отображается стрелками.

Чтобы создать дополнительное правило парсинга:

1. Создайте нормализатор (см. выше).

   Созданный нормализатор отобразится в окне в виде темного кружка.

2. Наведите указатель мыши на кружок и нажмите на появившуюся кнопку со значком плюса.

3. В открывшемся окне **Дополнительный парсинг события** задайте параметры дополнительного правила парсинга события:

   - Вкладка **Условия дополнительной нормализации**:

     Если вы хотите передавать сырое событие для дополнительной нормализации, в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**. По умолчанию указано значение **Нет**. Рекомендуется передавать сырое событие в нормализаторы типа json и xml. Если вы хотите передавать сырое событие для дополнительной нормализации на второй, третий и далее уровень вложенности, последовательно на каждом уровне вложенности в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**.

     Если вы хотите отправлять в дополнительный нормализатор только события с определенным полем, укажите его в поле **Поле, которое следует передать в нормализатор**.

     На этой вкладке вы также можете определить другие условия. При выполнении этих условий событие отправляется на дополнительный анализ.

   - Вкладка **Схема нормализации**:

     На этой вкладке можно настроить правила обработки событий, по аналогии с параметрами основного нормализатора (см. выше). Параметр **Сохранить исходное событие** недоступен. В поле **Примеры событий** отображаются значения, указанные при создании начального нормализатора.

   - Вкладка **Обогащение**:

     На этой вкладке можно настроить правила обогащения событий (см. выше).

4. Нажмите на кнопку **OK**.

Дополнительное правило парсинга добавлено в нормализатор и отображается в виде темного блока, на котором указаны условия, при котором это правило будет задействовано. Параметры дополнительного правила парсинга можно изменить, нажав на него. Если навести курсор мыши на правило дополнительного парсинга, отобразится кнопка с плюсом. Вы можете нажать на эту кнопку, чтобы создать дополнительное правило парсинга. С помощью кнопки со значком корзины нормализатор можно удалить.

В верхнем правом углу окна располагается окно поиска, где можно искать правила парсинга по названию.

Перейдите к следующему шагу мастера установки.

Шаг 4. Фильтрация событий

Это необязательный шаг мастера установки. На вкладке мастера установки **Фильтрация событий** можно выбрать или создать фильтр, в параметрах которого будут определены условия отбора событий. В коллектор можно добавить несколько фильтров. Фильтры можно менять местами, перетягивая их мышью за значок ⣿, и удалять. Фильтры объединены оператором И.

Чтобы добавить в набор ресурсов коллектора существующий фильтр,

Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите требуемый фильтр.

Чтобы добавить в набор ресурсов коллектора новый фильтр:

1. Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В разделе **Условия** задайте условия, которым должны соответствовать отсеиваемые события:

   - С помощью кнопки **Добавить условие** вы можете добавить условия фильтра. Вы можете выбрать два значения (два операнда, левый и правый) и назначить операцию, которую хотите выполнить с выбранными значениями. Результат операции – Истина (True) или Ложь (False).

     - В раскрывающемся списке **оператор** необходимо выбрать функцию, которую должен выполнять фильтр.

       В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

       Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

- В раскрывающихся списках **Левый операнд** и **Правый операнд** необходимо выбрать, откуда поступят данные, с которыми произведет действие фильтр. Отобразятся дополнительные параметры. Используйте их, чтобы определить точное значение, которое будет передано фильтру. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

- С помощью раскрывающегося списка **Если** можно выбрать, требуется ли создать отрицательное условие фильтра.

Условия можно удалить, нажав на кнопку ×.

- С помощью кнопки **Добавить группу** добавляются группы условий. Оператор **И** можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

  Группу условий можно удалить, нажав на кнопку ×.

- С помощью кнопки **Добавить фильтр** в условия добавляются существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**. В параметры вложенного фильтра можно перейти с помощью кнопки ↗.

  Вложенный фильтр можно удалить, нажав на кнопку ×.

Фильтр добавлен.

Перейдите к следующему шагу мастера установки.

Шаг 5. Агрегация событий

Это необязательный шаг мастера установки. На вкладке мастера установки **Агрегация событий** можно выбрать или создать правила агрегации, в параметрах которого будут определены условия для объединения однотипных событий. В коллектор можно добавить несколько правил агрегации.

Чтобы добавить в набор ресурсов коллектора существующее правило агрегации,

Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся списке выберите **Правило агрегации**.

Чтобы добавить в набор ресурсов коллектора новое правило агрегации:

1. Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся меню **Правило агрегации** выберите пункт **Создать**.

2. В поле **Название** введите название для создаваемого правила агрегации. Название должно содержать от 1 до 128 символов в кодировке Unicode.

3. В поле **Предел событий** укажите количество событий, которое должно быть получено, чтобы сработало правило агрегации и события были объединены. По умолчанию указано значение `100`.

4. В поле **Время ожидания событий** укажите количество секунд, в течение которых коллектор получает события для объединения. По истечении этого срока правило агрегации срабатывает и создается новое агрегационное событие. По умолчанию указано значение `60`.

5. В разделе **Группирующие поля** нажмите на кнопку **Добавить поле** и выберите поля, по которым будут определяться однотипные события. Выбранные события можно удалить с помощью кнопок со значком крестика.

6. В разделе **Уникальные поля** с помощью кнопки **Добавить поле** можно выбрать поля, при наличии которых коллектор исключит событие из процесса агрегации даже при наличии полей, указанных в разделе **Группирующие поля**. Выбранные события можно удалять, нажав на кнопки со значком крестика.

7. В разделе **Поля суммы** нажмите на кнопку **Добавить поле** и выберите поля, значения которых будут просуммированы в процессе агрегации. Выбранные события можно удалять, нажав на кнопки со значком крестика.

8. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правило агрегации добавлено. Его можно удалить, нажав на кнопку ×.

Перейдите к следующему шагу мастера установки.

Шаг 6. обогащение события;

Это необязательный шаг мастера установки. На вкладке мастера установки **Обогащение событий** можно указать, какими данными и из каких источников следует дополнить обрабатываемые коллектором события. События можно обогащать данными, полученными с помощью правил обогащения или с помощью LDAP.

Обогащение с помощью правил обогащения

Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить обогащение** или удалить с помощью кнопки ×. Можно использовать существующие правила обогащения или же создать правила непосредственно в мастере установки.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите **Добавить обогащение**.

Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коллектора.

Чтобы создать в наборе ресурсов новое правило обогащения:

1. Нажмите **Добавить обогащение**.

Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

- **константа**

  Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

  - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено.
  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа.

  Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива.

- **dictionary**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

  Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

  Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

  Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

  Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

  Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

  Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns;**

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10.

Доступные параметры:

- **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
- **Рабочие процессы** – максимальное количество запросов в один момент времени. По умолчанию указано значение `1`.
- **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Срок жизни кеша** – время жизни значений, хранящихся в кеше. По умолчанию указано значение `60`.
- **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

- cybertrace;

Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
- **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение `30`.
- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - **ip**
  - **url**
  - **hash**

  В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- часовой пояс

Этот тип обогащения используется в коллекторах и коррелляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

> Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

> При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:
>
> | Формат времени в обрабатываемом событии | Пример |
> |---|---|
> | +-чч:мм | -07:00 |
> | +-ччмм | -0700 |
> | +-чч | -07 |
>
> Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

- **геоданные.**

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

   С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. Можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события, нажав эту кнопку.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ✕.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.
   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В набор ресурсов для коллектора добавлено новое правило обогащения.

Обогащение с помощью LDAP

Чтобы включить обогащение с помощью LDAP:

1. Нажмите **Добавить сопоставление с учетными записями LDAP**.

Откроется блок параметров обогащения с помощью LDAP.

2. В блоке параметров **Сопоставление с учетными записями LDAP** с помощью кнопки **Добавить домен** укажите домен учетных записей. Доменов можно указать несколько.

3. В таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP:

- В столбце **Поле KUMA** укажите поле события KUMA, данные из которого следует сравнить с атрибутом LDAP.
- В столбце **LDAP-атрибут**, укажите атрибут, с которым необходимо сравнить поле события KUMA. Раскрывающийся список содержит стандартные атрибуты и может быть дополнен **пользовательскими атрибутами**.

Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

   Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартный атрибут `accountExpires` в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

Из Active Directory можно запросить следующие атрибуты учетных записей:

- accountExpires
- badPasswordTime
- cn
- co
- company
- department
- description
- displayName
- distinguishedName
- division
- employeeID
- givenName
- l
- lastLogon
- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf (по этому атрибуту события можно искать при корреляции)
- mobile
- name
- objectCategory
- objectGUID (этот атрибут запрашивается из Active Directory всегда)
- objectSID
- physicalDeliveryOfficeName

- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

После того, как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если вы добавили один и тот же атрибут для нескольких доменов, атрибут отображается в раскрывающемся списке только один раз. Вы можете просмотреть домены, наведя курсор на вопросительный знак. Названия доменов отображаются в виде ссылок. Если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

   После перезапуска коллектора KUMA начнет обогащать события учетными записями.

- В столбце **Поле для записи данных** укажите, в какое поле события KUMA следует поместить идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление было успешно.

С помощью кнопки **Добавить строку** в таблицу можно добавить строку, а с помощью кнопки ✕ – удалить. С помощью кнопки **Применить сопоставление по умолчанию** можно заполнить таблицу сопоставления стандартными значениями.

В блок ресурсов для коллектора добавлены правила обогащения события данными, полученными из LDAP.

При добавлении в существующий коллектор обогащения с помощью LDAP или изменении параметров обогащения требуется остановить и запустить сервис снова.

Перейдите к следующему шагу мастера установки.

Шаг 7. Маршрутизация

Это необязательный шаг мастера установки. На вкладке мастера установки **Маршрутизация** можно выбрать или создать точки назначения, в параметрах которых будут определено, куда следует перенаправлять обработанные коллектором события. Обычно события от коллектора перенаправляются в две точки: в коррелятор для анализа и поиска угроз; в хранилище для хранения, а также чтобы обработанные события можно было просматривать позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коллектора существующую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Параметры точки назначения можно открыть для редактирования в новой вкладке браузера с помощью кнопки .

3. Нажмите на кнопку **Сохранить**.

Выбранная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Чтобы добавить в набор ресурсов коллектора новую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры на вкладке **Основные параметры**:

   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.
   - Выберите **Тип** точки назначения:
     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.
     - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
     - Выберите **nats-jetstream**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.
   - Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

     Для всех типов, кроме **nats-jetstream**, **file** и **diode** с помощью кнопки **URL** можно указать несколько адресов отправки.
   - Для типов **nats-jetstream** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать символы в кодировке Unicode. Топик для Kafka имеет ограничение длины в 255 символов.

3. При необходимости укажите параметры на вкладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения:

   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.
   - **Прокси-сервер** – раскрывающийся список для выбора прокси-сервера.
   - **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
   - **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. По умолчанию указано значение `30`.
   - **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
   - **Идентификатор кластера** – идентификатор кластера NATS.
   - **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:
     - **Выключено** (по умолчанию) – не использовать шифрование TLS.
     - **Включено** – использовать шифрование, но без верификации.

- **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь к файлу, если выбран тип точки назначения **file**.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. По умолчанию указано значение `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

  Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**.

  Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

4. Нажмите на кнопку **Сохранить**.

Созданная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 8. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в KUMA создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коллектора отображается в разделе **Ресурсы → Коллекторы**. Его можно использовать для создания новых сервисов коллектора. При изменении этого набора ресурсов все службы, работающие на основе этого набора ресурсов, начнут использовать новые параметры после перезапуска служб. Для этого вы можете использовать кнопки **Сохранить и перезапустить службы** и **Сохранить и обновить конфигурации служб**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы → Активные сервисы**. Службы, созданные с помощью мастера установки, выполняют функции внутри приложения KUMA. Чтобы взаимодействовать с внешними частями сетевой инфраструктуры, вам необходимо установить аналогичные внешние службы на предназначенные для них серверы и активы. Например, внешний сервис коллектора следует установить на сервере, предназначенном для получения событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех активах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите на кнопку **Создать и сохранить сервис**.

На вкладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и активы.

Например:

/opt/kaspersky/kuma/kuma collector --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты.

2. Закройте мастер, нажав **Сохранить коллектор**.

Сервис коллектора создан в KUMA. Теперь аналогичный сервис необходимо установить на сервере, предназначенном для получения событий.

Если в коллекторы был выбран коннектор типа wmi или wec, потребуется также установить автоматически созданные агенты KUMA.

Установка коллектора в сетевой инфраструктуре KUMA

Коллектор состоит из двух частей: одна часть создается внутри Консоли KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий. В сетевой инфраструктуре устанавливается вторая часть коллектора.

Чтобы установить коллектор:

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Создайте папку /opt/kaspersky/kuma/.
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

   Убедитесь, что файл kuma имеет достаточные права для запуска. Если файл не является исполняемым, измените права для запуска с помощью следующей команды:

   ```
   sudo chmod +x /opt/kaspersky/kuma/kuma
   ```
4. Поместите в директорию /opt/kaspersky/kuma/ файл LICENSE из /kuma-ansible-installer/roles/kuma/files/ и примите лицензию, выполнив следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma license
   ```
5. Создайте пользователя kuma:

   ```
   sudo useradd --system kuma && usermod -s /usr/bin/false kuma
   ```
6. Выдайте пользователю kuma права на директорию /opt/kaspersky/kuma и все файлы внутри директории:

   ```
   sudo chown -R kuma:kuma /opt/kaspersky/kuma/
   ```

7. Выполните следующую команду:

   `sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из Консоли KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом>`

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://test.kuma.com:7210 --id XXXX --api.port YYYY`

   Если в результате выполнения команды были выявлены ошибки, проверьте корректность параметров. Например, наличие требуемого уровня доступа, сетевой доступности между сервисом коллектора и ядром, уникальность выбранного API-порта. После устранения ошибок продолжите установку коллектора.

   Если ошибки не выявлены, а статус коллектора в Консоли KUMA изменился на *зеленый*, остановите выполнение команды и перейдите к следующему шагу.

   > Команду можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коллектора, а также порт, который этот коллектор использует для связи.

   > При развертывании нескольких сервисов KUMA на одном устройстве в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

   > Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

8. Выполните команду повторно, добавив ключ `--install`:

   `sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из Консоли KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install`

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

9. Добавьте порт коллектора KUMA в исключения брандмауэра.

   > Для правильной работы приложения убедитесь, что компоненты KUMA могут взаимодействовать с другими компонентами и приложениями по сети через протоколы и порты, указанные во время установки компонентов KUMA.

Коллектор установлен. С его помощью можно получать и передавать на обработку данные из источника события.

Проверка правильности установки коллектора

Проверить готовность коллектора к получению событий можно следующим образом:

1. В Консоли KUMA откройте раздел **Ресурсы** → **Активные сервисы**.

2. Убедитесь, что у установленного вами коллектора зеленый статус.

Если статус коллектора отличается от зеленого, просмотрите журнал этого сервиса на машине, где он установлен, в директории /opt/kaspersky/kuma/collector/<идентификатор корректора>/log/collector. Ошибки записываются в журнал вне зависимости от того, включен или выключен режим отладки.

Если коллектор установлен правильно и вы уверены, что из источника событий приходят данные, то при поиске связанных с ним событий в таблице должны отображаться события.

*Чтобы проверить наличие ошибок нормализации с помощью раздела **События** Консоли KUMA:*

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в KUMA.
3. Убедитесь, что в разделе **Ресурсы** Консоли KUMA в раскрывающемся списке **Хранить исходное событие** ресурса **Нормализатор** выбрано значение **При возникновении ошибок**.
4. В разделе **События** в KUMA выполните поиск событий со следующими параметрами:

   - `ServiceID = <идентификатор коллектора, который требуется проверить>`
   - `Raw != ""`

   Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Grafana™:

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в KUMA.
3. Откройте раздел Метрики и перейдите по ссылке KUMA Collectors.
4. Проверьте, отображаются ли ошибки в разделе Errors (Ошибки) веб-виджета Normalization (Нормализация).

   Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

В коллекторах типа WEC и WMI необходимо убедиться, что для подключения к агенту используется уникальный порт. Этот порт указывается **в разделе** Транспорт мастера установки коллектора.

Обеспечение бесперебойной работы коллекторов

Бесперебойное поступление событий от источника событий в KUMA является важным условием защиты сетевой инфраструктуры. Бесперебойность можно обеспечить автоматическим перенаправлением потока событий на большее число коллекторов:

- На стороне KUMA необходимо установить два или больше одинаковых коллекторов.
- На стороне источника событий необходимо настроить управление потоками событий между коллекторами с помощью сторонних средств управления нагрузкой серверов, например rsyslog или nginx.

При такой конфигурации коллекторов поступающие события не будут теряться, когда сервер коллектора по какой-либо причине недоступен.

Необходимо учитывать, что при переключении потока событий между коллекторами агрегация событий будет происходить на каждом коллекторе отдельно.

Если коллектор KUMA не удается запустить, а в его журнале выявлена ошибка "panic: runtime error: slice bounds out of range [8:0]":

1. Остановите коллектор.

   `sudo systemctl stop kuma-collector-<идентификатор коллектора>`

2. Удалите файлы с кешем DNS-обогащения.

   `sudo rm -rf /opt/kaspersky/kuma/collector/<идентификатор коллектора>/cache/enrichment/DNS-*`

3. Удалите файлы с кешем событий (дисковый буфер). Выполняйте команду, только если можно пожертвовать событиями, находящимися в дисковых буферах коллектора.

   `sudo rm -rf /opt/kaspersky/kuma/collector/<идентификатор коллектора>/buffers/*`

4. Запустите сервис коллектора.

   `sudo systemctl start kuma-collector-<идентификатор коллектора>`

Управление потоком событий с помощью rsyslog

Чтобы включить управление потоками событий на сервере источника событий с помощью rsyslog:

1. Создайте два или более одинаковых коллекторов, с помощью которых вы хотите обеспечить бесперебойный прием событий.

2. Установите на сервере источника событий rsyslog (см. документацию rsyslog).

3. Добавьте в конфигурационный файл /etc/rsyslog.conf правила перенаправления потока событий между коллекторами:

   ```
   *.* @@<FQDN основного сервера коллектора>:<порт, на который коллектор принимает события>
   $ActionExecOnlyWhenPreviousIsSuspended on
   & @@<FQDN резервного сервера коллектора>:<порт, на который коллектор принимает события>
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

   Пример конфигурационного файла

   Пример конфигурационного файла, где указан один основной коллектор и два резервных. Коллекторы настроены на принятие событий на порт TCP 5140.

   ```
   *.* @@kuma-collector-01.example.com:5140
   $ActionExecOnlyWhenPreviousIsSuspended on
   & @@kuma-collector-02.example.com:5140
   & @@kuma-collector-03.example.com:5140
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

4. Перезапустите rsyslog, выполнив команду:

   `systemctl restart rsyslog`.

Управление потоками событий на сервере источника событий включено.

Управление потоком событий с помощью nginx

Для управления потоком событий средствами nginx необходимо создать и настроить ngnix-сервер, который будет принимать события от источника событий, а затем перенаправлять их на коллекторы.

Чтобы включить управление потоками событий на сервере источника событий с помощью nginx:

1. Создайте два или более одинаковых коллекторов, с помощью которых вы хотите обеспечить бесперебойный прием событий.

2. Установите nginx на сервере, предназначенном для управления потоком событий.

   - Команда для установки в Oracle Linux 8.6:

     ```
     $sudo dnf install nginx
     ```

   - Команда для установки в Ubuntu 20.4:

     ```
     $sudo apt-get install nginx
     ```

     При установке из sources, необходимо собрать с параметром `-with-stream`:
     `$sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`

3. На nginx-сервере в конфигурационный файл nginx.conf добавьте модуль stream с правилами перенаправления потока событий между коллекторами.

   Пример модуля stream

Пример модуля, в котором поток событий распределяется между коллекторами kuma-collector-01.example.com и kuma-collector-02.example.com, которые принимают события по протоколу TCP на порт 5140 и по протоколу UDP на порт 5141. Для балансировки используется ngnix-сервер nginx.example.com.

```
stream {
upstream syslog_tcp {
server kuma-collector-1.example.com:5140;
server kuma-collector-2.example.com:5140;
}
upstream syslog_udp {
server kuma-collector-1.example.com:5141;
server kuma-collector-2.example.com:5141;
}
server {
listen nginx.example.com:5140;
proxy_pass syslog_tcp;
}
server {
listen nginx.example.com:5141 udp;
proxy_pass syslog_udp;
proxy_responses 0;
}
}
worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile – ограничение на максимальное число открытых файлов (RLIMIT_NOFILE) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса.
# worker_connections – максимальное число соединений, которые одновременно может открыть рабочий процесс.
```

4. Перезапустите nginx, выполнив команду:

   ```
   systemctl restart nginx
   ```

5. На сервере источника событий перенаправьте события на ngnix-сервер.

Управление потоками событий на сервере источника событий включено.

Для тонкой настройки балансировки может потребоваться nginx Plus, однако некоторые методы балансировки, например Round Robin и Least Connections, доступны в базовой версии ngnix.

Подробнее о настройке nginx см. в документации nginx.

Предустановленные коллекторы

В поставку OSMP включены перечисленные в таблице ниже предустановленные коллекторы.

Предустановленные коллекторы

Name	Описание
[OOTB] CEF	Собирает события в формате CEF, поступающие по протоколу TCP.
[OOTB] KSC	Собирает события от Kaspersky Security Center по протоколу Syslog TCP.
[OOTB] KSC SQL	Собирает события от Kaspersky Security Center с использование запроса к базе данных MS SQL.
[OOTB] Syslog	Собирает события по протоколу Syslog.
[OOTB] Syslog-CEF	Собирает события в формате CEF, поступающих по протоколу UDP и имеющих заголовок Syslog.

Создание агента

Агент KUMA состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на сервере или активе сетевой инфраструктуры.

Создание агента производится в несколько этапов:

1. **Создание набора ресурсов агента в Консоли KUMA**
2. **Создание сервиса агента в Консоли KUMA**
3. **Установка серверной части агента на активе, с которого требуется передавать сообщения**

Агент KUMA для активов Windows может быть создан автоматически при создании коллектора с типом транспорта wmi или wec. Набор ресурсов и сервис таких агентов создаются в мастере установки коллектора, однако их все равно требуется установить на активе, с которого требуется передать сообщение.

Создание набора ресурсов для агента

Сервис агента в консоли KUMA создается на основе набора ресурсов для агента, в котором объединяются коннекторы и точки назначения.

Чтобы создать набор ресурсов для агента в консоли KUMA:

1. В консоли KUMA в разделе **Ресурсы** → **Агенты** нажмите **Добавить агент**.

   Откроется окно создания агента с активной вкладкой **Общие параметры**.

2. Заполните параметры на вкладке **Общие параметры**:

   - В поле **Название агента** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.
   - При необходимости переведите переключатель **Отладка** в активное положение, чтобы включить логирование операций сервиса.
   - В поле **Описание** можно добавить описание сервиса: до 256 символов в кодировке Unicode.

3. Создайте подключение для агента с помощью кнопки + и переключитесь на добавленную вкладку **Подключение <номер>**.

   Вкладки можно удалять с помощью кнопки ×.

4. В блоке параметров **Коннектор** добавьте коннектор:

- Если хотите выбрать существующий коннектор, выберите его в раскрывающемся списке.
- Если хотите создать коннектор, выберите в раскрывающемся списке **Создать** и укажите следующие параметры:
  - В поле **Название** укажите имя коннектора. Название должно содержать от 1 до 128 символов в кодировке Unicode.
  - В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:
    - tcp
    - udp
    - nats-jetstream
    - kafka
    - http
    - file
    - ftp
    - nfs
    - wmi
    - wec
    - snmp

    Типом агента считается тип использованного в нем коннектора. Единственным исключением являются агенты с назначением диодного типа. Такие агенты считаются диодными агентами.

    При использовании типа коннектора **tcp** или **udp** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса активов, с которых были получены события.

    Возможности по изменению уже созданных wec- или wmi-подключений в агентах, коллекторах и коннекторах ограничены. Тип подключения можно изменить с **wec** на **wmi** и обратно, однако типы **wec** или **wmi** не получится сменить на какой-либо другой тип подключения. При этом при изменении других типов подключений невозможно выбрать типы **wec** или **wmi**. Новые подключения можно создавать без ограничения по типам коннекторов.
- В поле **Описание** можно добавить описание ресурса: до 4000 символов в кодировке Unicode.

Коннектор добавлен в выбранное подключение набора ресурсов агента. Созданный коннектор доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

5. В блоке параметров **Точки назначения** добавьте точку назначения.

   - Если хотите выбрать существующую точку назначения, выберите ее в раскрывающемся списке.
   - Если хотите создать новую точку назначения, выберите в раскрывающемся списке **Создать** и укажите следующие параметры:
     - В поле **Название** укажите имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.
     - В раскрывающемся списке **Тип** выберите тип точки назначения и укажите ее параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:
       - **nats-jetstream** – используется для коммуникации через NATS.
       - **tcp** – используется для связи по протоколу TCP.
       - **http** – используется для связи по протоколу HTTP.
       - **diode** – используется для передачи событий с помощью диода данных.
       - **kafka** – используется для коммуникаций с помощью kafka.
       - **file** – используется для записи в файл.
   - В поле **Описание** можно добавить описание ресурса: до 4000 символов в кодировке Unicode.

   > Дополнительные параметры точки назначения агента (например, сжатие и режим TLS) должны совпадать с дополнительными параметрами точки назначения коллектора, с которым вы хотите связать агент.

   Точек назначения может быть несколько. Их можно добавить с помощью кнопки **Добавить точку назначения** и удалить с помощью кнопки ✕.

6. Повторите шаги 3–5 для каждого подключения агента, которое вы хотите создать.

7. Нажмите на кнопку **Сохранить**.

Набор ресурсов для агента создан и отображается в разделе **Ресурсы** → **Агенты**. Теперь можно создать сервис агента в KUMA.

Создание сервиса агента в Консоли KUMA

Когда набор ресурсов для агента создан, можно перейти к созданию сервиса агента в KUMA.

Чтобы создать сервис агента в Консоли KUMA:

1. В Консоли KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для агента и нажмите **Создать сервис**.

Сервис агента создан в Консоли KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы агента необходимо установить на каждом активе, с которого вы хотите передавать данные в коллектор. При установке используется идентификатор сервиса.

Установка агента в сетевой инфраструктуре KUMA

Когда сервис агента создан в KUMA, можно перейти к установке агента на активах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

Перед установкой убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Установка агента KUMA на активах Linux

Агент KUMA, установленный на устройствах Linux, останавливается при закрытии терминала или при перезапуске сервера. Чтобы избежать запуска агентов вручную, рекомендуется устанавливать агент с помощью системы, которая автоматически запускает приложения при перезапуске сервера, например, Supervisor. Чтобы автоматически запускать агенты, укажите в конфигурационном файле параметры автоматического запуска и автоматического перезапуска. Подробнее о настройке параметров см. официальную документацию систем автоматического запуска приложений. Пример настройки параметров в Supervisor, который вы можете адаптировать для своих нужд:

```
[program:agent_<имя агента>] command=sudo /opt/kaspersky/kuma/kuma agent --core
https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA

autostart=true

autorestart=true
```

Чтобы установить агент KUMA на актив Linux:

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Создайте следующие директории:
   - /opt/kaspersky/kuma/
   - /opt/kaspersky/agent/
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

`sudo /opt/kaspersky/kuma/kuma agent --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из Консоли KUMA> --wd <путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл kuma>`

Пример: `sudo /opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id XXXX --wd /opt/kaspersky/kuma/agent/XXXX`

Агент KUMA установлен на актив Linux. Агент пересылает данные в KUMA: можно настроить коллектор для их приема.

Установка агента KUMA на активах Windows

Перед установкой агента KUMA на активе Windows администратору сервера необходимо создать на активе Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.
Если вы хотите запустить агент под локальной учетной записью, для запуска потребуются права администратора и Log on as a service. Если вы хотите выполнить удаленный сбор и только чтение журналов под доменной учетной записью, будет достаточно прав EventLogReaders.

Чтобы установить агент KUMA на актив Windows:

1. Скопируйте файл kuma.exe в папку на активе Windows. Для установки рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

   Файл kuma.exe находится внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/.

2. Запустите командную строку на активе Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

   `kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под которым будет работать агент, включая домен> --install`

   Пример:

   `kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install`

   > Справочная информация об установщике доступна по команде `kuma help agent`.

4. Введите пароль для пользователя, под которым будет работать агент.

   Создана папка `C:\Program Files\Kaspersky Lab\KUMA\agent\<идентификатор агента>`, в нее установлен сервис агента KUMA. Агент пересылает события Windows в KUMA: можно настроить коллектор для их приема.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев. Агент можно перезапустить из Консоли KUMA, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента KUMA с активов Windows

Чтобы удалить агент KUMA с актива Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.

2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`

   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall`

Указанный агент KUMA удален с актива Windows. События Windows больше не отправляются в KUMA.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды:

```
kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под которым будет работать агент, включая домен>
```

Автоматически созданные агенты

При создании коллектора с коннекторами типа wec и wmi автоматически создаются агенты для приема событий Windows.

Автоматически созданные агенты имеют ряд особенностей:

- Автоматически созданные агенты могут иметь только одно подключение.

- Автоматически созданные агенты отображаются в разделе **Ресурсы** → **Агенты**, в конце их названия указаны слова `auto created`. Агенты можно просмотреть или удалить.

- Параметры автоматически созданных агентов указываются автоматически на основе параметров коллектора из разделов **Подключение источников** и **Транспорт**. Изменить параметры можно только в коллекторе, для которого был создан агент.

- В качестве описания автоматически созданного агента используется описание коллектора в разделе **Подключение источников**.

- Отладка автоматически созданного агента включается и выключается в разделе коллектора **Подключение источников**.

- При удалении коллектора с автоматически созданным агентом вам будет предложено удалить коллектор вместе с агентом или удалить только коллектор. При удалении только коллектора агент станет доступен для редактирования.

- При удалении автоматически созданных агентов тип коллектора меняется на **http**, а из поля **URL** коллектора удаляется адрес подключения.

- Если хотя бы одно название журнала Windows указано в коннекторе типа wec или wmi с ошибкой, агент не будет получать события из всех перечисленных в коннекторе журналов Windows. При этом статус агента

будет зеленый. Попытки получить события будут повторяться каждые 60 секунд, сообщения об ошибке будут добавляться в журнал сервиса.

В интерфейсе KUMA автоматически созданные агенты появляются одновременно с созданием коллектора. Они должны быть установлены на активе, который будет использоваться для пересылки сообщения.

Обновление агентов

При обновлении версий KUMA требуется обновить и установленные на удаленных машинах агенты WMI и WEC.

Чтобы обновить агент, используйте учетную запись с правами администратора и выполните следующие шаги:

1. В Консоли KUMA в разделе **Ресурсы** → **Активные сервисы** - **Агенты** выберите агент, который вы хотите обновить, и скопируйте его идентификатор.

   Идентификатор понадобится для последующего удаления агента и установки нового агента с тем же идентификатором.

2. В ОС Windows в разделе **Службы** откройте агент и нажмите **Стоп**.

3. В командном интерпретаторе перейдите в папку, где был установлен агент и выполните команду по удалению агента с сервера.

   kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall

4. Поместите в ту же папку новый агент.

5. В командном интерпретаторе перейдите в папку с новым агентом и из этой папки выполните команду установки, используя идентификатор агента из пункта 1.

   kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под которым будет работать агент, включая домен> --install

Агент обновлен.

Передача в KUMA событий из изолированных сегментов сети

Схема передачи данных

С помощью диодов данных можно передавать события из изолированных сегментов сети в KUMA. Передача данных организована следующим образом:

1. Установленный на изолированном сервере агент KUMA с точкой назначения **diode** принимает события и перемещает их в директорию, из которой события заберет диод данных.

   Агент накапливает события в буфере до его переполнения или в течение заданного пользователем срока после последней записи на диск. Затем события записываются в файл во временной директории агента. Файл перемещается в директорию, обрабатываемую диодом данных; в качестве его названия используется хеш-сумма (SHA256) содержимого файла и время создания файла.

2. Диод данных перемещает файлы из директории изолированного сервера в директорию внешнего сервера.

3. Установленный на внешнем сервере коллектор KUMA с коннектором **diode** считывает и обрабатывает события из файлов той директории, в которой размещает файлы диод данных.

   После считывания из файла всех событий он автоматически удаляется. Перед считыванием событий происходит верификация содержимого файлов по хеш-сумме в названии файла. Если содержимое не проходит верификацию, файл удаляется.

В указанной выше схеме компоненты KUMA отвечают за перемещение событий в определенную директорию внутри изолированного сегмента и за прием событий из определенной директории во внешнем сегменте сети. Перемещение файлов с событиями из директории изолированного сегмента сети в директорию внешнего сегменте сети осуществляет диод данных.

Для каждого источника данных внутри изолированного сегмента сети необходимо создать свой агент и коллектор KUMA, а также настроить диод данных на работу с отдельными директориями.

Настройка компонентов KUMA

Настройка компонентов KUMA для передачи данных из изолированных сегментов сети состоит из следующих этапов:

1. Создание сервиса коллектора во внешнем сегменте сети.

   На этом этапе необходимо создать и установить коллектор для получения и обработки файлов, которые диод данных будет перемещать из изолированного сегмента сети. Создать коллектор и все требуемые для него ресурсы можно с помощью мастера установки коллектора.

   На шаге **Транспорт** требуется выбрать или создать коннектор типа **diode**. В коннекторе необходимо указать директорию, в которую диод данных будет перемещать файлы из изолированного сегмента сети.

   Пользователь kuma, под которым работает коллектор, должен иметь права на чтение, запись и удаление в директории, в которую диод данных перемещает данные из изолированного сегмента сети.

2. Создание набора ресурсов агента KUMA.

   На этом этапе необходимо создать набор ресурсов агента KUMA, который будет в изолированном сегменте сети получать события и подготавливать их для передачи диоду данных. Набор ресурсов diode-агента имеет следующие особенности:

   - Точка назначения в агенте должна иметь тип **diode**. В этом ресурсе необходимо указать директорию, из которой диод данных будет перемещать файлы во внешний сегмент сети.
   - Для diode-агента невозможно выбрать коннекторы типа **sql** или **netflow**.
   - В коннекторе diode-агента должен быть выключен режим TLS.

3. Скачивание конфигурационного файла агента в виде JSON-файла.

   a. Набор ресурсов агента с точкой назначения типа diode необходимо скачать в виде JSON-файла.

   b. Если в наборе ресурсов агента использовались ресурсы секретов, конфигурационный файл необходимо вручную дополнить данными секретов.

4. Установка сервиса агента KUMA в изолированном сегменте сети.

   На этом этапе необходимо установить агент в изолированном сегменте сети на основе конфигурационного файла агента, созданного на предыдущем этапе. Установка возможна на устройствах Linux и Windows.

Настройка диода данных

Диод данных необходимо настроить следующим образом:

- Данные необходимо передавать атомарно из директории изолированного сервера (куда их помещает агент KUMA) в директорию внешнего сервера (где их считывает коллектор KUMA).
- Переданные файлы необходимо удалять с изолированного сервера.

Сведения о настройке диода данных можно получить в документации используемого в вашей организации диода данных.

Особенности работы

При работе с изолированными сегментами сети не поддерживаются работа с SQL и NetFlow.

При использовании указанной выше схемы невозможно администрирование агента через Консоль KUMA, поскольку он располагается в изолированном сегменте сети. В списке активных сервисов KUMA такие агенты не отображаются.

Конфигурационный файл diode-агента

Созданный набор ресурсов агента с точкой назначения типа diode можно скачать в виде конфигурационного файла. Этот файл используется при установке агента в изолированном сегменте сети.

Чтобы скачать конфигурационный файл,

В Консоли KUMA в разделе **Ресурсы** → **Агенты** выберите нужный набор ресурсов агента с точкой назначения diode и нажмите **Скачать конфигурацию**.

Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Секреты, используемые в наборе ресурсов агента, загружаются пустыми. Их идентификаторы указаны в файле в разделе "Секреты". Для использования файла конфигурации для установки агента в изолированном сегменте сети необходимо вручную дополнить файл конфигурации секретами (например, указать URL и пароли, используемые в коннекторе агента для получения событий).

Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к файлу на сервере, где будет установлен агент. Чтение файла должно быть доступно пользователю, от имени которого будет запускаться diode-агент.

Ниже приводится пример конфигурационного файла diode-агента с коннектором типа kafka.

```
{
"config": {
"id": "<идентификатор набора ресурсов агента>",
"name": "<название набора ресурсов агента>",
"proxyConfigs": [
{
"connector": {
"id": "<идентификатор коннектора. В этом примере приводится коннектор типа kafka, но в diode-агенте можно использовать коннекторы и других типов. Если коннектор создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
"name": "<название коннектора>",
"kind": "kafka",
"connections": [
{
"kind": "kafka",
"urls": [
"localhost:9093"
],
"host": "",
```

```
"port": "",
"secretID": "<идентификатор секрета>",
"clusterID": "",
"tlsMode": "",
"proxy": null,
"rps": 0,
"maxConns": 0,
"urlPolicy": "",
"version": "",
"identityColumn": "",
"identitySeed": "",
"pollInterval": 0,
"query": "",
"stateID": "",
"certificateSecretID": "",
"authMode": "pfx",
"secretTemplateKind": "",
"certSecretTemplateKind": ""
}
],
"topic": "<название топика kafka>",
"groupID": "<идентификатор группы kafka>",
"delimiter": "",
"bufferSize": 0,
"characterEncoding": "",
"query": "",
"pollInterval": 0,
"workers": 0,
"compression": "",
"debug": false,
"logs": [],
"defaultSecretID": "",
"snmpParameters": [
{
"name": "-",
"oid": "",
"key": ""
}
],
"remoteLogs": null,
"defaultSecretTemplateKind": ""
},
"destinations": [
{
"id": "<идентификатор точки назначения. Если точка назначения создана непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
"name": "<название точки назначения>",
"kind": "diode",
"connection": {
"kind": "file",
"urls": [
"<путь к директории, в которую точка назначения должна помещать события для передачи из изолированного сегмента сети диодом данных>",
"<путь к временной директории, в которую помещаются события для подготовки к передаче диодом данных>"
],
"host": "",
"port": "",
"secretID": "",
"clusterID": "",
"tlsMode": "",
"proxy": null,
"rps": 0,
"maxConns": 0,
"urlPolicy": "",
"version": "",
"identityColumn": "",
"identitySeed": "",
"pollInterval": 0,
"query": "",
"stateID": "",
"certificateSecretID": "",
"authMode": "",
"secretTemplateKind": "",
"certSecretTemplateKind": ""
},
"topic": "",
"bufferSize": 0,
"flushInterval": 0,
```

```
"diskBufferDisabled": false,
"diskBufferSizeLimit": 0,
"healthCheckPath": "",
"healthCheckTimeout": 0,
"healthCheckDisabled": false,
"timeout": 0,
"workers": 0,
"delimiter": "",
"debug": false,
"disabled": false,
"compression": "",
"filter": null,
"path": ""
}
]
}
],
"workers": 0,
"debug": false
},
"secrets": {
"<идентификатор секрета>": {
"pfx": "<зашифрованный pfx-ключ>",
"pfxPassword": "<пароль к зашифрованному pfx-ключу. Вместо действительного пароля из KUMA экспортируется значение changeit. В файле конфигурации необходимо вручную указать содержимое секретов>"
}
},
"tenantID": "<идентификатор тенанта>"
}
```


Описание полей секретов

Поля секрета

Название поля	Тип	Описание
`user`	Строка	Имя пользователя;
`password`	Строка	Пароль.
`token`	Строка	Токен
`urls`	массив строк.	Список URL
`publicKey`	Строка	Публичный ключ (используется в PKI)
`privateKey`	Строка	Приватный ключ (используется в PKI)
`pfx`	строка, содержащая base64-закодированное содержимое pfx	Содержимое pfx-файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды: `base64 -w0 src > dst`
`pfxPassword`	Строка	Пароль от pfx
`securityLevel`	Строка	Используется в snmp3. Возможные значения: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`
`community`	Строка	Используется в snmp1
`authProtocol`	Строка	Используется в snmp3. Возможные значения: `MD5`, `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`
`privacyProtocol`	Строка	Используется в snmp3. Возможные значения: `DES`, `AES`
`privacyPassword`	Строка	Используется в snmp3
`certificate`	строка, содержащая base64-закодированное содержимое pem	Содержимое pem-файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды: `base64 -w0 src > dst`

Установка Linux-агента в изолированном сегменте сети

Чтобы установить в изолированном сегменте сети агент KUMA на устройство Linux:

1. Поместите на Linux-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя KUMA.

   - Исполняемый файл /opt/kaspersky/kuma/kuma (файл kuma можно найти внутри установщика в папке /kuma-ansible-installer/roles/kuma/files/).

2. Выполните следующую команду:

   ```
   sudo ./kuma agent --cfg <путь к конфигурационному файлу агента> --wd <путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл kuma>
   ```

Сервис агента установлен и запущен на сервере в изолированном сегменте сети. Он получает события и передает их диоду данных для отправки во внешний сегмент сети.

Установка Windows-агента в изолированном сегменте сети

Перед установкой агента KUMA на активе Windows администратору сервера необходимо создать на активе Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

Чтобы установить в изолированном сегменте сети агент KUMA на устройство Windows:

1. Поместите на Window-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя, под которым будет работать агент.

   - Исполняемый файл kuma.exe. Файл можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

2. Запустите командную строку на активе Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

   ```
   kuma.exe agent --cfg <путь к конфигурационному файлу агента> --user <имя пользователя, под которым будет работать агент, включая домен> --install
   ```

Справочная информация об установщике доступна по команде:

```
kuma.exe help agent
```

4. Введите пароль для пользователя, под которым будет работать агент.

Создана папка `C:\Program Files\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>`, в нее установлен сервис агента KUMA. Агент перемещает события в папку для обработки диодом данных.

При установке агента конфигурационный файл агента перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA\agent\<идентификатор агента, указанный в конфигурационном файле>. Файл kuma.exe перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA.

При установке агента его конфигурационный файл не должен находиться в директории, в которую устанавливается агент.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев.

Удаление агента KUMA с активов Windows

Чтобы удалить агент KUMA с актива Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.
2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`
   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall`

Указанный агент KUMA удален с актива Windows. События Windows больше не отправляются в KUMA.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды:

```
kuma.exe agent --cfg <путь к конфигурационному файлу агента>
```

Передача в KUMA событий с машин Windows

Для передачи событий с машин Windows в KUMA используется связка агента и коллектора KUMA. Передача данных организована следующим образом:

1. Установленный на машине агент KUMA получает события Windows:

   - с помощью коннектора WEC: агент получает события, поступающие на устройство по подписке (subscription), и журналы сервера.

   - с помощью коннектора WMI: агент подключается к удаленным серверам, указанным в конфигурации, и получает события.

2. Агент без предварительной обработки передает события коллектору KUMA, указанному в точке назначения.

   Можно настроить агент таким образом, чтобы разные журналы отправлялись в разные коллекторы.

3. Коллектор принимает события от агента, выполняет полный цикл обработки события и отправляет обработанные события в точку назначения.

Получение событий с агента WEC рекомендуется при использовании централизованного получения событий с устройств Windows с помощью технологии Windows Event Forwarding (WEF). Агент необходимо установить на сервер, который выполняет сбор событий, он будет выполнять роль Windows Event Collector (WEC). Не рекомендуется устанавливать агенты KUMA на каждое конечное устройство, с которого планируется получать события.

Процесс настройки получения событий с использованием агента WEC подробно описан в приложении Настройка получения событий с устройств Windows с помощью Агента KUMA (WEC).

Подробнее о технологии Windows Event Forwarding см. в официальной документации Microsoft.

Получение событий с помощью агента WMI рекомендуется использовать в следующих случаях:

- Если отсутствует возможность использовать технологию WEF для реализации централизованного сбора событий, одновременно с этим запрещена установка стороннего ПО на сервере-источнике событий (например, агент KUMA).

- Если необходимо выполнить сбор событий с небольшого количества устройств - не более 500 устройств для одного агента KUMA.

Для подключения журналов событий Windows в качестве источника событий рекомендуется использовать мастер "Подключить источник". При использовании мастера в процессе создания коллектора с коннекторами типами WEC и WMI автоматически создаются агенты для приема событий Windows. Также ресурсы, необходимые для сбора событий Windows, можно создать вручную.

Создание и установка агента и коллектора для получения событий Windows происходит в несколько этапов:

1. **Создание набора ресурсов для агента**

   Коннектор агента:

   При создании агента на вкладке **Подключение** необходимо создать или выбрать коннектор типа WEC или WMI.

   Если хотя бы одно название журнала Windows указано в коннекторе типа WEC или WMI с ошибкой, или недоступен сервер WMI, агент будет получать события из всех перечисленных в коннекторе журналов Windows, кроме проблемного. При этом статус агента будет зеленый. Попытки получить события будут повторяться каждые 60 секунд, сообщения об ошибке будут добавляться в журнал сервиса.

   Точка назначения агента:

Тип точки назначения агента зависит от используемого вами способа передачи данных: nats, tcp, http, diode, kafka, file.

В качестве разделителя в точке назначения необходимо использовать значение `\0`.

Дополнительные параметры точки назначения агента (например, разделитель, сжатие и режим TLS) должны совпадать с дополнительными параметрами коннектора коллектора, с которым вы хотите связать агент.

2. **Создание сервиса агента в Консоли KUMA**

3. **Установка агента KUMA на машине Windows, с которой вы хотите получать события Windows.**

   Перед установкой убедитесь, что компоненты системы имеют доступ к сети и откройте необходимые сетевые порты:

   - Порт 7210, протокол TCP: от сервера с коллекторами к Ядру.
   - Порт 7210, протокол TCP: от сервера агента к Ядру.
   - Порт, настроенный при создании коннектора в поле **URL**: от сервера агента к серверу с коллектором.

4. **Создание и установка коллектора KUMA.**

   При создании набора ресурсов коллектора на шаге **Транспорт** необходимо создать или выбрать существующий коннектор, с помощью которого коллектор будет получать события от агента. Тип коннектора должен совпадать с типом точки назначения агента.

   Дополнительные параметры коннектора, такие как разделитель, сжатие и режим TLS, должны совпадать с дополнительными параметрами точки назначения агента, с которой вы хотите связать агент.

Для корректной работы некоторых плейбуков может потребоваться настройка дополнительного обогащения коллектора.

Чтобы изменить параметры правила обогащения в коллекторе KUMA:

1. Добавьте правило обогащения, нажав на кнопку Добавить правило обогащения, и укажите следующую информацию в соответствующих полях:
   - **Имя**: укажите произвольное имя для правила.
   - **Тип источника**: dns.
   - **URL**: IP-адрес контроллера домена.
   - **Запросов в секунду**: 5.
   - **Рабочие процессы**: 2.
   - **TTL кеш**: 3600.
2. Добавьте правило обогащения, нажав на кнопку Добавить правило обогащения, и выполните следующие действия:
   a. Заполните следующие поля:
      - **Имя**: укажите произвольное имя для правила.
      - **Тип источника**: event.

- **Поле источника**: DestinationNTDomain.
- **Целевое поле**: DestinationNTDomain.

b. Нажмите на кнопку **Добавить преобразование** и укажите следующую информацию в соответствующих полях:

- **Тип**: append.
- **Константа**: `.RU`.
- **Тип**: replace.
- **Символы**: `RU.RU`.
- **С символами**: `RU`.

3. Повторите шаги с шага 2 и укажите SourceNTDomain в качестве значения для параметров **Поле источника** и **Целевое поле**.

4. Добавьте обогащение данными LDAP и выполните следующие действия:

- В разделе **Сопоставление учетных записей LDAP** укажите имя контроллера домена.
- Нажмите на кнопку **Применить сопоставление по умолчанию**, чтобы заполнить таблицу сопоставления стандартными значениями.

Настройка источников событий

В этом разделе представлена информация о настройке получения событий из разных источников.

Настройка получения событий Auditd

KUMA позволяет осуществлять мониторинг и проводить аудит событий Auditd на устройствах Linux.

Перед настройкой получения событий убедитесь, что вы создали коллектор KUMA для событий Auditd.

Настройка получения событий Auditd состоит из следующих этапов:

1. Установка коллектора KUMA в сетевой инфраструктуре.
2. Настройка сервера источника событий.
3. Проверка поступления событий Auditd в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Auditd выполнена правильно, выполнив поиск связанных событий в Консоли KUMA.

Установка коллектора KUMA для получения событий Auditd

После создания коллектора для настройки получения событий с помощью rsyslog требуется установить коллектор на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка сервера источника событий

Для передачи событий от сервера в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера в коллектор:

1. Проверьте, что на сервере источнике событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующую команду:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. В папке /etc/rsyslog.d создайте файл audit.conf со следующим содержанием:

   ```
   $ModLoad imfile
   $InputFileName /var/log/audit/audit.log
   $InputFileTag tag_audit_log:
   $InputFileStateFile audit_log
   $InputFileSeverity info
   $InputFileFacility local6
   $InputRunFileMonitor
   *.* @<ip адрес коллектора KUMA>:<порт коллектора KUMA>
   ```

   Если вы хотите отправлять события по протоколу TCP, вместо последней строки в файле вставьте следующую:
   `*.* @@<ip адрес коллектора KUMA>:<порт коллектора KUMA>`.

3. Сохраните изменения в файле audit.conf.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   systemctl restart rsyslog.service
   ```

Сервер источника событий настроен. Данные о событиях передаются с сервера в коллектор KUMA.

Настройка получения событий KATA/EDR

Вы можете настроить получение событий приложения Kaspersky Anti Targeted Attack Platform в SIEM-систему KUMA.

Перед настройкой получения событий убедитесь, что вы создали коллектор KUMA для событий KATA/EDR.

При создании коллектора в Консоли KUMA убедитесь, что номер порта соответствует порту, указанному в пункте 4c Настройка для передачи событий Kaspersky Anti Targeted Attack Platform в KUMA, а тип коннектора соответствует типу, указанному в пункте 4d.

Для получения событий Kaspersky Anti Targeted Attack Platform с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

Настройка получения событий KATA/EDR состоит из следующих этапов:

1. Настройка пересылки событий KATA/EDR
2. Установка коллектора KUMA в сетевой инфраструктуре
3. Проверка поступления событий KATA/EDR в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий KATA/EDR выполнена правильно, выполнив поиск связанных событий в Консоли KUMA. События Kaspersky Anti Targeted Attack Platform отображаются в таблице с результатами поиска как KATA.

Настройка передачи событий KATA/EDR в KUMA

Чтобы настроить передачу событий из приложения Kaspersky Anti Targeted Attack Platform в KUMA:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.
2. В окне ввода учетных данных пользователя установите флажок **Локальный администратор** и введите данные Администратора.
3. Перейдите в раздел **Параметры** → **SIEM-система**.
4. Задайте следующие параметры:
   a. Установите флажки **Журнал активности** и **Обнаружения**.
   b. В поле **Устройство/IP** введите IP-адрес или имя устройства коллектора KUMA.
   c. В поле **Порт** укажите номер порта подключения к коллектору KUMA.
   d. В поле **Протокол** выберите из списка **TCP** или **UDP**.
   e. В поле **ID устройства** укажите идентификатор устройства сервера, который будет указан в журнале SIEM-систем как источник обнаружения.
   f. В поле **Периодичность сигнала** введите интервал отправки сообщений: от 1 до 59 минут.
   g. При необходимости, включите TLS-шифрование.
   h. Нажмите **Применить**.

Передача событий Kaspersky Anti Targeted Attack Platform в KUMA настроена.

Создание коллектора KUMA для получения событий KATA/EDR

После того как параметры передачи событий настроены, требуется создать коллектор в Консоли KUMA для событий Kaspersky Anti Targeted Attack Platform.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

При создании коллектора в Консоли KUMA убедитесь, что номер порта соответствует порту, указанному в пункте 4c Настройка для передачи событий Kaspersky Anti Targeted Attack Platform в KUMA, а тип коннектора соответствует типу, указанному в пункте 4d.

Для получения событий Kaspersky Anti Targeted Attack Platform с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

Установка коллектора KUMA для получения событий KATA/EDR

После создания коллектора для настройки получения событий Kaspersky Anti Targeted Attack Platform требуется установить новый коллектор на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка получения событий Kaspersky Security Center из MS SQL

KUMA позволяет получать информацию о событиях Kaspersky Security Center из базы данных MS SQL (далее MS SQL).

Перед настройкой убедитесь, что вы создали коллектор KUMA для событий Kaspersky Security Center из MS SQL.

При создании коллектора в Консоли KUMA на шаге **Транспорт** выберите коннектор **[OOTB] KSC SQL**.

Для получения событий Kaspersky Security Center из БД MS SQL на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSC from SQL**

Настройка получения событий состоит из следующих этапов:

1. Создание учетной записи в MS SQL.
2. Настройка службы SQL Server Browser.
3. Создание секрета.
4. Настройка коннектора.

5. Установка коллектора в сетевой инфраструктуре.

6. Проверка поступления событий из MS SQL в коллектор KUMA.

   Вы можете проверить, что настройка поступления событий из MS SQL выполнена правильно, выполнив поиск связанных событий в Консоли KUMA.

Создание учетной записи в MS SQL

Для получения событий Kaspersky Security Center из MS SQL требуется учетная запись, которая имеет права, необходимые для подключения и работы с базой данных.

Чтобы создать учетную запись для работы с MS SQL:

1. Войдите на сервер с установленной MS SQL для Kaspersky Security Center.

2. С помощью **SQL Server Management Studio** подключитесь к MS SQL под учетной записью с правами администратора.

3. В панели Object Explorer раскройте раздел **Security**.

4. Нажмите правой кнопкой мыши на папку **Logins** и в контекстном меню выберите **New Login**.

   Откроется окно **Login - New**.

5. На вкладке **General** нажмите на кнопку **Search** рядом с полем **Login name**.

   Откроется окно **Select User or Group**.

6. В поле **Enter the object name to select (examples)** укажите имя объекта и нажмите **OK**.

   Окно **Select User or Group** закроется.

7. В окне **Login - New** на вкладке **General** выберите опцию **Windows authentication**.

8. В поле **Default database** выберите БД Kaspersky Security Center.

   По умолчанию имя БД Kaspersky Security Center: KAV.

9. На вкладке **User Mapping** настройте права для учетной записи:

   a. В разделе **Users mapped to this login** выберите БД Kaspersky Security Center.

   b. В разделе **Database role membership for** установите флажки возле прав **db_datareader** и **public**.

10. На вкладке **Status** настройте права для подключения учетной записи к базе данных:

    - В разделе **Permission to connect to database engine** выберите **Grant**.

    - В разделе **Login** выберите **Enabled**.

11. Нажмите на кнопку **OK**.

    Окно **Login - New** закроется.

Чтобы проверить права учетной записи:

1. Запустите **SQL Server Management Studio** под созданной учетной записью.

2. Перейдите в любую таблицу MS SQL и сделайте выборку по таблице.

Настройка службы SQL Server Browser

После создания учетной записи в MS SQL требуется настроить службу SQL Server Browser.

Чтобы настроить службу SQL Server Browser:

1. Откройте **SQL Server Configuration Manager**.
2. В левой панели выберите **SQL Server Services**.

   Откроется список служб.
3. Откройте свойства службы **SQL Server Browser** одним из следующих способов:
   - Дважды нажмите на название службы **SQL Server Browser**.
   - Нажмите правой кнопкой мыши на название службы **SQL Server Browser** и в контекстном меню выберите **Properties**.
4. В открывшемся окне **SQL Server Browser Properties** выберите вкладку **Service**.
5. В поле **Start Mode** выберите **Automatic**.
6. Выберите вкладку **Log On** и нажмите на кнопку **Start**.

   Автоматический запуск службы **SQL Server Browser** включен.
7. Включите и настройте протокол **TCP/IP**, выполнив следующие действия:
   a. В левой панели раскройте раздел **SQL Server Network Configuration** и выберите подраздел **Protocols for <Имя SQL-сервера>**.
   b. Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстом меню выберите **Enable**.
   c. В появившемся окне **Warning** нажмите на кнопку **OK**.
   d. Откройте свойства протокола **TCP/IP** одним из следующих способов:
      - Дважды нажмите на протокол **TCP/IP**.
      - Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстном меню выберите **Properties**.
   e. Выберите вкладку **IP Addresses**, а затем в разделе **IPALL** в поле **TCP Port** укажите порт 1433.
   f. Нажмите на кнопку **Apply**, чтобы сохранить внесенные изменения.
   g. Нажмите на кнопку **OK**, чтобы закрыть окно.
8. Перезагрузите службу **SQL Server (<Имя SQL-сервера>)**, выполнив следующие действия:
   a. В левой панели выберите **SQL Server Services**.

b. В списке служб справа нажмите правой кнопкой мыши на службу **SQL Server (<Имя SQL-сервера>)** и в контекстном меню выберите **Restart**.

9. В **Брандмауэре защитника Windows в режиме повышенной безопасности** разрешите на сервере входящие подключения по порту TCP 1433.

Создание секрета в KUMA

После создания и настройки учетной записи в MS SQL требуется добавить секрет в Консоли KUMA. Этот ресурс используется для хранения учетных данных для подключения к MS SQL.

Чтобы создать секрет в KUMA:

1. В Консоли KUMA откройте раздел **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать секрет.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **urls**.

   d. В поле **URL** укажите строку вида:

   `sqlserver://[<domain>%5C]<username>:<password>@<server>:1433/<database_name>`

   где

   - `domain` – имя домена.
   - `%5C` – разделитель домена и пользователя. Представляет собой знак "\" в URL-формате.
   - `username` – имя созданной учетной записи MS SQL.
   - `password` – пароль созданной учетной записи MS SQL.
   - `server` – имя или IP-адрес сервера с базой данных MS SQL, установленной для Kaspersky Security Center.
   - `database_name` – имя БД Kaspersky Security Center. Имя по умолчанию: KAV.

   Пример:
   `sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV`

   Если в пароле учетной записи БД MS SQL используются специальные символы (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), переведите их в формат URL.

4. Нажмите на кнопку **Сохранить**.

Из соображений безопасности после сохранения секрета строка, указанная в поле URL, скрывается.

Настройка коннектора

Для подключения KUMA к БД MS SQL требуется настроить коннектор.

Чтобы настроить коннектор:

1. В Консоли KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.
2. В списке коннекторов справа найдите коннектор **[OOTB] KSC SQL** и откройте его для редактирования.

   Если коннектор недоступен для редактирования, скопируйте его и откройте для редактирования копию коннектора.

   Если коннектор **[OOTB] KSC SQL** отсутствует, обратитесь к системному администратору.
3. На вкладке **Основные параметры** в раскрывающихся списках **URL** выберите секрет, созданный для подключения к БД MS SQL.
4. Нажмите на кнопку **Сохранить**.

Настройка коллектора KUMA для получения событий Kaspersky Security Center из MS SQL

После того как параметры передачи событий настроены, требуется создать коллектор в Консоли KUMA для событий Kaspersky Security Center из MS SQL.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

При создании коллектора в Консоли KUMA на шаге **Транспорт** выберите коннектор **[OOTB] KSC SQL**.

Для получения событий Kaspersky Security Center из MS SQL на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSC from SQL**

Установка коллектора KUMA для получения событий Kaspersky Security Center из MS SQL

После завершения настройки коллектора для получения событий Kaspersky Security Center из MS SQL требуется установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка получения событий с устройств Windows с помощью Агента KUMA (WEC)

KUMA позволяет получать информацию о событиях с устройств Windows с помощью Агента KUMA типа WEC.

Настройка получения событий состоит из следующих этапов:

1. Настройка политик получения событий с устройств Windows.
2. Настройка централизованного получения событий с помощью службы Windows Event Collector.
3. Предоставление прав для просмотра событий.
4. Предоставление прав входа в качестве службы.
5. Настройка коллектора KUMA.
6. Установка коллектора KUMA.
7. Передача в KUMA событий с устройств Windows.

Настройка аудита событий с устройств Windows

Вы можете настроить аудит событий на устройствах Windows как на конкретном устройстве, так и на всех устройствах в домене.

В этом разделе описывается настройка аудита на отдельном устройстве, а также настройка аудита с помощью групповой политики домена.

Настройка политики аудита на устройстве Windows

Чтобы настроить политики аудита на устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.
3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.

5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Настройка политики аудита на устройстве завершена.

Настройка аудита с помощью групповой политики

Помимо настройки политики аудита на отдельном устройстве, вы также можете настроить аудит с помощью групповой политики домена.

Чтобы настроить аудит с помощью групповой политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.
3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.
5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

> Если вы хотите получать журналы Windows с большого количества серверов или если установка агентов KUMA на контроллеры домена не допускается, рекомендуется настроить перенаправление журналов Windows на отдельные серверы с настроенной службой Windows Event Collector.

Настройка политики аудита на сервере или рабочей станции завершена.

Настройка централизованного получения событий с устройств Windows с помощью службы Windows Event Collector

Служба Windows Event Collector позволяет централизованно получать данные о событиях на серверах и рабочих станциях под управлением ОС Windows. С помощью службы Windows Event Collector вы можете подписаться на события, которые регистрируются на удаленных устройствах.

Вы можете настроить следующие типы подписок на события:

- **Source-initiated subscriptions**. Удаленные устройства отправляют данные о событиях на сервер Windows Event Collector, адрес которого указывается в групповой политике. Подробнее о процедуре настройки подписки см. в разделе Настройка передачи данных с сервера источника событий.

- **Collector-initiated subscriptions**. Сервер Windows Event Collector подключается к удаленным устройствам и самостоятельно забирает события из локальных журналов. Подробнее о процедуре настройки подписки см. в разделе Настройка сервиса получения событий Windows.

Настройка передачи данных с сервера источника событий

Вы можете получать информацию о событиях на серверах и рабочих станциях, настроив передачу данных с удаленных устройств на сервер Windows Event Collector.

Предварительная подготовка

1. Проверьте, что служба Windows Remote Management настроена на сервере источника событий, выполнив следующую команду в консоли PowerShell:

   ```
   winrm get winrm/config
   ```

   Если служба Windows Remote Management не настроена, инициализируйте ее, выполнив следующую команду:

   ```
   winrm quickconfig
   ```

2. Если сервер источника событий является контроллером домена, откройте доступ по сети к журналам Windows, выполнив следующую команду в консоли PowerShel, запущенной от имени администратора:

   ```
   wevtutil set-log security /ca:’O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)
   ```

   Проверьте наличие доступа, выполнив следующую команду:

   ```
   wevtutil get-log security
   ```

Настройка брандмауэра сервера источника событий

Для того чтобы сервер Windows Event Collector мог получать записи журналов Windows, требуется открыть порты для входящих соединений на сервере источника событий.

Чтобы открыть порты для входящих соединений:

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `wf.msc` и нажмите **OK**.

   Откроется окно **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.

3. Перейдите в раздел **Правила для входящих подключений** и в панели **Действия** нажмите **Создать правило**.

   Откроется **Мастер создания правила для нового входящего пользователя**.

4. На шаге **Тип правила** выберите **Для порта**.

5. На шаге **Протоколы и порты** в качестве протокола выберите **Протокол TCP**. В поле **Определенные локальные порты** укажите номера портов:

   - `5985` (для доступа по HTTP)
   - `5986` (для доступа по HTTPS)

   Вы можете указать один из портов или оба.

6. На шаге **Действие** выберите **Разрешить подключение** (выбрано по умолчанию).

7. На шаге **Профиль** снимите флажки **Частный** и **Публичный**.

8. На шаге **Имя** укажите имя правила для нового входящего подключения и нажмите **Готово**.

Настройка передачи данных с сервера источника событий завершена.

Сервер Windows Event Collector должен обладать правами для чтения журналов Windows на сервере источника событий. Права могут быть предоставлены как учетной записи сервера Windows Event Collector, так и специальной пользовательской учетной записи. Подробнее о предоставлении прав см. в разделе Предоставление прав пользователю для просмотра журнала событий Windows.

Настройка сервиса получения событий Windows

Сервер Windows Event Collector может самостоятельно подключаться к устройствам и забирать данные о событиях любого уровня важности.

Чтобы настроить получение данных о событиях сервером Windows Event Collector:

1. На сервере-источнике событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `services.msc` и нажмите **OK**.

   Откроется окно **Службы**.

3. В списке служб найдите службу **Сборщик событий Windows** и запустите ее.

4. Откройте оснастку **Просмотр событий**, выполнив следующие действия:

   a. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

   b. В открывшемся окне введите запрос `eventvwr` и нажмите **OK**.

5. Перейдите в раздел **Подписки** и в панели **Действия** нажмите **Создать подписку**.

6. В открывшемся окне **Свойства подписки** задайте имя и описание подписки, а также следующие параметры:

   a. В поле **Конечный журнал** выберите из списка **Перенаправленные события**.

b. В разделе **Тип подписки и исходные компьютеры** нажмите на кнопку **Выбрать компьютеры**.

c. В открывшемся окне **Компьютеры** нажмите на кнопку **Добавить доменный компьютер**.

Откроется окно **Выбор: "Компьютер"**.

d. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена устройств, с которых вы хотите получать информацию о событиях. Нажмите на кнопку **OK**.

e. В окне **Компьютеры** проверьте список устройств, с которых сервер Windows Event Collector будет забирать данные о событиях и нажмите **OK**.

f. В окне **Свойства подписки** в поле **Собираемые события** нажмите на кнопку **Выбрать события**.

g. В открывшемся окне **Фильтр запроса** укажите, как часто и какие данные о событиях на устройствах вы хотите получать.

h. При необходимости в поле **<Все коды событий>** перечислите коды событий, информацию о которых вы хотите или не хотите получать. Нажмите на кнопку **OK**.

7. Если вы хотите использовать специальную учетную запись для просмотра данных о событиях, выполните следующие действия:

a. В окне **Свойства подписки** нажмите на кнопку **Дополнительно**.

b. В открывшемся окне **Дополнительные параметры подписки** в настройках учетной записи пользователя выберите **Определенный пользователь**.

c. Нажмите на кнопку **Пользователь и пароль** и задайте учетные данные выбранного пользователя.

Настройка сервиса получения событий завершена.

Чтобы проверить, что настройка выполнена правильно и данные о событиях поступают на сервер Windows Event Collector,

в оснастке **Просмотр событий** перейдите в раздел **Просмотр событий (Локальный)** → **Журналы Windows** → **Перенаправленные события**.

Предоставление прав для просмотра событий Windows

Вы можете предоставить права для просмотра событий Windows как для конкретного устройства, так и для всех устройств в домене.

Чтобы предоставить права для просмотра событий на конкретном устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `compmgmt.msc` и нажмите **OK**.

Откроется окно **Управление компьютером**.

3. Перейдите в раздел **Управление компьютером (локальным)** → **Локальные пользователи и группы** → **Группы**.

4. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

5. Внизу окна **Свойства: Читатели журнала событий** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите на кнопку **OK**.

Чтобы предоставить права для просмотра событий всех устройств в домене:

1. Зайдите в контроллер домена с правами администратора.
2. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
3. В открывшемся окне введите запрос `dsa.msc` и нажмите **OK**.

   Откроется окно **Active Directory Пользователи и Компьютеры**.

4. Перейдите в раздел **Active Directory Пользователи и Компьютеры** → **<Имя домена>** → **Builtin**.
5. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

   В окне **Свойства: Читатели журнала событий** откройте вкладку **Члены** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите на кнопку **OK**.

Предоставление прав входа в качестве службы

Вы можете предоставить право на вход в систему в качестве службы как конкретному устройству, так и всем устройствам в домене. Право входа в систему в качестве службы позволяет запустить процесс от имени учетной записи, которой это право предоставлено.

Чтобы предоставить право на вход в качестве службы устройству:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.
4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.
5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена учетных записей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите на кнопку **OK**.

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройствам в домене:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win+R**.
2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.
3. Перейдите в раздел **Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя**.
4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.
5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.
6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите на кнопку **OK**.

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Настройка коллектора KUMA для получения событий с устройств Windows

После завершения настройки политики аудита на устройствах, а также создания подписок на события и предоставления всех необходимых прав, требуется создать коллектор в Консоли KUMA для событий с устройств Windows.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

Для получения событий от устройств Windows в мастере установки коллектора KUMA укажите следующие параметры коллектора:

1. На шаге **Транспорт** укажите следующие параметры:
   a. В поле **Коннектор** выберите **Создать**.
   b. В поле **Тип** выберите **http**.
   c. В поле **Разделитель** выберите **\0**.
2. На вкладке **Дополнительные параметры** в поле **Режим TLS** выберите **С верификацией**.
3. На шаге **Парсинг событий** нажмите на кнопку **Добавить парсинг событий**.

4. В открывшемся окне **Основной парсинг событий** в поле **Нормализатор** выберите **[OOTB] Windows Extended v.1.0** и нажмите **OK**.

5. На шаге **Маршрутизация** добавьте следующие точки назначения:

   - **Хранилище**. Для отправки обработанных событий в хранилище.
   - **Коррелятор**. Для отправки обработанных событий в коррелятор.

   Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

6. На шаге **Проверка параметров** нажмите **Создать и сохранить сервис**.

7. Скопируйте появившуюся команду для установки коллектора KUMA.

Установка коллектора KUMA для получения событий с устройств Windows

После завершения настройки коллектора для получения событий Windows требуется установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка передачи в KUMA событий с устройств Windows с помощью Агента KUMA (WEC)

Чтобы завершить настройку передачи данных, требуется создать агент KUMA типа WEC, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

Подробнее о создании и установке агента KUMA типа WEC на устройства Windows см. в разделе Передача в KUMA событий с устройств Windows.

Настройка получения событий с устройств Windows с помощью Агента KUMA (WMI)

KUMA позволяет получать информацию о событиях с устройств Windows с помощью Агента KUMA типа WMI.

Настройка получения событий состоит из следующих этапов:

1. Настройка параметров аудита для работы с KUMA.
2. Настройка передачи данных с сервера источника событий.
3. Предоставление прав для просмотра событий.
4. Предоставление прав входа в качестве службы.
5. Создание коллектора KUMA.

   Для получения событий от устройств Windows в мастере установки коллектора KUMA на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Windows Extended v.1.0**.

6. Установка коллектора KUMA.

7. Передача в KUMA событий с устройств Windows.

   Чтобы завершить настройку передачи данных, требуется создать агент KUMA типа WMI, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

Настройка параметров аудита для работы с KUMA

Вы можете настроить аудит событий на устройствах Windows как на конкретном устройстве с помощью локальной политики, так и на всех устройствах в домене с помощью групповой политики.

В этом разделе описывается настройка аудита на отдельном устройстве, а также настройка аудита с помощью групповой политики домена.

Настройка аудита с помощью локальной политики

Чтобы настроить аудит с помощью локальной политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Политика аудита**.

4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.

5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Настройка политики аудита на устройстве завершена.

Настройка аудита с помощью групповой политики

Помимо настройки аудита на отдельном устройстве вы также можете настроить аудит с помощью групповой политики домена.

Чтобы настроить аудит с помощью групповой политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Политика аудита**.

4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.

5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Настройка политики аудита на сервере или рабочей станции завершена.

Настройка передачи данных с сервера источника событий

Предварительная подготовка

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `services.msc` и нажмите **OK**.

   Откроется окно **Службы**.

3. В списке служб найдите следующие службы:

   - Удаленный вызов процедур
   - RPC Endpoint Mapper

4. Убедитесь, что в столбце **Состояние** у этих служб отображается статус **Выполняется**.

Настройка брандмауэра сервера источника событий

Сервер Windows Management Instrumentation может получать записи журналов Windows, если открыты порты для входящих соединений на сервере источника событий.

Чтобы открыть порты для входящих соединений:

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `wf.msc` и нажмите **OK**.

   Откроется окно **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.

3. В окне **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности** перейдите в раздел **Правила для входящих подключений** и в панели **Действия** нажмите **Создать правило**.

   Откроется **Мастер создания правила для нового входящего подключения**.

4. В **Мастере создания правила для нового входящего подключения** на шаге **Тип правила** выберите **Для порта**.

5. На шаге **Протоколы и порты** в качестве протокола выберите **Протокол TCP**. В поле **Определенные локальные порты** укажите номера портов:

   - `135`
   - `445`
   - `49152-65535`

6. На шаге **Действие** выберите **Разрешить подключение** (выбрано по умолчанию).

7. На шаге **Профиль** снимите флажки **Частный** и **Публичный**.

8. На шаге **Имя** укажите имя правила для нового входящего подключения и нажмите **Готово**.

Настройка передачи данных с сервера источника событий завершена.

Предоставление прав для просмотра событий Windows

Вы можете предоставить права для просмотра событий Windows как для конкретного устройства, так и для всех устройств в домене.

Чтобы предоставить права для просмотра событий на конкретном устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `compmgmt.msc` и нажмите **OK**.

   Откроется окно **Управление компьютером**.

3. Перейдите в раздел **Управление компьютером (локальным)** → **Локальные пользователи и группы** → **Группы**.

4. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

5. Внизу окна **Свойства: Читатели журнала событий** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите на кнопку **OK**.

Чтобы предоставить права для просмотра событий всех устройств в домене:

1. Зайдите в контроллер домена с правами администратора.
2. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
3. В открывшемся окне введите запрос `dsa.msc` и нажмите **OK**.

   Откроется окно **Active Directory Пользователи и Компьютеры**.
4. В окне **Active Directory Пользователи и Компьютеры** перейдите в раздел **Active Directory Пользователи и Компьютеры** → **<Имя домена>** → **Builtin**.
5. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

   В окне **Свойства: Читатели журнала событий** откройте вкладку **Члены** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.
6. В окне **Выбор пользователя, компьютера или группы** в поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях. Нажмите на кнопку **OK**.

Предоставление прав входа в качестве службы

Вы можете предоставить право на вход в систему в качестве службы как конкретному устройству, так и всем устройствам в домене. Право входа в систему в качестве службы позволяет запустить процесс от имени учетной записи, которой это право предоставлено.

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройству:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.
3. В окне **Локальная политика безопасности** перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.
4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.
5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить пользователя или группу**.

   Откроется окно **Выбор "Пользователи или "Группы"**.
6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена учетных записей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите на кнопку **OK**.

Чтобы предоставить право на вход в качестве службы устройствам в домене:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить пользователя или группу**.

   Откроется окно **Выбор "Пользователи или "Группы"**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить право входа в систему в качестве службы. Нажмите на кнопку **OK**.

Настройка получения событий PostgreSQL

KUMA позволяет осуществлять мониторинг и проводить аудит событий PostgreSQL на устройствах Linux с помощью rsyslog.

Аудит событий проводится с помощью плагина pgAudit. Плагин поддерживает работу с PostgreSQL версии 9.5 и выше. Подробную информацию о плагине pgAudit см. по ссылке: https://github.com/pgaudit/pgaudit.

Настройка получения событий состоит из следующих этапов:

1. Установка плагина pdAudit.

2. Создание коллектора KUMA для событий PostgreSQL.

   Для получения событий PostgreSQL с помощью rsyslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] PostgreSQL pgAudit syslog**.

3. Установка коллектора в сетевой инфраструктуре KUMA.

4. Настройка сервера источника событий.

5. Проверка поступления событий PostgreSQL в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий PostgreSQL выполнена правильно в разделе Консоли KUMA Поиск связанных событий.

Установка плагина pgAudit

Чтобы установить плагин pgAudit:

1. В командном интерпретаторе выполните команды под учетной записью с правами администратора:

   ```
   sudo apt update
   sudo apt -y install postgresql-<PostgreSQL version>-pgaudit
   ```

Версию плагина необходимо выбрать в зависимости от версии PostgresSQL. Информацию о версиях PostgreSQL и необходимых версиях плагина см.по ссылке: https://github.com/pgaudit/pgaudit#postgresql-version-compatibility.

Пример:
```
sudo apt -y install postgresql-12-pgaudit
```

2. Найдите конфигурационный файл postgres.conf. Для этого в командной строке PostgresSQL выполните команду:

   ```
   show data_directory
   ```

   В ответе будет указано расположение конфигурационного файла.

3. Создайте резервную копию конфигурационного файла postgres.conf.

4. Откройте файл postgres.conf и скопируйте или замените имеющиеся значения на указанные ниже.

   ```
   ## pgAudit settings
   shared_preload_libraries = 'pgaudit'
   ## database logging settings
   log_destination = 'syslog'
   ## syslog facility
   syslog_facility = 'LOCAL0'
   ## event ident
   syslog_ident = 'Postgres'
   ## sequence numbers in syslog
   syslog_sequence_numbers = on
   ## split messages in syslog
   syslog_split_messages = off
   ## message encoding
   lc_messages = 'en_US.UTF-8'
   ## min message level for logging
   client_min_messages = log
   ## min error message level for logging
   log_min_error_statement = info
   ## log checkpoints (buffers, restarts)
   log_checkpoints = off
   ## log query duration
   log_duration = off
   ## error description level
   log_error_verbosity = default
   ## user connections logging
   log_connections = on
   ## user disconnections logging
   log_disconnections = on
   ## log prefix format
   ```

```
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
## log_statement
log_statement = 'none'
## hostname logging status. dns bane resolving affect
#performance!
log_hostname = off
## logging collector buffer status
#logging_collector = off
## pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```

5. Перезапустите службу PostgreSQL при помощи команды:

   ```
   sudo systemctl restart postgresql
   ```

6. Чтобы загрузить плагин pgAudit в PostgreSQL, в командной строке PostgreSQL выполните команду:

   ```
   CREATE EXTENSION pgaudit
   ```

Плагин pgAudit установлен.

Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена PostgreSQL, в коллектор:

1. Чтобы проверить, что на сервере источника событий установлен сервис rsyslog, выполните следующую команду под учетной записью с правами администратора:

   ```
   sudo systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. В директории /etc/rsyslog.d/ создайте файл pgsql-to-siem.conf со следующим содержанием:

   ```
   If $programname contains 'Postgres' then @< IP-адрес коллектора >:< порт коллектора >
   Например:
   If $programname contains 'Postgres' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'Postgres' then @@192.168.1.5:2514
   ```

   Сохраните изменения в конфигурационном файле pgsql-to-siem.conf.

3. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/pgsql-to-siem.conf
   $RepeatedMsgReduction off
   ```

Сохраните изменения в конфигурационном файле /etc/rsyslog.conf.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Настройка получения событий ИВК Кольчуга-К

Вы можете настроить получение событий системы ИВК Кольчуга-К в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий ИВК Кольчуга-К в KUMA.
2. Создание коллектора KUMA для получения событий ИВК Кольчуга-К.

   Для получения событий ИВК Кольчуга-К с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Kolchuga-K syslog**.

3. Установка коллектора KUMA для получения событий ИВК Кольчуга-К.
4. Проверка поступления событий ИВК Кольчуга-К в KUMA.

   Вы можете проверить, что настройка источника событий ИВК Кольчуга-К выполнена правильно в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий ИВК Кольчуга-К в KUMA

Чтобы настроить передачу событий межсетевого экрана ИВК КОЛЬЧУГА-К по syslog в коллектор KUMA:

1. Подключитесь к межсетевому экрану с правами администратора по протоколу SSH.
2. Создайте резервную копию файлов /etc/services и /etc/syslog.conf.
3. В конфигурационном файле /etc/syslog.conf укажите FQDN или IP-адрес коллектора KUMA. Например:

   . @kuma.example.com

   or

   . @192.168.0.100

   Сохраните изменения в конфигурационном файле /etc/syslog.conf.

4. В конфигурационном файле /etc/services укажите порт и протокол, который используется коллектором KUMA. Например:

   syslog 10514/udp

   Сохраните изменения в конфигурационном файле /etc/services.

5. Перезапустите syslog-сервер межсетевого экрана с помощью команды:

   ```
   service syslogd restart
   ```

Настройка получения событий КриптоПро NGate

Вы можете настроить получение событий приложения КриптоПро NGate в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий КриптоПро NGate в KUMA.
2. Создание коллектора KUMA для получения событий КриптоПро NGate.

   Для получения событий КриптоПро NGate в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] NGate syslog**.
3. Создание коллектора KUMA для получения событий КриптоПро NGate.
4. Проверка поступления событий КриптоПро NGate в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий КриптоПро NGate выполнена правильно, в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий КриптоПро NGate в KUMA

Чтобы настроить передачу событий из приложения КриптоПро NGate в KUMA:

1. Подключитесь к веб-интерфейсу системы управления NGate.
2. Подключите удаленные syslog-серверы к системе управления. Для этого выполните следующие действия:
   a. Откройте страницу списка syslog-серверов **External Services** → **Syslog Server** → **Add Syslog Server**.
   b. Введите параметры syslog-сервера и нажмите на значок ✔.
3. Выполните привязку syslog-серверов к конфигурации для записи журналов работы кластера. Для этого выполните следующие действия:
   a. В разделе **Clusters** → **Summary** выберите настраиваемый кластер.
   b. На вкладке **Configurations** нажмите на элемент **Configuration** нужного кластера для входа на страницу настроек конфигурации.
   c. В поле **Syslog Servers** настраиваемой конфигурации нажмите на кнопку **Назначить**.
   d. Установите флажки для syslog-серверов, которые вы хотите привязать, и нажмите на значок ✔.

      Вы можете привязать неограниченное количество серверов.

      Чтобы добавить новые syslog-серверы, нажмите на значок ✚.
   e. Опубликуйте конфигурацию для активации новых настроек.
4. Выполните привязку syslog-серверов к системе управления для записи журналов работы Администратора. Для этого выполните следующие действия:

a. Выберите пункт меню **Management Center Settings** и на открывшейся странице в блоке **Syslog servers** нажмите на кнопку **Assign**.

b. В окне **Assign Syslog Servers to Management Center** установите флажок для тех syslog-серверов, которые вы хотите привязать, затем нажмите на значок .

Вы можете привязать неограниченное количество серверов.

В результате события приложения КриптоПро NGate передаются в KUMA.

Настройка получения событий Ideco UTM

Вы можете настроить получение событий приложения Ideco UTM в KUMA по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий Ideco UTM в KUMA.
2. Создание коллектора KUMA для получения событий Ideco UTM.

   Для получения событий Ideco UTM в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор [OOTB] Ideco UTM syslog.
3. Установка коллектора KUMA для получения событий Ideco UTM.
4. Проверка поступления событий Ideco UTM в KUMA.

   Вы можете проверить, что настройка сервера источника событий Ideco UTM выполнена правильно, в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий Ideco UTM в KUMA

Чтобы настроить передачу событий из приложения Ideco UTM в KUMA:

1. Подключитесь к веб-интерфейсу Ideco UTM под учетной записью, обладающей административными привилегиями.
2. В меню **Пересылка системных сообщений** переведите переключатель **Syslog** в положение **включено**.
3. В параметре **IP-адрес** укажите IP-адрес коллектора KUMA.
4. В параметре Порт введите порт, который прослушивает коллектор KUMA.
5. Нажмите **Сохранить** для применения внесенных изменений.

Передача событий в Ideco UTM в KUMA будет настроена.

Настройка получения событий KWTS

Вы можете настроить получение событий из системы анализа и фильтрации веб-трафика Kaspersky Web Traffic Security (KWTS) в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KWTS в KUMA.
2. Создание коллектора KUMA для получения событий KWTS.

   Для получения событий KWTS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KWTS**.
3. Установка коллектора KUMA для получения событий KWTS.
4. Проверка поступления событий KWTS в коллектор KUMA.

   Вы можете проверить, что настройка передачи событий KWTS выполнена правильно в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий KWTS в KUMA

Чтобы настроить передачу событий KWTS в KUMA:

1. Подключитесь к серверу KWTS по протоколу SSH под учетной записью root.
2. Перед внесением изменений создайте резервные копии следующих файлов:
   - /opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template
   - /etc/rsyslog.conf
3. Убедитесь, что параметры конфигурационного файла /opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template имеют следующие значения, при необходимости внесите изменения:

   ```
   "siemSettings":
   {
   "enabled": true,
   "facility": "Local5",
   "logLevel": "Info",
   "formatting":
   {
   ```
4. Сохраните внесенные изменения
5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл /etc/rsyslog.conf.

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local5.* @<< IP-адрес коллектора KUMA >:< порт коллектора >>
   ```

   Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local5.* @@<< IP-адрес коллектора KUMA >:< порт коллектора >>
```

6. Сохраните внесенные изменения

7. Перезапустите сервис rsyslog с помощью следующей команды:

   ```
   sudo systemctl restart rsyslog.service
   ```

8. Перейдите в веб-интерфейс KWTS на вкладку **Параметры** – **Syslog** и включите опцию **Записывать информацию о профиле трафика**.

9. Нажмите на кнопку **Сохранить**.

Настройка получения событий KLMS

Вы можете настроить получение событий из системы анализа и фильтрации почтового трафика Kaspersky Linux Mail Server (KLMS) в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KLMS в KUMA

2. Создание коллектора KUMA для получения событий KLMS.

   Для получения событий KLMS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KLMS syslog CEF**.

3. Установка коллектора KUMA для получения событий KLMS.

4. Проверка поступления событий KLMS в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий KLMS выполнена правильно в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий KLMS в KUMA

Чтобы настроить передачу событий KLMS в KUMA:

1. Подключитесь к серверу KLMS по протоколу SSH и перейдите в меню **Technical Support Mode**.

2. С помощью утилиты klms-control выгрузите настройки в файл settings.xml:

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f
   /tmp/settings.xml
   ```

3. Убедитесь, что параметры файла /tmp/settings.xml имеют следующие значения, при необходимости внесите изменения:

   ```
   <siemSettings>
   <enabled>1</enabled>
   <facility>Local1</facility>
   ...
   </siemSettings>
   ```

4. Примените настройки с помощью следующей команды:

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```

5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл /etc/rsyslog.conf.

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local1.* @<< IP-адрес коллектора KUMA >:< порт коллектора >>
   ```

   Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

   ```
   local1.* @@<< IP-адрес коллектора KUMA >:< порт коллектора >>
   ```

6. Сохраните внесенные изменения

7. Перезапустите сервис rsyslog с помощью следующей команды:

   ```
   sudo systemctl restart rsyslog.service
   ```

Настройка получения событий KSMG

Вы можете настроить получение событий из систем анализа и фильтрации почтового трафика Kaspersky Secure Mail Gateway (KSMG) 1.1 в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий KSMG в KUMA

2. Создание коллектора KUMA для получения событий KSMG.

   Для получения событий KSMG в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSMG**.

3. Установка коллектора KUMA для получения событий KSMG.

4. Проверка поступления событий KSMG в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий KSMG выполнена правильно, в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий KSMG в KUMA

Чтобы настроить передачу событий KSMG в KUMA:

1. Подключитесь к серверу KSMG по протоколу SSH под учетной записью с правами администратора.

2. С помощью утилиты ksmg-control выгрузите настройки в файл settings.xml:

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-control --get-settings EventLogger -n -f
   /tmp/settings.xml
   ```

3. Убедитесь, что параметры файла /tmp/settings.xml имеют следующие значения, при необходимости внесите изменения:

   ```
   <siemSettings>
   <enabled>1</enabled>
   <facility>Local1</facility>
   ```

4. Примените настройки с помощью следующей команды:

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```

5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл /etc/rsyslog.conf.

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local1.* @<< IP-адрес коллектора KUMA >:< порт коллектора >>
   ```

   Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

   ```
   local1.* @@<< IP-адрес коллектора KUMA >:< порт коллектора >>
   ```

6. Сохраните внесенные изменения

7. Перезапустите сервис rsyslog с помощью следующей команды:

   ```
   sudo systemctl restart rsyslog.service
   ```

Настройка получения событий PT NAD

Вы можете настроить получение событий из PT NAD в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий PT NAD в KUMA.

2. Создание коллектора KUMA для получения событий PT NAD.

   Для получения событий PT NAD с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор [OOTB] PT NAD json.

3. Установка коллектора KUMA для получения событий PT NAD.

4. Проверка поступления событий PT NAD в коллектор KUMA.

Вы можете проверить, что настройка сервера источника событий PT NAD выполнена правильно в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий PT NAD в KUMA

Настройка передачи событий из PT NAD 11 в KUMA по Syslog включает следующие этапы:

1. Настройка модуля ptdpi-worker@notifier.
2. Настройка отправки syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации.

Настройка модуля ptdpi-worker@notifier.

Для включения отправки информации об обнаруженных угрозах информационной безопасности необходимо настроить модуль ptdpi-worker@notifier.

В многосерверной конфигурации инструкцию нужно выполнять на основном сервере.

Чтобы настроить модуль ptdpi-worker@notifier:

1. Откройте файл /opt/ptsecurity/etc/ptdpi.settings.yaml:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. В группе параметров **General settings** раскомментируйте параметр workers и добавьте notifier в список его значений.

   Например:

   ```
   workers: ad alert dns es hosts notifier
   ```

3. Добавьте в конец файла строку вида notifier.yaml.nad_web_url: <URL консоли PT NAD>

   Например:

   ```
   notifier.yaml.nad_web_url: https://ptnad.example.com
   ```

   Модуль ptdpi-worker@notifier будет использовать указанный URL для формирования ссылок на карточки сессий и активностей при отправке сообщений.

4. Перезапустите сенсор:

   ```
   sudo ptdpictl restart-all
   ```

Модуль ptdpi-worker@notifier настроен.

Настройка syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации

Параметры, перечисленные в следующей инструкции могут отсутствовать в конфигурационном файле. Если параметр отсутствует, вам нужно добавить его в файл самостоятельно.

В многосерверной конфигурации PT NAD настройка выполняется на основном сервере.

Чтобы настроить отправку syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации:

1. Откройте файл /opt/ptsecurity/etc/ptdpi.settings.yaml:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. По умолчанию PT NAD отправляет данные об активностях на русском языке. Чтобы получать данные на английском языке, измените значение параметра notifier.yaml.syslog_notifier.locale на "en".

   Например:

   ```
   notifier.yaml.syslog_notifier.locale: en
   ```

3. В параметре notifier.yaml.syslog_notifier.addresses добавьте секцию с параметрами отправки событий в KUMA.

   Параметр <Название подключения> может состоять только из букв латинского алфавита, цифр и символа подчеркивания.

   В параметре address необходимо указать IP-адрес коллектора KUMA.

   Остальные параметры можно не указывать, в таком случае будут использоваться значения по умолчанию.

   ```
   notifier.yaml.syslog_notifier.addresses:
   <Название подключения>:
   address: <Для отправки на удаленный сервер — протокол UDP (по умолчанию) или TCP, адрес и порт; для локального подключения — сокет домена Unix>
   doc_types: [<Перечисленные через запятую типы сообщений (alert для информации об атаках, detection для активностей и reputation для информации об индикаторах компрометации). По умолчанию отправляются все типы сообщений>]
   facility: <Числовое значение категории субъекта>
   ident: <Метка ПО>
   <Название подключения>:
   ...
   ```

   Далее представлен пример настройки отправки syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации, отправляемых на два удаленных сервера по протоколам TCP и UDP без записи в локальный журнал:

   ```
   notifier.yaml.syslog_notifier.addresses:
   remote1:
   address: tcp://198.51.100.1:1514
   remote2:
   address: udp://198.51.100.2:2514
   ```

4. Сохраните изменения в файле /opt/ptsecurity/etc/ptdpi.settings.yaml.

5. Перезапустите модуль ptdpi-worker@notifier:

   ```
   sudo ptdpictl restart-worker notifier
   ```

Настройка отправки событий в KUMA по Syslog выполнена.

Настройка получения событий с помощью плагина MariaDB Audit Plugin

KUMA позволяет проводить аудит событий с помощью плагина MariaDB Audit Plugin. Плагин поддерживает работу с MySQL 5.7 и MariaDB. Работа плагина аудита с MySQL 8 не поддерживается. Подробная информация о плагине доступна на официальном веб-сайте MariaDB.

Мы рекомендуем использовать плагин MariaDB Audit Plugin версии 1.2 и выше.

Настройка получения событий состоит из следующих этапов:

1. Настройка плагина MariaDB Audit Plugin для передачи событий MySQL и настройка Syslog-сервера для отправки событий.

2. Настройка плагина MariaDB Audit Plugin для передачи событий MariaDB и настройка Syslog-сервера для отправки событий.

3. Создание коллектора KUMA для событий MySQL 5.7 и MariaDB.

   Для получения событий MySQL 5.7 и MariaDB с помощью плагина MariaDB Audit Plugin в мастере установки коллектора KUMA на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] MariaDB Audit Plugin syslog**.

4. Установка коллектора в сетевой инфраструктуре KUMA.

5. Проверка поступления событий MySQL и MariaDB в коллектор KUMA.

   Чтобы проверить, что настройка сервера источника событий MySQL и MariaDB выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка плагина MariaDB Audit Plugin для передачи событий MySQL

Плагин MariaDB Audit Plugin поддерживается для MySQL 5.7 версии до 5.7.30 и поставляется в комплекте с MariaDB.

Чтобы настроить передачу событий MySQL 5.7 с помощью плагина MariaDB Audit Plugin:

1. Скачайте дистрибутив MariaDB и распакуйте его.

   Дистрибутив MariaDB доступен на официальном веб-сайте MariaDB. Операционная система дистрибутива MariaDB должна совпадать с операционной системой, на которой функционирует MySQL 5.7.

2. Подключитесь к MySQL 5.7 под учетной записью с правами администратора, выполнив команду:

   ```
   mysql -u <имя пользователя> -p
   ```

3. Чтобы получить директорию, в которой расположены плагины MySQL 5.7, в командной строке MySQL 5.7 выполните команду:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

4. В директории, полученной на шаге 3, скопируйте плагин MariaDB Audit Plugin из директории `<директория, куда был разархивирован дистрибутив>`/mariadb-server-`<версия>`/lib/plugins/server_audit.so.

5. В командном интерпретаторе операционной системы выполните команду:

   ```
   chmod 755 <директория, куда был разархивирован дистрибутив> server_audit.so
   ```

   Например:

   ```
   chmod 755 /usr/lib64/mysql/plugin/server_audit.so
   ```

6. В командном интерпретаторе MySQL 5.7 выполните команду:

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

7. Создайте резервную копию конфигурационного файла /etc/mysql/mysql.conf.d/mysqld.cnf.

8. В конфигурационном файле /etc/mysql/mysql.conf.d/mysqld.cnf в разделе `[mysqld]` добавьте следующие строки:

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   Если вы хотите отключить передачу событий для определенных групп событий аудита, удалите часть значений параметра `server_audit_events`. Описание параметров доступно на веб-сайте производителя плагина MariaDB Audit Plugin.

9. Сохраните изменения в конфигурационном файле.

10. Перезапустите сервис MariaDB, выполнив одну из следующих команд:

    - `systemctl restart mysqld` — для системы инициализации systemd.
    - `service mysqld restart` — для системы инициализации init.

Настройка плагина MariaDB Audit Plugin для MySQL 5.7 завершена. При необходимости вы можете выполнить следующие команды в командной строке MySQL 5.7:

- `show plugins` — для проверки списка текущих плагинов.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` — для проверки текущих настроек аудита.

Настройка плагина MariaDB Audit Plugin для передачи событий MariaDB

Плагин MariaDB Audit Plugin входит в состав дистрибутива MariaDB, начиная с версий 5.5.37 и 10.0.10.

Чтобы настроить передачу событий MariaDB с помощью плагина MariaDB Audit Plugin:

1. Подключитесь к MariaDB под учетной записью с правами администратора, выполнив команду:

   ```
   mysql -u <имя пользователя> -p
   ```

2. Чтобы проверить, что плагин есть в директории, где размещены плагины операционной системы, в командной строке MariaDB выполните команду:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

3. В командном интерпретаторе операционной системы выполните команду:

   ```
   ll <директория, полученная в результате выполнения предыдущей команды> | grep server_audit.so
   ```

   Если вывод команды пуст и плагина нет в директории, вы можете скопировать плагин MariaDB Audit Plugin в эту директорию или использовать более новую версию MariaDB.

4. В командном интерпретаторе MariaDB выполните команду:

```
install plugin server_audit soname 'server_audit.so'
```

5. Создайте резервную копию конфигурационного файла /etc/mysql/my.cnf.

6. В конфигурационном файле /etc/mysql/my.cnf в разделе `[mysqld]` добавьте следующие строки:

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   Если вы хотите отключить передачу событий для определенных групп событий аудита, удалите часть значений параметра `server_audit_events`. Описание параметров доступно на веб-сайте производителя плагина MariaDB Audit Plugin.

7. Сохраните изменения в конфигурационном файле.

8. Перезапустите сервис MariaDB, выполнив одну из следующих команд:

   - `systemctl restart mariadb` — для системы инициализации systemd.
   - `service mariadb restart` — для системы инициализации init.

Настройка плагина MariaDB Audit Plugin для MariaDB завершена. При необходимости вы можете выполнить следующие команды в командной строке MariaDB:

- `show plugins` — для проверки списка текущих плагинов.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` — для проверки текущих настроек аудита.

Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлена MySQL или MariaDB, в коллектор:

1. Перед внесением изменений создайте резервную копию конфигурационного файла /etc/rsyslog.conf.

2. Для отправки событий по протоколу UDP добавьте в конфигурационный файл /etc/rsyslog.conf строку:

   ```
   *.* @<IP-адрес коллектора KUMA>:<порт коллектора KUMA>
   ```

   Например:

   ```
   *.* @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, строка должна выглядеть следующим образом:

   ```
   *.* @@192.168.1.5:2514
   ```

   Сохраните изменения в конфигурационном файле /etc/rsyslog.conf.

3. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Настройка получения событий СУБД Apache Cassandra

KUMA позволяет получать информацию о событиях Apache Cassandra.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования событий Apache Cassandra в KUMA.
2. Создание коллектора KUMA для событий Apache Cassandra.

   Для получения событий Apache Cassandra в мастере установки коллектора KUMA необходимо выполнить следующие действия: на шаге **Транспорт** выберите коннектор типа **file**, на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Apache Cassandra file**.
3. Установка коллектора в сетевой инфраструктуре KUMA.
4. Проверка поступления событий Apache Cassandra в коллектор KUMA.

   Чтобы проверить, что настройка сервера источника событий Apache Cassandra выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка журналирования событий Apache Cassandra в KUMA

Чтобы настроить журналирование событий Apache Cassandra в KUMA:

1. Убедитесь, что на сервере, где установлена Apache Cassandra, есть 5 ГБ свободного дискового пространства.
2. Подключитесь к серверу Apache Cassandra под учетной записью с правами администратора.
3. Перед внесением изменений создайте резервные копии следующих конфигурационных файлов:
   - /etc/cassandra/cassandra.yaml
   - /etc/cassandra/logback.xml
4. Убедитесь, что параметры конфигурационного файла /etc/cassandra/cassandra.yaml имеют следующие значения, при необходимости внесите изменения:

   a. в секции `audit_logging_options` присвойте параметру `enabled` значение `true.`

   b. в разделе `logger` присвойте параметру `class_name` значение `FileAuditLogger`.
5. В конфигурационный файл /etc/cassandra/logback.xml добавьте следующие строки:

```
<!-- Audit Logging (FileAuditLogger) rolling file appender to audit.log -->
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
<file>${cassandra.logdir}/audit/audit.log</file>
<rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
<!-- rollover daily -->
<fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-
dd}.%i.zip</fileNamePattern>
```

```
<!-- each file should be at most 50MB, keep 30 days worth of history, but at most 5GB
-->
<maxFileSize>50MB</maxFileSize>
<maxHistory>30</maxHistory>
<totalSizeCap>5GB</totalSizeCap>
</rollingPolicy>
<encoder>
<pattern>%-5level [%thread] %date{ISO8601} %F:%L - %replace(%msg){'\n', '
'}%n</pattern>
</encoder>
</appender>
<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log -->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
<appender-ref ref="AUDIT"/>
</logger>
```

6. Сохраните изменения в конфигурационном файле.
7. Перезапустите службу Apache Cassandra с помощью следующих команд:
   a. `sudo systemctl stop cassandra.service`
   b. `sudo systemctl start cassandra.service`
8. После перезапуска проверьте статус Apache Cassandra с помощью следующей команды:
   `sudo systemctl status cassandra.service`
   Убедитесь, что в выводе команды есть последовательность символов:
   `Active: active (running)`

Настройка передачи событий Apache Cassandra завершена. События будут располагаться в директории /var/log/cassandra/audit/, в файле audit.log (${cassandra.logdir}/audit/audit.log).

Настройка получения событий FreeIPA

Вы можете настроить получение событий FreeIPA в KUMA по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий FreeIPA в KUMA.
2. Создание коллектора KUMA для получения событий FreeIPA.
   Для получения событий FreeIPA в мастере установки коллектора KUMA на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] FreeIPA**.
3. Установка коллектора KUMA в сетевой инфраструктуре.
4. Проверка поступления событий FreeIPA в KUMA.
   Чтобы проверить, что настройка сервера источника событий FreeIPA выполнена правильно, вы можете осуществить поиск связанных событий.

Настройка передачи событий FreeIPA в KUMA

Чтобы настроить передачу событий FreeIPA в KUMA по протоколу Syslog в формате JSON:

1. Подключитесь к серверу FreeIPA по протоколу SSH под учетной записью с правами администратора.
2. В директории /etc/rsyslog.d/ создайте файл freeipa-to-siem.conf.
3. В конфигурационный файл /etc/rsyslog.d/freeipa-to-siem.conf добавьте следующие строки:

```
template(name="ls_json" type="list" option.json="on")
{ constant(value="{")
constant(value="\"@timestamp\":\"") property(name="timegenerated"
dateFormat="rfc3339")
constant(value="\",\"@version\":\"1")
constant(value="\",\"message\":\"") property(name="msg")
constant(value="\",\"host\":\"") property(name="fromhost")
constant(value="\",\"host_ip\":\"") property(name="fromhost-ip")
constant(value="\",\"logsource\":\"") property(name="fromhost")
constant(value="\",\"severity_label\":\"") property(name="syslogseverity-text")
constant(value="\",\"severity\":\"") property(name="syslogseverity")
constant(value="\",\"facility_label\":\"") property(name="syslogfacility-text")
constant(value="\",\"facility\":\"") property(name="syslogfacility")
constant(value="\",\"program\":\"") property(name="programname")
constant(value="\",\"pid\":\"") property(name="procid")
constant(value="\",\"syslogtag\":\"") property(name="syslogtag")
constant(value="\"}\n")
}
*.* @<IP-адрес коллектора KUMA>:<порт коллектора KUMA>;ls_json
```

   Вы можете заполнить содержимое последней строки в соответствии с выбранным протоколом:

   `*.* @<192.168.1.10>:<1514>;ls_json` — для отправки событий по протоколу UDP

   `*.* @@<192.168.2.11>:<2514>;ls_json` — для отправки событий по протоколу TCP

4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

```
$IncludeConfig /etc/freeipa-to-siem.conf
$RepeatedMsgReduction off
```

5. Сохраните изменения в конфигурационном файле.
6. Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Настройка получения событий VipNet TIAS

Вы можете настроить получение событий VipNet TIAS в KUMA по протоколу syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий VipNet TIAS в KUMA.
2. Создание коллектора KUMA для получения событий VipNet TIAS.

   Для получения событий VipNet TIAS с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор [OOTB] Syslog-CEF.
3. Установка коллектора KUMA для получения событий VipNet TIAS.
4. Проверка поступления событий VipNet TIAS в KUMA.

   Вы можете проверить, что настройка сервера источника событий VipNet TIAS выполнена правильно, в разделе Консоли KUMA Поиск связанных событий.

Настройка передачи событий VipNet TIAS в KUMA

Чтобы настроить передачу событий VipNet TIAS в KUMA по протоколу syslog:

1. Подключитесь к веб-интерфейсу VipNet TIAS под учетной записью с правами администратора.
2. Перейдите в раздел **Управление** – **Интеграции**.
3. На странице **Интеграция** перейдите на вкладку Syslog.
4. На панели инструментов списка принимающих серверов нажмите **Новый сервер**.
5. В открывшейся карточке нового сервера выполните следующие действия:
   1. В поле **Адрес сервера** укажите IP-адрес или доменное имя коллектора KUMA.

      Например, 10.1.2.3 или syslog.siem.ru
   2. В поле **Порт** укажите входящий порт коллектора KUMA. По умолчанию установлен порт 514.
   3. В списке **Протокол** выберите протокол транспортного уровня, который прослушивает коллектор KUMA. По умолчанию выбран протокол UDP.
   4. В списке **Организация** с помощью флажков выберите организации инфраструктуры ViPNet TIAS.

      Сообщения будут отправляться только по инцидентам, обнаруженным на основании событий, полученных от сенсоров выбранных организаций инфраструктуры.
   5. В списке **Статус** с помощью флажков выберите статусы инцидентов.

      Сообщения будут отправляться только при назначении инцидентам выбранных статусов.
   6. В списке **Уровень важности** с помощью флажков выберите уровни важности инцидентов.

      Сообщения будут отправляться только об инцидентах выбранных уровней важности. По умолчанию в списке выбран только высокий уровень важности.
   7. В списке **Язык интерфейса** выберите язык, на котором вы хотите получать информацию об инцидентах в сообщениях. По умолчанию выбран русский язык.

6. Нажмите на кнопку **Добавить**.

7. На панели инструментов списка установите переключатель **Не передавать информацию об инцидентах в формате CEF** в состояние "включено".

   В результате при обнаружении новых и изменении статусов ранее выявленных инцидентов, в зависимости от выбранных при настройке статусов, будет выполняться передача соответствующей информации на указанные адреса принимающих серверов по протоколу syslog в формате CEF.

8. Нажмите **Сохранить изменения**.

Настройка отправки событий в коллектор KUMA выполнена.

Настройка получения событий Nextcloud

Вы можете настроить получение событий приложения Nextcloud 26.0.4 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита событий Nextcloud.
2. Настройка Syslog-сервера для отправки событий.

   Для передачи событий от сервера в коллектор используется сервис rsyslog.

3. Создание коллектора KUMA для получения событий Nextcloud.

   Для получения событий Nextcloud в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Nextcloud syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

4. Установка коллектора KUMA для получения событий Nextcloud.
5. Проверка поступления событий Nextcloud в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Nextcloud выполнена правильно в Консоли KUMA в разделе Поиск связанных событий.

Настройка аудита событий Nextcloud

Чтобы настроить передачу событий Nextcloud в KUMA:

1. На сервере, на котором установлено приложение Nextcloud, создайте резервную копию конфигурационного файла /home/localuser/www/nextcloud/config/config.php.
2. Отредактируйте конфигурационный файл Nextcloud /home/localuser/www/nextcloud/config/config.php.
3. Измените значения следующих параметров на приведенные ниже:

```
'log_type' => 'syslog',
'syslog_tag' => 'Nextcloud',
'logfile' => '',
'loglevel' => 0,
'log.condition' => [
'apps' => ['admin_audit'],
```

```
],
```

4. Перезагрузите сервис Nextcloud с помощью команды:

   ```
   sudo service restart nextcloud
   ```

Настройка отправки событий в коллектор KUMA выполнена.

Настройка Syslog-сервера для отправки событий Nextcloud

Чтобы настроить передачу событий от сервера, на котором установлено приложение Nextcloud, в коллектор:

1. В каталоге /etc/rsyslog.d/ создайте файл Nextcloud-to-siem.conf со следующим содержанием:

   ```
   If $programname contains 'Nextcloud' then @<IP-адрес коллектора>:<порт коллектора>
   ```

   Пример:

   ```
   If $programname contains 'Nextcloud' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'Nextcloud' then @<IP-адрес коллектора>:<порт коллектора>
   ```

2. Сохраните изменения в конфигурационном файле Nextcloud-to-siem.conf .

3. Создайте резервную копию файла /etc/rsyslog.conf.

4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/Nextcloud-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните внесенные изменения

6. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Передача событий Nextcloud в коллектор будет настроена.

Настройка получения событий Snort

Вы можете настроить получение событий приложения Snort версии 3 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования событий Snort.

2. Создание коллектора KUMA для получения событий Snort.

   Для получения событий Snort в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Snort 3 json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора KUMA для получения событий Snort.

4. Проверка поступления событий Snort в коллектор KUMA.

Вы можете проверить, что настройка сервера источника событий Snort выполнена правильно в Консоли KUMA в разделе Поиск связанных событий.

Настройка журналирования событий Snort

Убедитесь, что на сервере, на котором запущен Snort, есть минимум 500 МБ свободного дискового пространства для сохранения одного журнала событий Snort.
По достижении объема журнала 500 МБ Snort автоматически создаст файл, в имени которого будет указано текущее время в формате unixtime.
Рекомендуется отслеживать заполнение дискового пространства.

Чтобы настроить журналирование событий Snort:

1. Подключитесь к серверу, на котором установлен Snort, под учетной записью, обладающей административными привилегиями.

2. Измените конфигурационный файл Snort. Для этого в командном интерпретаторе выполните команду:

   ```
   sudo vi /usr/local/etc/snort/snort.lua
   ```

3. В конфигурационном файле измените содержимое блока alert_json:

   ```
   alert_json =
   {
   file = true,
   limit = 500,
   fields = 'seconds action class b64_data dir dst_addr dst_ap dst_port eth_dst eth_len \
   eth_src eth_type gid icmp_code icmp_id icmp_seq icmp_type iface ip_id ip_len msg mpls
   \
   pkt_gen pkt_len pkt_num priority proto rev rule service sid src_addr src_ap src_port \
   target tcp_ack tcp_flags tcp_len tcp_seq tcp_win tos ttl udp_len vlan timestamp',
   }
   ```

4. Для завершения настройки выполните следующую команду:

   ```
   sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l
   /var/log/snort -i <название интерфейса, который прослушивает Snort> -m 0x1b
   ```

В результате события Snort будут записываться в файл /var/log/snort/alert_json.txt.

Настройка получения событий Suricata

Вы можете настроить получение событий приложения Suricata версии 7.0.1 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий Suricata в KUMA.

2. Создание коллектора KUMA для получения событий Suricata.

Для получения событий Suricata в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Suricata json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора KUMA для получения событий Suricata.

4. Проверка поступления событий Suricata в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Suricata выполнена правильно в Консоли KUMA в разделе Поиск связанных событий.

Настройка журналирования событий Suricata.

Чтобы настроить журналирование событий Suricata:

1. Подключитесь по протоколу SSH к серверу, обладающему административными учетными записями пользователя.

2. Создайте резервную копию файла /etc/suricata/suricata.yaml.

3. Установите в конфигурационном файле /etc/suricata/suricata.yaml в секции eve-log следующие значения:

   ```
   - eve-log:
   enabled: yes
   filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
   filename: eve.json
   ```

4. Сохраните изменения в файле конфигурации /etc/suricata/suricata.yaml.

В результате события Suricata будут записываться в файл /usr/local/var/log/suricata/eve.json.

Suricata не поддерживает ограничение размера файла с событиями eve.json. При необходимости вы можете контролировать размер журнала с помощью ротации. Например, для настройки ежечасной ротации журнала добавьте в конфигурационный файл следующие строки:

```
outputs:

- eve-log:

filename: eve-%Y-%m-%d-%H:%M.json

rotate-interval: hour
```

Настройка получения событий FreeRADIUS

Вы можете настроить получение событий приложения FreeRADIUS версии 3.0.26 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка аудита событий FreeRADIUS.

2. Настройка Syslog-сервера для отправки событий FreeRADIUS.

3. Создание коллектора KUMA для получения событий FreeRADIUS.

   Для получения событий FreeRADIUS в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] FreeRADIUS syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

4. Установка коллектора KUMA для получения событий FreeRADIUS.

5. Проверка поступления событий FreeRADIUS в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий FreeRADIUS выполнена правильно в Консоли KUMA в разделе Поиск связанных событий.

Настройка аудита событий FreeRADIUS

Чтобы настроить аудит событий в системе FreeRADIUS:

1. Подключитесь к серверу, на котором установлена система FreeRADIUS, под учетной записью пользователя, обладающей правами администратора.

2. Создайте резервную копию конфигурационного файла FreeRADIUS с помощью команды:

   ```
   sudo cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius /3.0/radiusd.conf.bak
   ```

3. Откройте конфигурационный файл FreeRADIUS для редактирования с помощью команды:

   ```
   sudo nano /etc/freeradius/3.0/radiusd.conf
   ```

4. В секции log измените параметры следующим образом:

   ```
   destination = syslog
   syslog_facility = daemon
   stripped_names = no
   auth = yes
   auth_badpass = yes
   auth_goodpass = yes
   ```

5. Сохраните конфигурационный файл.

Аудит событий FreeRADIUS будет настроен.

Настройка Syslog-сервера для отправки событий FreeRADIUS

Для передачи событий от сервера FreeRADIUS в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий от сервера, на котором установлен FreeRADIUS, в коллектор:

1. В каталоге /etc/rsyslog.d/ создайте файл FreeRADIUS-to-siem.conf и добавьте в него следующую строку:

   ```
   If $programname contains 'radiusd' then @<IP-адрес коллектора>:<порт коллектора>
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'radiusd' then @<IP-адрес коллектора>:<порт коллектора>
   ```

2. Создайте резервную копию файла /etc/rsyslog.conf.

3. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/FreeRADIUS-to-siem.conf
   $RepeatedMsgReduction off
   ```

4. Сохраните внесенные изменения

5. Перезапустите службу rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Передача событий от сервера FreeRADIUS в коллектор KUMA будет настроена.

Настройка получения событий VMware vCenter

Вы можете настроить получение событий VMware vCenter в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка подключения к VMware vCenter.

2. Создание коллектора KUMA для получения событий VMware vCenter.

   Для получения событий VMWare Vcenter в мастере установки коллектора на шаге **Транспорт** выберите тип коннектора vmware. Укажите обязательные параметры:

   - URL, по которому доступен API VMware, например, https://vmware-server.com:6440.
   - Учетные данные VMware – секрет, в котором указаны логин и пароль для подключения к API VMware.

   На шаге **Парсинг событий** выберите нормализатор [OOTB] VMware vCenter API.

3. Установка коллектора KUMA для получения событий VMWare Vcenter.

4. Проверка поступления событий VMWare Vcenter в коллектор KUMA.

   Вы можете проверить, что сервер источника событий VMware vCenter настроен правильно, в разделе Консоли KUMA Поиск связанных событий.

Настройка параметров подключения к VMware vCenter

Чтобы настроить подключение к VMware Vcenter для получения событий:

1. Подключитесь к веб-интерфейсу VMware Vcenter под учетной записью, обладающей административными привилегиями.

2. Перейдите в раздел Security&Users и выберите Users.

3. Создайте учетную запись пользователя.

4. Перейдите в раздел Roles и назначьте созданной учетной записи роль Read-only: See details of objects, but not make changes.

   Учетные данные этой записи вы будете использовать в секрете коллектора.

Более подробная информация о создании учетных записей представлена в документации системы VMware Vcenter.

Настройка подключения к VMware vCenter для получения событий выполнена.

Настройка получения событий zVirt

Вы можете настроить получение событий приложения zVirt версии 3.1 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий zVirt в KUMA.
2. Создание коллектора KUMA для получения событий zVirt.

   Для получения событий zVirt в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] OrionSoft zVirt syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.
3. Установка коллектора KUMA для получения событий zVirt.
4. Проверка поступления событий zVirt в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий zVirt выполнена правильно в Консоли KUMA в разделе Поиск связанных событий.

Настройка передачи событий zVirt

Система zVirt может передавать события во внешние системы в режиме установки Hosted Engine.

Чтобы настроить передачу событий из zVirt в KUMA:

1. В веб-интерфейсе zVirt в разделе **Ресурсы** выберите **Виртуальные машины**.
2. Выделите машину, на которой запущена виртуальная машина HostedEngine, и нажмите **Изменить**.
3. В окне **Изменить виртуальную машину** перейдите в раздел **Журналирование**.
4. Установите флажок **Определить адрес Syslog-сервера**.
5. В поле ввода укажите данные коллектора в следующем формате: `<IP-адрес или FQDN коллектора KUMA>:<порт коллектора KUMA>`.
6. Если вы хотите использовать протокол TCP вместо UDP для передачи журналов, установите флажок **Использовать TCP-соединение**.

Передача событий будет настроена.

Настройка получения событий Zeek IDS

Вы можете настроить получение событий приложения Zeek IDS версии 1.8 в KUMA.

Настройка получения событий состоит из следующих этапов:

1. Преобразование формата журнала событий Zeek IDS.

   Нормализатор KUMA поддерживает работу с журналами Zeek IDS в формате JSON. Для передачи событий в нормализатор KUMA файлы журналов нужно преобразовать в формат JSON.

2. Создание коллектора KUMA для получения событий Zeek IDS.

   Для получения событий Suricata в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] ZEEK IDS json file**, на шаге **Транспорт** выберите тип коннектора **file**.

3. Установка коллектора KUMA для получения событий Zeek IDS.

4. Проверка поступления событий Zeek IDS в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Zeek IDS выполнена правильно, в Консоли KUMA в разделе Поиск связанных событий.

Преобразование формата журнала событий Zeek IDS.

По умолчанию события Zeek IDS записываются в файлы в каталог /opt/zeek/logs/current.

Нормализатор [OOTB] ZEEK IDS json file поддерживает работу с журналами Zeek IDS в формате JSON. Для передачи событий в нормализатор KUMA файлы журналов нужно преобразовать в формат JSON.

> Эту процедуру нужно повторять каждый раз перед получением событий Zeek IDS.

Чтобы преобразовать формат журнала событий Zeek IDS:

1. Подключитесь к серверу, на котором установлено приложения Zeek IDS, под учетной записью пользователя, обладающей правами администратора.

2. Создайте директорию, где будут храниться журналы событий в формате JSON, с помощью команды:

   ```
   sudo mkdir /opt/zeek/logs/zeek-json
   ```

3. Перейдите в эту директорию с помощью команды:

   ```
   sudo cd /opt/zeek/logs/zeek-json
   ```

4. Выполните команду, которая с помощью утилиты jq преобразует исходный формат журнала событий к необходимому:

   ```
   jq . -c <путь к файлу журнала, формат которого нужно изменить> >> <название нового файла>.log
   ```

   Пример:

   ```
   jq . -c /opt/zeek/logs/current/conn.log >> conn.log
   ```

   В результате выполнения команды в директории /opt/zeek/logs/zeek-json будет создан новый файл, если такого ранее не существовало. Если такой файл уже был в текущей директории, то в конец файла будет добавлена новая информация.

Мониторинг источников событий

В этом разделе представлена информация о мониторинге источников событий.

Состояние источников

В KUMA можно контролировать состояние источников, из которых поступают данные в коллекторы. На одном сервере может быть несколько источников событий, а данные из нескольких источников могут поступать в один коллектор.

Вы можете настроить автоматическое определение источников событий с помощью одного из следующих наборов полей:

- Пользовательский набор полей. Вы можете указать от 1 до 9 полей в нужной последовательности.
- Применить сопоставление по умолчанию: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Порядок полей изменить невозможно.

  Определение источников происходит, если следующие поля в событиях содержат непустые значения: DeviceProduct, DeviceAddress и/или DeviceHostname и TenantID (вам не нужно задавать значение поля TenantID, оно определяется автоматически). Поле DeviceProcessName может быть пустым. Если поле DeviceProcessName не пусто, а остальные обязательные поля заполнены, определяется новый источник.

  Определение источников событий в зависимости от непустых значений в полях событий

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName;	TenantID (определяется автоматически)	
+	+			+	Источник 1 определен
+		+		+	Источник 2 определен
+	+	+		+	Источник 3 определен
+	+		+	+	Источник 4 определен
+		+	+	+	Источник 5 определен
+	+	+	+	+	Источник 6 определен
	+	+		+	Источник не определен
	+		+	+	Источник не определен
		+	+	+	Источник не определен
+			+	+	Источник не определен

Для всей установки применяется только один набор полей. При обновлении до новой версии KUMA применяется набор полей по умолчанию. Только пользователь с ролью Главный администратор может настроить набор полей для определения источника события. После того как изменения в наборе полей сохранены, ранее определенные источники событий удаляются из Консоли KUMA и из базы данных. При необходимости вы можете вернуться к использованию набора полей для определения источников событий по умолчанию. Чтобы измененные параметры вступили в силу и приложение KUMA начала определять источники на основе новых параметров, необходимо перезапустить коллекторы.

Чтобы определить источники событий:

1. В Консоли KUMA перейдите в раздел **Состояние источников**.

2. В открывшемся окне **Состояния источников** нажмите на нажмите кнопку настройки параметров.

3. В открывшемся окне **Параметры обнаружения источника события** в раскрывающемся списке **Группирующие поля для обнаружения источников** выберите поля событий, по которым вы хотите определять источники событий.

   Вы можете указать от 1 до 9 полей в нужной последовательности. В пользовательской конфигурации KUMA определяет источники, в которых заполнено поле TenantID (вам не нужно задавать значение поля, оно определяется автоматически) и заполнено хотя бы одно поле из **Группирующие поля для определения источников**. Для числовых полей 0 считается пустым значением. Если для определения источника выбрано одно числовое поле, а значение числового поля равно 0, источник не обнаруживается.

   После того как вы сохранили измененный набор полей, создается событие аудита и все ранее определенные источники удаляются из Консоли KUMA и из базы данных, а примененные политики становятся неактивными.

4. Если вы хотите вернуться к списку полей для определения источника событий по умолчанию, нажмите **Применить сопоставление по умолчанию**. Порядок полей по умолчанию изменить невозможно. Если вы вручную укажете неправильный порядок полей, отобразится ошибка и кнопка сохранения параметров станет недоступной. Правильная последовательность полей по умолчанию: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Минимальная конфигурация для определения источников событий с использованием набора событий по умолчанию: непустые значения в полях DeviceProduct, DeviceAddress и/или DeviceHostName, и в поле TenantID (TenantID определяется автоматически).

5. Нажмите на кнопку **Сохранить**.

6. Перезапустите коллекторы, чтобы применить изменения и начать определение источников событий по заданному списку полей.

Определение источника настроено.

Чтобы просмотреть события, связанные с источником событий:

1. В Консоли KUMA перейдите в раздел **Состояние источников**.

2. В открывшемся окне **Источники событий** выберите источник события в списке. В столбце **Имя** в раскрывающемся списке для выбранного источника события нажмите на кнопку **События за <количество> дней**.

   Откроется раздел **Поиск угроз**, где вы можете просмотреть список событий для выбранного источника за последние 5 минут. Значения полей, заданные в параметрах определения источника событий, автоматически указываются в запросе. При необходимости в разделе **Поиск угроз** вы можете изменить период времени в запросе и снова нажать **Запустить запрос**, чтобы просмотреть данные за указанный период времени.

Ограничения

1. В конфигурации с установленным полем по умолчанию KUMA регистрирует источник события, только если необработанное событие содержит поле DeviceProduct и поля DeviceAddress и/или DeviceHostName.

   Если сырое событие не содержит поля DeviceProduct и DeviceAddress и/или DeviceHostName, вы можете:

   - Настроить обогащение в нормализаторе: на вкладке нормализатора **Обогащение** выберите тип данных **Событие**, укажите значение **Поле источника**, для поля **Целевое поле** выберите DeviceProduct + DeviceAddress и/или DeviceHostName и нажмите на кнопку OK.

- Использовать правило обогащения: выберите тип источника данных **Событие**, укажите **Поле источника** и в качестве значения **Целевое поле** выберите DeviceProduct + DeviceAddress и/или DeviceHostName, затем нажмите на кнопку **Создать**. Созданное правило обогащения необходимо привязать к коллектору на шаге Обогащение событий.

KUMA выполнит обогащение и зарегистрирует источник событий.

2. Если в KUMA поступают события с одинаковыми значениями, которые определяют источник, KUMA регистрирует разные источники при следующих условиях:

   - Значения обязательных полей совпадают, но для событий определяются разные тенанты.
   - Значения обязательных полей совпадают, но для одного из событий указано необязательное поле DeviceProcessName.
   - Значения обязательных полей совпадают, но у данных в этих полях не совпадает регистр.

Если вы хотите, чтобы KUMA регистрировала для таких событий один источник, вы можете дополнительно настроить поля в нормализаторе.

Списки источников формируются в коллекторах, объединяются в Ядре KUMA и отображаются в веб-интерфейсе приложения в разделе **Состояние источников** на вкладке **Список источников событий**. Данные обновляются ежеминутно.

Данные о частоте и количестве поступающих событий являются важным показателем состояния наблюдаемой системы. Вы можете настроить политики мониторинга, чтобы изменения отслеживались автоматически и при достижении индикаторами определенных граничных значений автоматически создавались уведомления. Политики мониторинга отображаются в консоли KUMA в разделе **Состояние источников** на вкладке **Политики мониторинга**.

При срабатывании политик мониторинга создаются события мониторинга с данными об источнике событий.

Список источников событий

Источники событий отображаются в таблице в разделе **Состояние источников → Список источников событий**. На одной странице отображается до 250 источников. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. При нажатии на источник событий открывается график поступления данных.

Источники событий можно искать по названию с помощью поля **Поиск**. Поиск осуществляется с помощью регулярных выражений (RE2).

При необходимости вы можете настроить период обновления данных в таблице. Доступные периоды обновления: **1 минута**, **5 минут**, **15 минут**, **1 час**. По умолчанию указано значение: **Не обновлять**. Настройка периода обновления может потребоваться для отслеживания изменений в списке источников.

Доступны следующие столбцы:

- **Статус** – статус источника:
  - зеленый – события поступают в пределах присвоенной политики мониторинга;
  - красный – частота или количество поступающих событий выходит за границы, определенные в политике мониторинга;

- серый – источнику событий не присвоена политика мониторинга.

Таблицу можно фильтровать по этому параметру.

- **Название** – название источника события. Имя формируется автоматически из значений полей, заданных в параметрах определения источника событий.

  Вы можете изменить название источника событий. Название может содержать не более 128 символов в кодировке Unicode.

- **Имя устройства или IP-адрес** – имя или IP-адрес устройства, с которого происходят события, если в параметрах определения источника событий указаны поля DeviceHostName или DeviceAddress.
- **Политика мониторинга** – название политики мониторинга, назначенной источнику событий.
- **Поток** – частота, с которой из источника поступают события.
- **Нижний порог** – нижняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Верхний порог** – верхняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Тенант** – тенант, к которому относятся события, поступающие из источника.

> По умолчанию на странице отображается и доступно для выбора, не больше 250 источников событий. Если источников событий больше, чтобы их можно было выбрать, необходимо загрузить дополнительные источники событий, нажав в нижней части окна на кнопку **Показать еще 250**.

Если выбрать источники событий, становятся доступны следующие кнопки:

- **Сохранить в CSV** – с помощью этой кнопки можно выгрузить данные выбранных источников событий в файл с названием event-source-list.csv в кодировке UTF-8.
- **Включить политику** и **Выключить политику** – с помощью этих кнопок для источников событий можно включить или выключить политику мониторинга. При включении требуется выбрать политику в раскрывающемся списке. При выключении требуется указать, на какой период необходимо отключить политику: временно или навсегда.

  Если для выбранного источника событий нет политики, кнопка **Включить политику** будет неактивна. Эта кнопка также будет неактивной в том случае, если выбраны источники из разных тенантов, однако у пользователя нет доступных политик в общем тенанте.

> В редких случаях из-за наложения внутренних процессов KUMA через несколько секунд после выключения политики ее статус может снова измениться с серого на зеленый. В таких случаях необходимо повторно выключить политику мониторинга.

- **Удалить источник событий** – с помощью этой кнопки источники событий можно удалить из таблицы. Статистика по этому источнику также будет удалена. Если данные из источника продолжают поступать в коллектор, источник событий снова появится в таблице, при этом его старая статистика учитываться не будет.

Политики мониторинга

Данные о частоте и количестве поступающих событий являются показателем состояния системы. Например, можно обнаружить, когда поток событий стал аномально большим, слишком слабым или вообще прекратился. Политики мониторинга предназначены для отслеживания таких ситуаций. В политике вы можете задать нижнее пороговое значение, дополнительно задать верхний порог, и каким образом будут считаться события: по частоте или по количеству.

Политику нужно применить к источнику события. После применения политики вы можете отслеживать статус источника: зеленый - все хорошо, и красный - поток вышел за пороговое значение. В случае красного статуса генерируется событие типа Monitoring. Также доступна отправка уведомлений по произвольному адресу электронной почты. Политики мониторинга источников событий отображаются в таблице в разделе **Состояние источников → Политики мониторинга**. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. Если вы нажмете на политику, откроется область данных с параметрами политики. Параметры можно изменить.

Чтобы добавить политику мониторинга:

1. В Консоли KUMA в разделе **Состояние источников → Политики мониторинга** нажмите **Добавить политику** и в открывшемся окне укажите параметры:

   a. В поле **Название политики** введите уникальное имя создаваемой политики. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать политика. От выбора тенанта зависит, для каких источников событий можно будет включить политику мониторинга.

   c. В раскрывающемся списке **Тип политики** выберите один из следующих вариантов:

      - **byCount** – по количеству событий за определенный промежуток времени.

      - **byEPS** – по количеству событий в секунду за определенный промежуток времени. Считается среднее значение за весь промежуток. Можно дополнительно отслеживать скачки в определенные периоды.

   d. В полях **Нижний порог** и **Верхний порог** установите границы, соответствующие нормальному поведению. Отклонения от этих значений активируют политику мониторинга, создают алерты и пересылают уведомления.

   e. В поле **Период подсчета** укажите, за какой период в политике мониторинга должны учитываться данные из источника мониторинга. Максимальное значение: 14 дней.

   f. При необходимости укажите электронные адреса, на которые следует отправить уведомления о срабатывании политики мониторинга KUMA. Для добавления каждого адреса необходимо нажимать на кнопку **Адрес электронной почты**.

      Для рассылки уведомлений необходимо настроить подключение к SMTP-серверу.

2. Нажмите на кнопку **Добавить**.

Политика мониторинга добавлена.

Чтобы удалить политику мониторинга,

Выберите одну или несколько политик, нажмите **Удалить политику** и подтвердите действие.

Невозможно удалить предустановленные политики мониторинга, а также политики, назначенные источникам данных.

Управление активами

Активы представляют собой компьютеры в организации. Вы можете добавить активы в KUMA, тогда KUMA будет автоматически добавлять идентификаторы активов при обогащении событий и при анализе событий вы получите дополнительную информацию о компьютерах в организации.

Вы можете добавить активы в KUMA следующими способами:

- Импортировать активы:
  - Из отчета MaxPatrol.
  - По расписанию: из Kaspersky Security Center и KICS for Networks.

    По умолчанию импорт активов выполняется каждые 12 часов, периодичность можно настроить. Также возможен импорт активов по запросу, при этом выполнение импорта по запросу не повлияет на время импорта по расписанию. KUMA импортирует из базы Kaspersky Security Center сведения об устройствах с установленным Kaspersky Security Center Network Agent, который подключался к Kaspersky Security Center, т.е. поле Connection time в базе SQL — непустое. KUMA импортирует следующую информацию об устройстве: имя, адрес, время подключения к Kaspersky Security Center, информацию об оборудовании и программном обеспечении, включая операционную систему, а также об уязвимостях, то есть информацию, полученную от Агентов администрирования Kaspersky Security Center.
- Создать активы вручную через веб-интерфейс или с помощью API.

  Вы можете добавить активы вручную. При этом необходимо вручную указать следующие данные: адрес, FQDN, название и версия операционной системы, аппаратные характеристики. Добавление информации об уязвимостях активов через веб-интерфейс не предусмотрено. Вы можете указать информацию об уязвимостях, если будете добавлять активы с помощью API.

Вы можете управлять активами KUMA: просматривать информацию об активах, искать активы, добавлять активы, редактировать их и удалять, а также экспортировать данные о них в CSV-файл.

Категории активов

Вы можете разбить активы по категориям и затем использовать категории в условиях фильтров или правил корреляции. Например, можно создавать алерты более высокого уровня важности для активов из более критичной категории. По умолчанию все активы находятся в категории **Активы без категории**. Устройство можно добавить в несколько категорий.

По умолчанию KUMA категориям активов присвоены следующие уровни критичности: Low, Medium, High, Critical. Вы можете создать пользовательские категории и организовать вложенность.

Категории можно наполнять следующими способами:

- **Вручную**
- **Активно**: динамически, если актив **соответствует заданным условиям**. Например, с момента перехода актива на указанную версию ОС или размещения актива в указанной подсети актив будет перемещен в заданную категорию.

1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

   Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять, нажав на кнопку **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
OS.	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
FQDN	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.
ПО	=, like	
КИИ	in	Можно выбрать более одного значения.
Последнее обновление антивирусных баз	>=,<=	
Последнее обновление информации	>=,<=	
Последнее обновление защиты	>=,<=	
Время начала последней сессии	>=,<=	
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Состояние постоянной защиты	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов.	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor.	=	
Видим в сети.	>=,<=	

3. Нажмите на кнопку **Условия проверки**, чтобы убедиться в правильности указанного фильтра. При нажатии на кнопку откроется окно **Активы, найденные по заданным условиям**, содержащее список активов, удовлетворяющих условиям поиска.

- **Реактивно**: при срабатывания корреляционного правила актив будет перемещаться в указанную группу.

В KUMA активы распределены по тенантам и категориям. Активы выстроены в древовидную структуру, где в корне находятся тенанты и от них ветвятся категории активов. Вы можете просмотреть дерево тенантов и категорий в разделе **Активы** → **Все активы** консоли KUMA. Если выбрать узел дерева, в правой части окна отображаются активы, относящиеся к соответствующей категории. Активы из подкатегорий выбранной категории отображаются, если вы укажете, что хотите отображать активы рекурсивно. Вы можете выделить флажками тенанты, активы которых хотите просматривать.

Чтобы вызвать контекстное меню категории, наведите указатель мыши на категорию и нажмите на значок с многоточием, который появится справа от названия категории. В контекстном меню доступны следующие действия:

Действия, доступные в контекстном меню категории

Действие	Описание
Показать активы	Просмотреть активы выбранной категории в правой части окна.
Отображать активы рекурсивно	Просмотреть активы из подкатегорий выбранной категории. Если вы хотите выйти из режима рекурсивного просмотра, выберите категорию для просмотра.
О категории	Просмотреть информации о выбранной категории в области деталей **Информация о категории**, которая отображается в правой части окна веб-интерфейса.
Начать категоризацию	Запустить автоматическую привязку активов к выбранной категории. Доступно для категорий с активным способом категоризации.
Добавить подкатегорию	Добавить подкатегорию к выбранной категории.
Изменить категорию	Изменить выбранную категорию.
Удалить категорию	Удалить выбранную категорию. Удалять можно только категории без активов или подкатегорий. В противном случае опция **Удалить категорию** будет неактивна.
Сделать вкладкой	Отобразить выбранную категорию на отдельной вкладке. Отменить это действие можно, выбрав в контекстном меню нужной категории **Убрать из вкладок**.

Добавление категории активов

Чтобы добавить категорию активов:

1. В Консоли KUMA перейдите в раздел **Активы**.
2. Откройте окно создания категории:
   - Нажмите на кнопку **Добавить категорию**.
   - Если вы хотите создать подкатегорию, в контекстном меню родительской категории выберите **Добавить подкатегорию**.

   В правой части окна консоли отобразится область деталей **Добавить категорию**.
3. Добавьте сведения о категории:
   - В поле **Название** введите название категории. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - В поле **Родительская категория** укажите место категории в дереве категорий:
     a. Нажмите на кнопку .

Откроется окно **Выбор категорий**, в котором отображается дерево категорий. Если вы создаете новую категорию, а не подкатегорию, то в окне может отображаться несколько деревьев категорий активов: по одному для каждого доступного вам тенанта. Выбор тенанта в этом окне невозможно отменить.

b. Выберите родительскую категорию для создаваемой вами категории.

c. Нажмите на кнопку **Сохранить**.

Выбранная категория отобразится в поле **Родительская категория**.

- В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию. Тенанта категории невозможно изменить.
- Назначьте уровень важности категории в раскрывающемся списке **Уровень важности**.
- При необходимости в поле **Описание** добавьте примечание: до 256 символов в кодировке Unicode.

4. В раскрывающемся списке **Способ категоризации** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:

   - **Вручную** – активы можно привязать к категории только вручную.
   - **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

     Активная категория активов

1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

   Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять, нажав на кнопку **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
OS.	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
FQDN	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.
ПО	=, like	
КИИ	in	Можно выбрать более одного значения.
Последнее обновление антивирусных баз	>=,<=	
Последнее обновление информации	>=,<=	
Последнее обновление защиты	>=,<=	
Время начала последней сессии	>=,<=	
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Состояние постоянной защиты	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов.	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor.	=	
Видим в сети.	>=,<=	

3. Нажмите на кнопку **Условия проверки**, чтобы убедиться в правильности указанного фильтра. При нажатии на кнопку откроется окно **Активы, найденные по заданным условиям**, содержащее список активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

5. Нажмите на кнопку **Сохранить**.

Новая категория добавлена в дерево категорий активов.

Настройка таблицы активов

В KUMA можно настроить содержимое и порядок отображения столбцов в таблице активов. Эти параметры хранятся локально на вашем компьютере.

Чтобы настроить параметры отображения таблицы активов:

1. В Консоли KUMA перейдите в раздел **Активы**.
2. В правом верхнем углу таблицы активов нажмите значок .
3. В раскрывшемся списке установите флажки напротив параметров, которые требуется отображать в таблице:
   - **FQDN**
   - **IP-адрес**
   - **Источник актива**
   - **Владелец**
   - **MAC-адрес**
   - **Создан**
   - **Последнее обновление**
   - **Тенант**
   - **Категория КИИ**

   Когда вы устанавливаете флажок, таблица активов обновляется и добавляется новый столбец. При снятии флажка столбец исчезает. Таблицу можно сортировать по некоторым столбцам.
4. Если требуется изменить порядок отображения столбцов, зажмите левую клавишу мыши на названии столбца и перетащите его в нужное место таблицы.

Параметры отображения таблицы активов настроены.

Поиск активов

В KUMA есть два режима поиска активов. Переключение между режимами поиска осуществляется с помощью кнопок в верхней левой части окна:

- – простой поиск по параметрам активов **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец**.
- – сложный поиск активов с помощью фильтрации по условиям и группам условий.

Найденные активы можно выделить, установив напротив них флажки, и экспортировать данные о них в виде CSV-файла.

Простой поиск

Чтобы найти актив:

1. В Консоли KUMA в разделе **Активы** убедитесь, что в верхней левой части окна активна кнопка .

   В верхней части окна отображается поле **Поиск**.

2. Введите поисковый запрос в поле **Поиск** и нажмите **ENTER** или значок .

   В таблице отобразятся активы, у которых параметры **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец** соответствуют критериям поиска.

Сложный поиск

Сложный поиск активов производится с помощью условий фильтрации, которые можно задать в верхней части окна:

- С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия.
- С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**.
- Условия и группы условий можно перетягивать мышкой.
- Условия, группы и фильтры можно удалить, нажав на кнопку .
- Параметры фильтрации можно отобразить в компактно, нажав на кнопку **Свернуть**. В этом случае отображается результирующее поисковое выражение. При нажатии на него условия поиска снова отображаются полностью.
- Параметры фильтрации можно обнулить с помощью кнопки **Очистить**.
- Операторы условий и доступные значения правого операнда зависят от выбранного левого операнда:

Левый операнд	Доступные операторы	Правый операнд
Номер сборки	=, >, >=, <, <=	Произвольное значение.
OS.	=, ilike	Произвольное значение.
IP-адрес	inSubnet, inRange	Произвольное значение или диапазон значений. Условие фильтрации для оператора inSubnet выполнится, если IP-адрес, который содержится в левом операнде входит в подсеть, которая указан в правом операнде. Например, для IP-адреса 10.80.16.206 в правом операнде следует указать подсеть в короткой нотации: `10.80.16.206/25`.
FQDN	=, ilike	Произвольное значение.
CVE	=, in	Произвольное значение.
Источник актива	in	• Kaspersky Security Center • KICS for Networks • Импортирован через API • Создан вручную

ОЗУ	=, >, >=, <, <=	Число.
Количество дисков	=, >, >=, <, <=	Число.
Количество сетевых карт	=, >, >=, <, <=	Число.
Свободных байт на диске	=, >, >=, <, <=	Число.
Последнее обновление антивирусных баз	>=, <=	Дата.
Последнее обновление информации	>=, <=	Дата.
Последнее обновление защиты	>=, <=	Дата.
Время начала последней сессии	>=, <=	Дата.
Расширенный статус KSC	in	• Устройство с установленным Агентом администрирования подключено к сети, но Агент администрирования неактивен. • Приложение установлено, но постоянная защита не работает. • Приложение установлено, но не запущено. • Количество обнаруженных вирусов слишком велико. • Приложение установлено, но статус постоянной защиты отличается от установленного администратором безопасности. • Не установлено приложение безопасности. • Полная проверка на вирусы выполнялась слишком давно. • Антивирусные базы обновлялись слишком давно. • Агент администрирования слишком долго был неактивен. • Устаревшая лицензия. • Количество невылеченных объектов слишком велико. • Требуется перезагрузка. • На устройстве установлено одно или несколько несовместимых приложений. • Устройство имеет одну или несколько уязвимостей. • Последний поиск обновлений операционной системы на устройстве выполнялся слишком давно. • Устройство не имеет надлежащего статуса шифрования. • Параметры мобильного устройства не соответствуют требованиям политики безопасности. • Есть необработанные инциденты. • Статус устройства был предложен управляемым приложением. • На устройстве недостаточно места на диске. Возникают ошибки синхронизации или на диске недостаточно места.
Состояние постоянной защиты	=	• Приостановлена.

		• Запускается. • Выполняется (если приложение безопасности не поддерживает категории состояния Выполняется). • Выполняется с максимальной защитой. • Выполняется с максимальным быстродействием. • Выполняется с рекомендуемыми параметрами. • Выполняется с пользовательскими параметрами. • Возникшая ошибка.
Статус шифрования	=	• На устройстве нет правил шифрования. • Шифрование выполняется. • Шифрование отменено пользователем. • Во время шифрования произошла ошибка. • Все правила шифрования устройства были выполнены. • Шифрование выполняется, устройство должно быть перезагружено. • На устройстве есть зашифрованные файлы без указанных правил шифрования.
Статус защиты от спама	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • В обработке. • Возникшая ошибка. • Не установлено. • Лицензия отсутствует.
Статус антивирусной защиты почтовых серверов.	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • В обработке. • Возникшая ошибка. • Не установлено. • Лицензия отсутствует.
Статус защиты данных от утечек	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается.

		• В обработке. • Возникшая ошибка. • Не установлено. • Лицензия отсутствует.
Идентификатор расширенного статуса KSC	=	• OK. • Предельный. • Требует внимания.
Статус Endpoint Sensor.	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • В обработке. • Возникшая ошибка. • Не установлено. • Лицензия отсутствует.
Видим в сети.	>=, <=	Дата.

Чтобы найти актив:

1. В Консоли KUMA в разделе **Активы** убедитесь, что в верхней левой части окна активна кнопка  .

   В верхней части окна отображается блок настройки фильтрации активов.

2. Задайте параметры фильтрации активов и нажмите на кнопку **Поиск**.

В таблице отобразятся активы, которые соответствуют критериям поиска.

Экспорт данных об активах

Данные об активах, отображаемых в таблице активов, можно экспортировать в виде CSV-файла.

Чтобы экспортировать данные об активах:

1. Настройте таблицу активов.

   В файл записываются только данные, указанные в таблице. Порядок отображения столбцов таблицы активов повторяется в экспортированном файле.

2. Найдите нужные активы и выберите их, установив рядом с ними флажки.

   При необходимости вы можете выбрать сразу все активы в таблице, установив флажок в левой части заголовка таблицы активов.

3. Нажмите на кнопку **Экспортировать в CSV**.

Данные об активах будут записаны в файл assets_<дата экспорта>_<время экспорта>.csv. Файл будет скачан в соответствии с параметрами вашего браузера.

Просмотр информации об активе

Чтобы просмотреть информацию об активе, откройте окно информации об активе одним из следующих способов:

- В Консоли KUMA перейдите в раздел **Активы**, выберите категорию с требуемыми активами и выберите актив.
- В Консоли KUMA перейдите в раздел **События**. Выполните поиск и фильтрацию событий. Выберите требуемое событие и перейдите по ссылке в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.

В окне информации об активе может отображаться следующая информация:

- **Название** – имя актива.

  Активы, импортированные в KUMA, сохраняют имена, которые были заданы для них в источнике. Вы можете изменить эти имена в Консоли KUMA.

- **Тенант** – название тенанта, которому принадлежит актив.
- **Источник актива** – источник информации об активе. Источников может быть несколько. Например, сведения можно добавить в Консоли KUMA или с помощью API, а также импортировать из Kaspersky Security Center, KICS for Networks и отчетов MaxPatrol.

  Добавляя в KUMA сведения об одном и том же активе из нескольких источников, следует учитывать правила слияния данных об активах.

- **Создано** – дата и время добавления актива в KUMA.
- **Последнее обновление** – дата и время изменения информации об активе.
- **Владелец** – владелец актива, если он указан.
- **IP-адрес** – IP-адрес актива (если есть).

  Если в KUMA есть несколько активов с одинаковыми IP-адресами, актив, добавленный позже, возвращается во всех случаях поиска активов по IP-адресу. Если в сети вашей организации допустимо наличие активов с одинаковыми IP-адресами, разработайте и используйте дополнительные атрибуты для идентификации активов. Это может оказаться важным при корреляции.

- **Полное доменное имя** – полностью определенное имя домена актива, если указано.
- **MAC-адрес** – MAC-адрес актива (если есть).
- **Операционная система** – операционная система актива.
- **Связанные алерты** – алерты, с которыми связан актив (если есть).

  Для просмотра списка алертов, с которыми связан актив, можно перейти по ссылке **Найти в алертах**. Откроется вкладка **Алерты** с поисковым выражением, позволяющим отфильтровать все активы с соответствующим идентификатором.

- **Информация о программном обеспечении** и **Информация об оборудовании** – если указаны параметры программного обеспечения и оборудования актива, они отображаются в этом разделе.

- Сведения об уязвимостях актива:

  - **Уязвимости Open Single Management Platform** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

    Вы можете узнать больше об уязвимости, нажав на значок , открывающий портал Kaspersky Threats. Вы также можете обновить список уязвимостей, нажав на ссылку **Обновить** и запросив обновленную информацию из Kaspersky Security Center.

  - **Уязвимости KICS for Networks** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS for Networks.

- Сведения об источниках актива:

  - **Последнее появление в сети** – время последнего получения сведений об активе из Kaspersky Security Center. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

  - **Идентификатор устройства** – идентификатор *Агента администрирования* Kaspersky Security Center, от которого получены сведения об активе. Эта информация доступна для активов, импортированных из Kaspersky Security Center. С помощью этого идентификатора определяется уникальность актива в Kaspersky Security Center.

  - **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks** – данные об экземпляре KICS for Networks, из которого был импортирован актив.

- **Настраиваемые поля** – данные, записанные в настраиваемые поля активов.

- Дополнительные сведения о параметрах защиты актива с установленным приложением Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux:

  - **Идентификатор расширенного статуса OSMP** – статус актива. Может иметь следующие значения:

    - OK.

    - Предельный.

    - Предупреждение.

  - **Расширенный статус OSMP** – информация о состоянии актива. Например, "Антивирусные базы обновлялись слишком давно".

  - **Статус постоянной защиты** – статус приложений "Лаборатории Касперского", установленных на активе. Например: "Выполняется (если антивирусное приложение не поддерживает категории состояния Выполняется)".

  - **Статус шифрования** – информация о шифровании актива. Например, "На устройстве нет правил шифрования".

  - **Статус защиты от спама** – состояние защиты от спама. Например, "Запущена".

  - **Статус антивирусной защиты почтовых серверов** – состояние антивирусной защиты почтовых серверов. Например, "Запущена".

  - **Статус защиты данных от утечек** – состояние защиты данных от утечек. Например, "Запущена".

- **Статус Endpoint Sensor** – состояние защиты данных от утечек. Например, "Запущена".
- **Последнее обновление антивирусных баз** – версия загруженных антивирусных баз.
- **Последнее обновление защиты** – время последнего обновления антивирусных баз.
- **Время начала последней сессии** – время последнего запуска системы.

  Эти сведения отображаются, если актив был импортирован из Kaspersky Security Center.

- **Категории** – категории, к которым относится актив (если есть).
- **КИИ категория** – сведения о том, является ли актив объектом критической информационной инфраструктуры (КИИ).

С помощью кнопки **Реагирование OSMP** вы можете запустить на активе выполнение задачи Kaspersky Security Center, а нажатием на кнопку **Переместить в группу OSMP** – переместить просматриваемый актив между группами администрирования Kaspersky Security Center.

Доступно при интеграции с Kaspersky Security Center.

Добавление активов

Вы можете добавлять информацию об активах следующими способами:

- Вручную.

  Вы можете добавить актив в Консоли KUMA или с помощью API.

- Импортировать активы.

  Вы можете импортировать активы из Kaspersky Security Center, KICS for Networks и отчетов MaxPatrol.

При добавлении активы, уже существующие в KUMA, могут объединяться с добавляемыми активами.

Алгоритм объединения активов:

1. Проверка на уникальность активов в Kaspersky Security Center или KICS for Networks активов:

   - Уникальность актива импортированного из Kaspersky Security Center, проверяется по параметру **Идентификатор устройства**, в котором указан идентификатор *агента администрирования* Kaspersky Security Center. Если идентификаторы у двух активов различаются, активы считаются разными, объединения данных не происходит.
   - Уникальность актива импортированного из KICS for Networks, определяется по комбинации параметров **IP-адрес**, **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks**. Если любой из параметров у двух активов различается, активы считаются разными, объединения данных не происходит.

   Если активы совпадают, алгоритм выполняется далее.

2. Проверка на совпадение значений в полях **IP**, **MAC**, **FQDN**.

Если хотя бы два из указанных полей совпадают, активы объединяются при условии, что другие поля не заполнены.

Возможные варианты совпадений:

- FQDN и IP-адрес активов. Поле **MAC** не заполнено.

  Проверка производится по всему массиву значений IP-адресов. Если IP-адрес актива входит в состав FQDN, значения считаются совпавшими.

- FQDN и MAC-адрес активов. Поле **IP** не заполнено.

  Проверка производится по всему массиву значений MAC-адресов. При полном совпадении хотя бы одного значения массива с FQDN значения считаются совпавшими.

- IP-адрес и MAC-адрес активов. Поле **FQDN** не заполнено.

  Проверка производится по всему массиву значений IP- и MAC-адресов. При полном совпадении хотя бы одного значения в массивах значения считаются совпавшими.

3. Проверка на совпадение хотя бы одного из полей **IP**, **MAC**, **FQDN** при условии, что два других поля не заполнены для одного или обоих активов.

   Активы объединяются, если значения в поле совпадают. Например, если для актива KUMA указаны FQDN и IP-адрес, а для импортируемого актива только IP-адрес с тем же значением, поля считаются совпавшими. В этом случае активы объединяются.

   Для каждого поля проверка производится отдельно и завершается при первом совпадении.

Вы можете посмотреть примеры сравнения полей активов здесь.

Информация об активах может формироваться из разных источников. Если добавляемый актив и актив KUMA содержат данные, полученные из одного и того же источника, эти данные перезаписываются. Например, актив Kaspersky Security Center при импорте в KUMA получил полное доменное имя и информацию о программном обеспечении. При импорте актива из Kaspersky Security Center с аналогичным полным доменным именем эти данные будут перезаписаны при условии, что они указаны для добавляемого актива. Все поля, в которых могут обновляться данные, приведены в таблице Обновляемые данные.

Обновляемые данные

Название поля	Принцип обновления
Name	Выбирается согласно следующему приоритету: • Задано вручную. • Получено из Kaspersky Security Center. • Получено KICS for Networks.
Владелец	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
IP-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, копия дублирующегося адреса удаляется.
FQDN	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks.

	• Задано вручную.
MAC-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, один из дублирующихся адресов удаляется.
Операционная система	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
Уязвимости	Данные активов KUMA дополняются информацией из добавляемых активов. В информации об активе данные группируются по названию источника. Устранение уязвимостей для каждого источника осуществляется отдельно.
Информация о программном обеспечении	Данные из KICS for Networks записываются всегда (при наличии). Для других источников выбирается первое значение согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
Информация об оборудовании	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано через API.

Обновленные данные отображаются в информации об активе. Вы можете просмотреть информацию об активе в Консоли KUMA.

При добавлении новых активов эти данные могут быть перезаписаны. Если данные, из которых сформирована информация об активе, не обновляются из источников более 30 дней, актив удаляется. При следующем добавлении актива из тех же источников создается новый актив.

При изменении в Консоли KUMA активов, информация о которых получена из Kaspersky Security Center или KICS for Networks, вы можете изменить следующие данные актива:

- Название.
- Категория.

Если информация об активе добавлена вручную, при редактировании в Консоли KUMA этих активов вы можете изменить следующие данные актива:

- Название.
- Название тенанта, которому принадлежит актив.
- IP-адрес.
- Полное доменное имя.
- MAC-адрес.
- Владелец.
- Категория.
- Операционная система.

- Информация об оборудовании.

Редактирование данных об активах через REST API недоступно. При импорте из REST API происходит обновление данных по правилам слияния информации об активах, приведенным выше.

Добавление информации об активах в Консоли KUMA

Чтобы добавить актив в Консоли KUMA:

1. В Консоли KUMA перейдите в раздел **Активы** и нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.

2. Введите параметры актива:

   - **Название актива** (обязательно).
   - **Тенант** (обязательно).
   - **IP-адрес** и/или **Полное доменное имя** (обязательно). Вы можете указать несколько FQDN через запятую.
   - **MAC-адрес.**
   - **Владелец.**

3. При необходимости присвойте активу одну или несколько категорий:

   a. Нажмите на кнопку .

   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить активу. С помощью значков и вы можете разворачивать и сворачивать списки категорий.

   c. Нажмите на кнопку **Сохранить**.

   Выбранные категории отобразятся в полях **Категории**.

4. При необходимости добавьте в раздел **Программное обеспечение** сведения об операционной системе актива.

5. При необходимости добавьте в раздел **Информация об оборудовании** сведения об оборудовании актива.

6. Нажмите на кнопку **Добавить**.

Актив создан и отображается в таблице активов в назначенной ему категории или в категории **Активы без категории**.

Импорт информации об активах из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все активы, которые находятся под защитой этого приложения. Вы можете импортировать информацию об активах, защищаемых Kaspersky Security Center, в KUMA. Для этого вам требуется предварительно настроить интеграцию между приложениями.

В KUMA предусмотрены следующие типы импорта активов из OSMP:

- Импорт информации обо всех активах всех Серверов OSMP.
- Импорт информации об активах выбранного Сервера администрирования Kaspersky Security Center.

Импорт информации обо всех активах всех Серверов администрирования Kaspersky Security Center.

1. В Консоли KUMA выберите раздел **Активы**.
2. Нажмите на кнопку **Импортировать активы**.

   Откроется окно **Импорт активов Open Single Management Platform**.
3. В раскрывающемся списке выберите тенант, для которого вы хотите выполнить импорт.

   В этом случае приложение загружает информацию обо всех активах всех Серверов администрирования, для которых настроено подключение к выбранному тенанту.

   Если вы хотите импортировать информацию обо всех активах всех Серверов администрирования для всех тенантов, выберите **Все тенанты**.
4. Нажмите на кнопку **ОК**.

Информация об активах будет импортирована.

Чтобы импортировать информацию об активах одного Сервера администрирования:

1. В Консоли KUMA перейдите в раздел **Параметры → Open Single Management Platform**.

   Откроется окно **Интеграция с Open Single Management Platform по тенантам**.
2. Выберите тенант, для которого вы хотите импортировать активы.

   Откроется окно **Интеграция с Open Single Management Platform**.
3. Нажмите на подключение для требуемого Сервера администрирования Kaspersky Security Center.

   Откроется окно с параметрами этого подключения к Kaspersky Security Center.
4. Выполните одно из следующих действий:

   - Если вы хотите импортировать все активы, подключенные к выбранному Серверу администрирования Kaspersky Security Center, нажмите на кнопку **Импортировать активы**.
   - Если вы хотите импортировать только активы, которые подключены к подчиненному серверу или включены в одну из групп (например, группу Нераспределенные устройства), выполните следующие действия:

     a. Нажмите на кнопку **Загрузить иерархию**.

     b. Установите флажки рядом с именами подчиненных серверов или групп, из которых вы хотите импортировать информацию об активах.

     c. Установите флажок **Импортировать активы из новых групп**, если вы хотите импортировать активы из новых групп.

     Если ни один флажок не установлен, при импорте выгружается информация обо всех активах выбранного Сервера администрирования Kaspersky Security Center.

     d. Нажмите на кнопку **Сохранить**.

e. Нажмите на кнопку **Импортировать активы**.

Информация об активах будет импортирована.

Импорт информации об активах из MaxPatrol

В OSMP можно импортировать сведения об активах из отчетов о результатах сканирования сетевых устройств системы MaxPatrol. Импортированные активы отображаются в группе **Активы**. При необходимости вы можете редактировать параметры активов.

Вы можете импортировать информацию об активе из отчета MaxPatrol или из MaxPatrol VM.

Импорт информации об активах из отчета MaxPatrol

Импорт происходит через API с помощью утилиты maxpatrol-tool на сервере, где установлено Ядро KUMA.

Утилита входит в комплект поставки KUMA и расположена в архиве установщика в директории /kuma-ansible-installer/roles/kuma/files.

Импорт поддерживается из MaxPatrol 8.

Чтобы импортировать данные об активах из отчета MaxPatrol:

1. Сформируйте в MaxPatrol отчет сканирования сетевых активов в формате **XML file** и скопируйте файл отчета на сервер Ядра KUMA. Подробнее о задачах на сканирование и форматах выходных файлов см. в документации MaxPatrol.

   Импорт данных из отчетов в формате **SIEM integration file** не поддерживается. Требуется выбрать формат **XML file**.

2. Создайте файл с токеном для доступа к KUMA REST API. Для удобства рекомендуется разместить его в папке отчета MaxPatrol. Файл не должен содержать ничего, кроме токена.

   Требования к учетным записям, для которых генерируется API-токен:

   - Роль Администратора или Аналитика.
   - Доступ к тенанту, в который будут импортированы активы.
   - Настроены права на использование API-запросов GET /users/whoami и POST /api/v1/assets/import.

     Для импорта активов из MaxPatrol рекомендуется создать отдельного пользователя с минимально необходимым набором прав на использование API-запросов.

3. Скопируйте утилиту maxpatrol-tool на сервер с Ядром KUMA и сделайте файл утилиты исполняемым с помощью команды:

   ```
   chmod +x <путь до файла maxpatrol-tool на сервере с Ядром KUMA>
   ```

4. Запустите утилиту maxpatrol-tool:

```
./maxpatrol-tool --kuma-rest <адрес и порт сервера KUMA REST API> --token <путь и имя файла с API-токеном> --tenant <название тенанта, куда будут помещены активы> <путь и имя файла с отчетом MaxPatrol> --cert <путь к файлу сертификата Ядра KUMA>
```

Пример: `./maxpatrol-tool --kuma-rest example.kuma.com:7223 --token token.txt --tenant Main example.xml --cert /opt/kaspersky/kuma/core/certificates/ca.cert`

Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения полного отчета о полученных активах `--verbose, -v`. Подробное описание доступных флагов и команд приведено в таблице Флаги и команды утилиты maxpatrol-tool. Также для просмотра информации о доступных флагах и командах вы можете использовать команду `--help`.

Информация об активах будет импортирована из отчета MaxPatrol в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

```
Пример:
inserted 2 assets;
updated 1 asset;
errors occurred: []
```

Поведение утилиты при импорте активов:

- KUMA перезаписывает данные импортированных через API активов и удаляет сведения об их устраненных уязвимостях.
- KUMA пропускает активы с недействительными данными. Сведения об ошибках отображаются при использовании флага `--verbose`.
- Если в одном отчете MaxPatrol есть активы с одинаковыми IP-адресами и полными именами домена (FQDN), эти активы объединяются. Сведения об их уязвимостях и программном обеспечении также объединяются в одном активе.

При загрузке активов из MaxPatrol активы с аналогичными IP-адресами и полными именами доменов (FQDN), ранее импортированные из Kaspersky Security Center, перезаписываются.

Чтобы этого избежать, вам требуется настроить фильтрацию активов по диапазону с помощью команды:

`--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`

Активы, соответствующие условиям фильтрации, не загружаются. Описание команды вы можете просмотреть в таблице *Флаги и команды утилиты maxpatrol-tool*.

Флаги и команды утилиты maxpatrol-tool

Флаги и команды	Описание
`--kuma-rest <адрес и порт сервера KUMA REST API>, -a <адрес и порт сервера KUMA REST API>`	Адрес сервера с Ядром KUMA, куда будет производиться импорт активов, с указанием порта. Например, `example.kuma.com:7223`. По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
`--token <путь и имя файла с API-токеном>, -t <путь и имя файла с API-токеном>`	Путь и имя файла, содержащее токен для доступа к REST API. Файл должен содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Администратора или Аналитика.
`--tenant <название тенанта>, -T <название тенанта>`	Название тенанта KUMA, в который будут импортированы активы из отчета MaxPatrol.
`--dns <диапазоны IP-адресов> или -d <диапазоны IP-адресов>`	Используется для обогащения IP-адресов FQDN из указанных диапазонов с помощью DNS, если для этих адресов FQDN не был указан. Пример: `--dns 0.0.0.0-9.255.255.255,11.0.0.0-255.255.255,10.0.0.2`

`--dns-server <IP-адрес DNS-сервера>, -s <IP-адрес DNS-сервера>`	Адрес DNS-сервера, к которому должна обращаться утилита для получения информации о FQDN. Пример: `--dns-server 8.8.8.8`
`--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`	Диапазоны адресов активов, которые при импорте следует пропустить. Пример: `--ignore 8.8.0.0-8.8.255.255, 10.10.0.1`
`--verbose, -v`	Выведение полного отчета о полученных активах и ошибках, возникших в процессе импорта.

`--help, -h`
`help`
	Получение справочной информации об утилите или команде.
	Примеры:
	`./maxpatrol-tool help`
	`./maxpatrol-tool < команда > --help`

`version`	Получение информации о версии утилиты maxpatrol-tool.
`completion`	Создание скрипта автозавершения для указанной оболочки.
`--cert <путь до файла с сертификатом Ядра KUMA>`	Путь к сертификату Ядра KUMA. По умолчанию сертификат располагается в папке с установленным приложением: /opt/kaspersky/kuma/core/certificates/ca.cert.

Примеры:

- `./maxpatrol-tool --kuma-rest example.kuma.com:7223 --token token.txt --tenant Main example.xml --cert /example-directory/ca.cert` – импорт активов в KUMA из отчета MaxPatrol example.xml.
- `./maxpatrol-tool help` – получение справки об утилите.

Возможные ошибки

Сообщение об ошибке	Описание
must provide path to xml file to import assets	Не указан путь к файлу отчета MaxPatrol.
incorrect IP address format	Некорректный формат IP-адреса. Может возникнуть при указании некорректных диапазонов IP.
no tenants match specified name	Для указанного названия тенанта не было найдено подходящих тенантов с помощью REST API.
unexpected number of tenants (%v) match specified name. Tenants are: %v	Из KUMA вернулось больше одного тенанта для указанного названия тенанта.
could not parse file due to error: %w	Ошибка чтения xml-файла с отчетом MaxPatrol.
error decoding token: %w	Ошибка чтения файла с API-токеном.
error when importing files to KUMA: %w	Ошибка передачи сведений об активах в KUMA.
skipped asset with no FQDN and IP address	У одного из активов в отчете не было FQDN и IP-адреса. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid FQDN: %v	У одного из активов в отчете был некорректный FQDN. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid IP address: %v	У одного из активов в отчете был некорректный IP-адрес. Сведения об этом активе не были отправлены в KUMA.
KUMA response: %v	При импорте сведений об активах произошла ошибка с указанным ответом.
unexpected status code %v	При импорте сведений об активах от KUMA был получен неожиданный код HTTP.

Импорт информации об активах из MaxPatrol VM

Дистрибутив OSMP включает утилиту kuma-ptvm, которая состоит из исполняемого файла и конфигурационного файла. Утилита поддерживает операционные системы Windows и Linux. Утилита позволяет подключаться к API MaxPatrol VM для получения данных об устройствах и их атрибутах, включая уязвимости, а также позволяет изменять данные активов и импортировать данные с использованием API OSMP. Импорт данных поддерживается для MaxPatrol VM 1.1.

Настройка импорта информации об активе из MaxPatrol VM в Ядро KUMA включает следующие этапы:

1. Подготовка OSMP и MaxPatrol VM.

   Вам нужно создать учетные записи пользователей и токен OSMP для операций API.

2. Создание конфигурационного файла с параметрами экспорта и импорта данных.

3. Импорт данных активов в Ядро KUMA с использованием утилиты kuma-ptvm:

   a. Данные экспортируются из MaxPatrol VM и сохраняются в директории утилиты. Информация для каждого тенанта сохраняется в отдельный файл в формате JSON.

      При необходимости вы можете изменить полученные файлы.

   b. Информация из файлов импортируется в Ядро KUMA.

При повторном импорте существующих активов, активы, которые уже существуют в Ядре KUMA, перезаписываются. Таким образом, удаляются закрытые уязвимости.

Известные ограничения:

- Если один и тот же IP-адрес указан для двух активов с разными FQDN, Ядро KUMA импортирует такие активы как два разных актива. Эти активы не объединяются.
- Если на активе установлено два приложения с одинаковыми данными в полях названия, версии и поставщика, Ядро KUMA импортирует эти данные как одно приложение, несмотря на разные пути установки приложения на активе.
- Если FQDN актива содержит пробел или подчеркивание (_), данные таких активов не импортируются в Ядро KUMA. В журнале событий будет указано, что активы были пропущены при импорте.
- Если во время импорта происходит ошибка, сведения об ошибке регистрируются и импорт останавливается.

Подготовительные действия:

1. Создайте отдельную учетную запись в OSMP и в MaxPatrol VM с минимально необходимым набором разрешений для использования API запросов.
2. Создайте учетные записи пользователей, для которых вы позже сгенерируете токен API.

   Требования к учетным записям, для которых генерируется API-токен:

   - Главный администратор, Администратор тенанта, Аналитик 2-го уровня или Аналитик 1-го уровня.
   - Доступ к тенанту, в который будут импортированы активы.
   - В учетной записи пользователя, в разделе прав доступа к API, установлен флажок для POST /xdr/api/v2.1/kuma/assets/import.

3. Сгенерировать токен для доступа к XDR REST API.

Чтобы создать конфигурационный файл:

1. Перейдите в папку утилит KUMA:

   ```
   cd /opt/kaspersky/kuma/utils/
   ```

2. Скопируйте шаблон kuma-ptvm-config-template.yaml, чтобы создать конфигурационный файл с именем kuma-ptvm-config.yaml.

   ```
   cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
   ```

3. Измените параметры в конфигурационном файле kuma-ptvm-config.yaml.

4. Сохраните изменения в файле.

Конфигурационный файл будет создан.

Чтобы импортировать информацию об активе:

1. Если вы хотите импортировать информацию об активе из MaxPatrol VM в Ядро KUMA без промежуточной проверки экспортированных данных, запустите утилиту kuma-ptvm со следующими параметрами:

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download --upload`

2. Если вы хотите проверить правильность данных, экспортированных из MaxPatrol VM, перед их импортом в Ядро KUMA:

   a. Запустите утилиту kuma-ptvm со следующими параметрами:

      `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download`

      Для каждого тенанта, указанного в конфигурационном файле, будет создан отдельный файл с именем в формате<tenant ID>.JSON. Также во время экспорта создается файл "tenants", содержащий список файлов JSON для загрузки в Ядро KUMA. Все файлы сохраняются в директории утилиты.

   b. Просмотрите экспортированные файлы активов и при необходимости внесите следующие изменения:

      - Назначьте активы соответствующим тенантам.
      - Вручную перенесите данные активов из файла тенанта "default" в файлы соответствующих тенантов.
      - В файле "tenants" измените список тенантов, активы которых вы хотите импортировать в Ядро KUMA.

   c. Импортируйте информацию об активе в Ядро KUMA:

      `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --upload`

      Чтобы просмотреть информацию о доступных командах утилиты, выполните команду --help.

   Информация об активе импортируется из MaxPatrol VM в Ядро KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

Возможные ошибки:

При запуске утилиты kuma-ptvm может возвращаться ошибка "tls: failed to verify certificate: x509: certificate is valid for localhost".

Чтобы решить проблему:

- Выпустите сертификат в соответствии с документацией MaxPatrol. Это рекомендованный способ решить эту ошибку.
- Выключите проверку сертификата.

  Чтобы выключить проверку сертификата, добавьте следующую строку в конфигурационный файл в разделе Параметры MaxPatrol:

  `ignore_server_cert: true`

В результате утилита запускается без ошибок.

Импорт информации об активах из KICS for Networks

После создания интеграции с KICS for Networks задачи на получение данных об активах KICS for Networks создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную.

Чтобы запустить задачу на обновление данных об активах KICS for Networks для тенанта:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.
3. Нажмите на кнопку **Импортировать активы**.

   В Консоли KUMA в разделе Диспетчер задач добавлена **задача** на получение данных об учетных записях выбранного тенанта.

Примеры сравнения полей активов при импорте

Каждый импортируемый актив сравнивается с активом KUMA.

Проверка на совпадение значений в полях IP, MAC, FQDN по двум полям

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив KUMA	Есть	Есть	Не заполнено
Импортируемый актив 1	Есть, совпадает	Есть, совпадает	Есть
Импортируемый актив 2	Есть, совпадает	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть, совпадает	Не заполнено	Есть

Импортируемый актив 4	Не заполнено	Есть, совпадает	Есть
Импортируемый актив 5	Есть, совпадает	Не заполнено	Не заполнено
Импортируемый актив 6	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и IP, по полю MAC нет противоречия. Активы объединены.
- Импортируемый актив 2 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и IP. Активы объединены.
- Импортируемый актив 3 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и MAC, по полю IP нет противоречия. Активы объединены.
- Импортируемый актив 4 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 5 и актив KUMA: для обоих активов заполнено и совпадает поле FQDN, по полям IP и MAC нет противоречия. Активы объединены.
- Импортируемый актив 6 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.

Проверка на совпадение значений в полях IP, MAC, FQDN по одному полю

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив KUMA	Не заполнено	Есть	Не заполнено
Импортируемый актив 1	Есть	Есть, совпадает	Есть
Импортируемый актив 2	Есть	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 2 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 3 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.
- Импортируемый актив 4 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.

Назначение активу категории

Чтобы назначить категорию одному активу:

1. В Консоли KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив.
4. В открывшемся окне нажмите на кнопку **Изменить**.
5. В поле **Категории** нажмите на кнопку .
6. Выберите категорию.

   Если вы хотите перенести актив в раздел **Активы без категории**, вам требуется удалить существующие для актива категории, нажав на кнопку ×.
7. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Чтобы назначить категорию нескольким активам:

1. В Консоли KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Установите флажки рядом с активами, для которых вы хотите изменить категорию.
4. Нажмите на кнопку **Привязать к категории**.
5. В открывшемся окне выберите категорию.
6. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Не назначайте активам категорию `Categorized assets`.

Изменение параметров активов

В KUMA можно изменять параметры активов. У добавленных вручную активов можно изменять все параметры. У активов, импортированных из Kaspersky Security Center, можно изменить только название актива и его категорию.

Чтобы изменить параметры актива:

1. В Консоли KUMA перейдите в раздел **Активы** и нажмите на актив, который вы хотите удалить.

   В правой части окна откроется область **Информация об активе**.

2. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить актив**.

3. Внесите необходимые изменения в доступные поля:

   - **Название актива** (обязательно). Это единственное поле, доступное для редактирования у активов, импортированных из Kaspersky Security Center или KICS for Networks.
   - **IP-адрес** и/или **Полное доменное имя** (обязательно). Вы можете указать несколько FQDN через запятую.
   - **MAC-адрес.**
   - **Владелец.**
   - **Информация о программном обеспечении**:
     - **Название ОС**
     - **Версия ОС**
   - **Информация об оборудовании**:

     Параметры оборудования

В раздел **Информация об оборудовании** можно добавить сведения об оборудовании актива:

Доступные поля для описания CPU актива:

- **Название процессора**
- **Частота процессора**
- **Количество ядер процессора**

  Активу можно добавить процессоры с помощью ссылки **Добавить процессор**.

Доступные поля для описания диска актива:

- **Свободных байт на диске**
- **Объем диска**

  Активу можно добавить диски с помощью ссылки **Добавить диск**.

Доступные поля для описания RAM актива:

- **Частота оперативной памяти**
- **Общий объем ОЗУ**

Доступные поля для описания сетевой карты актива:

- **Название сетевой карты**
- **Производитель сетевой карты**
- **Версия драйвера сетевой карты**

  Активу можно добавить сетевые карты с помощью ссылки **Добавить сетевую карту**.

- Настраиваемые поля.
- Категория КИИ.

4. Назначьте или измените активу категорию:

   a. Нажмите на кнопку .
   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить активу.

   c. Нажмите на кнопку **Сохранить**.

Выбранные категории отобразятся в полях **Категории**.

Кроме того, можно выбрать актив и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий актива.

Не назначайте активам категорию `Categorized assets`.

5. Нажмите на кнопку **Сохранить**.

Параметры актива изменены.

Архивирование активов

В KUMA функция архивирования доступна для следующих типов активов:

- Для активов, импортированных из Kaspersky Security Center и KICS.

  Если KUMA не получила информацию об активе в момент импорта, актив автоматически переводится в состояние архивного и хранится в базе данных в течение срока, который вы можете задать в параметре **Срок хранения архивных активов**. Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно Архивный актив станет активным, если KUMA получит информацию об активе от источника до истечения срока хранения архивных активов.

- Для объединенных активов.

  При импорте KUMA выполняет проверку на уникальность среди активов, импортированных из Kaspersky Security Center и KICS, и активов, добавленных вручную. Если поля импортированного актива и добавленного вручную актива совпадают, активы объединяются в один актив, который считается импортированным и может стать архивным.

Активы, добавленные вручную в веб-интерфейсе или с помощью API, не архивируются.

Актив становится архивным при следующих условиях:

- KUMA не получила информацию об активе от Kaspersky Security Center или KICS for Networks.
- Отключена интеграция с Kaspersky Security Center.

  Если вы отключили интеграцию с Kaspersky Security Center, в течение 30 дней актив будет считаться активным. По истечении 30 дней актив автоматически переводится в состояние архивного и хранится в базе данных в течение времени, указанного в параметре **Срок хранения архивных активов**.

Обновление актива не происходит в следующих случаях:

- Данные об активе Kaspersky Security Center не обновлялись больше срока хранения архивных активов.
- Данные об активе отсутствуют в Kaspersky Security Center или KICS for Networks.
- Соединение с Сервером администрирования Kaspersky Security Center отсутствует больше 30 дней.

Чтобы настроить срок хранения архивных активов:

1. В Консоли KUMA выберите раздел **Параметры** → **Активы**.

   Отобразится окно **Активы**.

2. Введите в поле **Срок хранения архивных активов** желаемое значение.

Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно

3. Нажмите на кнопку **Сохранить**.

Срок хранения архивных активов будет настроен.

Информация об архивном активе остается доступной для просмотра в карточке алертов и инцидентов.

Чтобы просмотреть карточку архивного актива:

1. В Консоли KUMA выберите раздел **Алерты** или **Инциденты**.

   Отобразится список алертов или инцидентов.

2. Откройте карточку алерта или инцидента, связанного с архивным активом.

   Вам будет доступен просмотр информации в карточке архивного актива.

Удаление активов

Если вам больше не нужно получать информацию от актива или информация об активе долгое время не обновлялась, в KUMA есть возможность удаления активов. Возможность удаления доступна для всех ролей, кроме аналитика первого уровня. Если после удаления актива в KUMA сведения о нем начнут поступать из Kaspersky Security Center, KUMA создаст актив с новым идентификатором.

В KUMA доступны следующие способы удаления активов:

- Автоматически.

  KUMA автоматически удаляет только архивные активы. KUMA удалит архивный актив, если информация об активе не обновлялась больше срока хранения архивных активов.

- Вручную.

Чтобы удалить актив вручную:

1. В Консоли KUMA выберите раздел **Активы** и нажмите на актив, который вы хотите удалить.

   В правой части консоли откроется окно **Информация об активе**.

2. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

3. Нажмите на кнопку **ОК**.

Актив будет удален и больше не будет отображаться в карточке алерта или в карточке инцидента.

Обновление приложений сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center

Вы можете обновлять приложения сторонних производителей, в том числе приложения Microsoft, установленные на активах Kaspersky Security Center, и закрывать уязвимости этих приложений.

Предварительно вам нужно создать задачу *Установка требуемых обновлений и закрытие уязвимостей* на выбранном сервере Администрирования Kaspersky Security Center со следующими параметрами:

- Приложение – Kaspersky Security Center.
- Тип задачи – *Установка требуемых обновлений и закрытие уязвимостей*.
- Устройства, которым будет назначена задача – вам требуется назначить задачу корневой группе администрирования.
- Правила для установки обновлений:
  - Устанавливать только утвержденные обновления.
  - Закрывать уязвимости с уровнем критичности равным или выше (необязательный параметр).

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (*Средний*, *Высокий* или *Предельный*). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.
- Запуск по расписанию – расписание, в соответствии с которым выполняется задача.

О способах создания задачи см. подробнее в *справке Kaspersky Security Center*.

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Далее вам требуется установить обновления для приложений сторонних производителей и закрыть уязвимости на активах в KUMA.

Чтобы установить обновления и закрыть уязвимости приложений сторонних производителей на активе в KUMA:

1. Откройте окно информации об активе одним из следующих способов:
   - В Консоли KUMA перейдите в раздел **Активы**, выберите категорию с требуемыми активами и выберите актив.
   - В Консоли KUMA выберите раздел **События**. Выполните поиск и фильтрацию событий. Выберите требуемое событие и перейдите по ссылке в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.
2. В окне информации об активе раскройте список **Уязвимости Kaspersky Security Center**.
3. Установите флажки рядом с приложениями, которые вы хотите обновить.
4. Нажмите на ссылку **Загрузить обновления**.
5. В открывшемся окне установите флажок рядом с идентификатором уязвимости, которую вы хотите закрыть.
6. Если в столбце **Лицензионное соглашение принято** для выбранного идентификатора отображается **Нет**, нажмите на кнопку **Принять обновления**.

7. Перейдите по ссылке в столбце **URL Лицензионного соглашения** и ознакомьтесь с текстом Лицензионного соглашения.

8. Если вы с ним согласны, в Консоли KUMA нажмите на кнопку **Принять Лицензионные соглашения**.

   Напротив идентификатора уязвимости, для которого было принято Лицензионное соглашение, в столбце **Лицензионные соглашения приняты** отобразится **Да**.

9. Повторите шаги 7–10 для каждого требуемого идентификатора уязвимости.

10. Нажмите на кнопку **OK**.

Обновления будут загружены и установлены на активы, того сервера Администрирования, где была запущена задача, а также на активы всех подчиненные серверы Администрирования.

> Условия Лицензионного соглашения для обновления и закрытия уязвимостей требуется принять на каждом подчиненном сервере Администрирования отдельно.

Обновления устанавливаются на активы, на которых была обнаружена уязвимость.

Вы можете обновить список уязвимостей для актива в окне информации об активе, нажав на ссылку **Обновить**.

Перемещение активов в выбранную группу администрирования

Вы можете перемещать активы в выбранную группу администрирования Kaspersky Security Center. В этом случае на активы будут распространятся групповые политики и задачи. Подробнее о политиках и задачах Kaspersky Security Center см. *справку Kaspersky Security Center*.

Группы администрирования добавляются в KUMA при загрузке иерархии во время импорта активов из Kaspersky Security Center. Предварительно вам требуется настроить интеграцию KUMA с Kaspersky Security Center.

Чтобы переместить один актив в выбранную группу администрирования:

1. Откройте окно информации об активе одним из следующих способов:

   - В Консоли KUMA перейдите в раздел **Активы**, выберите категорию с требуемыми активами и выберите актив.

   - В Консоли KUMA перейдите в раздел **Алерты**, перейдите по ссылке с нужным алертом и в разделе **Связанные активы** выберите актив.

2. В окне информации об активе нажмите на кнопку **Переместить в группу KSC**.

3. Нажмите на кнопку **Переместить в группу KSC**.

4. В открывшемся окне выберите группу.

   > Выбранная группа должна принадлежать тому же тенанту, которому принадлежит актив.

5. Нажмите на кнопку **Сохранить**.

Выбранный актив будет перемещен.

Чтобы переместить несколько активов в выбранную группу администрирования:

1. В Консоли KUMA выберите раздел **Активы**.
2. Выберите категорию с требуемыми активами.
3. Установите флажки рядом с активами, которые хотите переместить в группу.
4. Нажмите на кнопку **Переместить в группу KSC**.

   Кнопка активна, если все выбранные активы принадлежат одному серверу Администрирования.

5. В открывшемся окне выберите группу.
6. Нажмите на кнопку **Сохранить**.

   Выбранные активы будут перемещены.

Вы можете посмотреть, к какой группе принадлежит актив, в информации об активе.

Сведения об активах Kaspersky Security Center обновляются в KUMA в момент импорта информации об активах из Kaspersky Security Center. Это означает, что может возникнуть ситуация, когда в Kaspersky Security Center активы были перемещены между группами администрирования, однако в KUMA эти сведения еще не отображаются. При попытке переместить такой актив в группу администрирования, в которой он уже находится, KUMA возвращает ошибку **Не удалось переместить активы в другую группу KSC**.

Аудит активов

В KUMA можно настроить создание событий аудита активов при следующих условиях:

- Актив добавлен в KUMA. Отслеживается создание актива вручную, а также создание при импорте через REST API, импорте из Kaspersky Security Center или KICS for Networks.
- Параметры актива изменены. Отслеживается изменение значение следующих полей актива:
  - Name
  - IP-адрес
  - MAC-адрес
  - FQDN
  - Операционная система

  Изменения полей может происходить при обновлении актива во время импорта.

- Актив удален из KUMA. Отслеживается удаление активов вручную, а также автоматическое удаление активов, импортированных из Kaspersky Security Center и KICS for Networks, данные о которых перестали поступать.

- Сведения об уязвимости добавлены в актив. Отслеживается появление у активов новых данных об уязвимостях. Сведения об уязвимостях могут быть добавлены в актив, например, при импорте активов из Kaspersky Security Center или KICS for Networks.

- Уязвимость актива закрыта. Отслеживается удаление из актива сведений об уязвимости. Уязвимость считается закрытой, если данные о ней перестают поступать из всех источников, из которых ранее были получены сведения о ее появлении.

- Актив добавлен в категорию. Отслеживается присвоении активу категории активов.

- Актив удален из категории. Отслеживается удаление актива из категории активов.

По умолчанию, если аудит активов включен, при описанных выше условиях KUMA создает не только события аудита (`Type = 4`), но и базовые события (`Type = 1`).

События аудита активов можно отправлять, например, на хранение или в коррелляторы.

Настройка аудита активов

Чтобы настроить аудит активов:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Аудит активов**.

2. Выполните одно из действий с тенантом, для которого вы хотите настроить аудит активов:

   - Добавьте тенант с помощью кнопки **Добавить тенант**, если аудит активов для требуемого тенанта настраивается впервые.

     В открывшемся окне **Аудит активов** выберите имя для нового тенанта.

   - Выберите существующий тенант в таблице, если аудит активов для требуемого тенанта уже был настроен.

     В открывшемся окне **Аудит активов** имя тенанта уже задано и редактировать его нельзя.

   - Клонируйте настройки существующего тенанта, чтобы создать копию конфигурации условий для тенанта, для которого вы хотите настроить аудит активов впервые. Для этого установите флажок напротив тенанта, конфигурацию которого требуется копировать, и нажмите **Клонировать**. В открывшемся окне **Аудит активов** выберите имя тенанта, в котором будет использована конфигурация исходного тенанта.

3. Выберите для каждого условия создания событий аудита активов, куда будут отправляться создаваемые события:

   a. В блоке параметров нужного типа событий аудита активов в раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, куда следует отправлять создаваемые события:

      - Выберите **Хранилище**, если хотите, чтобы события отправлялись в хранилище.

      - Выберите **Коррелятор**, если хотите, чтобы события отправлялись в коррелятор.

      - Выберите **Другое**, если хотите выбрать иную точку назначения.

К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

Откроется окно **Добавить точку назначения**, где вам требуется параметры пересылки событий.

b. В раскрывающемся списке **Точка назначения** выберите существующую точку назначения или выберите пункт **Создать**, если хотите создать новую точку назначения.

При создании новой точки назначения заполните параметры, как указано в описании точки назначения.

c. Нажмите на кнопку **Сохранить**.

Точка назначения добавлена к условию создания событий аудита активов. Для каждого условия можно добавить несколько точек назначения.

4. Нажмите на кнопку **Сохранить**.

Аудит активов настроен. События аудита активов будут создаваться для тех условий, для которых были добавлены точки назначения. Нажмите на кнопку **Сохранить**.

Хранение и поиск событий аудита активов

События аудита активов считаются базовыми и не заменяют собой событий аудита. События аудита активов можно искать по следующим параметрам:

Поле события	Значение
DeviceVendor	`"Лаборатория Касперского".`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

Включение и выключение аудита активов

Можно включить или выключить аудит активов для тенанта:

Чтобы включить или выключить аудит активов для тенанта:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Аудит активов** и выберите тенант, для которого вы хотите включить или выключить аудит активов.

Откроется окно **Аудит активов**.

2. Установите или снимите в верхней части окна флажок **Выключено**.

3. Нажмите на кнопку **Сохранить**.

По умолчанию при включенном аудите активов в KUMA при возникновении условия аудита одновременно создаются два типа событий: базовое событие и событие аудита.

Вы можете отключить создание базовых событий одновременно с событиями аудита.

Чтобы включить или выключить для отдельного условия создание базовых событий:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Аудит активов** и выберите тенант, для которого вы хотите включить или выключить условие создания событий аудита активов.

   Откроется окно **Аудит активов**.

2. Установите или снимите напротив нужных условий флажок **Выключено**.

3. Нажмите на кнопку **Сохранить**.

Для условий с установленным флажком **Выключено** будут создаваться только события аудита, а базовые события создаваться не будут.

Настраиваемые поля активов

В дополнение к существующим полям модели данных актива можно создать настраиваемые поля активов. Данные из настраиваемых полей активов отображаются при просмотре информации об активе. Данные в настраиваемые поля можно записывать вручную или через API.

Вы можете создать или изменить настраиваемые поля в Консоли KUMA в разделе **Параметры** → **Активы** в таблице **Настраиваемые поля**. Таблица имеет следующие столбцы:

- **Название** – название настраиваемого поля, которое отображается при просмотре информации об активе.
- **Значение по умолчанию** – значение, которое записывается в настраиваемое поле при добавлении актива в KUMA.
- **Маска** – регулярное выражение, которому должно соответствовать значение, записываемое в поле.

Чтобы создать настраиваемое поле активов:

1. В разделе Консоли KUMA **Параметры** → **Активы** нажмите на кнопку **Добавить поле**.

   В таблице **Настраиваемые поля** добавится пустая строка. Вы можете добавить сразу несколько строк с параметрами настраиваемого поля.

2. Заполните столбцы с параметрами настраиваемого поля:

   - **Название** (обязательно) – от 1 до 128 символов в кодировке Unicode.
   - **Значение по умолчанию** – от 1 до 1024 символов в кодировке Unicode.
   - **Маска** – от 1 до 1024 символов в кодировке Unicode.

3. Нажмите на кнопку **Сохранить**.

К модели данных активов добавлено настраиваемое поле.

Чтобы удалить или изменить настраиваемое поле активов:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Активы**.

2. Сделайте необходимые изменения в таблице **Настраиваемые поля**:

   - Вы можете удалить настраиваемые поля, нажав на значок ✕ напротив строки с параметрами нужного поля. При удалении поля также удаляются записанные в это поле данные для всех активов.

- Вы можете изменить значения параметров полей. При изменении значения по умолчанию уже записанные в поля активов данные не меняются.
- Измените порядок отображения полей, перетягивая строки мышью за значок ⣿.

3. Нажмите на кнопку **Сохранить**.

Изменения внесены.

Активы критической информационной инфраструктуры

В KUMA можно помечать активы, относящиеся к критической информационной инфраструктуре (КИИ) Российской Федерации. Это позволяет ограничивать возможности пользователей KUMA по обращению с алертами и инцидентами, к которым относятся активы, относящиеся к объектам КИИ.

Присваивать активам КИИ-категорию можно, если в KUMA действует лицензия с модулем ГосСОПКА.

Присвоить активу КИИ-категорию могут Главные администраторы, а также пользователи, в профиле которых установлен флажок **Доступ к объектам КИИ**. Если ни одно из этих условий не выполнено, для пользователя действуют следующие ограничения:

- Не отображается блок параметров **Категория КИИ** в окнах **Информация об активе** и **Изменить актив**. Невозможно просмотреть или изменить КИИ-категорию актива.
- Не доступны для просмотра алерты и инциденты, к которым относятся активы с КИИ категорией. Над такими алертами и инцидентами невозможно производить никакие операции, в таблице алертов и инцидентов они не отображаются.
- Не отображается столбец **CII** в таблицах алертов и инцидентов.
- Недоступны операции поиска и закрытия алертов через REST API.

Категория КИИ актива отображается в окне **Информация об активе** в блоке параметров **Категория КИИ.**

Чтобы изменить КИИ-категорию актива:

1. В Консоли KUMA в разделе **Активы** выберите нужный актив.

   Откроется окно **Информация об активе**.

2. Нажмите на кнопку **Изменить** и в раскрывающемся списке выберите одно из доступных значений:

   - **Информационный ресурс не является объектом КИИ** – значение по умолчанию, которое означает, что у актива нет категории КИИ. С таким активом, а также с алертами и инцидентами, к которым относится этот актив, могут взаимодействовать пользователи, у которых в профиле не установлен флажок **Доступ к объектам КИИ**.
   - **Объект КИИ без категории значимости**.
   - **Объект КИИ третьей категории значимости**.
   - **Объект КИИ второй категории значимости**.
   - **Объект КИИ первой категории значимости**.

3. Нажмите на кнопку **Сохранить**.

Интеграция с другими решениями

В этом разделе описано, как интегрировать KUMA с другими приложениями для расширения возможностей приложения.

Интеграция с Kaspersky Security Center

Вы можете создавать или изменять параметры интеграции Kaspersky Security Center в Консоли OSMP.

В Консоли KUMA вы можете просмотреть интеграцию с выбранными Серверами администрирования Kaspersky Security Center для одного, нескольких или всех тенантов KUMA. Если включена интеграция с Kaspersky Security Center, вы можете вручную импортировать активы, изменить интервал автоматического импорта по расписанию, просмотреть иерархию Серверов администрирования Kaspersky Security Center или временно выключить импорт по расписанию.

Настройка интервала обновления данных для активов Kaspersky Security Center

Чтобы настроить интервал обновления данных об активе из Kaspersky Security Center:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center**.

2. В раскрывающемся списке **Тенант** выберите тенант, для которого вы хотите настроить обновление параметров.

3. В поле **Период обновления данных в часах** укажите период времени, по истечении которого KUMA обновляет данные об устройствах Kaspersky Security Center.

   Интервал указывается в часах и должен быть целым числом.

   По умолчанию временной интервал составляет 12 часов.

4. Нажмите на кнопку **Сохранить**.

Параметры обновления данных активов Kaspersky Security Center для выбранного тенанта настроены.

Если нужный тенант отсутствует в списке тенантов, используйте Консоль OSMP, чтобы добавить его в список тенантов.

Расписание импорта активов Kaspersky Security Center

Чтобы настроить расписание импорта активов Kaspersky Security Center:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center**.

2. Выберите тенант, для которого вы хотите запланировать импорт активов Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. При необходимости снимите флажок **Выключено**, чтобы включить интеграцию с Kaspersky Security Center для выбранного тенанта. По умолчанию флажок снят.

   Если вы хотите временно выключить интеграцию с Kaspersky Security Center для выбранного тенанта, установите флажок **Выключено**. Импорт активов Kaspersky Security Center по расписанию выключен.

4. В поле **Период обновления данных** укажите период времени, по истечении которого KUMA обновляет данные об устройствах Kaspersky Security Center.

   Интервал указывается в часах и должен быть целым числом.

   По умолчанию временной интервал составляет 12 часов.

5. Нажмите на кнопку **Сохранить**.

Указанные параметры для импорта активов Kaspersky Security Center по расписанию для выбранного тенанта применены.

Ручной импорт активов Kaspersky Security Center

Чтобы вручную импортировать активы Kaspersky Security Center:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center**.

2. В раскрывающемся списке **Тенант** выберите тенант, для которого вы хотите вручную импортировать активы Kaspersky Security Center.

   Откроется окно **Параметры подключения**.

3. В окне Параметры подключения:

   a. Для флажка **Выключено** выполните одно из следующих действий:

   - Снимите флажок, если вы хотите включить интеграцию с Kaspersky Security Center для выбранного тенанта.
   - Установите флажок, если вы хотите выключить интеграцию с Kaspersky Security Center для выбранного тенанта.

     По умолчанию флажок снят.

   b. Если вы хотите импортировать активы из групп, созданных в Kaspersky Security Center, установите флажок **Импортировать активы из новых групп**.

4. Нажмите **Импортировать активы Kaspersky Security Center**.

5. Нажмите на кнопку **Сохранить**.

Активы Kaspersky Security Center для указанного тенанта импортируются независимо от настроенного расписания.

Просмотр иерархии Серверов администрирования Kaspersky Security Center

Чтобы просмотреть иерархию Серверов администрирования Kaspersky Security Center:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center**.

2. В раскрывающемся списке **Тенант** выберите тенант, для которого вы хотите просмотреть иерархию.

   Откроется окно **Параметры подключения**.

3. В окне **Параметры подключения** нажмите **Загрузить иерархию**.

Иерархия Серверов администрирования Kaspersky Security Center для указанного тенанта отображается в окне **Параметры подключения**.

Импорт событий из базы Kaspersky Security Center

В KUMA можно получать события из SQL-базы Kaspersky Security Center. Получение событий производится с помощью коллектора, в котором используются следующие ресурсы:

- Предустановленный коннектор [OOTB] KSC MSSQL или [OOTB] KSC MySQL.
- Предустановленный нормализатор [OOTB] KSC from SQL.

Настройка импорта событий из Kaspersky Security Center состоит из следующих шагов:

1. Создание копии предустановленного коннектора.

   Параметры предустановленного коннектора недоступны для редактирования, поэтому для настройки параметров подключения к серверу базы данных требуется создать копию предустановленного коннектора.

2. Создание коллектора:

   - В веб-интерфейсе.
   - На сервере.

Чтобы настроить импорт событий из Kaspersky Security Center:

1. Создайте копию предустановленного коннектора, соответствующего типу базы данных Kaspersky Security Center:

   a. В Консоли KUMA в разделе **Ресурсы** → **Коннекторы** найдите в структуре папок нужный предустановленный коннектор, установите флажок рядом с этим коннектором и нажмите **Дублировать**.

   b. В открывшемся окне **Создание коннектора** на вкладке **Основные параметры** в поле **Запрос по умолчанию** при необходимости замените имя базы данных KAV на имя используемой вами базы данных Kaspersky Security Center.

   Пример запроса к SQL-базе Kaspersky Security Center

```
SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

ev.product_name AS product_name, ev.product_version AS product_version,

ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As
msg,

CASE

WHEN ev.rise_time is not NULL THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time )

ELSE ev.rise_time

END

AS endTime,

CASE

WHEN ev.registration_time is not NULL

THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )

ELSE ev.registration_time

END

AS kscRegistrationTime,

cast(ev.par7 as varchar(4000)) as sourceUserName,

hs.wstrWinName as dHost,

hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,

CAST(hs.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp % 256 AS VARCHAR) AS sourceAddress,

serv.wstrWinDomain as kscNtDomain,

CAST(serv.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp % 256 AS VARCHAR) AS kscIP,

CASE
```

```
WHEN virus.tmVirusFoundTime is not NULL

THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )

ELSE ev.registration_time

END

AS virusTime,

virus.wstrObject As filePath,

virus.wstrVirusName as virusName,

virus.result_ev as result

FROM KAV.dbo.ev_event as ev

LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId

INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1

Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus

where registration_time >= DATEADD(minute, -191, GetDate())
```

c. Установите курсор в поле **URL** и в раскрывшемся списке в строке используемого секрета нажмите на значок .

d. В открывшемся окне **Секрет** в поле **URL** укажите адрес для подключения к серверу в следующем формате:

`sqlserver://user:password@kscdb.example.com:1433/database`

где

- `user` – учетная запись с правами public и db_datareader к нужной базе данных;
- `password` – пароль учетной записи;
- `kscdb.example.com:1433` – адрес и порт сервера базы данных;
- `database` – название базы данных Kaspersky Security Center. По умолчанию – KAV.

Нажмите на кнопку **Сохранить**.

e. В окне **Создание коннектора** в разделе **Подключение** в поле **Запрос** при необходимости замените имя базы данных KAV на имя используемой вами базы данных Kaspersky Security Center.

Это действие нужно выполнять, если вы планируете использовать столбец идентификатора, к которому относится запрос.

Нажмите на кнопку **Сохранить**.

2. Установите коллектор в веб-интерфейсе:

a. Запустите мастер установки коллектора одним из следующих способов:

- В Консоли KUMA в разделе **Ресурсы** нажмите на кнопку **Подключить источник**.
- В Консоли KUMA в разделе **Ресурсы** → **Коллекторы** нажмите на кнопку **Добавить коллектор**.

b. На шаге 1 **Подключение источников** в мастере установки укажите название коллектора и выберите тенант.

c. На шаге 2 **Транспорт** в мастере установки выберите созданную на шаге 1 копию коннектора.

d. На шаге 3 **Парсинг событий** в мастере установки на вкладке **Схемы парсинга** нажмите **Добавить парсинг событий**.

e. В открывшемся окне **Основной парсинг событий** на вкладке **Схема нормализации** в раскрывающемся списке **Нормализатор** выберите **[OOTB] KSC from SQL** и нажмите **OK**.

f. При необходимости укажите остальные параметры в соответствии с вашими требованиями к коллектору. Для импорта событий настройка параметров на остальных шагах мастера установки не обязательна.

g. На шаге 8 **Проверка параметров** в мастере установки нажмите **Создать и сохранить сервис**.

В нижней части окна отобразится команда, которая понадобится для установки коллектора на сервере. Скопируйте эту команду.

h. Закройте мастер установки коллектора, нажав **Сохранить коллектор**.

3. Установите коллектор на сервере.

Для этого на сервере, предназначенном для получения событий Kaspersky Security Center, выполните команду, скопированную после создания коллектора в веб-интерфейсе.

В результате коллектор будет установлен и сможет принимать события из SQL-базы Kaspersky Security Center.

Вы можете просмотреть события Kaspersky Security Center в разделе веб-интерфейса **События**.

Интеграция с Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response (далее также KEDR) – функциональный блок приложения Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту активов локальной сети организации.

Вы можете настроить интеграцию KUMA с Kaspersky Endpoint Detection and Response, чтобы управлять действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response, и активах Kaspersky Security Center. Команды для выполнения операций принимаются сервером Kaspersky Endpoint Detection and Response, который затем передает эти команды Kaspersky Endpoint Agent, установленному на активах.

Также вы можете импортировать события в KUMA и получать информацию об алертах Kaspersky Endpoint Detection and Response (подробнее о получении деталях алертах см. в разделе *Настройка интеграции с SIEM-системой* в справке Kaspersky Anti Targeted Attack Platform).

При интеграции KUMA с Kaspersky Endpoint Detection and Response вы можете выполнять следующие операции на активах Kaspersky Endpoint Detection and Response с Kaspersky Endpoint Agent:

- Управлять сетевой изоляцией активов.

- Управлять правилами запрета.
- Запускать приложения.

За инструкцией по настройке интеграции для управления действиями по реагированию вам требуется обратиться к вашему аккаунт-менеджеру или в службу технической поддержки.

Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kafka

При импорте событий из Kaspersky Endpoint Detection and Response телеметрия передается открытым текстом и может быть перехвачена злоумышленником.

Вы можете импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.0, 4.1, 5.0 и 5.1 с помощью коннектора Kafka.

При импорте событий из Kaspersky Endpoint Detection and Response 4.0 и 4.1 действует ряд ограничений:

- Импорт событий доступен, если в приложении Kaspersky Endpoint Detection and Response используются лицензионные ключи KATA и KEDR.
- Импорт событий **не** доступен, если в составе приложения Kaspersky Endpoint Detection and Response используется компонент Sensor, установленный на отдельном сервере.

Для импорта событий вам потребуется выполнить действия на стороне Kaspersky Endpoint Detection and Response и на стороне KUMA.

Импорт событий Kaspersky Endpoint Detection and Response 4.0 или 4.1

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.0 или 4.1, выполните следующие действия:

На стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.

   Отобразится меню администратора компонента приложения.
3. В меню администратора компонента приложения выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. Выполните следующую команду:

```
sudo -i
```

7. В конфигурационном файле `/etc/sysconfig/apt-services` в поле `KAFKA_PORTS` удалите значение `10000`.

   Если к серверу Central Node подключены серверы Secondary Central Node или компонент Sensor, установленный на отдельном сервере, вам требуется разрешить соединение с сервером, на котором вы изменили конфигурационный файл, по порту 10000.

   Мы не рекомендуем использовать этот порт для каких-либо внешних подключений, кроме KUMA. Чтобы ограничить подключение по порту 10000 только для KUMA, выполните команду:

   ```
   iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP
   ```

8. В конфигурационном файле `/usr/bin/apt-start-sedr-iptables` в поле `WEB_PORTS` добавьте значение `10000` через запятую без пробела.

9. Выполните следующую команду:

   ```
   sudo sh /usr/bin/apt-start-sedr-iptables
   ```

Подготовка к экспорту событий на стороне Kaspersky Endpoint Detection and Response будет завершена.

На стороне KUMA:

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> centralnode` в один из следующих файлов:

   - `%WINDIR%\System32\drivers\etc\hosts` – для Windows.
   - `/etc/hosts file` – для Linux.

2. В Консоли KUMA создайте коннектор типа Kafka.

   При создании коннектора укажите следующие параметры:

   - В поле **URL** укажите `<IP-адрес сервера Central Node>:10000`.
   - В поле **Topic** укажите `EndpointEnrichedEventsTopic`.
   - В поле **Consumer group** укажите любое уникальное имя.

3. В Консоли KUMA создайте коллектор.

   В качестве транспорта для коллектора используйте коннектор, созданный на предыдущем шаге. В качестве нормализатора для коллектора используйте [OOTB] KEDR telemetry.

При успешном завершении создания и установки коллектора события Kaspersky Endpoint Detection and Response будут импортированы в KUMA. Вы можете найти и просмотреть эти события в таблице событий.

Импорт событий Kaspersky Endpoint Detection and Response 5.0 и 5.1

При импорте событий из Kaspersky Endpoint Detection and Response 5.0 и 5.1 действует ряд ограничений:

- Импорт событий доступен только для не высоко доступной версии Kaspersky Endpoint Detection and Response.
- Импорт событий доступен, если в приложении Kaspersky Endpoint Detection and Response используются лицензионные ключи KATA и KEDR.
- Импорт событий **не** доступен, если в составе приложения Kaspersky Endpoint Detection and Response используется компонент Sensor, установленный на отдельном сервере.

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 5.0 или 5.1, выполните следующие действия:

На стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.

   Отобразится меню администратора компонента приложения.
3. В меню администратора компонента приложения выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. В конфигурационном файле `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.py` укажите дополнительный порт `10000` для константы `WEB_PORTS`:

   ```
   WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
   ```

   ```
   Для версии Kaspersky Endpoint Detection and Response 5.1 этот шаг выполнять не нужно, порт указан по умолчанию.
   ```
7. Выполните следующие команды:

   ```
   kata-firewall stop
   ```

   ```
   kata-firewall start --cluster-subnet <маска сети для адресации серверов кластера>
   ```

Подготовка к экспорту событий на стороне Kaspersky Endpoint Detection and Response будет завершена.

На стороне KUMA:

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> kafka.services.external.dyn.kata` в один из следующих файлов:
   - `%WINDIR%\System32\drivers\etc\hosts` – для Windows.
   - `/etc/hosts file` – для Linux.
2. В Консоли KUMA создайте коннектор типа Kafka.

При создании коннектора укажите следующие параметры:

- В поле **URL** укажите `<IP-адрес сервера Central Node>:10000`.
- В поле **Topic** укажите `EndpointEnrichedEventsTopic`.
- В поле **Consumer group** укажите любое уникальное имя.

3. В Консоли KUMA создайте коллектор.

   В качестве транспорта для коллектора используйте коннектор, созданный на предыдущем шаге. В качестве нормализатора для коллектора рекомендуется использовать нормализатор *[OOTB] KEDR telemetry*.

При успешном завершении создания и установки коллектора события Kaspersky Endpoint Detection and Response будут импортированы в KUMA. Вы можете найти и просмотреть эти события в таблице событий.

Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kata/edr

Импорт событий Kaspersky Endpoint Detection and Response с устройств с помощью коннектора 'kata/edr' состоит из следующих шагов:

1. Выполнение конфигурации на стороне KUMA для получения событий.

   Для этого вам нужно создать и установить в KUMA коллектор с коннектором kata/edr или изменить существующий коллектор, а затем сохранить измененные параметры и перезапустить коллектор.

2. Принятие запроса авторизации KUMA на стороне KEDR для начала отправки событий в KUMA.

В результате интеграция будет настроена и события KEDR будут поступать в KUMA.

Создание коллектора для получения событий из KEDR

Чтобы создать коллектор для получения событий из KEDR:

1. Войдите в Консоль KUMA одним из следующих способов:
   - В главном меню Консоли OSMP перейдите в **Параметры** → **KUMA**.
   - В браузере перейдите по адресу `https://kuma.<smp domain>:7220`.
2. Перейдите в раздел **Ресурсы** → **Коллекторы** выберите **Добавить коллектор**.
3. В открывшемся окне **Создание коллектора** на шаге **Подключение источников** укажите произвольное Название коллектора и выберите в раскрывающемся списке подходящий тенант.
4. На шаге 2 **Транспортировка** выполните следующие действия:
   - На вкладке **Основные параметры**:
     a. В поле **Коннектор** выберите **Создать** или в том же поле начните набирать название коннектора, если хотите использовать уже созданный коннектор.
     b. В раскрывающемся списке **Тип коннектора** выберите коннектор **kata/edr**.

После того, как вы выберите тип коннектора kata/edr, отобразятся дополнительные поля для заполнения.

c. В поле **URL** укажите адрес подключения к серверу KEDR в формате `<имя устройства или IP-адрес устройства>:<порт подключения, по умолчанию 443>`. Если KEDR развернут в кластере, с помощью кнопки **Добавить** вы можете добавить все узлы. KUMA будет подключаться последовательно к каждому указанному узлу. Если KEDR установлена в распределенной конфигурации, на стороне KUMA необходимо настроить отдельный коллектор для каждого сервера KEDR.

d. В поле **Секрет** выберите **Создать**, чтобы создать новый секрет. В открывшемся окне **Создание секрета** укажите название секрета и нажмите **Сгенерировать и скачать сертификат и закрытый ключ шифрования соединения**.

В результате в папку загрузок браузера Загрузки скачивается архив certificate.zip, который содержит файл ключа key.pem и файл сертификата cert.pem. Распакуйте архив.

В Консоли KUMA нажмите на кнопку **Загрузить сертификат** и выберите файл cert.pem. Нажмите **Загрузить закрытый ключ** и выберите key.pem. Нажмите на кнопку **Создать**. Секрет будет добавлен в раскрывающийся список **Секрет**, который выбирается автоматически.

Также можно выбрать созданный секрет из списка **Секрет**. KUMA использует выбранный секрет для подключения к KEDR.

e. Поле **Внешний ID** содержит идентификатор для внешних систем. Этот идентификатор отображается в веб-интерфейсе KEDR при авторизации сервера KUMA. KUMA генерирует идентификатор автоматически и поле **Внешний ID** будет автоматически предзаполнено.

- При необходимости укажите параметры на вкладке **Дополнительные параметры**:

a. Чтобы получать детализированную информацию в журнале коллектора, переведите переключатель **Отладка** в активное положение.

b. В поле **Кодировка символов** выберите кодировку исходных данных, к которым будет применена конвертация в UTF-8. Мы рекомендуем применять конвертацию только в том случае, если в полях нормализованного события отображаются недопустимые символы. По умолчанию значение не выбрано.

c. Укажите **Максимальное количество событий** в одном запросе к KEDR. По умолчанию указано значение 0. Это означает, что применяется значение, настроенное на сервере KEDR по умолчанию (подробности см. в справке KATA). Вы можете указать произвольное значение, не превышающее значение на стороне KEDR. Если указанное вами значение превысит значение параметра **Максимальное количество событий**, заданное на сервере KEDR, в журнале коллектора KUMA будет ошибка "*Bad Request: max_events N is greater than allowed value*".

d. Заполните поле **Время ожидания получения событий**, чтобы получать события по истечении заданного периода. По умолчанию указано значение 0. Это означает, что применяется значение, настроенное на сервере KEDR по умолчанию (подробности см. в справке KATA).

Сервер KEDR использует два параметра: максимальное количество событий и время ожидания получения событий. События отправляются, когда накапливается указанное количество событий или по истечении заданного времени, в зависимости от того, что произойдет раньше. Если заданное время истекло, а заданного количества событий не набралось, сервер KEDR передаст те, что есть.

e. В поле **Время ожидания ответа** укажите максимальное значение ожидания ответа от сервера KEDR в секундах. Значение по умолчанию: 1800 сек, отображается как 0. В поле **Время ожидания ответа** указано клиентское ограничение. Значение параметра **Время ожидания ответа** должно быть больше, чем серверное - **Время ожидания получения событий**, чтобы не прервать текущую задачу сбора событий новым запросом и дождаться ответа сервера. Если ответ от сервера KEDR все же не поступил, KUMA повторит запрос.

f. В поле **Фильтр KEDRQL** укажите условия фильтрации запроса. В результате со стороны KEDR будут поступать уже отфильтрованные события. Подробнее о доступных полях для фильтрации см. в справке KATA.

5. На шаге 3 **Парсинг** нажмите **Добавить парсинг событий** и в открывшемся окне **Основной парсинг событий** выберите в раскрывающемся списке нормализатор [OOTB] KEDR telemetry.

6. Чтобы завершить создание коллектора в веб-интерфейсе, нажмите **Создать и сохранить сервис**. Затем скопируйте в веб-интерфейсе команду установки коллектора и выполните команду установки в интерпретаторе командной строки на устройстве KUMA, где вы хотите установить коллектор.

   Пример команды для установки коллектора:

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://<KUMA Core server FQDN>:7210 --id <service ID copied from the KUMA Console> --api.port <port used for communication with the installed component>
   ```

   Полное доменное имя Ядра KUMA по умолчанию `kuma.<smp domain>`. Порт, который используется для подключения к Ядру KUMA, невозможно изменить. По умолчанию установлен порт 7210.

   Если вы редактировали существующий коллектор, нажмите **Сохранить и перезапустить сервисы**.

Коллектор создан и готов к отправке запросов. Коллектор отображается в разделе **Ресурсы** → **Активные службы** с желтым статусом, пока KEDR не примет запрос на авторизацию от KUMA.

Авторизация KUMA на стороне KEDR

После того, как в KUMA создан коллектор, необходимо на стороне KEDR принять запрос авторизации KUMA, чтобы запросы от KUMA начали поступать в KEDR. После принятой авторизации коллектор KUMA автоматически по расписанию отправляет запрос в KEDR и ждет ответа. Все время ожидания статус коллектора будет желтый, а после получения первого ответа на отправленный запрос статус коллектора сменится на зеленый.

В результате интеграция настроена и вы можете просмотреть поступающие из KEDR события в разделе KUMA → **События**.

При первом запросе поступит часть исторических событий, которые произошли до момента интеграции. Когда все исторические события поступят, начнут поступать текущие события. Если вы измените значение параметра **URL** или **Внешний ID** для существующего коллектора, KEDR примет запрос как новый и после запуска коллектора KUMA с измененными параметрами вы снова получите часть исторических событий. Если вы не хотите получать исторические события, перейдите в настройки нужного коллектора, настройте в нормализаторе сопоставление полей `timestamp` KEDR и KUMA, и на шаге мастера установки коллектора **Фильтрация событий** укажите фильтр по `timestamp` так, чтобы `timestamp` событий был больше, чем `timestamp` запуска коллектора.

Возможные ошибки и способы решения

Если в журнале коллектора ошибка "*Conflict: An external system with the following ip and certificate digest already exists. Either delete it or provide a new certificate*", необходимо создать новый секрет с новым сертификатом в коннекторе коллектора.

Если в журнале коллектора возникает ошибка "*Continuation token not found*" в ответ на запрос событий, нужно создать новый коннектор, прикрепить его к коллектору и перезапустить коллектор, или создать новый секрет с новым сертификатом в коннекторе коллектора. Если нет необходимости получать события, которые были сформированы до возникновения ошибки, следует настроить в коллекторе фильтр по `timestamp`.

Настройка отображения ссылки на обнаружение Kaspersky Endpoint Detection and Response в алерте KUMA

При получении обнаружений Kaspersky Endpoint Detection and Response в KUMA создается алерт для каждого обнаружения. Вы можете настроить отображение ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации об алерте KUMA.

Вы можете настроить отображение ссылки на обнаружение, если используете только один сервер Central Node Kaspersky Endpoint Detection and Response. Если Kaspersky Endpoint Detection and Response используется в режиме распределенного решения, настроить отображение ссылок в KUMA на обнаружения Kaspersky Endpoint Detection and Response невозможно.

Для настройки отображения ссылки на обнаружение в информации об алерте KUMA вам требуется выполнить действия в веб-интерфейсе Kaspersky Endpoint Detection and Response и KUMA.

В веб-интерфейсе Kaspersky Endpoint Detection and Response вам нужно настроить интеграцию приложения с KUMA в качестве SIEM-системы. Подробнее о том, как настроить интеграцию, см. в справке *Kaspersky Anti Targeted Attack Platform* в разделе *Настройка интеграции с SIEM-системой*.

Настройка отображения ссылки в Консоли KUMA включает следующие этапы:

1. Добавление актива, содержащего информацию о сервере Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения, и назначение этому активу категории.
2. Создание правила корреляции.
3. Создание коррелятора.

Вы можете использовать преднастроенное корреляционное правило. В этом случае настройка отображения ссылки в Консоли KUMA включает следующие этапы:

1. Создание коррелятора.

   В качестве правила корреляции вам нужно выбрать правило `[OOTB] KATA Alert`.
2. Добавление актива, содержащего информацию о сервере Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения, и назначение этому активу категории `KATA standAlone`.

Шаг 1. Добавление актива и назначение ему категории

Предварительно вам нужно создать категорию, которая будет назначена добавляемому активу.

Чтобы добавить категорию:

1. В Консоли KUMA выберите раздел **Активы**.
2. На вкладке **Все активы** разверните список категорий тенанта, нажав на кнопку **+** рядом с его названием.
3. Выберите требуемую категорию или подкатегорию и нажмите на кнопку **Добавить категорию**.

   В правой части окна веб-интерфейса отобразится область деталей **Добавить категорию**.
4. Укажите параметры категории:

a. В поле **Название** введите название категории.

b. В поле **Родительская категория** укажите место категории в дереве категорий. Для этого нажмите на кнопку и выберите родительскую категорию для создаваемой вами категории.

   Выбранная категория отобразится в поле **Родительская категория**.

c. При необходимости укажите значения для следующих параметров:

   - Назначьте уровень важности категории в раскрывающемся списке **Уровень важности**.

     Указанный уровень важности присваивается корреляционным событиям и алертам, связанным с этим активом.

   - При необходимости в поле **Описание** добавьте описание категории.

   - В раскрывающемся списке **Способ категоризации** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:

     - **Вручную** – активы можно привязать к категории только вручную.

     - **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют **заданному фильтру**.

1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

   Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять, нажав на кнопку **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
OS.	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
FQDN	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.
ПО	=, like	
КИИ	in	Можно выбрать более одного значения.
Последнее обновление антивирусных баз	>=,<=	
Последнее обновление информации	>=,<=	
Последнее обновление защиты	>=,<=	
Время начала последней сессии	>=,<=	
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Состояние постоянной защиты	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов.	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor.	=	
Видим в сети.	>=,<=	

3. Нажмите на кнопку **Условия проверки**, чтобы убедиться в правильности указанного фильтра. При нажатии на кнопку откроется окно **Активы, найденные по заданным условиям**, содержащее список активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

5. Нажмите на кнопку **Сохранить**.

Чтобы добавить актив:

1. В Консоли KUMA выберите раздел **Активы**.
2. Нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.
3. Укажите следующие параметры актива:

   a. В поле **Название актива** введите имя актива.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать актив.

   c. В поле **IP-адрес** укажите IP-адрес сервера Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения.

   d. В поле **Категории** выберите категорию, которую добавили на предыдущем этапе.

   > Если вы используете предустановленное корреляционное правило, вам нужно выбрать категорию `KATA standAlone`.

   e. При необходимости укажите значения для следующих полей:

   - В поле **Полное доменное имя** укажите FQDN сервера Central Node Kaspersky Endpoint Detection and Response.
   - В поле **MAC-адрес** укажите MAC-адрес сервера Central Node Kaspersky Endpoint Detection and Response.
   - В поле **Владелец** укажите имя владельца актива.
4. Нажмите на кнопку **Сохранить**.

Шаг 2. Добавление правила корреляции

Чтобы добавить правило корреляции:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Правила корреляции** и нажмите на кнопку **Создать правило корреляции**.
3. На вкладке **Общие** укажите следующие параметры:

   a. В поле **Название** укажите название правила.

   b. В раскрывающемся списке **Тип** выберите **simple**.

   c. В поле **Наследуемые поля** добавьте следующие поля: DeviceProduct, DeviceAddress, EventOutcome, SourceAssetID, DeviceAssetID.

   d. При необходимости укажите значения для следующих полей:

   - В поле **Частота срабатывания** укажите максимальное количество срабатываний правила в секунду.

- В поле **Уровень важности** укажите уровень важности алертов и корреляционных событий, которые будут созданы в результате срабатывания правила.
- В поле **Описание** укажите любую дополнительную информацию.

4. На вкладке **Селекторы** → **Параметры** укажите следующие параметры:

   a. В раскрывающемся списке **Фильтр** выберите **Создать**.

   b. В поле **Условия** нажмите на кнопку **Добавить группу**.

   c. В поле с оператором для добавленной группы выберите **И**.

   d. Добавьте условие для фильтрации по значению KATA:

      1. В поле **Условия** нажмите на кнопку **Добавить условие**.
      2. В поле с условием выберите **Если**.
      3. В поле **Левый операнд** выберите **поле события**.
      4. В поле **Поле события** выберите **DeviceProduct**.
      5. В поле **Оператор** выберите =.
      6. В поле **Правый операнд** выберите **константа**.
      7. В поле **Значение** введите KATA.

   e. Добавьте условие для фильтрации по категории:

      1. В поле **Условия** нажмите на кнопку **Добавить условие**.
      2. В поле с условием выберите **Если**.
      3. В поле **Левый операнд** выберите **поле события**.
      4. В поле **Поле события** выберите **DeviceAssetID**.
      5. В поле **Оператор** выберите **inCategory**.
      6. В поле **Правый операнд** выберите **константа**.
      7. Нажмите на кнопку  .
      8. Выберите категорию, в которую вы поместили актив сервера Central Node Kaspersky Endpoint Detection and Response.
      9. Нажмите на кнопку **Сохранить**.

   f. В поле **Условия** нажмите на кнопку **Добавить группу**.

   g. В поле с оператором для добавленной группы выберите **ИЛИ**.

   h. Добавьте условие для фильтрации по идентификатору класса события:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.
3. В поле **Левый операнд** выберите **поле события**.
4. В поле **Поле события** выберите **DeviceEventClassID**.
5. В поле **Оператор** выберите =.
6. В поле **Правый операнд** выберите **константа**.
7. В поле **Значение** введите **taaScanning**.

i. Повторите шаги 1–7 пункта f для каждого из следующих идентификаторов классов событий:

- file_web.
- file_mail.
- file_endpoint.
- file_external.
- ids.
- url_web.
- url_mail.
- dns.
- iocScanningEP.
- yaraScanningEP.

5. На вкладке **Действия** укажите следующие параметры:

a. В разделе **Действия** откройте раскрывающийся список **На каждом событии**.

b. Установите флажок **Отправить на дальнейшую обработку**.

c. В разделе **Обогащение** нажмите на кнопку **Добавить обогащение**.

d. В раскрывающемся списке **Тип источника данных** выберите **шаблон**.

e. В поле **Шаблон** введите *https://{{.DeviceAddress}}:8443/katap/#/alerts?id={{.EventOutcome}}*.

f. В раскрывающемся списке **Целевое поле** выберите **DeviceExternalID**.

g. При необходимости переведите переключатель **Отладка** в активное положение, чтобы зарегистрировать информацию, связанную с работой ресурса, в журнал.

6. Нажмите на кнопку **Сохранить**.

Шаг 3. Создание коррелятора

Вам нужно запустить мастер установки коррелятора. На шаге 3 мастера вам требуется выбрать правило корреляции, добавленное при выполнении этой инструкции.

После завершения создания коррелятора в информации об алертах, созданных при получении обнаружений из Kaspersky Endpoint Detection and Response, будет отображаться ссылка на эти обнаружения. Ссылка отображается в информации о корреляционном событии (раздел **Поиск угроз**), в поле **DeviceExternalID**.

Если вы хотите, чтобы в поле DeviceHostName в информации об обнаружении отображался FQDN сервера Central Node Kaspersky Endpoint Detection and Response, вам нужно создать запись для этого сервера в системе DNS и на шаге 4 мастера создать правило обогащения с помощью DNS.

Интеграция с Kaspersky CyberTrace

Kaspersky CyberTrace (далее CyberTrace) – это инструмент, который объединяет потоки данных об угрозах с решениями SIEM. Он обеспечивает пользователям мгновенный доступ к данным аналитики, повышая их осведомленность при принятии решений, связанных с безопасностью.

Вы можете интегрировать CyberTrace с KUMA одним из следующих способов:

- Интегрировать функцию поиска индикаторов CyberTrace для обогащения событий KUMA информацией потоков данных CyberTrace.
- Интегрировать в KUMA веб-интерфейс CyberTrace целиком, чтобы обеспечить полный доступ к CyberTrace.

  Интеграция с консолью CyberTrace доступна только в том случае, если ваша лицензия CyberTrace включает многопользовательскую функцию.

Интеграция поиска по индикаторам CyberTrace

Чтобы выполнить интеграцию поиска по индикаторам CyberTrace, следует выполнить следующие шаги:

1. Настроить CyberTrace для приема и обработки запросов от KUMA.

   Вы можете настроить интеграцию с KUMA сразу после установки CyberTrace в мастере первоначальной настройки или позднее в веб-интерфейсе CyberTrace.

2. Создать правила обогащения событий в KUMA.

   В правиле обогащения вы можете указать, какими данными из CyberTrace вы хотите дополнить событие.

3. Создать коллектор для получения событий, которые вы хотите обогатить данными из CyberTrace.

4. Привязать правило обогащения к коллектору.

5. Сохранить и создать сервис:

   - Если вы привязали правило к новому коллектору, нажмите **Сохранить и создать**, в открывшемся окне скопируйте идентификатор коллектора и используйте скопированный идентификатор для установки коллектора на сервере через интерфейс командной строки.

- Если вы привязали правило к уже существующему коллектору, нажмите **Сохранить и перезапустить сервисы**, чтобы применить параметры.

Настройка интеграции поиска по индикаторам CyberTrace завершена и события KUMA будут обогащаться данными из CyberTrace.

Пример проверки обогащения данными из CyberTrace.

По умолчанию проверка соединения с CyberTrace в KUMA отсутствует.

Если вы хотите проверить интеграцию с CyberTrace и убедиться, что обогащение событий выполняется, вы можете повторить шаги из следующего примера или адаптировать пример с учетом своих потребностей. В примере показана проверка интеграции, в результате которой обогащение будет выполнено и событие будет содержать заданный тестовый URL.

Чтобы выполнить проверку:

1. Создайте тестовое правило обогащения с параметрами, перечисленными в таблице ниже.

Параметр	Значение
Name	Test CT enrichment
Тенант	Общий
Тип источника	CyberTrace
URL	<URL сервера cybertrace, которому вы хотите отправлять запросы>:9999
Сопоставление	Поле KUMA: RequestURL Индикатор CyberTrace: url
Отладка	Включено

1. Создайте тестовый коллектор со следующими параметрами:

   На шаге **2 Транспорт** укажите коннектор http.

   На шаге **3 Парсинг** событий укажите нормализатор и выберите метод парсинга json, задайте сопоставление полей RequestUrl – RequestUrl.

   На шаге **6 Обогащение** укажите правило обогащения Test CT enrichment.

   На шаге **7 Маршрутизация** укажите хранилище, куда следует отправлять события.

2. Нажмите на кнопку **Создать и сохранить сервис**.

   В окне появится готовая команда для установки коллектора.

3. Нажмите **Копировать**, чтобы скопировать команду в буфер обмена, и запустите команду через интерфейс командной сроки. Дождитесь выполнения команды, вернитесь в Консоль KUMA и нажмите на кнопку **Сохранить коллектор**.

   Тестовый коллектор создан, и тестовое правило обогащения привязано к коллектору.

4. Через интерфейс командной строки отправьте в коллектор запрос, который вызовет появление события и последующее обогащение значением тестового URL `http://fakess123bn.nu`. Например:

```
curl --request POST \
  --url http://<идентификатор устройства, на котором установлен коллектор>:<порт коллектора>/input \
  --header 'Content-Type: application/json' \
  --data '{"RequestUrl":"http://fakess123bn.nu"}'
```

5. Перейдите в раздел KUMA **События** и выполните следующий запрос, чтобы ограничить выдачу событий и найти обогащенное событие:

   ```
   SELECT * FROM `events` WHERE RequestUrl = 'http://fakess123bn.nu' ORDER BY Timestamp DESC LIMIT 250
   ```

   Результаты:

   Обогащение выполнено успешно, в событии появилось поле **RequestURL** со значением `http://fakess123bn.nu`, а также TI-индикатор и категория индикатора с данными CyberTrace.

Если в результате проверки обогащение не выполнено, например TI-индикатор отсутствует, мы рекомендуем:

1. Проверить параметры коллектора и правила обогащения.
2. Выгрузить журналы коллектора с помощью следующей команды и просмотреть полученные журналы на наличие ошибок:

   ```
   tail -f /opt/kaspersky/kuma/collector/<идентификатор коллектора>/log/collector
   ```

Настройка CyberTrace для приема и обработки запросов

Вы можете настроить CyberTrace для приема и обработки запросов от KUMA сразу после установки в мастере первоначальной настройки или позднее в веб-интерфейсе приложения.

Чтобы настроить CyberTrace для приема и обработки запросов в мастере первоначальной настройки:

1. Дождитесь запуска мастера первоначальной настройки CyberTrace после установки приложения.

   Откроется окно **Welcome to Kaspersky CyberTrace**.

2. В раскрывающемся списке **<select SIEM>** выберите тип SIEM-системы, от которой вы хотите получать данные, и нажмите на кнопку **Next**.

   Откроется окно **Параметры подключения**.

3. Выполните следующие действия:

   a. В блоке параметров **Service listens on** выберите вариант **IP and port**.

   b. В поле **IP address** введите `0.0.0.0`.

   c. В поле **Port** введите укажите порт для получения событий, порт по умолчанию `9999`.

   d. В блоке параметров **Service sends events to** в поле **IP address or hostname** укажите `127.0.0.1` и в поле **Port** укажите `9998`.

   Остальные значения оставьте по умолчанию.

   e. Нажмите на кнопку **Далее**.

   Откроется окно **Параметры прокси-сервера**.

4. Если в вашей организации используется прокси-сервер, укажите параметры соединения с ним. Если нет, оставьте все поля незаполненными и нажмите на кнопку **Next**.

   Откроется окно **Licensing Settings**.

5. В поле **Kaspersky CyberTrace license key** добавьте лицензионный ключ для приложения CyberTrace.

6. В поле **Kaspersky Threat Data Feeds certificate** добавьте сертификат, позволяющий скачивать с серверов обновлений списки данных (data feeds), и нажмите на кнопку **Next**.

CyberTrace будет настроен.

Чтобы настроить CyberTrace для приема и обработки запросов в веб-интерфейсе приложения:

1. В веб-интерфейсе CyberTrace выберите раздел **Settings** – **Service**.

2. В блоке параметров **Connection Settings** выполните следующие действия:

   a. Выберите вариант **IP and port**.

   b. В поле **IP address** введите `0.0.0.0`.

   c. В поле **Port** укажите порт для приема событий, порт по умолчанию `9999`.

3. В блоке параметров **Web interface** в поле **IP address or hostname** введите `127.0.0.1`.

4. В верхней панели инструментов нажмите на кнопку **Restart the CyberTrace Service**.

5. Выберите раздел **Settings** – **Events format**.

6. В поле **Alert events format** введите `%Date% alert=%Alert%%RecordContext%`.

7. В поле **Detection events format** введите `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`.

8. В поле **Records context format** введите `|%ParamName%=%ParamValue%`.

9. В поле **Actionable fields context format** введите `%ParamName%:%ParamValue%`.

CyberTrace будет настроен.

После обновления конфигурации CyberTrace требуется перезапустить сервер CyberTrace.

Создание правил обогащения событий

Чтобы создать правила обогащения событий:

1. В Консоли KUMA перейдите в раздел **Ресурсы** → **Правила обогащения** и в левой части окна выберите или создайте папку, в которую требуется поместить новое правило.

   Отобразится список доступных правил обогащения.

2. Нажмите на кнопку **Добавить правило обогащения**, чтобы создать новое правило.

   Откроется окно правила обогащения.

3. Укажите параметры правила обогащения:

   a. В поле **Название** введите уникальное имя правила. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип источника** выберите **cybertrace**.

   d. Укажите **URL** сервера CyberTrace, к которому вы хотите подключиться. Например, *example.domain.com:9999*.

   e. При необходимости укажите в поле **Количество подключений** максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

f. В поле **Запросов в секунду** введите количество запросов к серверу CyberTrace, которое сможет выполнять KUMA в секунду. По умолчанию указано значение `1000`.

g. В поле **Время ожидания** укажите время в секундах, в течение которого KUMA должна ожидать ответа от сервера CyberTrace. Событие не будет отправлено в коррелятор, пока не истечет время ожидания или не будет получен ответ. Если ответ получен до истечения времени ожидания, он добавляется в поле события `TI`, и обработка события продолжается. По умолчанию указано значение `30`.

h. В блоке параметров **Сопоставление** требуется указать поля событий, которые следует отправить в CyberTrace на проверку, а также задать правила сопоставления полей событий KUMA с типами индикаторов CyberTrace:

- В столбце **Поле KUMA** выберите поле, значение которого требуется отправить в CyberTrace.
- В столбце **Индикатор CyberTrace** выберите тип индикатора CyberTrace для каждого выбранного поля:
  - **ip**
  - **url**
  - **hash**

В таблице требуется указать как минимум одну строку. Нажав на кнопку **Добавить строку**, можно добавить строку, а на кнопку ✕ – удалить.

i. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

j. При необходимости в поле **Описание** добавьте до 4000 символов в кодировке Unicode.

k. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

4. Нажмите на кнопку **Сохранить**.

Создано правило обогащения.

Интеграция поиска по индикаторам CyberTrace настроена. Созданное правило обогащения можно добавить к коллектору. Требуется перезапустить коллекторы KUMA, чтобы применить новые параметры.

Если какие-либо из полей CyberTrace в области деталей события содержат "[{" или "}]", это означает, что информация из потока данных об угрозах из CyberTrace была обработана некорректно и некоторые данные, возможно, не отображаются. Информацию из потока данных об угрозах можно получить, скопировав из события KUMA значение поля **TI indicator** событий и выполнив поиск по этому значению на портале CyberTrace в разделе индикаторов. Вся информация будет отображаться в разделе CyberTrace **Indicator context**.

Интеграция интерфейса CyberTrace

Вы можете интегрировать веб-интерфейс CyberTrace в Консоль KUMA. Когда эта интеграция включена, в Консоли KUMA появляется раздел **CyberTrace** с доступом к веб-интерфейсу CyberTrace. Вы можете настроить интеграцию в Консоли KUMA в разделе **Параметры** → **Kaspersky CyberTrace** .

Чтобы интегрировать веб-интерфейс CyberTrace в KUMA:

1. В Консоли KUMA откройте раздел **Ресурсы** → **Секреты**.

Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать секрет. Этот ресурс используется для хранения учетных данных для подключения к серверу CyberTrace.

Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип** выберите **credentials**.

   d. В полях **Пользователь** и **Пароль** введите учетные данные для вашего сервера CyberTrace.

   e. При необходимости в поле **Описание** добавьте до 4000 символов в кодировке Unicode.

4. Нажмите на кнопку **Сохранить**.

   Учетные данные сервера CyberTrace сохранены и могут использоваться в других ресурсах KUMA.

5. В Консоли KUMA перейдите в раздел **Параметры → Kaspersky CyberTrace**.

   Откроется окно с параметрами интеграции CyberTrace.

6. Измените необходимые параметры:

   - **Выключено** – снимите этот флажок, если хотите включить интеграцию веб-интерфейса CyberTrace в Консоль KUMA.
   - **Адрес сервера** (обязательно) – введите адрес сервера CyberTrace.
   - **Порт** (обязательно) – введите порт сервера CyberTrace, порт для доступа к веб-интерфейсу по умолчанию 443.

7. В раскрывающемся списке **Секрет** выберите секрет, который вы создали ранее.

8. Вы можете настроить доступ к веб-интерфейсу CyberTrace следующими способами:

   - Использовать hostname или IP при входе в Консоль KUMA.

     Для этого в разделе **Разрешить устройства** нажмите **Добавить устройство** и в появившемся поле укажите IP или hostname устройства.

   - Использовать FQDN при входе в Консоль KUMA.

     Если для работы в консоли вы используете браузер Mozilla Firefox, данные в разделе CyberTrace могут не отображаться. В таком случае настройте отображение данных (см. ниже).

9. Нажмите на кнопку **Сохранить**.

CyberTrace теперь интегрирован с KUMA: раздел **CyberTrace** отображается в Консоли KUMA.

*Чтобы настроить отображение данных в разделе **CyberTrace** при использовании FQDN для входа в KUMA в Mozilla Firefox:*

1. Очистите кеш браузера.

2. В строке браузера введите FQDN Консоли KUMA с номером порта 7222: https://kuma.example.com:7222.

   Отобразится окно с предупреждением о вероятной угрозе безопасности.

3. Нажмите на кнопку **Подробнее**.

4. В нижней части окна нажмите на кнопку **Принять риск и продолжить**.

   Для URL Консоли KUMA будет создано исключение.

5. В строке браузера введите URL Консоли KUMA с номером порта 7220.

6. Перейдите в раздел **CyberTrace**.

Данные отобразятся в разделе.

Обновление списка запрещенных объектов CyberTrace (Internal TI)

Если веб-интерфейс CyberTrace интегрирован в Консоль KUMA, можно обновлять список запрещенных объектов CyberTrace или **Internal TI** данными из событий KUMA.

Чтобы обновить Internal TI в CyberTrace:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   Откроется контекстное меню.

2. Выберите **Добавить в Internal TI CyberTrace**.

Выбранный объект добавлен в список запрещенных объектов в CyberTrace.

Интеграция с Kaspersky Threat Intelligence Portal

Портал Kaspersky Threat Intelligence Portal объединяет все знания Лаборатории Касперского о киберугрозах и их взаимосвязи в единую веб-службу. При интеграции с KUMA он помогает пользователям KUMA быстрее принимать обоснованные решения, предоставляя им данные о веб-адресах, доменах, IP-адресах, данных WHOIS / DNS.

Доступ к Kaspersky Threat Intelligence Portal предоставляется на платной основе. Лицензионные сертификаты создаются специалистами Лаборатории Касперского. Чтобы получить сертификат для Kaspersky Threat Intelligence Portal, обратитесь к вашему персональному техническому менеджеру Лаборатории Касперского.

Инициализация интеграции

Чтобы интегрировать Kaspersky Threat Intelligence Portal в KUMA:

1. В Консоли KUMA откройте раздел **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать секрет. Этот ресурс используется для хранения данных вашей учетной записи Kaspersky Threat Intelligence Portal.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **ktl**.

   d. В полях **Пользователь** и **Пароль** введите данные своей учетной записи Kaspersky Threat Intelligence Portal.

   e. В поле **Описание** можно добавить описание секрета.

4. Загрузите ключ сертификата Kaspersky Threat Intelligence Portal:

   a. Нажмите **Загрузить PFX** и выберите PFX-файл с сертификатом.

   Имя выбранного файла отображается справа от кнопки **Загрузить PFX**.

   b. В поле **Пароль PFX** введите пароль для PFX-файла.

5. Нажмите на кнопку **Сохранить**.

   Ваши учетные данные Kaspersky Threat Intelligence Portal сохранены и могут использоваться в других ресурсах KUMA.

6. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Threat Lookup**.

   Отобразится список доступных подключений.

7. Убедитесь, что флажок **Выключено** снят.

8. В раскрывающемся списке **Секрет** выберите секрет, который вы создали ранее.

   Можно создать секрет, нажав на кнопку со значком плюса. Созданный секрет будет сохранен в разделе **Ресурсы** → **Секреты**.

9. При необходимости в раскрывающемся списке **Прокси-сервер** выберите прокси-сервер.

10. Нажмите на кнопку **Сохранить**.

11. После сохранения параметров войдите в консоль и примите **Условия использования**. Иначе в API возвращается ошибка.

Процесс интеграции Kaspersky Threat Intelligence Portal с KUMA завершен.

После интеграции Kaspersky Threat Intelligence Portal и KUMA в области деталей события можно запрашивать сведения об устройствах, доменах, URL-адресах, IP-адресах и хешах файлов (MD5, SHA1, SHA256).

Запрос данных от Kaspersky Threat Intelligence Portal

Чтобы запросить данные от Kaspersky Threat Intelligence Portal:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

2. Установите флажки рядом с типами данных, которые нужно запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

3. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. По умолчанию указано значение `10`.

4. Нажмите **Запрос**.

Задача *ktl* создана. По ее завершении события дополняются данными из Kaspersky Threat Intelligence Portal, которые можно просмотреть в таблице событий, окне обнаружения или окне корреляционного события.

Просмотр данных от Kaspersky Threat Intelligence Portal

Чтобы просмотреть данные из Kaspersky Threat Intelligence Portal,

Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени последнего обновления этих данных.

Информация, полученная от Kaspersky Threat Intelligence Portal, кешируется. Если нажать на домен, веб-адрес, IP-адрес или хеш файла в области деталей события, для которого у KUMA уже есть доступная информация, вместо окна **Обогащение Threat Lookup** отобразятся данные из Kaspersky Threat Intelligence Portal с указанием времени их получения. Эти данные можно обновить.

Обновление данных от Kaspersky Threat Intelligence Portal

Чтобы обновить данные, полученные от Kaspersky Threat Intelligence Portal:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal.

2. Нажмите **Обновить** в области деталей события с данными, полученными с портала Kaspersky Threat Intelligence Portal.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

3. Установите флажки рядом с типами данных, которые вы хотите запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

4. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. По умолчанию указано значение `10`.

5. Нажмите **Обновить**.

   Создается задача *KTL* и запрашиваются новые данные, полученные из Kaspersky Threat Intelligence Portal.

6. Закройте окно **Обогащение Threat Lookup** и область подробной информации о KTL.

7. Откройте область подробной информации о событии из таблицы событий, окна алертов или окна корреляционных событий и перейдите по ссылке, соответствующей домену, веб-адресу, IP-адресу или хешу файла, для которого вы обновили информацию на Kaspersky Threat Intelligence Portal, и выберите **Показать информацию из Threat Lookup**.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени.

Подключение по протоколу LDAP

Подключения по протоколу LDAP создаются и управляются в Консоли KUMA в разделе **Параметры** → **LDAP-сервер**. В разделе **Интеграция с LDAP-сервером по тенантам** отображаются тенанты, для которых созданы подключения по протоколу LDAP. Тенанты можно создать или удалить.

Если выбрать тенант, откроется окно **Интеграция с LDAP-сервером**, в котором отображается таблица с существующими LDAP-подключениями. Подключения можно создать или изменить. В этом же окне можно изменить частоту обращения к LDAP-серверам и установить срок хранения устаревших данных.

После включения интеграции информация об учетных записях Active Directory становится доступной в окне алертов, в окне с подробной информацией о корреляционных событиях, а также окне инцидентов. При выборе имени учетной записи в разделе **Связанные пользователи** откроется окно **Информация об учетной записи** с данными, импортированными из Active Directory.

Данные из LDAP можно также использовать при обогащении событий в коллекторах и в аналитике.

Импортируемые атрибуты Active Directory

Из Active Directory можно запросить следующие атрибуты учетных записей:

- accountExpires
- badPasswordTime
- cn
- co
- company
- department
- description
- displayName
- distinguishedName
- division
- employeeID
- givenName
- l
- lastLogon
- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf (по этому атрибуту события можно искать при корреляции)
- mobile
- name
- objectCategory
- objectGUID (этот атрибут запрашивается из Active Directory всегда)
- objectSID
- physicalDeliveryOfficeName

- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

Включение и выключение LDAP-интеграции

Можно включить или выключить сразу все LDAP-подключения тенанта, а можно включить или выключить только определенное LDAP-подключение.

Чтобы включить или отключить все LDAP-подключения тенанта:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер** и выберите тенант, у которого вы хотите включить или выключить все подключения к LDAP.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Установите или снимите флажок **Выключено**.

3. Нажмите на кнопку **Сохранить**.

Чтобы включить или отключить определенное LDAP-подключение:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер** и выберите тенант, у которого вы хотите включить или выключить подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Выберите нужное подключение и в открывшемся окне установите или снимите флажок **Выключено**.

3. Нажмите на кнопку **Сохранить**.

Добавление тенанта в список тенантов для интеграции с LDAP-сервером

Чтобы добавить тенант в список тенантов для интеграции с LDAP-сервером:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Нажмите на кнопку **Добавить тенант**.

   Отобразится окно **Интеграция с LDAP-сервером**.

3. В раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.

4. Нажмите на кнопку **Сохранить**.

Выбранный тенант добавлен в список тенантов для интеграции с LDAP-сервером.

Чтобы добавить тенант из списка тенантов для интеграции с LDAP-сервером:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер**.

   Отобразится таблица **Интеграция с LDAP-сервером по тенантам**.

2. Установите флажок рядом с тенантом, который необходимо удалить, и нажмите на кнопку **Удалить**.

3. Подтвердите удаление тенанта.

Выбранный тенант удален из списка тенантов для интеграции с LDAP-сервером.

Создание подключения к LDAP-серверу

Чтобы создать LDAP-подключение к Active Directory:

1. Откройте раздел **Параметры** → **LDAP-сервер** Консоли KUMA.

2. Выберите или создайте тенант, для которого хотите создать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Нажмите на кнопку **Добавить подключение**.

   Откроется окно **Параметры подключения**.

4. Добавьте секрет с учетными данными для подключения к серверу Active Directory. Для этого выполните следующие действия:

   a. Если вы добавили секрет ранее, в раскрывающемся списке **Секрет** выберите существующий секрет типа **credentials**.

      Выбранный секрет можно изменить, нажав на кнопку .

   b. Если вы хотите создать секрет, нажмите на кнопку +.

      Откроется окно **Секрет**.

   c. В поле **Название** (обязательно) введите название секрета: от 1 до 128 символов в кодировке Unicode.

   d. В полях **Пользователь** и **Пароль** (обязательно) введите учетные данные для подключения к серверу Active Directory.

      Вы можете указать имя пользователя в одном из следующих форматов: <имя пользователя>@<домен> или <домен><имя пользователя>.

e. В поле **Описание** введите описание до 4000 символов в кодировке Unicode.

f. Нажмите на кнопку **Сохранить**.

5. В поле **Название** (обязательно) введите уникальное имя LDAP-подключения.

   Длина должна быть от 1 до 128 символов в кодировке Unicode.

6. В поле **URL** (обязательно) введите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

   > Вы можете указать через запятую адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

7. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Тип** выберите один из следующих вариантов:

   - **startTLS**.

     При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается.

     > Убедитесь, что порт 389 открыт. В противном случае соединение с контроллером домена будет невозможно.

   - **ssl**.

     При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

   - **незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

8. Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат. Для этого выполните следующие действия:

   a. Если вы загрузили сертификат ранее, выберите его в раскрывающемся списке **Сертификат**.

      Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

   b. Если вы хотите загрузить новый сертификат, справа от списка **Сертификат** нажмите на кнопку +.

      Откроется окно **Секрет**.

   c. В поле **Название** введите название, которое будет отображаться в списке сертификатов после его добавления.

   d. По кнопке **Загрузить файл сертификата** добавьте файл с сертификатом Active Directory. Поддерживаются открытые ключи сертификата X.509 в Base64.

   e. Если требуется, укажите любую информацию о сертификате в поле **Описание**.

   f. Нажмите на кнопку **Сохранить**.

   Сертификат будет загружен и отобразится в списке **Сертификат**.

9. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

   Если в поле **URL** указано несколько адресов, KUMA будет ожидать ответа от первого сервера указанное количество секунд. Если в течение этого времени не будет получено никакого ответа, приложение свяжется со следующим сервером. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

10. В поле **Base DN** введите базовое отличительное имя директории, в которой должен выполняться поисковый запрос.

11. В поле **Пользовательские атрибуты учетных записей AD** укажите **дополнительные атрибуты, с использованием которых вы хотите обогащать события**.

Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

   Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартный атрибут `accountExpires` в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

Из Active Directory можно запросить следующие атрибуты учетных записей:

- accountExpires
- badPasswordTime
- cn
- co
- company
- department
- description
- displayName
- distinguishedName
- division
- employeeID
- givenName
- l
- lastLogon
- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf (по этому атрибуту события можно искать при корреляции)
- mobile
- name
- objectCategory
- objectGUID (этот атрибут запрашивается из Active Directory всегда)
- objectSID
- physicalDeliveryOfficeName

- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

После того, как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если вы добавили один и тот же атрибут для нескольких доменов, атрибут отображается в раскрывающемся списке только один раз. Вы можете просмотреть домены, наведя курсор на вопросительный знак. Названия доменов отображаются в виде ссылок. Если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

   После перезапуска коллектора KUMA начнет обогащать события учетными записями.

12. Установите флажок **Выключено**, если не хотите использовать это LDAP-подключение.

    По умолчанию флажок снят.

13. Нажмите на кнопку **Сохранить**.

LDAP-подключение к Active Directory создано и отображается в окне **Интеграция с LDAP-сервером**.

Информация об учетных записях из Active Directory будет запрошена сразу после сохранения подключения, а затем будет обновляться с указанной периодичностью.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Создание копии подключения к LDAP-серверу

Вы можете создать LDAP-подключение, скопировав уже существующее подключение. В этом случае в созданное подключение дублируются все параметры исходного подключения.

Чтобы скопировать LDAP-подключение:

1. Откройте раздел **Параметры** → **LDAP-сервер** Консоли KUMA и выберите тенант, для которого вы хотите скопировать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Выберите нужное подключение.

3. В открывшемся окне **Параметры подключения** нажмите на кнопку **Дублировать подключение**.

   Отобразится окно создания нового подключения. К названию подключения будет добавлено слово `копия`.

4. Если требуется, измените нужные параметры.

5. Нажмите на кнопку **Сохранить**.

Создано новое подключение.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Изменение подключения к LDAP-серверу

Чтобы изменить подключение к LDAP-серверу:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Выберите тенант, для которого вы хотите изменить подключение к LDAP-серверу.

   Откроется окно **Интеграция с LDAP-сервером**.

3. Нажмите на подключение с LDAP-серверу, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к LDAP-серверу.

4. Измените значения необходимых параметров.

5. Нажмите на кнопку **Сохранить**.

Подключение к LDAP-серверу изменено. Перезапустите сервисы KUMA, использующие обогащение данными LDAP-серверов, чтобы изменения вступили в силу.

Изменение частоты обновления данных

KUMA обращается к LDAP-серверу для обновления данных об учетных записях. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов.
- При создании пользователем задачи на обновление данных об учетных записях.

При обращении к LDAP-серверам создается задача в Консоли KUMA в разделе **Диспетчер задач**.

Чтобы изменить расписание обращений KUMA к LDAP-серверам:

1. В Консоли KUMA перейдите в раздел **Параметры → LDAP-сервер → Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. В поле **Период обновления данных** укажите требуемую частоту в часах. По умолчанию указано значение 12.

Расписание обращений изменено.

Изменение срока хранения данных

Полученные данные об учетных записях, если сведения о них перестают поступать от сервера Active Directory, по умолчанию хранятся в KUMA в течение 90 дней. По прошествии этого срока данные удаляются.

После удаления данных об учетных записях в KUMA новые и существующие события не обогащаются этой информацией. Информация об учетных записях также будет недоступна в алертах. Если вы хотите просматривать информацию об учетных записях на протяжении всего времени хранения алерта, требуется установить срок хранения данных об учетных записях больше, чем срок хранения алерта.

Чтобы изменить срок хранения данных об учетных записях:

1. В Консоли KUMA перейдите в раздел **Параметры → LDAP-сервер → Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

3. В поле **Время хранения данных** укажите количество дней, в течение которого требуется хранить полученные от LDAP-сервера данные.

Срок хранения данных об учетных записях изменен.

Запуск задач на обновление данных об учетных записях

После создания подключения к серверу Active Directory задачи на получение данных об учетных записях создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную. Загрузить данные можно для всех подключений требуемого тенанта, так и для одного подключения.

Чтобы запустить задачу на обновление данных об учетных записях для всех LDAP-подключений тенанта:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Нажмите на кнопку **Импортировать учетные записи**.

В Консоли KUMA в разделе **Диспетчер задач** добавлена задача на получение данных об учетных записях выбранного тенанта.

Чтобы запустить задачу на обновление данных об учетных записях для одного LDAP-подключения тенанта:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Выберите требуемое подключение к LDAP-серверу.

   Откроется окно **Параметры подключения**.
4. Нажмите на кнопку **Импортировать учетные записи**.

В Консоли KUMA в разделе Диспетчер задач добавлена **задача** на получение данных об учетных записях из выбранного подключения тенанта.

Удаление подключения к LDAP-серверу

Чтобы удалить LDAP-подключения к Active Directory:

1. В Консоли KUMA перейдите в раздел **Параметры** → **LDAP-сервер** и выберите тенант, которому принадлежит нужное подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Нажмите на подключение LDAP, которое вы хотите удалить, а затем нажмите на кнопку **Удалить**.

3. Подтвердите удаление подключения.

LDAP-подключение к Active Directory удалено.

Интеграция с Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks (далее "KICS for Networks") – приложение, предназначенное для защиты инфраструктуры промышленного предприятия от угроз информационной безопасности и обеспечения бесперебойной работы. Приложение анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети.

KICS for Networks версии 4.0 и выше можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Импортировать из KICS for Networks в KUMA сведения об активах.
- Отправлять из KUMA в KICS for Networks команды на изменение статусов активов.

> В отличие от KUMA, в KICS for Networks активы называются устройствами.

Интеграцию KICS for Networks и KUMA необходимо настроить на стороне обоих приложений:

1. В KICS for Networks необходимо создать коннектор KUMA и сохранить файл свертки этого коннектора.
2. В KUMA с помощью файла свертки коннектора создается подключение к KICS for Networks.

> Описываемая в этом разделе интеграция касается импорта сведений об активах. KICS for Networks можно также настроить на отправку событий в KUMA. Для этого необходимо в KICS for Networks создать коннектор типа SIEM/Syslog, а на стороне KUMA – настроить коллектор.

Настройка интеграции в KICS for Networks

> Интеграция поддерживается с KICS for Networks версий 4.0 и выше.

> Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

На стороне KICS for Networks настройка интеграции заключается в создании *коннектора типа KUMA*. В KICS for Networks коннекторы – это специальные модули приложений, которые обеспечивают обмен данными KICS for Networks со сторонними системами, в том числе с KUMA. Подробнее о создании коннекторов см. в документации KICS for Networks.

При добавлении в KICS for Networks коннектора автоматически создается *файл свертки* для этого коннектора. Это зашифрованный файл конфигурации для подключения к KICS for Networks, который используется при настройке интеграции на стороне KUMA.

Настройка интеграции в KUMA

Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

Чтобы настроить в KUMA интеграцию с KICS for Networks:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks по тенантам**.

2. Выберите или создайте тенант, для которого хотите создать интеграцию с KICS for Networks.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

3. Нажмите на поле **Файл свертки** и выберите файл свертки коннектора, созданный в KICS for Networks.

4. В поле **Пароль файла свертки** введите пароль файла свертки.

5. Установите флажок **Включить реагирование**, если вы хотите изменять статусы активов KICS for Networks с помощью правил реагирования KUMA.

6. Нажмите на кнопку **Сохранить**.

В KUMA настроена интеграция с KICS for Networks, в окне отображается IP-адрес узла, на котором будет работать коннектор KICS for Networks, а также его идентификатор.

Включение и выключение интеграции с KICS for Networks

Чтобы включить или выключить для тенанта интеграцию с KICS for Networks:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks** и выберите тенант, у которого вы хотите включить или выключить интеграцию с KICS for Networks.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

2. Установите или снимите флажок **Выключено**.

3. Нажмите на кнопку **Сохранить**.

Изменение частоты обновления данных

KUMA обращается к KICS for Networks для обновления сведений об активах. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 3 часа.
- При создании пользователем задачи на обновление данных об активах.

При обращении к KICS for Networks создается задача в Консоли KUMA в разделе **Диспетчер задач**.

Чтобы изменить расписание импорта сведений об активах KICS for Networks:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.
3. В поле **Период обновления данных** укажите требуемую частоту в часах. По умолчанию указано значение 3.

Расписание импорта изменено.

Особенности импорта информации об активах из KICS for Networks

Импорт активов

Активы импортируются в соответствии с правилами импорта активов. Импортируются только активы со статусами **Разрешенное** и **Неразрешенное**.

Активы KICS for Networks идентифицируются по комбинации следующих параметров:

- IP-адрес экземпляра KICS for Networks, с которым настроена интеграция.
- Идентификатор коннектора KICS for Networks, с помощью которого настроена интеграция.
- Идентификатор, присвоенный активу (или "устройству") в экземпляре KICS for Networks.

Импорт сведений об уязвимостях

При импорте активов в KUMA также поступают сведения об активных уязвимостях KICS for Networks. Если в KICS for Networks уязвимость была помечена как устраненная или незначительная, сведения о ней удаляются из KUMA при следующем импорте.

Сведения об уязвимостях активов отображаются в окне **Информация об активе** в блоке параметров **Уязвимости** на языке локализации KICS for Networks.

> В KICS for Networks уязвимости называются рисками и разделяются на несколько типов. В KUMA импортируются все типы рисков.

Срок хранения импортированных данных

Если сведения о ранее импортированном активе перестают поступать из KICS for Networks, актив удаляется по прошествии 30 дней.

Изменение статуса актива KICS for Networks

После настройки интеграции вы можете менять статусы активов KICS for Networks из KUMA. Статусы можно менять автоматически и вручную.

Статусы активов можно менять, только если вы включили реагирование в настройках подключения к KICS for Networks.

Изменение статуса актива KICS for Networks вручную

Пользователи с ролями Главный администратор, Администратор и Аналитик в доступных им тенантах могут вручную менять статусы активов, импортированных из KICS for Networks.

Чтобы вручную изменить статус актива KICS for Networks:

1. В Консоли KUMA перейдите в раздел **Активы** и нажмите на актив, который вы хотите удалить.

   В правой части окна откроется область **Информация об активе**.

2. В раскрывающемся списке **Статус KICS for Networks** выберите статус, который необходимо присвоить активу KICS for Networks. Доступны статусы *Разрешенное* или *Неразрешенное*.

Статус актива изменен. Новый статус отображается в KICS for Networks и в KUMA.

Изменение статуса актива KICS for Networks автоматически

Автоматическое изменение статусов активов KICS for Networks реализовано с помощью правил реагирования. Правила необходимо добавить в коррелятор, который будет определять условия их срабатывания.

Интеграция с Neurodat SIEM IM

Система Neurodat SIEM IM предназначена для мониторинга информационной безопасности.

Вы можете настроить передачу событий KUMA в Neurodat SIEM IM. На основе поступающих событий и правил корреляции в системе Neurodat SIEM IM автоматически формируются инциденты информационной безопасности.

Чтобы настроить интеграцию с Neurodat SIEM IM:

1. Подключитесь к серверу Neurodat SIEM IM по протоколу SSH под учетной записью с административными привилегиями.

2. Создайте резервную копию конфигурационного файла /opt/apache-tomcat-<версия сервера>/conf/neurodat/soz_settings.properties.

3. В конфигурационном файле /opt/apache-tomcat-<версия сервера>/conf/neurodat/soz_settings.properties установите указанные значения для следующих параметров:

- `kuma.on=true`

  Этот параметр является признаком взаимодействия с Neurodat SIEM IM с KUMA.

- `job_kuma=com.cbi.soz.server.utils.scheduler.KumaIncidentsJob`

- `jobDelay_kuma=5000`

- `jobPeriod_kuma=60000`

4. Сохраните изменения конфигурационного файла.

5. Перезапустите сервис tomcat с помощью команды:

   ```
   sudo systemctl restart tomcat
   ```

6. Получите токен для пользователя в KUMA. Для этого выполните следующие действия:

   a. В Консоли KUMA в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Профиль**.

   Откроется окно **Пользователь** с параметрами вашей учетной записи.

   b. Нажмите на кнопку **Сгенерировать токен**.

   Откроется окно **Новый токен**.

   c. Если требуется, установите срок действия токена:

   - Установите флажок **Без окончания срока действия**.

   - В поле **Срок действия** с помощью календаря укажите дату и время истечения срока действия создаваемого токена.

   d. Нажмите на кнопку **Сгенерировать токен**.

   В области деталей пользователя отобразится поле **Токен** с автоматически созданным токеном. Скопируйте его.

   При закрытии окна токен больше не отображается. Если вы не скопировали токен перед закрытием окна, вам нужно будет сгенерировать новый токен.

   e. Нажмите на кнопку **Сохранить**.

7. Войдите в Neurodat SIEM IM под учетной записью admin или другой учетной записью, обладающей ролью Администратор для настраиваемой организации или Администратор всех организаций.

8. В пункте меню **Администрирование** → **Структура организации** выберите или создайте организацию, которая будет получать инциденты из KUMA.

9. На форме организации выполните следующие действия:

   a. Установите флажок **Настроить интеграцию с KUMA**.

   b. В поле **IP адрес и сетевой порт KUMA** укажите адрес API KUMA, например `https://192.168.58.27:7223/api/v1/`.

   c. В поле **Ключ API KUMA** укажите токен пользователя, полученный на шаге 6.

   d. Сохраните данные организации.

Настройка интеграции с KUMA будет завершена.

Neurodat SIEM IM выполнит проверку доступа к KUMA и в случае успеха отобразит сообщение о готовности получать данные из KUMA.

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (далее также "KASAP") – это платформа для онлайн-обучения, с помощью которой пользователи смогут усвоить правила соблюдения информационной безопасности, узнать о связанных с ней угрозах, подстерегающих их в ежедневной деятельности, и потренироваться на практических примерах.

Платформу KASAP можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Изменять группы обучения пользователей.
- Просматривать информацию о курсах, пройденных пользователями, и полученных ими сертификатах.

Интеграция KASAP и KUMA заключается в настройте API-подключения к платформе KASAP. Процесс происходит в обоих продуктах:

1. В KASAP необходимо создать токен для авторизации API-запросов и получить адрес для API-запросов.
2. В KUMA необходимо указать адрес для API-запросов в KASAP, добавить токен для авторизации API-запросов, а также указать адрес электронной почты администратора KASAP для получения уведомлений.

Создание токена в KASAP и получение ссылки для API-запросов

Для авторизации API-запросов из KUMA в KASAP их необходимо подписывать токеном, созданном в платформе KASAP. Только администраторы компании могут создать токены.

Создание токена

Чтобы создать токен:

1. Войдите в веб-интерфейс KASAP.
2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.
3. Нажмите на кнопку **Новый токен** и в открывшемся окне выберите методы API, используемые при интеграции:
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
4. Нажмите на кнопку **Сгенерировать токен**.

5. Скопируйте токен и сохраните его любым удобным способом. Этот токен необходим для настройки интеграции в KUMA.

> Токен не хранится в системе KASAP в открытом виде. После закрытия окна **Получить токен** он становится недоступным для просмотра. Если вы закрыли это окно, не скопировав токен, вам требуется нажать на кнопку **Новый токен** повторно, чтобы система сгенерировала новый токен.

Выданный токен действителен 12 месяцев. По истечении этого срока токен будет отозван. Выпущенный токен будет также отозван, если он не используется в течении 6 месяцев.

Получение ссылки для API-запросов

Чтобы получить ссылку, используемую в KASAP для API-запросов:

1. Войдите в консоль платформы KASAP.
2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.
3. Ссылка для обращения к KASAP через Open API расположена в нижней части окна. Скопируйте ссылку и сохраните ее любым удобным способом. Эта ссылка необходима для настройки интеграции в KUMA.

Настройка интеграции в KUMA

Чтобы настроить в KUMA интеграцию с KASAP:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Kaspersky Automated Security Awareness Platform**.

   Откроется окно **Интеграция с Kaspersky Automated Security Awareness Platform**.
2. В поле **Секрет** с помощью кнопки + создайте секрет типа **token**, указав в нем токен, полученный в платформе KASAP:
   a. В поле **Название** введите название для секрета. Имя должно содержать от 1 до 128 символов Юникода.
   b. В поле **Токен** введите токен для авторизации API-запросов в KASAP.
   c. При необходимости добавьте описание секрета в поле **Описание**.
   d. Нажмите на кнопку **Сохранить**.
3. В поле **URL для OpenAPI KASAP** укажите адрес, используемый платформой KASAP для API-запросов.
4. В поле **Адрес электронной почты администратора KASAP** укажите адрес электронной почты администратора KASAP, который должен получать уведомления при добавлении пользователей в группы обучения через KUMA.
5. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера, который следует использовать для подключения к платформе KASAP.
6. При необходимости выключить или включить интеграцию с KASAP установите или снимите флажок **Выключено**.

7. Нажмите на кнопку **Сохранить**.

В KUMA настроена интеграция с KASAP. Теперь при просмотре информации об алертах и инцидентах можно выбрать относящихся к ним пользователей, чтобы просмотреть, какие курсы обучения прошли пользователи, а также изменить их группу обучения.

Просмотр данных о пользователях KASAP и изменение учебных групп

После настройки интеграции KASAP и KUMA в алертах и инцидентах при просмотре данных о связанных с ними пользователях становятся доступны данные из KASAP:

- Учебная группа, к которой принадлежит пользователь.
- Сведения о пройденных курсах.
- Сведения о запланированном обучении и текущем прогрессе.
- Сведения о полученных сертификатах.

Чтобы просмотреть данные о пользователе из KASAP:

1. В Консоли KUMA в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.
2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.
3. Выберите вкладку **Данные о курсах KASAP**.

В окне отображаются данные пользователя из KASAP.

Вы можете изменить учебную группу пользователя KASAP.

Чтобы изменить учебную группу KASAP:

1. В Консоли KUMA в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.
2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.
3. В раскрывающемся списке **Присвоить пользователю группу KASAP** выберите учебную группу KASAP, в которую вы хотите поместить пользователя.
4. Нажмите **Применить**.

Пользователь будет перемещен в выбранную группу KASAP, администратор компании платформы KASAP получит уведомление об изменении состава учебных групп, а для выбранной учебной группы начнет пересчитываться учебный план.

Подробнее об учебных группах и начале обучения см. в документации KASAP.

Отправка уведомлений в Telegram

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

Вы можете настроить отправку уведомлений в Telegram о срабатывании правил корреляции KUMA. Это позволит уменьшить время реакции на угрозы и при необходимости расширить круг информированных лиц.

Настройка отправки уведомлений в Telegram состоит из следующих этапов:

1. **Создание и настройка бота в Telegram**

   Уведомления о срабатывании правил корреляции отправляет специально созданный бот. Он может отправлять уведомления в личный или групповой чат Telegram.

2. **Создание скрипта для отправки уведомлений**

   Вам необходимо создать скрипт и сохранить его на сервере, где установлен коррелятор.

3. **Настройка отправки уведомлений в KUMA**

   Настройте правило реагирования KUMA, запускающее скрипт для отправки уведомлений, и добавьте это правило в коррелятор.

Создание и настройка бота в Telegram

Чтобы создать и настроить бот в Telegram:

1. В приложении Telegram найдите бот BotFather и откройте чат с ним.
2. В чате нажмите на кнопку **Старт**.
3. Создайте новый бот при помощи команды:

   ```
   /newbot
   ```

4. Введите имя бота.
5. Введите логин бота.

   Бот будет создан. Вы получите ссылку на чат вида t.me/<логин бота> и токен для обращения к боту.

6. Если вы хотите использовать бота в групповом чате,а не в личных сообщениях, необходимо изменить настройки приватности:

   a. В чате бота BotFather введите команду:

   ```
   /mybots
   ```

   b. Выберите нужный бот из списка.

   c. Нажмите **Bot Settings** → **Group Privacy** и выберите опцию **Turn off**.

Бот сможет отправлять сообщения в групповые чаты.

7. Откройте чат с созданным ботом по ссылке вида t.me/<логин бота>, полученной на шаге 5, и нажмите на кнопку **Старт**.

8. Если вы хотите, чтобы бот отправлял личные сообщения пользователю:

   a. В чате с созданным ботом отправьте произвольное сообщение.

   b. Перейдите по ссылке https://t.me/getmyid_bot и нажмите на кнопку **Старт**.

   c. В ответе вы получите значение `Current chat ID`. Это значение понадобится при настройке отправки сообщений.

9. Если вы хотите, чтобы бот отправлял сообщения в групповой чат:

   a. Добавьте бот https://t.me/getmyid_bot в групповой чат, предназначенный для получения уведомлений от KUMA.

   Бот пришлет в групповой чат сообщение, в котором будет указано значение `Current chat ID`. Это значение понадобится при настройке отправки сообщений.

   b. Удалите бот из группы.

10. Отправьте тестовое сообщение через бот. Для этого в адресную строку браузера вставьте следующую ссылку:

    `https://api.telegram.org/bot<token>/sendMessage?chat_id=<chat_id>&text=test`

    где `<token>` – значение, полученное на шаге 5, `<chat_id>` – значение, полученное на шаге 8 или 9.

В результате в личном или групповом чате должно появиться тестовое сообщение, а в ответе браузера JSON не должен содержать ошибок.

Создание скрипта для отправки уведомлений

Чтобы создать скрипт:

1. В консоли сервера, на котором установлен коррелятор, создайте файл скрипта и добавьте в него следующие строки:

```
#!/bin/bash
set -eu
CHAT_ID=<значение Current chat ID, полученное на шаге 8 или 9 инструкции по настройке бота Telegram>
TG_TOKEN=<значение токена, полученное на шаге 5 инструкции по настройке бота Telegram>
RULE=$1
TEXT="Сработало правило <b>$RULE</b>"
curl --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

   Если на сервере коррелятора нет доступа к интернету, вы можете использовать прокси-сервер:

```
#!/bin/bash
set -eu
CHAT_ID=<значение Current chat ID, полученное на шаге 8 или 9 инструкции по настройке бота Telegram>
TG_TOKEN=<значение токена, полученное на шаге 5 инструкции по настройке бота Telegram>
RULE=$1
```

```
TEXT="Сработало правило <b>$RULE</b>"
PROXY=<адрес и порт прокси-сервера>
curl --proxy $PROXY --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT"
--data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

2. Сохраните скрипт в директорию коррелятора, расположенную по пути /opt/kaspersky/kuma/correlator/<ID коррелятора, который будет реагировать на события>/scripts/.

   Информацию о том, как узнать ID коррелятора, см. в разделе Получение идентификатора сервиса.

3. Назначьте пользователя kuma владельцем файла и дайте права на исполнение при помощи следующих команд:

   ```
   chown kuma:kuma /opt/kaspersky/kuma/correlator/<ID коррелятора, который будет
   реагировать>/scripts/<имя скрипта>.sh
   chmod +x /opt/kaspersky/kuma/correlator/<ID коррелятора, который будет
   реагировать>/scripts/<имя скрипта>.sh
   ```

Настройка отправки уведомлений в KUMA

Чтобы настроить отправку уведомлений KUMA в Telegram:

1. Создайте правило реагирования:

   a. В Консоли KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **Добавить правило реагирования**.

   b. В открывшемся окне **Создание правила реагирования** в поле **Название** укажите название правила.

   c. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   d. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

   e. В поле **Название скрипта** укажите имя скрипта.

   f. В поле **Аргументы скрипта** укажите `{{.Name}}`.

      В качестве аргумента выполнения скрипта будет передаваться имя корреляционного события.

   g. Нажмите на кнопку **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

   a. В разделе **Ресурсы** → **Корреляторы** выберите коррелятор, в папку которого вы поместили созданный скрипт для отправки уведомлений.

   b. В дереве шагов выберите **Правила реагирования**.

   c. Нажмите на кнопку **Добавить**.

   d. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 1 этой инструкции.

   e. В дереве шагов выберите **Проверка параметров**.

   f. Нажмите на кнопку **Сохранить и перезапустить сервисы**.

g. Нажмите на кнопку **Сохранить**.

Отправка уведомлений о срабатывании правил KUMA в Telegram будет настроена.

Интеграция с UserGate

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

UserGate – решение, которое обеспечивает безопасность сетевой инфраструктуры, позволяет защитить персональные данные от рисков, связанных с внешними вторжениями, несанкционированным доступом, вирусами и вредоносными приложениями.

Интеграция с UserGate позволяет настроить автоматическую блокировку угроз по IP-адресу, URL или доменному имени при срабатывании правил реагирования KUMA.

Настройка интеграции состоит из следующих этапов:

1. Настройка интеграции в UserGate
2. Подготовка скрипта для правила реагирования
3. Настройка правила реагирования KUMA

Настройка интеграции в UserGate

Чтобы настроить интеграцию в UserGate:

1. Подключитесь к веб-интерфейсу UserGate под учетной записью администратора.
2. Перейдите в раздел **UserGate** → **Администраторы** → **Профили администраторов** и нажмите **Добавить**.
3. В окне **Настройка профиля** укажите имя профиля, например `API`.
4. На вкладке **Разрешения для API** добавьте разрешения на чтение и запись для следующих объектов:
   - content
   - core
   - firewall
   - nlists
5. Нажмите на кнопку **Сохранить**.
6. В разделе **UserGate** → **Администраторы** нажмите **Добавить** → **Добавить локального администратора**.
7. В окне **Свойства администратора** укажите логин и пароль администратора.

В поле **Профиль администратора** выберите профиль, созданный на шаге 3.

8. Нажмите на кнопку **Сохранить**.

9. В адресной строке браузера после адреса и порта UserGate допишите `?features=zone-xml-rpc` и нажмите **ENTER**.

10. Перейдите в раздел **Сеть** → **Зоны** и для зоны того интерфейса, через который будет осуществляться взаимодействие по API, перейдите на вкладку **Контроль доступа** и установите флажок рядом с сервисом **XML-RPC для управления**.

    В список разрешенных адресов при необходимости можно добавить IP-адрес коррелятора KUMA, по правилам корреляции которого должна срабатывать блокировка в UserGate.

11. Нажмите на кнопку **Сохранить**.

Подготовка скрипта для интеграции с UserGate

Чтобы подготовить скрипт к использованию:

1. Скопируйте идентификатор коррелятора, по правилам корреляции которого должна срабатывать блокировка URL, IP-адреса или доменного имени в UserGate:

   a. В Консоли KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Установите флажок рядом с коррелятором, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

   Идентификатор коррелятора будет помещен в буфер обмена.

2. Скачайте скрипт по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. Откройте файл скрипта и в блоке **Enter UserGate Parameters** в параметрах **login** и **password** укажите данные учетной записи администратора UserGate, которая была создана на шаге 7 настройки интеграции в UserGate.

4. Разместите скачанный скрипт на сервере коррелятора KUMA по пути /opt/kaspersky/kuma/correlator/<ID коррелятора из шага 1>/scripts/.

5. Подключитесь к серверу коррелятора по протоколу SSH и перейдите по пути из шага 4 при помощи команды:

   ```
   cd /opt/kaspersky/kuma/correlator/<ID коррелятора из шага 1>/scripts/
   ```

6. Выполните следующую команду:

   ```
   chmod +x ug.py && chown kuma:kuma ug.py
   ```

Скрипт будет готов к использованию.

Настройка правила реагирования для интеграции с UserGate

Чтобы настроить правило реагирования:

1. Создайте правило реагирования:

a. В Консоли KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **Добавить правило реагирования**.

b. В открывшемся окне **Создание правила реагирования** в поле **Название** укажите название правила.

c. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

d. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

e. В поле **Название скрипта** укажите имя скрипта. `ug.py`.

f. В поле **Аргументы скрипта** укажите:

- одну из операций в соответствии с типом блокируемого объекта:
  - `blockurl` – заблокировать доступ по URL;
  - `blockip` – заблокировать доступ по IP-адресу;
  - `blockdomain` – заблокировать доступ по доменному имени.
- `-i {{< поле KUMA, из которого будет взято значение блокируемого объекта, в зависимости от операции >}}`

  Пример:
  `blockurl -i {{.RequetstUrl}}`

g. В блоке **Условия** добавьте условия, соответствующие правилам корреляции, при срабатывании которых необходима блокировка в UserGate.

h. Нажмите на кнопку **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

a. В разделе **Ресурсы** → **Корреляторы** выберите коррелятор, который будет выполнять реагирование и в папку которого вы поместили скрипт.

b. В дереве шагов выберите **Правила реагирования**.

c. Нажмите на кнопку **Добавить**.

d. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 1 этой инструкции.

e. В дереве шагов выберите **Проверка параметров**.

f. Нажмите на кнопку **Сохранить и обновить параметры сервисов**.

g. Нажмите на кнопку **Сохранить**.

Правило реагирования будет привязано к коррелятору и готово к использованию.

Интеграция с Kaspersky Web Traffic Security

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

Вы можете настроить интеграцию с системой анализа и фильтрации веб-трафика Kaspersky Web Traffic Security (далее также "KWTS").

Настройка интеграции заключается в создании правил реагирования KUMA, которые позволяют запускать задачи KWTS. Задачи должны быть предварительно созданы в веб-интерфейсе KWTS.

Настройка интеграции состоит из следующих этапов:

1. Настройка интеграции в KWTS
2. Подготовка скрипта для правила реагирования
3. Настройка правила реагирования KUMA

Настройка интеграции в KWTS

Чтобы подготовиться к интеграции в KWTS:

1. Подключитесь к веб-интерфейсу KWTS под учетной записью администратора и создайте роль с правами на просмотр и создание/изменение правила.

   Подробнее о создании роли см. *справку Kaspersky Web Traffic Security*.

2. Назначьте созданную роль пользователю с NTML-аутентификацией.

   Вместо этого вы можете использовать учетную запись локального администратора.

3. В разделе **Правила** перейдите на вкладку **Доступ** и нажмите **Добавить правило**.

4. В раскрывающемся списке **Действие** выберите **Заблокировать**.

5. В раскрывающемся списке **Фильтрация трафика** выберите значение **URL** и в поле справа укажите несуществующий или заведомо вредоносный адрес.

6. В поле **Название правила** укажите название правила.

7. Включите использование правила с помощью переключателя **Статус**.

8. Нажмите на кнопку **Добавить**.

9. В веб-интерфейсе KWTS откройте только что созданное правило.

10. Запишите значение ID, отображаемое в конце адреса страницы в адресной строке браузера.

    Это значение будет использовано при настройке правила реагирования в KUMA.

Подготовка к интеграции в KWTS будет завершена.

Подготовка скрипта для интеграции с KWTS

Чтобы подготовить скрипт к использованию:

1. Скопируйте идентификатор коррелятора, по правилам корреляции которого должна срабатывать блокировка URL, IP-адреса или доменного имени в KWTS:

   a. В Консоли KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.

   b. Установите флажок рядом с коррелятором, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

   Идентификатор коррелятора будет помещен в буфер обмена.

2. Скачайте скрипт и библиотеку по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. Разместите скачанный скрипт на сервере коррелятора KUMA по пути /opt/kaspersky/kuma/correlator/<`ID коррелятора из шага 1`>/scripts/.

4. Подключитесь к серверу коррелятора по протоколу SSH и перейдите по пути из шага 3 при помощи команды:

   ```
   cd /opt/kaspersky/kuma/correlator/<ID коррелятора из шага 1>/scripts/
   ```

5. Выполните следующую команду:

   ```
   chmod +x kwts.py kwtsWebApiV6.py && chown kuma:kuma kwts.py kwtsWebApiV6.py
   ```

Скрипт будет готов к использованию.

Настройка правила реагирования для интеграции с KWTS

Чтобы настроить правило реагирования:

1. Создайте правило реагирования:

   a. В Консоли KUMA выберите раздел **Ресурсы** → **Правила реагирования** и нажмите на кнопку **Добавить правило реагирования**.

   b. В открывшемся окне **Создание правила реагирования** в поле **Название** укажите название правила.

   c. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   d. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

   e. В поле **Название скрипта** укажите имя скрипта. kwts.py.

   f. В поле **Аргументы скрипта** укажите:

   - `--host` – адрес сервера KWTS.
   - `--username` – имя учетной записи пользователя, созданной в KWTS, или локального администратора.
   - `--password` – пароль учетной записи пользователя KWTS.
   - `--rule_id` – ID правила, созданного в KWTS.

- Укажите один из ключей в соответствии с типом блокируемого объекта:
  - `--url` – укажите поле события KUMA, из которого вы хотите получать URL, например `{{.RequestUrl}}`.
  - `--ip` – укажите поле события KUMA, из которого вы хотите получать IP-адрес, например `{{.DestinationAddress}}`.
  - `--domain` – укажите поле события KUMA, из которого вы хотите получать доменное имя, например `{{.DestinationHostName}}`.
- `--ntlm` – укажите этот ключ, если пользователь KWTS был создан с NTLM-аутентификацией.

Пример:
```
--host <address> --username <user> --password <pass> --rule_id <id> --url {{.RequestUrl}}
```

g. В блоке **Условия** добавьте условия, соответствующие правилам корреляции, по срабатыванию которых необходима блокировка в KWTS.

h. Нажмите на кнопку **Сохранить**.

2. Добавьте созданное правило реагирования в коррелятор:

a. В разделе **Ресурсы** → **Корреляторы** выберите коррелятор, который будет выполнять реагирование и в папку которого вы поместили скрипт.

b. В дереве шагов выберите **Правила реагирования**.

c. Нажмите на кнопку **Добавить**.

d. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 1 этой инструкции.

e. В дереве шагов выберите **Проверка параметров**.

f. Нажмите на кнопку **Сохранить и обновить параметры сервисов**.

g. Нажмите на кнопку **Сохранить**.

Правило реагирования будет привязано к коррелятору и готово к использованию.

Интеграция с Kaspersky Secure Mail Gateway

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

Вы можете настроить интеграцию с системой анализа и фильтрации почтового трафика Kaspersky Secure Mail Gateway (далее также "KSMG").

Настройка интеграции заключается в создании правил реагирования KUMA, которые позволяют запускать задачи KSMG. Задачи должны быть предварительно созданы в веб-интерфейсе KSMG.

Настройка интеграции состоит из следующих этапов:

1. Настройка интеграции в KSMG
2. Подготовка скрипта для правила реагирования
3. **Настройка правила реагирования KUMA**

Настройка интеграции в KSMG

Чтобы подготовиться к интеграции в KSMG:

1. Подключитесь к веб-интерфейсу KSMG под учетной записью администратора и создайте роль с правами на просмотр и создание/изменение правила.

   Подробнее о создании роли см. *справку Kaspersky Secure Mail Gateway*.

2. Назначьте созданную роль пользователю с NTML-аутентификацией.

   Вы можете использовать учетную запись локального администратора Administrator.

3. В разделе **Правила** нажмите **Создать**.

4. В левой панели выберите раздел **Общие**.

5. Включите использование правила с помощью переключателя **Статус**.

6. В поле **Название правила** введите название нового правила.

7. В блоке параметров **Режим** выберите один из вариантов обработки сообщений, соответствующий критериям этого правила.

8. В блоке параметров **Отправитель** на вкладке **Адреса эл. почты** укажите несуществующий или заведомо вредоносный адрес отправителя.

9. В блоке параметров **Получатель** на вкладке **Адреса эл. почты** укажите требуемых получателей или символ "*", чтобы выбрать всех получателей.

10. Нажмите на кнопку **Сохранить**.

11. В веб-интерфейсе KSMG откройте только что созданное правило.

12. Запишите значение ID, отображаемое в конце адреса страницы в адресной строке браузера.

    Это значение будет использовано при настройке правила реагирования в KUMA.

Подготовка к интеграции в KSMG будет завершена.

Подготовка скрипта для интеграции с KSMG

Чтобы подготовить скрипт к использованию:

1. Скопируйте идентификатор коррелятора, по правилам корреляции которого должна срабатывать блокировка IP-адреса или адреса электронной почты отправителя сообщения в KSMG:

a. В Консоли KUMA перейдите в раздел **Ресурсы** → **Активные сервисы**.

b. Установите флажок рядом с коррелятором, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

Идентификатор коррелятора будет помещен в буфер обмена.

2. Скачайте скрипт и библиотеку по следующей ссылке:

https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. Разместите скачанный скрипт на сервере коррелятора KUMA по пути /opt/kaspersky/kuma/correlator/<ID коррелятора из шага 1>/scripts/.

4. Подключитесь к серверу коррелятора по протоколу SSH и перейдите по пути из шага 3 при помощи команды:

```
cd /opt/kaspersky/kuma/correlator/<ID коррелятора из шага 1>/scripts/
```

5. Выполните следующую команду:

```
chmod +x ksmg.py ksmgWebApiV2.py && chown kuma:kuma ksmg.py ksmgWebApiV2.py
```

Скрипт будет готов к использованию.

Импорт информации об активах из RedCheck

Эта интеграция является примером и может потребовать дополнительной настройки в зависимости от используемых версий и особенностей инфраструктуры.
Условия премиальной технической поддержки не распространяются на эту интеграцию, запросы на поддержку рассматриваются без гарантированного времени ответа.

RedCheck – это система контроля защищенности и управления информационной безопасностью организации.

Вы можете импортировать в KUMA сведения об активах из отчетов сканирования сетевых устройств, проведенного с помощью RedCheck.

Импорт доступен из простых отчетов "Уязвимости" и "Инвентаризация" в формате CSV, сгруппированных по устройствам.

Импортированные активы отображаются в Консоли KUMA в разделе **Активы**. При необходимости вы можете редактировать параметры активов.

Импорт данных происходит через API с помощью утилиты redcheck-tool.py. Для работы утилиты требуется Python версии 3.6 или выше и следующие библиотеки:

- csv
- re
- json
- requests
- argparse

- sys

Чтобы импортировать данные об активах из отчета RedCheck:

1. Сформируйте в RedCheck отчет о сканировании сетевых активов в формате CSV и скопируйте файл отчета на сервер со скриптом.

   Подробнее о задачах на сканирование и форматах выходных файлов см. в документации RedCheck.

2. Создайте файл с токеном для доступа к KUMA REST API.

   Учетная запись, для которой создается токен, должна отвечать следующим требованиям:

   - Роль Администратора или Аналитика.
   - Доступ к тенанту, в который будут импортированы активы.
   - Права на использование API-запросов GET /assets, GET /tenants, POST/assets/import.

3. Скачайте скрипт по следующей ссылке:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

4. Скопируйте утилиту redcheck-tool.py на сервер с Ядром KUMA и сделайте файл утилиты исполняемым при помощи команды:

   ```
   chmod +x <путь до файла redcheck-tool.py>
   ```

5. Запустите утилиту redcheck-tool.py с помощью следующей команды:

   ```
   python3 redcheck-tool.py --kuma-rest <адрес и порт сервера KUMA REST API> --token <API-токен> --tenant <название тенанта, куда будут помещены активы> --vuln-report <полный путь к файлу отчета "Уязвимости"> --inventory-report <полный путь к файлу отчета "Инвентаризация">
   ```

   Пример:
   ```
   python3 --kuma-rest example.kuma.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant Main --vuln-report /home/user/vuln.csv --inventory-report /home/user/inventory.csv
   ```

   Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения расширенного отчета о полученных активах `-v`. Подробное описание доступных флагов и команд приведено в таблице "Флаги и команды утилиты redcheck-tool.py". Также для просмотра информации о доступных флагах и командах вы можете использовать команду `--help`.

Информация об активах будет импортирована из отчета RedCheck в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

Пример:
```
inventory has been imported for 2 host(s)
software has been imported for 5 host(s)
vulnerabilities has been imported for 4 host(s)
```

Пример расширенной информации об импорте:
```
[inventory import] Host: localhost Code: 200 Response: {'insertedIDs': {'0': '52ca11c6-a0e6-4dfd-8ef9-bf58189340f8'}, 'updatedCount': 0, 'errors': []}
[inventory import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {'0': '1583e552-5137-4164-92e0-01e60fb6edb0'}, 'updatedCount': 0, 'errors': []}
[software import][error] Host: localhost Skipped asset with FQDN localhost or IP 127.0.0.1
[software import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.1 Code: 200 Response: {'insertedIDs': {'0': '0628f683-c20c-4107-abf3-d837b3dbbf01'}, 'updatedCount': 0, 'errors': []}
[vulnerabilities import] Host: localhost Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
```

```
[vulnerabilities import] Host: 10.0.0.3 Code: 200 Response: {'insertedIDs': {'0': 'ed01e0a8-dcb0-4609-ab2b-
91e50092555d'}, 'updatedCount': 0, 'errors': []}
inventory has been imported for 2 host(s)
software has been imported for 1 host(s)
vulnerabilities has been imported for 4 host(s)
```

Поведение утилиты при импорте активов:

- KUMA перезаписывает данные импортированных через API активов и удаляет сведения об их устраненных уязвимостях.
- KUMA пропускает активы с недействительными данными.

Флаги и команды утилиты redcheck-tool.py

Флаги и команды	Обязательное ли поле	Описание
`--kuma-rest <адрес и порт сервера KUMA>`	Да	По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
`--token <токен>`	Да	Значение в параметре должно содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Администратора или Аналитика.
`--tenant <название тенанта>`	Да	Название тенанта KUMA, в который будут импортированы активы из отчета RedCheck.
`--vuln-report <полный путь к файлу отчета "Уязвимости">`	Да	Файл отчета "Уязвимости" в формате CSV.
`--inventory-report <полный путь к файлу отчета "Инвентаризация">`	Нет	Файл отчета "Инвентаризация" в формате CSV.
`-v`	Нет	Отображение расширенной информации об импорте активов.

Возможные ошибки

Сообщение об ошибке	Описание
Tenant %w not found	Имя тенанта не найдено.
Tenant search error: Unexpected status Code: %d	При поиске тенанта был получен неожиданный код ответа HTTP.
Asset search error: Unexpected status Code: %d	При поиске актива был получен неожиданный код ответа HTTP.
[%w import][error] Host: %w Skipped asset with FQDNlocalhost or IP 127.0.0.1	При импорте информации инвентаризации/уязвимостей было пропущено устройство cfqdn=localhost или ip=127.0.0.1.

Настройка получения событий Sendmail

Вы можете настроить получение событий из почтового агента Sendmail в SIEM-систему KUMA.

Настройка получения событий состоит из следующих этапов:

1. Настройка журналирования Sendmail.
2. Настройка сервера источника событий.
3. Создание коллектора KUMA.

   Для получения событий Sendmail в мастере установки коллектора используйте следующие значения:

   - На шаге **Парсинг событий** выберите нормализатор **[OOTB] Sendmail syslog**.
   - На шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

4. Установка коллектора KUMA.

5. Проверка поступления событий Sendmail в коллектор KUMA.

   Вы можете проверить, что настройка сервера источника событий Sendmail выполнена правильно в Консоли KUMA в разделе Поиск связанных событий.

Настройка журналирования Sendmail

По умолчанию события системы Sendmail записываются в syslog.

Чтобы убедиться в правильности настройки журналирования:

1. Подключитесь по SSH к серверу, на котором установлена система Sendmail.

2. Выполните следующую команду:

   ```
   cat /etc/rsyslog.d/50-default.conf
   ```

   Команда должна вернуть следующую строку:

   ```
   mail.* -/var/log/mail.log
   ```

Если журналирование настроено корректно, вы можете перейти к настройке передачи событий Sendmail.

Настройка передачи событий Sendmail

Для передачи событий от сервера, на котором установлен почтовый агент Sendmail, в коллектор KUMA используется сервис rsyslog.

Чтобы настроить передачу событий Sendmail в коллектор:

1. Подключитесь к серверу, на котором установлен Sendmail, под учетной записью с административными привилегиями.

2. В директории /etc/rsyslog.d/ создайте файл Sendmail-to-siem.conf и добавьте в него строку:

   ```
   If $programname contains 'sendmail' then @<<IP-адрес коллектора>:<порт коллектора>>
   ```

   Пример:

   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'sendmail' then @@<<IP-адрес коллектора>:<порт коллектора>>
   ```

3. Создайте резервную копию файла /etc/rsyslog.conf.

4. В конфигурационный файл /etc/rsyslog.conf добавьте следующие строки:

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните внесенные изменения

6. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Управление KUMA

В этом разделе описываются общие параметры KUMA.

Просмотр метрик KUMA

В Консоли KUMA в качестве системы контроля используется решение VictoriaMetrics. Каждые пять секунд VictoriaMetrics использует HTTP-интерфейс для извлечения метрик Ядра KUMA, коллекторов, коррелляторов, хранилищ и агентов. Сервис kuma-core генерирует конфигурацию решения VictoriaMetrics, которое также определяет получение метрик, далее также микросервис Ядра KUMA. Когда вы создаете или удаляете сервис, Ядро KUMA автоматически добавляет или удаляет соответствующую метрику в конфигурации решения VictoriaMetrics.

Полученные метрики можно просматривать с помощью решения Grafana. RPM-пакет сервиса kuma-core генерирует конфигурацию решения Grafana и создает отдельную панель мониторинга для визуализации показателей каждого сервиса. Графики в разделе **Метрики** появляются с задержкой примерно в 1,5 минуты.

Информацию о метриках см. в Консоли KUMA в разделе **Метрики**. При выборе этого раздела открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра KUMA. Если в разделе **Метрики** вы видите core: <номер порта>, это означает, что KUMA развернута в конфигурации высокой доступности и метрики получены с устройства, на котором было установлено Ядро KUMA. В прочих конфигурациях отображается имя устройства, с которого KUMA получает метрики.

Чтобы определить, на каком устройстве работает Ядро, в терминале одного из контроллеров выполните следующую команду:

```
k0s kubectl get pod -n kuma -o wide
```

Логин и пароль Grafana по умолчанию: `admin` и `admin`.

Метрики коллектора

Название метрики	Описание
IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество обработанных событий в секунду.
Output EPS	Количество событий, отправляемых точке назначения в секунду.
Output Latency	Время в миллисекундах, прошедшее после отправки пакета событий точке назначения и после получения от нее ответа. Отображается среднее значение.
Output Errors	Количество ошибок, возникающих в секунду при отправке пакетов событий в точку назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например, если запрос был недействительным.

Output Disk Buffer SIze	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается нулевое значение, в дисковой буфер коллектора не помещен ни один пакет событий и сервис работает правильно.
Write Network BPS	Количество байтов, поступающих в сеть в секунду.
Connector errors	Количество ошибок в журналах событий коннектора.
Normalization (Нормализация) – показатели, относящиеся к нормализаторам.	
Raw & Normalized event size	Размер сырого события и размер нормализованного события. Отображается среднее значение.
Errors	Количество ошибок нормализации в секунду.
Filtration – показатели, относящиеся к фильтрам.	
EPS	Количество событий, соответствующих условиям фильтра, отправляемых на дальнейшую обработку в секунду. Коллектор обрабатывает отфильтрованные события только в том случае, если пользователь добавил фильтр в конфигурацию сервиса коллектора.
Aggregation (Агрегация) – показатели, относящиеся к правилам агрегации.	
EPS	Количество событий, полученных и созданных правилом агрегации в секунду. Этот показатель помогает определить эффективность правил агрегации.
Buckets	Количество контейнеров в правиле агрегации.
Enrichment – показатели, относящиеся к правилам обогащения.	
Cache RPS	Количество запросов к локальному кешу в секунду.
Source RPS	Количество запросов в секунду, отправленных источнику обогащения, например словарю.
Source Latency	Время в миллисекундах, прошедшее после отправки запроса источнику обогащения и после получения от него ответа. Отображается среднее значение.
Queue	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors	Количество ошибок в секунду при отправке запросов к источнику обогащения.

Показатели корреляторов

Название метрики	**Описание**
IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество обработанных событий в секунду.
Output EPS	Количество событий, отправляемых точке назначения в секунду.
Output Latency	Время в миллисекундах, прошедшее после отправки пакета событий точке назначения и после получения от нее ответа. Отображается среднее значение.
Output Errors	Количество ошибок, возникающих в секунду при отправке пакетов событий в точку назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например, если запрос был недействительным.

Output Disk Buffer SIze	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается нулевое значение, в дисковой буфер коллектора не помещен ни один пакет событий и сервис работает правильно.
Correlation – показатели, относящиеся к правилам корреляции.	
EPS	Количество событий корреляции в секунду, созданных правилом корреляции.
Buckets	Количество контейнеров в правиле корреляции стандартного типа.
Rate Limiter Hits	Количество превышений правилом корреляции предельного значения срабатываний в секунду.
Active Lists OPS	Количество запросов на выполнение операций, отправленных активному листу в секунду, и сами операции.
Active Lists Records	Количество записей в активном листе.
Active Lists On-Disk Size	Размер активного листа на диске в байтах.
Enrichment – показатели, относящиеся к правилам обогащения.	
Cache RPS	Количество запросов к локальному кешу в секунду.
Source RPS	Количество запросов в секунду, отправленных источнику обогащения, например словарю.
Source Latency	Время в миллисекундах, прошедшее после отправки запроса источнику обогащения и после получения от него ответа. Отображается среднее значение.
Queue	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors	Количество ошибок в секунду при отправке запросов к источнику обогащения.
Response – показатели, связанные с правилами реагирования.	
RPS	Количество срабатываний правила реагирования в секунду.

Метрики хранилища

Название метрики	**Описание**
ClickHouse/General – показатели, относящиеся к общим параметрам кластера ClickHouse.	
Active Queries	Количество активных запросов, отправленных кластеру ClickHouse. Эта метрика отображается для каждого экземпляра ClickHouse.
QPS	Количество запросов в секунду, отправленных кластеру ClickHouse.
Failed QPS	Количество неудачных запросов в секунду, отправленных кластеру ClickHouse.
Allocated memory	Объем оперативной памяти в гигабайтах, выделенной процессу ClickHouse.
ClickHouse/Insert – метрики, относящиеся к вставке событий в экземпляр ClickHouse.	
Insert EPS	Количество событий в секунду, вставленных в экземпляр ClickHouse.
Insert QPS	Количество запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse.
Failed Insert QPS	Количество неудачных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse.

Delayed Insert QPS	Количество отложенных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Запросы были отложены узлом ClickHouse из-за превышения мягкого ограничения активного объединения запросов.
Rejected Insert QPS	Количество отклоненных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Запросы были отложены узлом ClickHouse из-за превышения жесткого ограничения активного объединения запросов.
Active Merges	Количество активных объединений запросов.
Distribution Queue	Количество временных файлов с событиями, которые не удалось вставить в экземпляр ClickHouse из-за его недоступности. Эти события не могут быть найдены с помощью поиска.
ClickHouse/Select – показатели, относящиеся к выборкам событий в экземпляре ClickHouse.	
Select QPS	Количество запросов на выборку событий в секунду в экземпляре ClickHouse, отправленных кластеру ClickHouse.
Failed Select QPS	Количество неудачных запросов на выборку событий в секунду в экземпляре ClickHouse, отправленных кластеру ClickHouse.
ClickHouse/Replication – метрики, относящиеся к репликам узлов ClickHouse.	
Active Zookeeper Connections	Количество активных подключений к узлам кластера Zookeeper. При нормальной работе это количество должно быть равно количеству узлов в кластере Zookeeper.
Read-only Replicas	Количество реплик узлов ClickHouse, доступных только для чтения. При нормальной работе таких реплик узлов ClickHouse нет.
Active Replication Fetches	Количество активных процессов скачивания данных с узла ClickHouse при репликации данных.
Active Replication Sends	Количество активных процессов отправки данных узлу ClickHouse при репликации данных.
Active Replication Consistency Checks	Количество активных проверок согласованности данных на репликах узлов ClickHouse при репликации данных.
ClickHouse/Networking – показатели, относящиеся к сети кластера ClickHouse.	
Active HTTP Connections	Количество активных подключений к HTTP-серверу кластера ClickHouse.
Active TCP Connections	Количество активных подключений к TCP-серверу кластера ClickHouse.
Active Interserver Connections	Количество активных межсервисных соединений между узлами ClickHouse.

Метрики Ядра KUMA

Название метрики	**Описание**
Raft – метрики, связанные с чтением и обновлением состояния Ядра KUMA.	
Lookup RPS	Количество запросов процедуры поиска в секунду, отправленных в Ядро KUMA, и сами процедуры.
Lookup Latency	Время в миллисекундах, затраченное на выполнение процедур поиска и на выполнение самих процедур. Отображается время для 99-го процентиля процедур поиска. Один процент процедур поиска может занять больше времени.
Propose RPS	Количество запросов на выполнение процедур обновления состояния, отправленных Ядру KUMA в секунду, и сами процедуры.
Propose Latency	Время в миллисекундах, затраченное на выполнение процедур обновления состояния и на выполнение самих процедур. Отображается время для 99-го процентиля процедур обновления состояния. Один процент процедур обновления

	состояния может занять больше времени.
API – метрики, относящиеся к запросам API.	
RPS	Количество запросов API к Ядру KUMA в секунду.
Latency	Время в миллисекундах, затраченное на обработку одного запроса API к Ядру KUMA. Отображается среднее значение.
Errors	Количество ошибок в секунду при отправке API-запросов к Ядру KUMA.
Notification Feed – показатели, относящиеся к активности пользователей.	
Subscriptions	Количество клиентов, подключенных к Ядру KUMA через SSE для получения сообщений сервера в реальном времени. Это число обычно равно количеству клиентов, использующих Консоль KUMA.
Errors	Количество ошибок в секунду при отправке уведомлений пользователям.
Schedulers – показатели, относящиеся к задачам Ядра KUMA.	
Активная	Количество повторяющихся активных системных задач. Задачи, созданные пользователем, игнорируются.
Latency	Время в миллисекундах, затраченное на выполнение задачи. Отображается среднее значение.
Errors	Количество ошибок в секунду, возникших при выполнении задач.

Метрики агента KUMA

Название метрики	**Описание**
IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество обработанных событий в секунду.
Output EPS	Количество событий, отправляемых точке назначения в секунду.
Output Latency	Время в миллисекундах, прошедшее после отправки пакета событий точке назначения и после получения от нее ответа. Отображается среднее значение.
Output Errors	Количество ошибок, возникающих в секунду при отправке пакетов событий в точку назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например, если запрос был недействительным.
Output Disk Buffer Slze	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается нулевое значение, в дисковой буфер коллектора не помещен ни один пакет событий и сервис работает правильно.
Write Network BPS	Количество байтов, поступающих в сеть в секунду.

Метрики маршрутизаторов событий

Название метрики	**Описание**
IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество обработанных событий в секунду.

Output EPS	Количество событий, отправляемых точке назначения в секунду.
Output Latency	Время в миллисекундах, прошедшее после отправки пакета событий точке назначения и после получения от нее ответа. Отображается среднее значение.
Output Errors	Количество ошибок, возникающих в секунду при отправке пакетов событий в точку назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например, если запрос был недействительным.
Output Disk Buffer Slze	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается нулевое значение, в дисковой буфер коллектора не помещен ни один пакет событий и сервис работает правильно.
Write Network BPS	Количество байтов, поступающих в сеть в секунду.
Connector Errors	Количество ошибок в журналах событий коннектора.

Метрики, общие для всех сервисов

Название метрики	Описание
Process – общие метрики процесса.	
Memory	Использование оперативной памяти (RSS) в мегабайтах.
DISK BPS	Количество байтов, считываемых с диска или записываемых на диск в секунду.
Network BPS	Количество байтов, получаемых/передаваемых в сеть в секунду.
Network Packet Loss	Количество сетевых пакетов, потерянных в секунду.
GC Latency	Время в миллисекундах, затраченное на выполнение цикла сборщика мусора GO (Garbage Collector). Отображается среднее значение.
Goroutines	Количество активных горутин. Это число отличается от количества потоков операционной системы.
OS – показатели, относящиеся к операционной системе.	
Load	Средняя нагрузка.
Процессор	Загрузка процессора в процентах.
Memory	Использование оперативной памяти (RSS) в процентах.
Disk	Использование дискового пространства в процентах.

Срок хранения метрик

По умолчанию данные о работе KUMA хранятся 3 месяца. Этот срок можно изменить.

Чтобы изменить срок хранения метрик KUMA:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service в параметре ExecStart измените флаг `--retentionPeriod=<срок хранения метрик в месяцах>`, подставив нужный срок. Например, `--retentionPeriod=4` означает, что метрики будут храниться 4 месяца.

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-victoria-metrics`

Срок хранения метрик изменен.

Работа с задачами KUMA

При работе в консоли приложения вы можете выполнять различные операции с помощью задач. Например, вы можете выполнить импорт активов или экспортировать информацию о событиях KUMA в TSV-файл.

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Диспетчер задач** окна консоли. Вы можете просматривать задачи, созданные вами (текущим пользователем).

Пользователь с ролью Главного администратора может просматривать задачи всех пользователей.

В таблице задач содержится следующая информация:

- **Статус** – статус задачи. Задаче может быть присвоен один из следующих статусов:
  - *Мигает зеленая точка* – задача активна.
  - **Завершено** – задача выполнена.
  - **Отмена** – задача отменена пользователем.
  - **Ошибка** – задача не была завершена из-за ошибки. Сообщение об ошибке отображается при наведении курсора мыши на значок восклицательного знака.
- **Задача** – тип задачи. В приложении доступны следующие типы задач:
  - **Экспорт событий** – экспорт событий KUMA.
  - **Threat Lookup** – запрос данных с портала Kaspersky Threat Intelligence Portal.
  - **Ретроспективная проверка** – задание на воспроизведение событий.
  - **Импорт активов OSMP** – импорт данных об активах с Серверов администрирования Kaspersky Security Center.
  - **Импорт учетных записей** – импорт данных о пользователях из Active Directory.
  - **Импорт активов KICS for Networks** – импорт данных об активах из KICS for Networks.
  - **Обновление репозитория** - обновления репозитория KUMA для получения пакетов с ресурсами из указанного в настройках источника.

- **Создал** – пользователь, создавший задачу. Если задача создана автоматически, в столбце указано **Задача по расписанию**.

  Этот столбец отображается только для пользователей с ролями Главный администратор и Администратор тенанта.

- **Создана** – время создания задачи.

- **Последнее обновление** – время обновления задачи.

- **Тенант** – название тенанта, в котором была запущена задача.

Формат даты задачи зависит от языка локализации, выбранного в параметрах приложения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.

- Русская локализация: ДД.ММ.ГГГГ.

Настройка отображения таблицы задач

Вы можете настроить отображение столбцов, а также порядок их следования в таблице задач.

Чтобы настроить отображение и порядок следования столбцов в таблице задач:

1. В Консоли KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. В заголовочной части таблицы нажмите на кнопку .

3. В открывшемся окне выполните следующие действия:

   - Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   - Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите сбросить параметры, нажмите на ссылку **По умолчанию**.

5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на название столбца, зажмите левую клавишу мыши и перетащите столбец в нужное место.

Отображение столбцов в таблице задач будет настроено.

Просмотр результатов выполнения задачи

Чтобы просмотреть результат выполнения задачи:

1. В Консоли KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Показать результат**.

Откроется окно с результатом выполнения задачи.

Повторный запуск задачи

Чтобы перезапустить задачу:

1. В Консоли KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Перезапустить**.

Задача будет запущена повторно.

Прокси-серверы

Прокси-серверы используются для хранения параметров конфигурации прокси-серверов, например в точках назначения. Поддерживается тип http.

Доступные параметры:

- **Название** (обязательно) – уникальное имя прокси-сервера. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Секрет отдельно** – если этот флажок установлен, в окне отображается обязательное поле **URL**, в котором можно указать URL подключения, и раскрывающийся список **Секрет** с секретами типа "credentials". Таким образом вы сможете просматривать информацию о подключении без необходимости повторно создавать большое количество подключений, если изменился пароль учетной записи, которую вы использовали для подключений. Если флажок снят, поля **URL** и **Секрет** недоступны. По умолчанию флажок снят.
- **URL** (обязательное) – поле для указания URL подключения. URL используется вместе с секретом типа "credentials". Поле доступно, если установлен флажок **Секрет отдельно**.
- **Секрет** – раскрывающийся список для выбора существующего секрета или создания секрета типа "credentials". Раскрывающийся список доступен, когда установлен флажок **Секрет отдельно**.
- **Брать URL из секрета** (обязательно) – раскрывающийся список для выбора ресурса секрета, в котором хранятся URL прокси-серверов. При необходимости секрет можно указать в окне создания прокси-сервера с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
- **Не использовать на доменах** – один или несколько доменов, к которым требуется прямой доступ.
- **Описание** – вы можете добавить до 4000 символов в кодировке Unicode.

Подключение к SMTP-серверу

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Пользователи будут получать уведомления, если в параметрах их профиля установлен флажок **Получать уведомления по почте**.

Для обработки уведомлений KUMA можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в Консоли KUMA в разделе **Параметры → Общие → Параметры подключения к SMTP-серверу**.

Чтобы настроить подключение к SMTP-серверу:

1. В Консоли KUMA перейдите в раздел **Параметры → Общие**.
2. В блоке параметров **Параметры подключения к SMTP-серверу** измените необходимые параметры:
   - **Выключено** – установите этот флажок, если хотите отключить подключение к SMTP-серверу.
   - **Адрес сервера** (обязательно) – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.
   - **Порт** (обязательно) – порт подключения к почтовому серверу. Значение должно быть целым числом от 1 до 65 535.
   - **От кого** (обязательно) – адрес электронной почты отправителя сообщения. Например, `kuma@company.com`.
   - **Псевдоним сервера Ядра KUMA** – название сервера Ядра KUMA, которое используется в вашей сети. Должно отличаться от полного доменного имени (FQDN).
   - При необходимости в раскрывающемся списке **Секрет** выберите секрет типа **credentials**, в котором записаны учетные данные для подключения к SMTP-серверу.

     Добавить секрет

1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

   Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

   Секрет будет добавлен и отобразится в списке **Секрет**.

- Выберите периодичность уведомлений в раскрывающемся списке **Регулярность уведомлений мониторинга**.

  Уведомления о срабатывании политики мониторинга от источника будут повторяться через выбранный период, пока статус источника не станет вновь зеленым.

  Если вы выберете значение **Не повторять**, уведомление о срабатывании политики мониторинга придет только один раз.

- Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен.

3. Нажмите на кнопку **Сохранить**.

Соединение с SMTP-сервером настроено, пользователи могут получать сообщения электронной почты от KUMA.

Работа с задачами Kaspersky Security Center

Вы можете подключить активы Kaspersky Security Center к KUMA и загружать на эти активы обновления баз и модулей приложений или запускать на них антивирусную проверку с помощью задач Kaspersky Security Center. Задачи запускаются в Консоли KUMA.

Для запуска задач Kaspersky Security Center на активах, подключенных к KUMA, рекомендуется использовать следующий сценарий:

1. **Создание в Консоли администрирования Kaspersky Security Center учетной записи пользователя**

   Данные этой учетной записи используются при создании секрета для установки соединения с Kaspersky Security Center и могут использоваться при создании задачи.

   Подробнее о создании учетной записи и назначении прав пользователю см. в *справке Kaspersky Security Center*.

2. **О создании задач KUMA в Kaspersky Security Center**

3. Настройка интеграции KUMA с Kaspersky Security Center

4. Импорт информации об активах Kaspersky Security Center в KUMA

5. Назначение категории импортированным активам

   После импорта активы автоматически помещаются в группу **Устройства без категории**. Вы можете назначить импортированным активам одну из существующих категорий или создать категорию и назначить ее активам.

6. **Запуск задач на активах**

   Вы можете запускать задачи вручную в информации об активе или настроить автоматический запуск задач.

О создании задач KUMA в Kaspersky Security Center

Вы можете запустить на активах Kaspersky Security Center, подключенных к KUMA, задачу обновления антивирусных баз и модулей приложения и задачу антивирусной проверки. На активах должны быть установлены приложения Kaspersky Endpoint Security для Windows или Endpoint Security for Windows для Linux. Задачи создаются в Консоли OSMP.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security для Windows см. в справке *Kaspersky Endpoint Security для Windows*.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security для Linux см. в справке *Kaspersky Endpoint Security для Linux*.

Имя задач должно начинаться с "kuma" (без учета регистра и без кавычек). Например, `KUMA antivirus check`. В противном случае задача не отображается в списке доступных задач в Консоли KUMA.

Запуск задач Kaspersky Security Center вручную

Вы можете вручную запускать на активах Kaspersky Security Center, подключенных к KUMA, задачу обновления антивирусных баз и модулей приложения и задачу антивирусной проверки. На активах должны быть установлены приложения Kaspersky Endpoint Security для Windows или Endpoint Security for Windows для Linux.

Предварительно вам нужно настроить интеграцию Kaspersky Security Center с KUMA и создать задачи в Kaspersky Security Center.

Чтобы запустить задачу Kaspersky Security Center вручную:

1. В Консоли KUMA перейдите в раздел **Активы** и выберите актив, импортированный из Kaspersky Security Center.

   Откроется окно **Информация об активе**.

2. Нажмите на **Реагирование OSMP**.

Кнопка отображается, если подключение к Kaspersky Security Center, к которому принадлежит выбранный актив, включено.

3. В открывшемся окне **Выберите задачу** установите флажки рядом с задачами, которые вы хотите запустить, и нажмите на кнопку **Запустить**.

Kaspersky Security Center запускает выбранные задачи.

Некоторые типы задач доступны только для определенных активов.

Информация об уязвимостях и программном обеспечении доступна только для активов с операционной системой Windows.

Автоматический запуск задач Kaspersky Security Center

Вы можете настроить автоматический запуск задачи обновления антивирусных баз и модулей приложения и задачи антивирусной проверки на активах Kaspersky Security Center, подключенных к KUMA. На активах должны быть установлены приложения Kaspersky Endpoint Security для Windows или Endpoint Security for Windows для Linux.

Предварительно вам нужно настроить интеграцию Kaspersky Security Center с KUMA и создать задачи в Kaspersky Security Center.

Настройка автоматического запуска задач Kaspersky Security Center включает следующие этапы:

Шаг 1. Добавление правила корреляции

Чтобы добавить правило корреляции:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Правила корреляции** и нажмите на кнопку **Добавить правило корреляции**.
3. На вкладке **Общие** укажите следующие параметры:
   a. В поле **Название** укажите название правила.
   b. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
   c. В раскрывающемся списке **Тип** выберите **simple**.
   d. В поле **Наследуемые поля** добавьте следующие поля: DestinationAssetID.
   e. При необходимости укажите значения для следующих полей:
      - В поле **Частота срабатывания** укажите максимальное количество срабатываний правила в секунду.
      - В поле **Уровень важности** укажите уровень важности алертов и корреляционных событий, которые будут созданы в результате срабатывания правила.

- В поле **Описание** укажите любую дополнительную информацию.

4. На вкладке **Селекторы** → **Параметры** выполните следующие действия:

   a. В раскрывающемся списке **Фильтр** выберите **Создать**.

   b. В поле **Условия** нажмите на кнопку **Добавить группу**.

   c. В поле с оператором для добавленной группы выберите **И**.

   d. Добавьте условие для фильтрации по значению поля DeviceProduct:

      1. В поле **Условия** нажмите на кнопку **Добавить условие**.
      2. В поле с условием выберите **Если**.
      3. В поле **Левый операнд** выберите поле события.
      4. В поле **Поле события** выберите DeviceProduct.
      5. В поле **Оператор** выберите =.
      6. В поле **Правый операнд** выберите **константа**.
      7. В поле **Значение** введите `OSMP`.

   e. Добавьте условие для фильтрации по значению поля Name:

      1. В поле **Условия** нажмите на кнопку **Добавить условие**.
      2. В поле с условием выберите **Если**.
      3. В поле **Левый операнд** выберите поле события.
      4. В поле события выберите Name.
      5. В поле **Оператор** выберите =.
      6. В поле **Правый операнд** выберите **константа**.
      7. В поле **Значение** введите название события. При возникновении этого события задача запускается автоматически.

         Например, если вы хотите, чтобы задача *Антивирусная проверка* запускалась при регистрации событий Kaspersky Security Center *Обнаружен вредоносный объект*, вам нужно указать в поле **значение** это имя.

         Имя события можно посмотреть в поле **Name** в информации о событии.

5. На вкладке **Действия** укажите следующие параметры:

   a. В разделе **Действия** откройте раскрывающийся список **На каждом событии**.

   b. Установите флажок **Отправить на дальнейшую обработку**.

   Другие поля заполнять не требуется.

6. Нажмите на кнопку **Сохранить**.

Правило корреляции будет создано.

Шаг 2. Создание коррелятора

Вам нужно запустить мастер установки коррелятора. На шаге 3 мастера вам требуется выбрать правило корреляции, добавленное при выполнении этой инструкции.

В поле DeviceHostName должно отображаться доменное имя (FQDN) актива. Если оно не отображается, вам нужно создать запись для этого актива в системе DNS и на шаге 4 мастера создать правило обогащения с помощью DNS.

Шаг 3. Добавление фильтра

Чтобы добавить фильтр:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Фильтры** и нажмите на кнопку **Добавить фильтр**.
3. В поле **Название** укажите название фильтра.
4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
5. В поле **Условия** нажмите на кнопку **Добавить группу**.
6. В поле с оператором для добавленной группы выберите **И**.
7. Добавьте условие для фильтрации по значению поля DeviceProduct:
   a. В поле **Условия** нажмите на кнопку **Добавить условие**.
   b. В поле с условием выберите **Если**.
   c. В поле **Левый операнд** выберите поле события.
   d. В поле **Поле события** выберите Type.
   e. В поле **Оператор** выберите =.
   f. В поле **Правый операнд** выберите **константа**.
   g. В поле **значение** введите 3.
8. Добавьте условие для фильтрации по значению поля Name:
   a. В поле **Условия** нажмите на кнопку **Добавить условие**.
   b. В поле с условием выберите **Если**.
   c. В поле **Левый операнд** выберите поле события.
   d. В поле события выберите Name.
   e. В поле **Оператор** выберите =.
   f. В поле **Правый операнд** выберите **константа**.

g. В поле **значение** введите имя правила корреляции, созданного на шаге 1.

Шаг 4. Добавление правила реагирования

Чтобы добавить правило реагирования:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Правила реагирования** и нажмите на кнопку **Добавить правило реагирования**.
3. В поле **Название** укажите название правила.
4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
5. В раскрывающемся списке **Тип** выберите **Реагирование через OSMP**.
6. В раскрывающемся списке **Задача Open Single Management Platform** выберите задачу Kaspersky Security Center, которую требуется запустить.
7. В раскрывающемся списке **Поле события** выберите DestinationAssetID.
8. В поле **Рабочие процессы** укажите количество процессов, которые сервис может запускать одновременно.

   По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис коррелятора.

- В поле **Описание** вы можете добавить до 4000 символов в кодировке Unicode.
- В раскрывающемся списке **Фильтр** выберите фильтр, добавленный на шаге 3 этой инструкции.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если правила реагирования принадлежат общему тенанту, то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от Сервера администрирования Kaspersky Security Center, к которому подключен главный тенант.

Если в правиле реагирования выбрана задача, которая отсутствует на Сервере администрирования Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

Шаг 5. Добавление правила реагирования в коррелятор

Чтобы добавить правило реагирования в коррелятор:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. Выберите **Корреляторы**.
3. В списке корреляторов выберите коррелятор, добавленный на шаге 2 этой инструкции.
4. В дереве шагов выберите **Правила реагирования**.

5. Нажмите на кнопку **Добавить**.

6. В раскрывающемся списке **Правило реагирования** выберите правило, добавленное на шаге 4 этой инструкции.

7. В дереве шагов выберите **Проверка параметров**.

8. Нажмите на кнопку **Сохранить и перезапустить сервисы**.

9. Нажмите на кнопку **Сохранить**.

Правило реагирования будет добавлено в коррелятор.

Автоматический запуск задачи обновления антивирусных баз и модулей приложения или задачи антивирусной проверки на активах Kaspersky Security Center, подключенных к KUMA, будет настроен. Задачи запускаются при обнаружении угрозы на активах и получении KUMA соответствующих событий.

Проверка статуса задач Kaspersky Security Center

В Консоли KUMA можно проверить, была ли запущена задача Kaspersky Security Center или завершен ли поиск событий из коллектора, который прослушивает события Kaspersky Security Center.

Чтобы выполнить проверку статуса задач Kaspersky Security Center:

1. Выберите раздел KUMA **Ресурсы** → **Активные сервисы**.

2. Выберите коллектор, настроенный на получение событий с Сервера администрирования Kaspersky Security Center, и нажмите на кнопку **Перейти к событиям**.

Откроется новая вкладка браузера в разделе **События** KUMA. В таблице отобразятся события с Сервера администрирования Kaspersky Security Center. Статус задач отображается в столбце **Название**.

Поля событий Kaspersky Security Center:

- **Name** (Название) – статус или тип задачи.
- **Message** (Сообщение) – сообщение о задаче или событии.
- **FlexString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, полученного от Kaspersky Security Center. Например, `FlexString1Label=TaskName`.
- **FlexString<номер>** (Настраиваемое поле <номер>) – значение атрибута, указанного в поле поля FlexString<номер>Label. Например, `FlexString1=Download updates`.
- **DeviceCustomNumber<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к состоянию задачи. Например, `DeviceCustomNumber1Label=TaskOldState`.
- **DeviceCustomNumber<номер>** (Настраиваемое поле <номер>) – значение, относящееся к состоянию задачи. Например, `DeviceCustomNumber1=1` означает, что задача выполняется.
- **DeviceCustomString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к обнаруженной уязвимости: например, название вируса, уязвимого приложения.
- **DeviceCustomString<номер>** (Настраиваемое поле <номер>) – значение, относящееся к обнаруженной уязвимости. Например, пары атрибут-значение `DeviceCustomString1Label=VirusName` и

`DeviceCustomString1=EICAR-Test-File` означают, что обнаружен тестовый вирус EICAR.

Журналы KUMA

Журналы компонентов.

По умолчанию для всех компонентов KUMA в журнале регистрируются только ошибки. Чтобы получать детализированные данные в журналах, следует настроить в параметрах компонента режим **Отладка**.

Журнал пополняется, пока не достигнет размера 5 ГБ. По достижении 5 ГБ журнал событий архивируется и события начинают записываться в новый журнал событий. Архивы хранятся в папке с журналами в течение 7 дней, по истечении 7 дней архив удаляется. Одновременно на сервере хранится не более четырех заархивированных журналов. При появлении нового архива журнала, если архивов становится больше четырех, самый давний архив удаляется.

Режим **Отладка** доступен для следующих компонентов:

Сервисы:
• Хранилище
• Коррелляторы
• Коллекторы
• Агенты
	Как включить: в параметрах сервиса с помощью переключателя **Отладка**.
	
	Где хранятся: в директории установки сервиса. Например, /opt/kaspersky/kuma/<имя сервиса>/log/<имя сервиса>. Журналы событий сервисов можно скачать в Консоли KUMA в разделе **Ресурсы** → **Активные сервисы**, выбрав нужный сервис и нажав на кнопку **Журнал событий**.
	
	Журналы на машинах Linux можно просмотреть с помощью команды journalctl и tail. Например:
	• Хранилище. Чтобы вернуть последние журналы из хранилища, установленного на сервере, выполните следующую команду:
	`journalctl -f -u kuma-storage-< идентификатор хранилища >`
	• Коррелляторы. Чтобы вернуть последние журналы из коррелляторов, установленных на сервере, выполните следующую команду:
	`journalctl -f -u kuma-correlator-< идентификатор коррелятора >`
	• Коллекторы. Чтобы вернуть последние журналы определенного коллектора, установленного на сервере, выполните следующую команду:
	`journalctl -f -u kuma-collector-< идентификатор коллектора >`
	• Агенты. Чтобы вернуть последние журналы агента, установленного на сервере, выполните следующую команду:
	`tail -f /opt/kaspersky/agent/< идентификатор агента >/log/agent`
	Активность агентов на устройствах под управлением Windows всегда регистрируется, если им назначено разрешение на вход в систему в качестве службы. Данные указываются более подробно, если установлен флажок **Отладка**. Журналы агентов на машинах Windows можно просмотреть в файле %PROGRAMDATA%\Kaspersky Lab\KUMA\<идентификатор агента>\agent.log. Журналы агентов на машинах Linux хранятся в директории установки агента.

Ресурсы: • Коннекторы • Точки назначения • Правила обогащения	Как включить: в параметрах сервиса, к которому привязан ресурс, с помощью переключателя **Отладка**. Где хранятся: журналы хранятся на машине, на которой установлен сервис, использующий требуемый ресурс. Детализированные данные для ресурсов можно посмотреть в журнале сервиса, к которому привязан ресурс.

Уведомления KUMA

Стандартные уведомления

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Для этого необходимо настроить подключение к SMTP-серверу, а также установить флажок **Получать уведомления по почте** для пользователей, которым должны приходить уведомления.

KUMA автоматически уведомляет пользователей о следующих событиях:

- Создан отчет (уведомление получают пользователи, перечисленные в параметрах расписания шаблона отчета).
- Выполнена задача (уведомление получают пользователи, создавшие задачу).
- Доступны новые пакеты с ресурсами. Их можно получить путем обновления хранилища KUMA (уведомление получают пользователи, чей адрес электронной почты указан в параметрах задачи).

Работа с геоданными

В KUMA можно загрузить список соответствий IP-адресов или диапазонов IP-адресов географическим данным, чтобы затем использовать эту информацию при обогащении событий.

Формат геоданных

Геоданные можно загрузить в KUMA в виде CSV-файла в кодировке UTF-8. В качестве разделителя используется запятая. В первой строке файла указаны заголовки полей: `Network,Country,Region,City,Latitude,Longitude`.

Описание CSV-файла

Имя заголовка поля в CSV	Описание поля	Пример
`Сеть`	IP-адрес в одном из следующих форматов: • IP-адрес; • диапазон IP-адресов; • IP-адрес в формате CIDR. Допускается перемешивание ipv4- и ipv6-адресов. Обязательное поле.	• `192.168.2.24` • `192.168.2.25-192.168.2.35` • `131.10.55.70/8` • `2001:DB8::0/120`
`Country`	Принятое в вашей организации обозначение страны. Например, ее название или код. Обязательное поле.	• `Russia` • `RU`
`Region`	Принятое в вашей организации обозначение области. Например, ее название или код.	• `Sverdlovsk Oblast` • `RU-SVE`
`City`	Принятое в вашей организации обозначение города. Например, ее название или код.	• `Yekaterinburg` • `65701000001`

`Latitude`	Широта описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`56.835556`
`Longitude`	Долгота описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`60.612778`

Конвертация геоданных из MaxMind и IP2Location

В KUMA можно использовать геоданные, полученные из MaxMind и IP2Location, однако перед использованием файлы требуется конвертировать в поддерживаемый KUMA формат. Конвертацию можно произвести с помощью приведенного ниже скрипта. Убедитесь, что файлы не содержат повторяющихся записей. Например, если в файле несколько столбцов, разные записи могут содержать данные из одной сети с одинаковыми геоданными. Такие файлы невозможно конвертировать. Чтобы успешно выполнить конвертацию, убедитесь, что дублирующиеся строки отсутствуют и все строки уникальны по какому-либо полю.

Загрузить скрипт

Для запуска скрипта требуется Python 2.7 или выше.

Команда запуска скрипта:

```
python converter.py --type <тип обрабатываемых геоданных: "maxmind" или "ip2location">
--out <директория, в которую будет помещен CSV-файл с геоданными в формате KUMA> --
input <путь к ZIP-архиву с геоданными из MaxMind или IP2location>
```

При запуске скрипта с флагом `--help` отображается справка по доступным параметрам запуска скрипта:
`python converter.py --help`

Команда для конвертации файла с российской базой диапазонов IP-адресов из ZIP-архива MaxMind:

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out
geoip_maxmind_ru.csv
```

Без указания параметра `--lang` скрипт по умолчанию получает информацию из файла GeoLite2-City-Locations-en.csv из ZIP-архива.

Отсутствие параметра `--lang` для MaxMind равнозначно команде:

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

Команда для конвертации файла из ZIP-архива IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out
geoip_ip2location.csv
```

Команда для конвертации файла из нескольких ZIP-архивов IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP
IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out geoip_ip2location_ipv4_ipv6.csv
```

Параметр `--lang` для IP2Location не используется.

Обязательные наборы полей

Исходные файлы MaxMind GeoLite2-City-Blocks-IPv4.csv и GeoLite2-City-Blocks-IPv6.csv должны содержать следующий набор полей:

network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

Пример набора исходных данных:

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000

1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

Остальные файлы CSV с кодом локали должны содержать следующий набор полей:

geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

Пример набора исходных данных:

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0

7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

Исходные файлы IP2Location должны содержать данные о диапазонах сетей, Country, Region, City, Latitude, Longitude

Пример набора исходных данных:

```
"0","16777215","-","-","-","-","0.000000","0.000000","-","-"

"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"

"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+0
```

Если исходные файлы будут содержать другой набор полей, отличный от указанного в этом разделе, или каких-то полей будет не хватать, после конвертации отсутствующие поля в итоговом файле CSV будут пустыми.

Импорт и экспорт геоданных

При необходимости в KUMA вы можете вручную импортировать и экспортировать геоданные. Геоданные импортируются и экспортируются в файле формате CSV. При успешном импорте геоданных ранее добавленные данные перезаписываются и в KUMA создается событие аудита.

Чтобы импортировать геоданные в KUMA:

1. Подготовьте CSV-файл с геоданными.

   Геоданные, полученные из MaxMind и IP2Location, требуется конвертировать в поддерживаемый KUMA формат.

2. В Консоли KUMA перейдите в раздел **Параметры** → **Общие**.

3. В блоке параметров **Геоданные** нажмите на кнопку **Импортировать из файла** и выберите CSV-файл с геоданными.

   Дождитесь окончания импорта геоданных. При обновлении страницы загрузка данных прерывается.

Геоданные загружены в KUMA.

Чтобы экспортировать геоданные из KUMA,

1. В Консоли KUMA перейдите в раздел **Параметры** → **Общие**.

2. В блоке параметров **Геоданные** нажмите на кнопку **Экспортировать**.

Геоданные будут скачаны в виде CSV-файла (в кодировке UTF-8) с названием geoip.csv в соответствии с настройками вашего браузера.

Данные экспортируются в том же формате, в каком они были загружены, за исключением диапазонов IP-адресов. Если в KUMA в импортированном файле диапазон адресов указан в формате `1.0.0.0/24`, то в файле экспорта диапазон отобразится в формате `1.0.0.0-1.0.0.255`.

Сопоставление геоданных по умолчанию

Если при настройке правила обогащения геоданными в качестве источника IP-адреса выбрать поля события `SourceAddress`, `DestinationAddress` и `DeviceAddress`, становится доступна кнопка **Применить сопоставление по умолчанию**. Нажав на эту кнопку, вы можете добавить преднастроенные пары соответствий атрибутов геоданных и полей события (см. таблицы ниже).

Соответствия по умолчанию для поля события SourceAddress

Атрибут геоданных	Поле события
Country	`SourceCountry`
Region	`SourceRegion`
City	`SourceCity`
Latitude	`SourceLatitude`
Longitude	`SourceLongitude`

Соответствия по умолчанию для поля события DestinationAddress

Атрибут геоданных	Поле события
Country	DestinationCountry
Region	DestinationRegion
City	DestinationCity
Latitude	DestinationLatitude
Longitude	DestinationLongitude

Соответствия по умолчанию для поля события DeviceAddress

Атрибут геоданных	Поле события
Country	DeviceCountry
Region	DeviceRegion
City	DeviceCity
Latitude	DeviceLatitude
Longitude	DeviceLongitude

Руководство пользователя

В этой главе представлены сведения о работе с SIEM-системой KUMA.

Ресурсы KUMA

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления связи с заданным веб-адресом или преобразования данных по определенным правилам. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов, на основе которых в свою очередь создаются сервисы KUMA.

Ресурсы содержатся в Консоли KUMA в разделе консоли KUMA **Ресурсы** в блоке **Ресурсы**. Доступные типы ресурсов:

- **Правила корреляции** – в ресурсах этого типа содержатся правила определения в событиях закономерностей, указывающих на угрозы. Если условия, заданные в этих ресурсах, выполняются, создается корреляционное событие.
- **Нормализаторы** – в ресурсах этого типа содержатся правила для приведения поступающих событий к формату, принятому в KUMA. После обработки в нормализаторе "сырое" событие становится нормализованным и может обрабатываться другими ресурсами и сервисами KUMA.
- **Коннекторы** – в ресурсах этого типа содержатся параметры для установления сетевых подключений.
- **Правила агрегации** – в ресурсах этого типа содержатся правила для объединения нескольких однотипных базовых событий в одно агрегационное событие.
- **Правила обогащения** – в ресурсах этого типа содержатся правила для дополнения событий информацией из сторонних источников.

- **Точки назначения** – в ресурсах этого типа содержатся параметры для пересылки событий в пункт дальнейшей обработки или хранения.
- **Фильтры** – в ресурсах этого типа содержатся условия для отсева или выделения отдельных событий из потока событий.
- **Правила реагирования** – ресурсы этого типа используются в корреляторах для запуска, например, скриптов или задач Kaspersky Security Center при выполнении определенных условий.
- **Шаблоны уведомлений** – ресурсы этого типа используются при рассылке уведомлений о новых алертах.
- **Активные листы** – ресурсы этого типа используются корреляторами для динамической работы с данными при анализе событий по правилам корреляции.
- **Словари** – ресурсы этого типа используются для хранения ключей и их значений, которые могут потребоваться другим ресурсам и сервисам KUMA.
- **Прокси-серверы** – в ресурсах этого типа содержатся параметры использования прокси-серверов.
- **Секреты** – ресурсы этого типа используются для безопасного хранения конфиденциальной информации (например, учетных данных), которые должны использоваться KUMA для взаимодействия с внешними службами.
- **Контекстные таблицы** – ресурсы этого типа используются корреляторами KUMA для анализа событий в соответствии с правилами корреляции.

При нажатии на тип ресурса открывается окно, в котором отображается таблица с имеющимися ресурсами этого типа. Таблица содержит следующие столбцы:

- **Название** – имя ресурса. Может использоваться для поиска и сортировки ресурсов.
- **Последнее обновление** – дата и время последнего обновления ресурса. Может использоваться для сортировки ресурсов.
- **Создал** – имя пользователя, создавшего ресурс.
- **Описание** – описание ресурса.

Максимальный размер таблицы не ограничен. Если вы хотите выбрать все ресурсы, прокрутите таблицу до конца и установите флажок **Выбрать все**, таким образом все доступные в таблице ресурсы будут выбраны.

Ресурсы можно расположить по папкам. В левой части окна отображается структура папок: корневые папки соответствуют тенантам и содержат перечень всех ресурсов тенанта. Во всех остальных папках, вложенных в корневую, отображаются ресурсы отдельной папки. Когда папка выбрана, содержащиеся в ней ресурсы отображаются в таблице в правой части окна.

Ресурсы можно создавать, редактировать, копировать, перемещать между папками и удалять. Ресурсы можно также экспортировать и импортировать.

KUMA поставляется с набором предустановленных ресурсов, их можно узнать по названию [OOTB] <название_ресурса>. OOTB-ресурсы защищены от внесения изменений.

Если вы хотите адаптировать предустановленный OOTB-ресурс к инфраструктуре своей организации:

1. В разделе **Ресурсы**-<тип ресурсов> и выберите OOTB-ресурс, который вы хотите изменить.
2. В верхней части Консоли KUMA нажмите на кнопку **Дублировать**, а затем нажмите на кнопку **Сохранить**.

3. В веб-интерфейсе появится новый ресурс с названием [OOTB]<название_ресурса> - копия.

4. Внесите необходимые изменения в созданную копию предустановленного ресурса и сохраните изменения.

Адаптированный ресурс доступен для использования.

Операции с ресурсами

Вы можете управлять ресурсами KUMA: создавать, перемещать, копировать, редактировать и удалять ресурсы, а также импортировать и экспортировать их. Перечисленные операции доступны для всех ресурсов, вне зависимости от типа ресурса.

Ресурсы KUMA располагаются в папках. Вы можете добавлять, переименовывать, перемещать и удалять папки ресурсов.

Создание, переименование, перемещение и удаление папок с ресурсами

Ресурсы можно расположить по папкам. В левой части окна отображается структура папок: корневые папки соответствуют тенантам и содержат перечень всех ресурсов тенанта. Во всех остальных папках, вложенных в корневую, отображаются ресурсы отдельной папки. Когда папка выбрана, содержащиеся в ней ресурсы отображаются в таблице в правой части окна.

Папки можно создавать, переименовывать, перемещать и удалять.

Чтобы создать папку:

1. Выберите в дереве папку, в которой требуется новая папка.

2. Нажмите на кнопку **Добавить папку**.

Папка будет создана.

Чтобы переименовать папку:

1. Найдите нужную папку в структуре папок.

2. Наведите курсор на название папки.

   Рядом с названием папки появится значок ⋯.

3. В раскрывающемся списке ⋯ выберите **Переименовать**.

   Название папки станет доступным для редактирования.

4. Введите новое название папки и нажмите **ENTER**.

> Название папки не может быть пустым.

Папка будет переименована.

Чтобы переместить папку,

Нажмите название папки и перетащите ее в требуемое место в структуре папок.

> Папки невозможно переместить из одного тенанта в другой

Чтобы удалить папку:

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

   Рядом с названием папки появится значок ⋯.
3. В раскрывающемся списке ⋯ выберите **Удалить**.

   Появится окно подтверждения.
4. Нажмите на кнопку **OK**.

Папка будет удалена.

> Приложение не удаляет папки, которые содержат файлы или вложенные папки.

Создание, дублирование, перемещение, редактирование и удаление ресурсов

Вы можете создавать, перемещать, копировать, редактировать и удалять ресурсы.

Чтобы создать ресурс:

1. В разделе **Ресурсы** → **<тип ресурса>** выберите или создайте папку, в которую требуется добавить новый ресурс.

   Корневые папки соответствуют тенантам. Чтобы ресурс был доступен определенному тенанту, его следует создать в папке этого тенанта.
2. Нажмите на кнопку **Добавить <тип ресурса>**.

   Откроется окно для настройки параметров выбранного типа ресурсов. Доступные параметры зависят от типа ресурса.
3. Введите уникальное имя ресурса в поле **Название**.
4. Укажите обязательные параметры (они отмечены красной звездочкой).
5. При желании укажите дополнительные параметры (это необязательное действие).
6. Нажмите на кнопку **Сохранить**.

Ресурс будет создан и доступен для использования в сервисах и других ресурсах.

Чтобы переместить ресурс в новую папку:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажки рядом с ресурсами, которые вы хотите переместить. Можно выбрать сразу несколько ресурсов.

   Рядом с выбранными ресурсами отобразится значок ⣿.
3. Перетащите ресурсы в нужную папку с помощью значка ⣿.

Ресурсы будут перемещены в новые папки.

> Вы можете перемещать ресурсы только в папки того тенанта, в рамках которого были созданы ресурсы. Перемещение ресурсов в папки другого тенанта недоступно.

Чтобы скопировать ресурс:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажок рядом с ресурсом, которые вы хотите скопировать, и нажмите **Дублировать**.

   Отображается окно с параметрами ресурса, который вы выбрали для копирования. Доступные параметры зависят от типа ресурса.

   В поле **Название** отображается `<название выбранного ресурса> - копия`.
3. Измените нужные параметры.
4. Введите уникальное имя в поле **Название**.
5. Нажмите на кнопку **Сохранить**.

Копия ресурса будет создана.

Чтобы изменить ресурс:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Выберите ресурс.

   Отображается окно с параметрами выбранного ресурса. Доступные параметры зависят от типа ресурса.
3. Измените нужные параметры.
4. Нажмите на кнопку **Сохранить**.

Ресурс будет обновлен. Если этот ресурс используется в сервисе, перезапустите сервис, чтобы он задействовал новые параметры.

Чтобы удалить ресурс:

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажок рядом с ресурсом, которые вы хотите удалить, и нажмите **Удалить**.

Откроется окно подтверждения.

3. Нажмите на кнопку **OK**.

Ресурс будет удален.

Привязать корреляторы к корреляционному правилу

Для созданных корреляционных правил доступна опция **Привязать корреляторы**.

Чтобы привязать корреляторы:

1. В Консоли **KUMA** перейдите в раздел **Ресурсы** → **Правила корреляции**, выберите созданное правило корреляции и нажмите на кнопку **Привязать корреляторы**.

2. В открывшемся окне **Корреляторы** выберите один или несколько корреляторов, установив рядом флажок.

3. Нажмите на кнопку **OK**.

Корреляторы привязаны к правилу корреляции.

Правило будет добавлено последним в очередь для выполнения в каждом выбранном корреляторе. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Корреляторы** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок **Вверх** или **Вниз** установите необходимый порядок выполнения правил.

Обновление ресурсов

"Лаборатория Касперского" регулярно выпускает пакеты с ресурсами, доступные для импорта из репозитория. Вы можете указать адрес электронной почты в параметрах задачи **Обновление хранилища**. После первого выполнения задачи KUMA начинает рассылку уведомлений о доступных для обновления пакетах на указанный адрес. Вы можете выполнить обновление репозитория, проанализировать содержимое каждого обновления и принять решение об импорте и внедрении новых ресурсов в эксплуатируемую инфраструктуру. KUMA поддерживает обновление с серверов Лаборатории Касперского и из пользовательского источника, в том числе без прямого доступа к интернету с использованием механизма "зеркала обновления". При использовании в инфраструктуре других приложений "Лаборатории Касперского", можно подключить KUMA к уже существующем зеркалам обновления. Подсистема обновлений расширяет возможности KUMA для реагирования на изменения в картине угроз и инфраструктуре. Возможность использовать систему без прямого доступа в интернет помогает обеспечить конфиденциальность данных, обрабатываемых системой.

Чтобы обновить ресурсы, вам необходимо выполнить следующие шаги:

1. Обновить репозиторий, чтобы доставить в репозиторий пакеты с ресурсами. Обновление репозитория доступно в двух режимах:

   - Автоматическое обновление.

   - Обновление вручную.

2. Импортировать пакеты с ресурсами из обновленного репозитория в тенант.

Чтобы сервис начал использовать обновленные ресурсы, после выполнения импорта убедитесь, что ресурсы привязаны. В случае необходимости привяжите ресурсы к коллекторам, корреляторам или агентам и обновите параметры.

Чтобы настроить автоматическое обновление:

1. В разделе **Параметры – Обновление репозитория** настройте **Интервал обновления в часах**. Значение по умолчанию - 24 часа.

2. Укажите **Источник обновления**. Доступны следующие параметры:

   - Серверы обновлений "Лаборатории Касперского"

     Вы можете посмотреть список серверов в Базе знаний, статья 15998.

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

       В случае использования локальной папки у системного пользователя kuma должен быть доступ для чтения к этой папке и ее содержимому.

3. Укажите **Адреса электронной почты для рассылки уведомлений**, нажав на кнопку **Добавить**. На указанные адреса электронной почты будет поступать рассылка уведомлений о том, что в репозитории появились новые пакеты или новая версия тех пакетов, которые вы когда-либо импортировали в тенант.

   Если вы указываете электронную почту пользователя KUMA, в профиле пользователя должен быть установлен флажок **Получать уведомления по почте**. Для почты, которая не принадлежит ни одному пользователю KUMA, письмо будет приходит без дополнительных настроек. Параметры подключения к SMTP-серверу должны быть указаны во всех случаях.

4. Нажмите на кнопку **Сохранить**. Вскоре запустится задача обновления. Затем задача запускается по расписанию.

Чтобы запустить обновление репозитория вручную:

1. Если вы хотите отключить автоматическое обновление, в разделе **Параметры – Обновление репозитория** установите флажок **Отключить автоматическое обновление**. По умолчанию флажок снят. Также вы можете запустить обновление репозитория вручную, не отключая автоматическое обновление. Запуск обновления вручную не влияет на график выполнения автоматического обновления.

2. Укажите **Источник обновления**. Доступны следующие параметры:

   - Серверы обновлений "Лаборатории Касперского"

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и ее содержимому.

3. Укажите **Адреса электронной почты для рассылки уведомлений**, нажав на кнопку **Добавить**. На указанные адреса электронной почты будет поступать рассылка уведомлений о том, что в репозитории появились новые пакеты или новая версия тех пакетов, которые вы когда-либо импортировали в тенант.

   Если вы указываете электронную почту пользователя KUMA, в профиле пользователя должен быть установлен флажок **Получать уведомления по почте**. Для почты, которая не принадлежит ни одному пользователю KUMA, письмо будет приходит без дополнительных настроек. Параметры подключения к SMTP-серверу должны быть указаны во всех случаях.

4. Нажмите **Запустить обновление**. Таким образом, вы одновременно сохраните настройки и вручную запустите выполнение задачи **Обновление репозитория**.

Настройка пользовательского источника с использованием Kaspersky Update Utility

Вы можете обновлять ресурсы без доступа к интернету через пользовательский источник обновления с помощью утилиты Kaspersky Update Utility.

Настройка состоит из следующих шагов:

1. Настройка пользовательского источника с помощью Kaspersky Update Utility:
   a. Установка и настройка Kaspersky Update Utility на одном из компьютеров локальной сети организации.
   b. Настройка копирования обновлений в папку общего доступа в параметрах Kaspersky Update Utility.
2. Настройка обновления репозитория KUMA из пользовательского источника.

Настройка пользовательского источника с помощью Kaspersky Update Utility:

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта Службы технической поддержки "Лаборатории Касперского".

1. В Kaspersky Update Utility включите скачивание обновлений для KUMA:
   - В разделе **Приложения** – **Контроль периметра** установите флажок рядом с KUMA, чтобы включить возможность обновления.
   - Если вы работаете с Kaspersky Update Utility через командную строку, в конфигурационном файле updater.ini в секции [ComponentSettings] добавьте следующую строку или укажите значение `true` для уже существующей строки:

     ```
     KasperskyUnifiedMonitoringAndAnalysisPlatform_XDR_1_1=true
     ```
2. В разделе **Загрузки** укажите источник обновлений. По умолчанию в качестве источника используются сервера обновления "Лаборатории Касперского".
3. В разделе **Загрузки** в группе параметров **Папки для обновлений** укажите папку общего доступа, в которую Kaspersky Update Utility будет загружать обновления. Доступны следующие параметры:
   - Укажите локальную папку на устройстве, где установлена Kaspersky Update Utility. Разверните HTTP-сервер, который будет отдавать обновления, и опубликуйте на нем эту локальную папку. В KUMA в разделе **Параметры** - **Обновление репозитория** - **Пользовательский источник** укажите URL к локальной папке, опубликованной на HTTP-сервере.
   - Укажите локальную папку на устройстве, где установлена Kaspersky Update Utility. Сделайте эту локальную папку доступной по сети. Примонтируйте доступную по сети локальную папку на устройстве с KUMA. В KUMA в разделе **Параметры** - **Обновление репозитория** - **Пользовательский источник** укажите полный путь к этой локальной папке.

Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

Экспорт ресурсов

Если для пользователя скрыты общие ресурсы, он не может экспортировать ни общие ресурсы, ни ресурсы, в которых используются общие ресурсы.

Чтобы экспортировать ресурсы:

1. В разделе **Ресурсы** нажмите **Экспортировать ресурсы**.

   Откроется окно **Экспортировать ресурсы** с деревом всех доступных ресурсов.

2. В поле **Пароль** введите пароль, который необходимо использовать для защиты экспортируемых данных.

3. В раскрывающемся списке **Тенант** выберите тенант, ресурсы которого вы хотите экспортировать.

4. Установите флажки рядом с ресурсами, которые вы хотите экспортировать.

   Если выбранные ресурсы связаны с другими ресурсами, эти ресурсы также будут экспортированы.

5. Нажмите на кнопку **Экспортировать**.

Ресурсы в защищенном паролем файле сохранятся на вашем компьютере в зависимости от настроек вашего браузера. Ресурсы секретов экспортируются пустыми.

Импорт ресурсов

Чтобы импортировать ресурсы:

1. В разделе **Ресурсы** нажмите **Импорт ресурсов**.

   Откроется окно **Импорт ресурсов**.

2. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать импортируемые ресурсы.

3. В раскрывающемся списке **Источник импорта** выберите один из следующих вариантов:

   - **Файл**

     При выборе этого варианта необходимо указать пароль и нажать на кнопку **Импортировать**.

   - **Репозиторий**

     При выборе этого варианта отображается список доступных для импорта пакетов. Мы рекомендуем убедиться, что дата обновления репозитория относительно недавняя и при необходимости настроить автоматическое обновление.

     Вы можете выбрать один или несколько пакетов для импорта и нажать на кнопку **Импортировать**. Зависимые ресурсы Общего тенанта будут импортированы в Общий тенант, остальные ресурсы будут импортированы в выбранный тенант. Отдельных прав для учетной записи на Общий тенант не требуется, необходимо только наличие права на импорт в выбранном тенанте.

     Импортированные ресурсы можно только удалить. Если вы хотите переименовать, изменить или переместить импортированный ресурс, вам нужно сделать дубликат ресурса. Для этого нажмите на кнопку **Дублировать** и выполните необходимые действия с дубликатом ресурса. При импорте следующих версий пакета дубликат не будет обновлен, поскольку он уже представляет собой отдельный объект.

4. Разрешите конфликты между импортированными из файла и существующими ресурсами, если они возникли. Подробнее о конфликтах ресурсов см. ниже.

a. Если имя, тип и guid импортированных ресурсов полностью совпадает с именем, типом и guid существующего ресурса, открывается окно **Конфликты** с таблицей, в которой отображаются тип и имя конфликтующих ресурсов. Разрешите отображаемые конфликты:

- Если вы хотите заменить существующий ресурс новым, нажмите **Заменить**.

  Нажмите **Заменить все**, чтобы заменить все конфликтующие ресурсы.

- Если вы хотите оставить существующий ресурс, нажмите **Пропустить**.

  Для зависимых ресурсов - то есть привязанных к другим ресурсам - недоступна опция **Пропустить**, зависимые ресурсы можно только **Заменить**.

  Нажмите **Пропустить все**, чтобы сохранить все существующие ресурсы.

b. Нажмите на кнопку **Устранить**.

Ресурсы импортируются в KUMA. Ресурсы секретов импортируются пустыми.

Импорт ресурсов, использующих расширенную схему событий

Если вы импортируете нормализатор, использующий одно или несколько полей расширенной схемы событий, в KUMA будет автоматически создано поле расширенной схемы, использующееся в нормализаторе.

Если вы импортируете прочие типы ресурсов, использующих в своей логике поля расширенной схемы событий, ресурсы будут успешно импортированы. Для обеспечения работы импортированных ресурсов необходимо создать соответствующие поля расширенной схемы событий в ресурсе типа "нормализатор".

Если в KUMA будет импортирован нормализатор, использующий поле расширенной схемы событий и такое поле уже существует в KUMA, будет использовано созданное ранее поле.

О разрешении конфликтов

Когда ресурсы импортируются в KUMA из файла, приложение сравнивает их с существующими ресурсами, сверяя следующие параметры:

- Имя и тип. Если имя и тип импортируемого ресурса совпадают с параметрами существующего ресурса, имя импортированного ресурса автоматически изменяется.

- идентификатор; Если идентификаторы двух ресурсов совпадают, возникает конфликт, который должен разрешить пользователь. Такая ситуация может возникнуть, когда вы импортируете ресурсы на тот же сервер KUMA, с которого они были экспортированы.

При разрешении конфликта вы можете либо *заменить существующий ресурс* импортированным, либо *оставить существующий ресурс*.

Некоторые ресурсы связаны между собой: например, в некоторых типах коннекторов обязательно нужно указывать секрет коннектора. Секреты также импортируются, если они привязаны к коннектору. Такие связанные ресурсы экспортируются и импортируются вместе.

Особенности импорта:

1. Ресурсы импортируются в выбранный тенант.

2. Если связанный ресурс находился в Общем тенанте, при импорте он снова будет в Общем тенанте.

3. В окне **Конфликты** в столбце **Родительский объект** всегда отображается самый верхний родительский ресурс из выбранных при импорте.

4. Если во время импорта возникает конфликт, и вы выбираете замену существующего ресурса новым, все связанные с ним ресурсы также будут автоматически заменены импортированными ресурсами.

Известные ошибки:

1. Привязанный ресурс попадает в тенант, указанный при импорте, а не в Общий тенант, как указано в окне **Конфликты**, при следующих условиях:

   a. привязанный ресурс изначально находится в Общем тенанте;

   b. в окне **Конфликты** вы выбираете **Пропустить** для всех родительских объектов привязанного ресурса из Общего тенанта;

   c. привязанный ресурс из Общего тенанта оставляете для замены.

2. После выполнения импорта в фильтре у категорий не указан тенант при следующих условиях:

   a. фильтр содержит привязанные категории активов из разных тенантов;

   b. имена категорий активов одинаковы;

   c. вы импортируете этот фильтр с привязанными категориями активов на новый сервер.

3. В Тенант 1 дублируется имя категории активов при следующих условиях:

   a. в Тенант 1 у вас есть фильтр с привязанными категориями активов из Тенант 1 и Общего тенанта;

   b. имена привязанных категорий активов одинаковы;

   c. вы импортируете такой фильтр из Тенант 1 в Общий тенант.

4. Невозможно импортировать конфликтующие ресурсы в один тенант.

   Ошибка "Невозможно импортировать конфликтующие ресурсы в один тенант" означает, что в импортируемом пакете есть конфликтующие ресурсы из разных тенантов и их нельзя импортировать в Общий тенант.

   Решение: Выберите для импорта пакета другой тенант, не Общий. Тогда при импорте ресурсы, изначально расположенные в Общем тенанте, будут импортированы в Общий тенант, а ресурсы из другого тенанта — в выбранный при импорте тенант.

5. Только Главный администратор может импортировать ресурсы в Общий тенант.

   Ошибка "Только Главный администратор может импортировать категории в Общий тенант" означает, что в импортируемом пакете есть ресурсы с привязанными общими категориями активов. Категории или ресурсы с привязанными общими категориями активов можно увидеть в журнале Ядра KUMA. Путь к журналу Ядра:

   /opt/kaspersky/kuma/core/log/core

   Решение: Выберите один из следующих вариантов:

   - Уберите из импорта ресурсы, к которым привязаны общие категории: снимите флажок рядом с соответствующими ресурсами.

   - Выполните импорт под учетной записью пользователя с правами Главного администратора.

6. Только главный администратор может импортировать ресурсы в Общий тенант.

   Ошибка "Только Главный администратор может импортировать ресурсы в Общий тенант" означает, что в импортируемом пакете есть ресурсы с привязанными общими ресурсами. Ресурсы с привязанными общими ресурсами можно увидеть в журнале Ядра KUMA. Путь к журналу Ядра:

   /opt/kaspersky/kuma/core/log/core

   Решение: Выберите один из следующих вариантов:

   - Уберите из импорта ресурсы, к которым привязаны ресурсы из Общего тенанта, и сами общие ресурсы: снимите флажок рядом с соответствующими ресурсами.
   - Выполните импорт под учетной записью пользователя с правами Главного администратора.

Точки назначения

Точки назначения задают сетевые параметры для передачи нормализованных событий. Точки назначения используются в коллекторах и коррелляторах для описания того, куда передавать обработанные события. В основном, в роли точек назначения выступают коррелятор и хранилище.

Параметры точек назначения указываются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:

- **nats-jetstream** – используется для коммуникации через NATS.
- **tcp** – используется для связи по протоколу TCP.
- **http** – используется для связи по протоколу HTTP.
- **diode** – используется для передачи событий с помощью диода данных.
- **kafka** – используется для коммуникаций с помощью kafka.
- **file** – используется для записи в файл.
- **storage** – используется для передачи данных в хранилище.
- **correlator** – используется для передачи данных в коррелятор.

Тип nats-jetstream

Тип **nats-jetstream** используется для коммуникации через NATS.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр.

	Тип точки назначения, **nats-jetstream**.
URL	Обязательный параметр. URL, с которым необходимо установить связь.
Топик	Обязательный параметр. Тема сообщений NATS. Должно содержать символы в кодировке Unicode.
Разделитель	Используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
Авторизация	Тип авторизации при подключении к указанному URL. Доступны следующие значения: • **выключена** – значение по умолчанию. • **обычная** – при выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору. Добавить секрет 1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**. Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**. 2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +. Откроется окно **Секрет**. 3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных. 4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете. 6. Нажмите на кнопку **Сохранить**. Секрет будет добавлен и отобразится в списке **Секрет**.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Идентификатор кластера	Идентификатор кластера NATS.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF

	Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.

Режим TLS	Использование шифрования TLS. Доступные значения:
	• **Выключено –** значение по умолчанию, не использовать шифрование TLS.
	• **Включено –** использовать шифрование, но без верификации сертификата.
	• **С верификацией –** использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
	• **Нестандартный CA –** использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.
	Создание сертификата, подписанного центром сертификации
	Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):
	1. Создать ключ, который будет использоваться центром сертификации.
	Пример команды:
	`openssl genrsa -out ca.key 2048`
	2. Создать сертификат для только что созданного ключа.
	Пример команды:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя устройства центра сертификации>" -out ca.crt`
	3. Создать приватный ключ и запрос на его подписание в центре сертификации.
	Пример команды:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя устройства сервера KUMA>" -out server.csr`
	4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.
	Пример команды:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Полученный сертификат `server.crt` следует загрузить в Консоль KUMA в секрет типа **certificate**, который затем нужно выбрать в раскрывающемся списке **Нестандартный CA**.
	При использовании TLS невозможно указать IP-адрес в качестве URL.

Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.

Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип tcp

Тип **tcp** используется для связи по протоколу TCP.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **tcp**.

URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6. При использовании адресов IPv6 необходимо также указывать интерфейс в формате `[адрес%интерфейс]:порт`. Например: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Время ожидания	Время ожидания ответа (в секундах) другого сервиса или компонента. По умолчанию указано значение `30`.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.
Режим TLS	Использование шифрования TLS с использованием сертификатов в формате pem x509. Доступные значения: • **Выключено**: не использовать шифрование TLS. Значение по умолчанию. • **Включено** – использовать шифрование, но без верификации сертификатов. • **С верификацией –** использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/. При использовании TLS невозможно указать IP-адрес в качестве URL.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип http

Тип **http** используется для связи по протоколу HTTP.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **http**.
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`.

	Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).
Авторизация	Тип авторизации при подключении к указанному URL Доступны следующие значения: • **выключена** – значение по умолчанию. • **обычная** – при выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору. **Добавить секрет** 1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**. Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**. 2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +. Откроется окно **Секрет**. 3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных. 4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете. 6. Нажмите на кнопку **Сохранить**. Секрет будет добавлен и отобразится в списке **Секрет**.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Время ожидания	Время ожидания ответа (в секундах) другого сервиса или компонента. По умолчанию указано значение `30`.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.
Режим TLS	Использование шифрования TLS. Доступные значения: • **Выключено –** значение по умолчанию, не использовать шифрование TLS. • **Включено –** использовать шифрование, но без верификации сертификата.

- **С верификацией –** использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
- **Нестандартный CA –** использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

Создание сертификата, подписанного центром сертификации

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды:

   ```
   openssl genrsa -out ca.key 2048
   ```

2. Создать сертификат для только что созданного ключа.

   Пример команды:

   ```
   openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя устройства центра сертификации>" -out ca.crt
   ```

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды:

   ```
   openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя устройства сервера KUMA>" -out server.csr
   ```

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды:

   ```
   openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. Полученный сертификат `server.crt` следует загрузить в Консоль KUMA в секрет типа **certificate**, который затем нужно выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

Политика выбора URL

В раскрывающемся списке можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько. Доступные значения:

- **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.
- **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.
- **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

Разделитель

В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется \n.

Path	Путь, который необходимо добавить для URL-запроса. Например, если указать путь `/input`, а в качестве URL ввести `10.10.10.10`, то от точки назначения будут исходить запросы `10.10.10.10/input`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Количество служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Путь проверки работоспособности	URL для отправки запросов для получения данных о работоспособности системы, с которой устанавливает связь ресурс точки назначения.
Ожидание проверки работоспособности	Частота проверки работоспособности в секундах.
Проверка работоспособности отключена	Флажок, который отключает проверку работоспособности.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип diode

Тип **diode** используется для передачи событий с помощью диода данных.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **diode**.

Директория, из которой диод данных получает события

Обязательный параметр.

Директория, откуда диод данных перемещает события. Путь может содержать до 255 символов в кодировке Unicode.

Ограничения при использовании префиксов к путям на серверах Windows

На серверах Windows необходимо указывать абсолютные пути к директориям. Невозможно использовать директории, названия которых соответствуют указанным ниже регулярным выражениям:

- `^[a-zA-Z]:\\Program Files`
- `^[a-zA-Z]:\\Program Files \(x86\)`
- `^[a-zA-Z]:\\Windows`
- `^[a-zA-Z]:\\Program Files\\Kaspersky Lab\\KUMA`

Ограничения при использовании префиксов к путям на серверах Linux

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/

	• /opt/kaspersky/kuma/mongodb/log/ • /opt/kaspersky/kuma/victoria-metrics/log/
Временная директория	Директория, в которой события готовятся для передачи диоду данных. События хранятся в файле по истечении времени ожидания (по умолчанию 10 секунд) или при переполнении буфера. Подготовленный файл перемещается в директорию, указанную в поле **Директория, из которой диод данных получает события**. В качестве названия файла с событиями используется хеш-сумма (SHA256) содержимого файла. Временная директория не должна совпадать с директорией, из которой диод данных получает события.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Сжатие	Можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**. Этот параметр должен совпадать для коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`. Этот параметр должен совпадать для коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип kafka

Тип **kafka** используется для коммуникаций с помощью kafka.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **kafka**.
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

	Вы можете добавить несколько адресов, нажав на кнопку URL.
Топик	Обязательный параметр. Тема сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".
Разделитель	Используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
Авторизация	Тип авторизации при подключении к указанному URL. Доступны следующие значения: • **выключена** – значение по умолчанию. • **PFX** – сертификат должен быть сгенерирован с закрытым ключом в формате контейнера PKCS#12 в доверенном центре сертификации. Затем сертификат нужно экспортировать из хранилища и загрузить его в Консоли KUMA в виде PFX-секрета. • Добавить PFX-секрет 1. Если вы загрузили PFX-сертификат ранее, выберите его в раскрывающемся списке **Секрет**. Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**. 2. Если вы хотите добавить новый сертификат, справа от списка **Секрет** нажмите на кнопку +. Откроется окно **Секрет**. 3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных. 4. По кнопке **Загрузить PFX** выберите файл, в который вы экспортировали сертификат с закрытым ключом, в формате PKCS#12-контейнера. 5. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата. 6. Нажмите на кнопку **Сохранить**. Сертификат будет добавлен и отобразится в списке **Секрет**. • **обычная –** требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору. Добавить секрет

1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

   Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

Секрет будет добавлен и отобразится в списке **Секрет**.

Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Время ожидания	Время ожидания ответа (в секундах) другого сервиса или компонента. По умолчанию указано значение `30`.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.
Режим TLS	Использование шифрования TLS. Доступные значения: • **Выключено –** значение по умолчанию, не использовать шифрование TLS. • **Включено** – использовать шифрование, но без верификации сертификата. • **С верификацией –** использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/. • **Нестандартный CA –** использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта. Создание сертификата, подписанного центром сертификации

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды:

   ```
   openssl genrsa -out ca.key 2048
   ```

2. Создать сертификат для только что созданного ключа.

   Пример команды:

   ```
   openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя устройства центра сертификации>" -out ca.crt
   ```

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды:

   ```
   openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя устройства сервера KUMA>" -out server.csr
   ```

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды:

   ```
   openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. Полученный сертификат `server.crt` следует загрузить в Консоль KUMA в секрет типа **certificate**, который затем нужно выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется `\n`.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 c`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип файла

Тип **file** используется для записи в файл.

При удалении точки назначения типа file, используемой в каком-либо сервисе, этот сервис необходимо перезапустить.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **file**.

URL	Обязательный параметр. Путь к файлу, в который необходимо записать события. Ограничения при использовании префиксов к путям файлов

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

	• /opt/kaspersky/kuma/clickhouse/logs/ • /opt/kaspersky/kuma/mongodb/log/ • /opt/kaspersky/kuma/victoria-metrics/log/
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Разделитель	В раскрывающемся списке можно выбрать символ, который будет определять границу между событиями. По умолчанию используется \n.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Выходной формат	Формат отправки событий во внешний источник. Доступные значения: • JSON • CEF Если выбран формат CEF, отправляемое событие содержит заголовок CEF и только непустые поля.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип storage

Тип **storage** используется для передачи данных в хранилище.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **storage**.
URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

	Вы можете добавить несколько адресов, нажав на кнопку **URL**. В поле **URL** поддерживается поиск сервисов по FQDN, IP-адресу и названию. Особенности поиска по указанным в поле значениям: • `<Поисковое значение>` – поиск ведется по FQDN, IP-адресам и названиям сервисов. • `<Первое поисковое значение, оканчивающееся на одну или несколько цифр>:<второе поисковое значение>` – поиск по первому значению ведется по FQDN, IP-адресам сервисов, а второе значение используется для поиска по порту. • `:<значение>` – поиск ведется по порту.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Прокси-сервер	Раскрывающийся список для выбора прокси-сервера.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Политика выбора URL	Раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько: • **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL. • **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него. • **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Ожидание проверки работоспособности	Частота проверки работоспособности в секундах.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип correlator

Тип **correlator** используется для передачи данных в коррелятор.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Переключатель **Состояние**	Используется, если события нужно отправлять в точку назначения. По умолчанию отправка событий включена.
Тип	Обязательный параметр. Тип точки назначения, **correlator**.

URL	Обязательный параметр. URL, с которым необходимо установить связь. Доступные форматы: `устройство:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт`. Пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`). Вы можете добавить несколько адресов, нажав на кнопку **URL**. В поле **URL** поддерживается поиск сервисов по FQDN, IP-адресу и названию. Особенности поиска по указанным в поле значениям: • `<Поисковое значение>` – поиск ведется по FQDN, IP-адресам и названиям сервисов. • `<Первое поисковое значение, оканчивающееся на одну или несколько цифр>:<второе поисковое значение>` – поиск по первому значению ведется по FQDN, IP-адресам сервисов, а второе значение используется для поиска по порту. • `:<значение>` – поиск ведется по порту.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Прокси-сервер	Раскрывающийся список для выбора прокси-сервера.
Размер буфера	Используется для установки размера буфера. Значение по умолчанию: 1 КБ; максимальное: 64 МБ.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию – 10 ГБ.
Политика выбора URL	Раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько: • **Любой**. События отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL. • **Сначала первый**. События отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него. • **Сбалансированный** – пакеты с событиями будут равномерно распределены по доступным URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.
Интервал очистки буфера	Время (в секундах) между отправкой данных в точку назначения. Значение по умолчанию – `1 с`.
Количество обработчиков	Поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
Ожидание проверки работоспособности	Частота проверки работоспособности в секундах.
Отладка	Переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. Значение по умолчанию – **Выключено**.
Дисковый буфер	Раскрывающийся список, в котором можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер включен. Дисковый буфер используется, если коллектор не может направить в точку назначения нормализованные события. Объем выделенного дискового пространства ограничен значением параметра **Размер дискового буфера**. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер.
Фильтр	В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Предустановленные точки назначения

В поставку OSMP включены перечисленные в таблице ниже точки назначения.

Предустановленные точки назначения

Название точки назначения	Описание
[OOTB] Correlator	Отправляет события в коррелятор.
[OOTB] Storage	Отправляет события в хранилище.

Нормализаторы

Нормализаторы предназначены для приведения исходных событий, которые поступают из разных источников в различных форматах, к модели данных событий KUMA. Нормализованные события становятся доступны для обработки другими ресурсами и сервисами KUMA.

Нормализатор состоит из *основного* и необязательных *дополнительных правил парсинга событий*. С помощью создания основного и множества дополнительных правил парсинга можно реализовать сложную логику обработки событий. Данные передаются по древовидной структуре правил парсинга в зависимости от условий, заданных в параметре **Условия дополнительной нормализации**. Последовательность создания правил парсинга имеет значение: событие обрабатывается последовательно и последовательность обработки обозначена стрелками.

Нормализация событий теперь доступна в следующих вариантах:

- 1 коллектор – 1 нормализатор

  Мы рекомендуем использовать такой способ, если у вас много событий одного типа или много IP-адресов, откуда могут приходить события одного типа. Можно настроить один коллектор только с одним нормализатором и это будет оптимально с точки зрения производительности.

- 1 коллектор – несколько нормализаторов с привязкой к IP

  Такой способ доступен для коллекторов с коннектором типа UDP, TCP, HTTP. Если в коллекторе на шаге Транспорт указан коннектор UDP, TCP, HTTP, на шаге Парсинг событий на вкладке Настройки парсинга вы можете задать несколько IP-адресов и указать, какой нормализатор использовать для событий, поступающих с заданных адресов. Доступны следующие типы нормализаторов: `json`, `cef`, `regexp`, `syslog`, `csv`, `kv`, `xml`. Для нормализаторов типа `syslog` и `regexp` вы можете задать дополнительные условия нормализации в зависимости от значения поля DeviceProcessName.

Нормализатор создается в несколько этапов:

1. **Подготовка к созданию нормализатора**

   Нормализатор можно создать в Консоли KUMA:

   - В разделе **Ресурсы** → **Нормализаторы**.
   - При создании коллектора на шаге **Парсинг событий**.

   Затем в нормализаторе необходимо создать правила парсинга.

2. **Создание основного правила парсинга событий**

   Основное правило парсинга создается нажатием на кнопку **Добавить парсинг событий**. При этом открывается окно **Парсинг событий**, в котором вы можете задать параметры основного правила парсинга:

   - Задать параметры парсинга событий.
   - Задать параметры обогащения событий.

   Основное правило парсинга событий отображается в нормализаторе в виде темного кружка. Параметры основного правила парсинга можно просмотреть или изменить, нажав на его кружок. При наведении курсора мыши на кружок отображается знак плюса. Нажмите на него, чтобы добавить правила парсинга.

   Название основного правила парсинга используется в KUMA в качестве названия нормализатора.

3. **Создание дополнительных правил парсинга событий**

   При нажатии на значок плюса, который отображается при наведении указателя мыши на кружок или блок, обозначающей нормализатор событий, откроется окно **Дополнительный парсинг событий**, в котором вы можете задать параметры дополнительного правила парсинга:

- Определить условия, при которых данные будут поступать в новый нормализатор.
- Задать параметры парсинга событий.
- Задать параметры обогащения событий.

Дополнительное правило парсинга событий отображается в нормализаторе виде темного блока. В блоке отображаются условия срабатывания правила дополнительного парсинга, имя правила дополнительного парсинга и поле события. Когда это поле события доступно, данные передаются в нормализатор. Параметры дополнительного правила парсинга можно просмотреть или изменить, нажав его блок.

Если навести курсор мыши на правило дополнительного нормализатора, появится кнопка с плюсом. Вы можете нажать на эту кнопку, чтобы создать дополнительное правило парсинга событий. С помощью кнопки со значком корзины нормализатор можно удалить.

4. **Завершение создания нормализатора**

   Создание нормализатора завершается нажатием кнопки **Сохранить**.

В верхнем правом углу в поле поиска можно искать дополнительные правила парсинга по названию.

Для ресурсов нормализатора в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы → Нормализаторы**.

Параметры парсинга событий

При создании правил парсинга событий в окне параметров нормализатора на вкладке **Схема нормализации** вы можете настроить правила приведения поступающих событий к формату KUMA.

Чтобы определить параметры парсинга событий:

1. В поле **Имя** (обязательное поле) введите уникальное имя правила парсинга. Имя должно содержать от 1 до 128 символов Юникода. Название основного правила парсинга будет использоваться в качестве названия нормализатора.

2. В поле **Тенант** (обязательное поле) введите имя тенанта, которому принадлежит ресурс.

   Этот параметр недоступен для дополнительных правил парсинга.

3. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требующие заполнения.

   Доступные методы парсинга:

   - **json**

Этот метод парсинга используется для обработки данных в формате JSON, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла.

При обработке файлов с иерархически выстроенными данными можно обращаться к полям вложенных объектов, поочередно через точку указывая названия параметров. Например, к параметру `username` из строки `"user":{"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованы некорректно.

В сложных схемах нормализации, где используются дополнительные нормализаторы, все вложенные объекты обрабатываются на первом уровне нормализации за исключением случаев, когда условия дополнительной нормализации не заданы и, следовательно, в дополнительный нормализатор передается обрабатываемое событие целиком.

В качестве разделителя строк могут выступать символы `\n` и `\r\n`. Строки должны быть в кодировке UTF-8.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** выберите в раскрывающемся списке **Использовать сырое событие** значение **Да**.

- **cef**

  Этот метод парсинга используется для обработки данных в формате CEF.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- **regexp**

Этот метод парсинга используется для создания собственных правил обработки данных в формате с использованием регулярных выражений.

В поле блока параметров **Нормализация** добавьте регулярное выражение (синтаксис RE2) с именованными группами захвата. Имя группы и ее значение будут интерпретироваться как поле и значение необработанного события, которое может быть преобразовано в поле события в формате KUMA.

Чтобы добавить правила обработки событий:

1. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например "(?P<name>regexp)". Регулярное выражение, добавленное в параметр **Нормализация**, должно полностью совпадать с событием. Также при разработке регулярного выражения рекомендуется использовать специальные символы, обозначающие начало и конец текста: ^, $.

   Можно добавить несколько регулярных выражений с помощью кнопки **Добавить регулярное выражение**. Если нужно удалить регулярное выражение, нажмите на ✕ кнопку .

3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Теперь вы можете выбрать соответствующее поле KUMA в столбце рядом с каждой группой захвата. Если вы назвали группы захвата в соответствии с форматом CEF, вы можете использовать автоматическое сопоставление CEF, установив флажок **Использовать синтаксис CEF для нормализации**.

Правила обработки событий добавлены.

- **syslog**

  Этот метод парсинга используется для обработки данных в формате syslog.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- **csv**

  Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

  При выборе этого метода необходимо в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя допускается использовать любой однобайтовый символ ASCII.

- **kv**

Этот метод парсинга используется для обработки данных в формате ключ-значение.

При выборе этого метода необходимо указать значения в следующих обязательных полях:

- **Разделитель пар** – укажите символ, которые будет служит разделителем пар ключ-значение. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем значений.

- **Разделитель значений** – укажите символ, который будет служить разделителем между ключом и значением. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем пар ключ-значение.

- xml

Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** выберите в раскрывающемся списке **Использовать сырое событие** значение **Да**.

При выборе этого метода в блоке параметров **Атрибуты XML** можно указать ключевые атрибуты, которые следует извлекать из тегов. Если в структуре XML в одном теге есть атрибуты с разными значениями, можно определить нужное значение, указав ключ к нему в столбце **Исходные данные** таблицы **Сопоставление**.

Чтобы добавить ключевые атрибуты XML,

Нажмите на кнопку **Добавить поле** и в появившемся окне укажите путь к нужному атрибуту.

Можно добавить несколько атрибутов. Атрибуты можно удалить по одному с помощью значка с крестиком или все сразу с помощью кнопки **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

Нумерация тегов

Начиная с версии KUMA 2.1.3 доступна **Нумерация тегов**. Опция предназначена для выполнения автоматической нумерации тегов в событиях в формате XML, чтобы можно было распарсить событие с одинаковыми тегами или неименованными тегами, такими как <Data>.

В качестве примера мы используем функцию **Нумерация тегов** для нумерации тегов атрибута EventData [события Microsoft Windows PowerShell event ID 800](#).

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    <System>
        <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-8497-1e730c959516}" EventSourceName="NTDS" />
        <EventID Qualifiers="0000">0000</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>15</Task>
        <Opcode>0</Opcode>
        <Keywords>0x8080000000000000</Keywords>
        <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
        <EventRecordID>55647</EventRecordID>
        <Correlation />
        <Execution ProcessID="1" ThreadID="1" />
        <Channel>service</Channel>
        <Computer>computer</Computer>
        <Security UserID="0000" />
    </System>
    <EventData>
        <Data>583</Data>
        <Data>36</Data>
        <Data>192.168.0.1:5084</Data>
        <Data>level</Data>
        <Data>name,lDAPDisplayName</Data>
        <Data />
        <Data>5545</Data>
        <Data>3</Data>
        <Data>0</Data>
        <Data>0</Data>
        <Data>0</Data>
        <Data>15</Data>
        <Data>none</Data>
    </EventData>
</Event>
```

Чтобы выполнить парсинг таких событий необходимо:

- Настроить нумерацию тегов.

- Настроить мапинг данных для пронумерованных тегов с полями события KUMA.

KUMA 3.0.x поддерживает одновременное использование параметров **XML-атрибутов** и **Нумерация тегов** в одном дополнительном нормализаторе. Если атрибут содержит неименованные теги или одинаковые теги, рекомендуется использовать функцию **Нумерация тегов**. Если атрибут содержит только именованные теги, используйте **Атрибуты XML**. Чтобы использовать эту функциональность в дополнительных нормализаторах, вам нужно последовательно включить параметр "Сохранить исходное событие" в каждом дополнительном нормализаторе на пути, по которому событие следует к целевому дополнительному нормализатору, и в самом целевом дополнительном нормализаторе.

В качестве примера использования этой функции вы можете обратиться к нормализатору MicrosoftProducts, параметр "Сохранить исходное событие" включен последовательно в дополнительных нормализаторах "AD FS" и "424".

Чтобы настроить парсинг событий с тегами, содержащими одинаковое название или теги без названия:

1. Создайте новый нормализатор или откройте существующий нормализатор для редактирования.

2. В окне нормализатора **Основной парсинг событий** в раскрывающемся списке **Метод парсинга** выберите значение xml и в поле **Нумерация тегов** нажмите **Добавить поле**.

   В появившемся поле укажите полный путь к тегу, элементам которого следует присвоить порядковый номер. Например, Event.EventData.Data. Первый номер, который будет присвоен тегу – 0. Если тег пустой, например, <Data />, ему также будет присвоен порядковый номер.

3. Чтобы настроить мапинг данных, в группе параметров **Сопоставление** нажмите **Добавить строку** и выполните следующие действия:

   a. В появившейся строке в поле **Исходные данные** укажите полный путь к тегу и его индекс. Для события Microsoft Windows из примера выше полный путь с индексами будет выглядеть следующим образом:

      - Event.EventData.Data.0
      - Event.EventData.Data.1
      - Event.EventData.Data.2 и так далее

   b. В раскрывающемся списке **Поле KUMA** выберите поле в событии KUMA, в которое попадет значение из пронумерованного тега после выполнения парсинга.

4. Чтобы сохранить изменения:

   - Если вы создали новый нормализатор, нажмите **Сохранить**.
   - Если вы редактировали существующий нормализатор, нажмите **Обновить параметры** в коллекторе, к которому привязан нормализатор.

Настройка парсинга завершена.

- netflow5

Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип netflow5 выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для типа **netflow5** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow9**

  Этот метод парсинга используется для обработки данных в формате NetFlow v9.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип netflow9 выбран для основного парсинга, дополнительная нормализация недоступна.

  В правилах сопоставления по умолчанию для типа **netflow9** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sflow5**

  Этот метод парсинга используется для обработки данных в формате sflow5.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип sflow5 выбран для основного парсинга, дополнительная нормализация недоступна.

- **ipfix**

  Этот метод парсинга используется для обработки данных в формате IPFIX.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**. Если тип ipfix выбран для основного парсинга, дополнительная нормализация недоступна.

  В правилах сопоставления по умолчанию для типа **ipfix** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sql** – этот метод становится доступным, только при использовании коннектора типа sql

  Нормализатор использует этот метод для обработки данных, полученных с помощью выборки из базы данных.

4. В раскрывающемся списке **Сохранить исходное событие** укажите, надо ли сохранять исходное "сырое" событие во вновь созданном нормализованном событии. Доступные значения:

   - **Не сохранять** – не сохранять исходное событие. Это значение используется по умолчанию.
   - **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке службы. В этом случае каждый раз, когда у события есть непустое поле `Raw`, это означает, что возникла проблема.

     Если поля с названиями `*Address` или `*Date*` не соответствуют правилам нормализации, такие поля игнорируются. При этом не возникает ошибка нормализации и значения полей не попадают в поле `Raw` нормализованного события, даже если был указан параметр **Сохранить исходное событие → При возникновении ошибок**.

   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

   Этот параметр недоступен для дополнительных правил парсинга.

5. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля исходного события в нормализованном событии, если для них не были настроены правила сопоставления (см. ниже). Данные сохраняются в поле события `Extra`. Нормализованные события можно искать и фильтровать по данным, хранящимся в поле `Extra`.

   Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

По умолчанию поля не сохраняются.

6. В поле **Описание** укажите описание ресурса: до 4000 символов в кодировке Unicode.

   Этот параметр недоступен для дополнительных правил парсинга.

7. При необходимости поле **Примеры событий** укажите пример данных, которые вы хотите обработать.

   Этот параметр недоступен для методов парсинга **netflow5**, **netflow9**, **sflow5**, **ipfix**, **sql**.

   Поле **Примеры событий** заполняется данными, полученными из сырого события, если парсинг события был выполнен успешно и тип полученных из сырого события данных совпадает с типом поля KUMA.

   Например, значение "192.168.0.1", заключенное в кавычки не будет отображено в поле SourceAddress, при этом значение 192.168.0.1 будет отображено в поле **Примеры событий**.

8. В таблице **Сопоставление** настройте сопоставление полей сырого события с полями событий в формате KUMA:

   a. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите преобразовать в поле события KUMA.

      Подробнее о формате полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

      Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку 🔧, откроется окно **Преобразование**, в котором при нажатии на кнопку **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

b. В столбце **Поле KUMA** в раскрывающемся списке выберите требуемое поле события KUMA. Поля можно искать, вводя в поле их названия.

Рекомендации для полей столбцов KUMA

Рекомендуется настроить сопоставление для следующих полей KUMA. Иначе вы не сможете просматривать наблюдаемые объекты в деталях алертов и инцидентов.

Рекомендуемые поля KUMA зависят от типов наблюдаемых объектов:

- Для наблюдаемых объектов типа MD5 и SHA256:
  - FileHash
- Для наблюдаемых объектов типа URL:
  - RequestUrl
- Для наблюдаемых объектов типа IP-адреса:
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress
  - SourceTranslatedAddress
  - SourceAddress
- Для наблюдаемых объектов типа Доменное имя:
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain
  - SourceDnsDomain
  - SourceNtDomain
- Для наблюдаемых объектов типа UserName:
  - DestinationUserName
  - SourceUserName

- Для наблюдаемых объектов типа HostName:
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. Если название поля события KUMA, выбранного на предыдущем шаге, начинается с `DeviceCustom*` и `Flex*`, в поле **Подпись** можно добавить уникальную пользовательскую метку.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

Чтобы KUMA могла выполнить обогащение событий данными про активы, и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам необходимо настроить сопоставление полей для адреса устройства и имени устройства в зависимости от назначения актива. Например, сопоставление для SourceAddress и SourceHostName, или DestinationAddress и DestinationHostName. В результате обогащения в карточке события появится поле SourceAssetID или DestinationAssetID и ссылка, по которой можно будет перейти в карточку актива. Также в результате обогащения сведения об активе будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события KUMA.

Если размер поля события KUMA оказывается меньше длины помещаемого в него значения, значение обрезается до размера поля события.

Расширенная схема события

При нормализации событий, помимо полей стандартной схемы событий KUMA, могут быть использованы поля расширенной схемы событий. Информация о типах полей расширенной схемы событий приведена в таблице далее.

Использование значительного количества уникальных полей расширенной схемы событий может привести к снижению производительности системы, увеличению объема дискового пространства, необходимого для хранения событий, сложности восприятия данных.

Мы рекомендуем предварительно продумать и сформировать минимально необходимый набор дополнительных полей расширенной схемы событий и использовать его в нормализаторах и корреляции.

Для использования полей расширенной схемы событий необходимо выполнить следующее:

- открыть существующий или создать новый нормализатор событий;
- заполнить основные параметры нормализатора;
- нажать на кнопку "Добавить строку";
- в параметре Исходные данные указать название исходного поля в сыром событии;
- в параметре Поле KUMA указать имя создаваемого поля расширенной схемы событий, см. таблицу далее. Также можно использовать одно из существующих полей расширенной схемы событий.

Поля расширенной модели данных нормализованного события

Название поля	Тип данных	Доступность в нормализаторе	Описание

Указывается в параметре Поле KUMA			
S.<имя поля>	Строка	Все типы	Поле с типом "Строка"
N.<имя поля>	Число	Все типы	Поле с типом "Число"
F.<имя поля>	Число с плавающей точкой	Все типы	Поле с типом "Число с плавающей точкой"
SA.<имя поля>	Массив строк	KV, JSON	Поле с типом "Массив строк". Порядок элементов массива соответствует порядку элементов сырого события.
NA.<имя поля>	Массив целых чисел	KV, JSON	Поле с типом "Массив целых чисел". Порядок элементов массива соответствует порядку элементов сырого события.
FA.<имя поля>	Массив чисел с плавающей точкой	KV, JSON	Поле с типом "Чисел с плавающей точкой". Порядок элементов массива соответствует порядку элементов сырого события.

Префиксы "S.", "N.", "F.", "SA.", "NA.", "FA." обязательны при создании полей расширенной схемы событий, префиксы должны использовать только заглавные буквы.

Вместо <filed_name> необходимо задать имя поля. В имени поля допустимо использовать символы английского алфавита, числа. Использование символа "пробел" не допускается.

- Нажать на кнопку OK.
- Нажать на кнопку Сохранить для заверения редактирования нормализатора событий.

Нормализатор сохранен, дополнительное поле создано. После сохранение нормализатора дополнительное поле может быть использовано в других нормализаторах.

Примечание: в случае, если данные, находящиеся в поля сырого события, не соответствуют типу поля KUMA, то в процессе нормализации событий значение не будет сохранено. Например, строка "test" не может быть помещена в числовое поле KUMA DeviceCustomNumber1.

С точки зрения нагрузки на сервер хранения при операциях при операциях поиска событий, подготовки отчетов и иных операциями с событиями в хранилище наиболее предпочтительными являются поля схемы событий KUMA, затем идут поля расширенной схемы событий., затем поля Extra.

Обогащение в нормализаторе

При создании правил парсинга событий в окне параметров нормализатора на вкладке **Обогащение** вы можете настроить правила дополнения полей нормализованного события другими данными с помощью правил обогащения. Эти правила хранятся в параметрах нормализатора, в котором они были созданы.

Чтобы создать обогащение, нужно нажать на кнопку **Добавить обогащение**. Правил обогащения может быть несколько. При необходимости обогащения можно удалять с помощью кнопки ✕.

Параметры, доступные в блоке параметров правила обогащения:

- **Тип источника** (обязательно) – раскрывающийся список для выбора типа обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

  Доступные типы источников обогащения:

  - **константа**

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

- В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено.
- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива.

- dictionary

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- table

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

- В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
- В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра Тип источника данных выбран тип "Событие", а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом "Массив строк", а целевым полем является поле с типом "Строка", значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем "Массив строк" и целевое поле полем "Массив строк", значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **Целевое поле** (обязательно) – раскрывающийся список для выбора поля события KUMA, в которое следует поместить данные.

  Этот параметр недоступен для типа источника обогащения **таблица**.

Условия передачи данных в дополнительный нормализатор

При создании дополнительных правил парсинга событий вы можете указать условия. При выполнении этих условий события отправляются на обработку в созданное правило парсинга. Условия можно задать в окне **Дополнительное правило парсинга** на вкладке **Условия дополнительной нормализации**. В основных правилах парсинга эта вкладка отсутствует.

Доступные параметры:

- **Использовать сырое событие** – если вы хотите передавать сырое событие для дополнительной нормализации, в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**. По умолчанию указано значение **Нет**. Рекомендуется передавать сырое событие в нормализаторы типа json и xml. Если вы хотите передавать сырое событие для дополнительной нормализации на второй, третий и далее уровень вложенности, последовательно на каждом уровне вложенности в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**.

- **Поле, которое следует передать в нормализатор** – используется для указания поля события в том случае, если вы хотите отправлять на дополнительный парсинг только события с заданными в параметрах нормализатора полями.

Если оставить это поле пустым, в дополнительный нормализатор будет передано событие целиком.

- Блок фильтров – используется для формулирования сложных условий, которым должны удовлетворять события, поступающие в нормализатор.

  Вы можете нажать на кнопку **Добавить условие**, чтобы добавить строку с полями для определения условия (см. ниже).

  Нажав на кнопку **Добавить группу**, можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить другие группы условий и отдельные условия.

  Условия и группы можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

Параметры условий фильтра:

- **Левый операнд** и **Правый операнд** – используются для указания значений, которые будет обрабатывать оператор.

  В левом операнде следует указывать исходное поле событий, поступающих в нормализатор. Например, если в окне **Основной парсинг событий** настроено сопоставление eventType - DeviceEventClass, то в окне **Дополнительный парсинг событий** на вкладке **Условия дополнительной нормализации** в поле левого операнда для фильтра следует указать eventType. Данные обрабатываются только как текстовые строки.

- Операторы:

  - **=** – полное совпадение левого и правого операндов.
  - **startsWith** – левый операнд начинается с символов, указанных в правом операнде.
  - **endsWith** – левый операнд заканчивается символами, указанными в правом операнде.
  - **match** – левые операнд соответствует регулярному выражению (RE2), указанному в правом операнде.
  - **in** – левый операнд соответствует одному из значений, указанных в правом операнде.

Входящие данные можно преобразовать, нажав на кнопку 🔧. Откроется окно **Преобразование**, в котором вы можете нажать на кнопку **Добавить преобразование**, чтобы создать правила изменения исходных данных перед тем, как над ними будут совершены какие-либо действия. В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

Поддерживаемые источники событий

KUMA поддерживает нормализацию событий, которые поступают от систем, перечисленных в таблице "Поддерживаемые источники событий". Нормализаторы для указанных систем включены в поставку.

Поддерживаемые источники событий

Название системы	Название нормализатора	Тип	Описание нормализатора
1C EventJournal	[OOTB] 1C EventJournal Normalizer	xml	Предназначен для обработки журнала событий системы 1С. Источник событий — журнал регистрации 1С.
1C TechJournal	[OOTB] 1C TechJournal Normalizer	regexp	Предназначен для обработки технологического журнала событий. Источник событий — технологический журнал 1С.
Absolute Data and Device Security (DDS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
AhnLab Malware Defense System (MDS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ahnlab UTM	[OOTB] Ahnlab UTM	regexp	Предназначен для обработки событий от системы Ahnlab. Источник событий - системные, операционные журналы, подключения, модуль IPS.
AhnLabs MDS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Apache Cassandra	[OOTB] Apache Cassandra file	regexp	Предназначен для обработки событий в журналах СУБД Apache Cassandra версии 4.0.
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Avigilon Access Control Manager (ACM)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Ayehu eyeShare	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BeyondTrust's BeyondInsight	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	Syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по Syslog.
Bloombase StoreSafe	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BMC CorreLog	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Bricata ProAccel	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Brinqa Risk Analytics	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	Предназначен для обработки событий от системы Symantec Endpoint Protection.
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	Предназначен для обработки событий, поступающих по syslog от системы Canonical LXD версии 5.18.
Checkpoint	[OOTB] Checkpoint Syslog CEF by CheckPoint	Syslog	Предназначен для обработки событий, поступающих от источника событий Checkpoint по протоколу Syslog в формате CEF.
Cisco Access Control Server (ACS)	[OOTB] Cisco ACS syslog	regexp	Предназначен для обработки событий системы Cisco Access Control Server (ACS), поступающих по Syslog.
Cisco ASA	[OOTB] Cisco ASA Extended v 0.1	Syslog	Предназначен для обработки событий устройств Cisco ASA. Cisco ASA базовый расширенный набор событий.
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	Предназначен для обработки журнала событий прокси-сервера Cisco Email Security Appliance (WSA), файл access.log.
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	Предназначен для обработки событий системы Cisco Identity Services Engine (ISE), поступающих по Syslog.
Cisco Netflow v5	[OOTB] NetFlow v5	netflow5	Предназначен для обработки событий, поступающих Cisco Netflow версии 5.
Cisco NetFlow v9	[OOTB] NetFlow v9	netflow9	Предназначен для обработки событий, поступающих Cisco Netflow версии 9.

Cisco Prime	[OOTB] Cisco Prime syslog	Syslog	Предназначен для обработки событий системы Cisco Prime версии 3.10, поступающих по syslog.
Cisco Secure Email Gateway (SEG)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cisco Secure Firewall Management Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Citrix NetScaler	[OOTB] Citrix NetScaler	regexp	Предназначен для обработки событий, поступающих от балансировщика нагрузки Citrix NetScaler версии 13.7.
Claroty Continuous Threat Detection	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CloudPassage Halo	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Codemaster Mirada	[OOTB] Codemaster Mirada syslog	Syslog	Предназначен для обработки событий системы Codemaster Mirada, поступающих по syslog.
Corvil Network Analytics	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cribl Stream	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CrowdStrike Falcon Host	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CyberArk Privileged Threat Analytics (PTA)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CyberPeak Spektr	[OOTB] CyberPeak Spektr syslog	Syslog	Предназначен для обработки событий системы CyberPeak Spektr версии 3, поступающих по syslog.
DeepInstinct	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Delinea Secret Server	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Digital Guardian Endpoint Threat Detection	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
DNS сервер BIND	[OOTB] BIND Syslog [OOTB] BIND file	Syslog regexp	[OOTB] BIND Syslog предназначен для обработки событий DNS-сервера BIND, поступающих по Syslog. [OOTB] BIND file предназначен для обработки журналов событий DNS-сервера BIND.
Dovecot	[OOTB] Dovecot Syslog	Syslog	Предназначен для обработки событий почтового сервера Dovecot, поступающих по Syslog. Источник событий — журналы POP3/IMAP.
Dragos Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
EclecticIQ Intelligence Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Edge Technologies AppBoard and enPortal	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Eltex MES Switches	[OOTB] Eltex MES Switches	regexp	Предназначен для обработки событий от сетевых устройств Eltex.
Eset Protect	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
F5 BigIP Advanced Firewall	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Manager (AFM)			
FFRI FFR yarai	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FireEye CM Series	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FireEye Malware Protection System	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Forcepoint NGFW	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Forcepoint SMC	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiGate	[OOTB] Syslog-CEF	regexp	Предназначен для обработки событий в формате CEF.
Fortinet FortiGate	[OOTB] FortiGate syslog KV	Syslog	Предназначен для обработки событий, поступающих от межсетевых экранов FortiGate по syslog. Источник событий - журналы FortiGate в формате key-value.
Fortinet Fortimail	[OOTB] Fortimail	regexp	Предназначен для обработки событий системы защиты электронной почты FortiMail. Источник событий — журналы почтовой системы Fortimail.
Fortinet FortiSOAR	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FreeIPA	[OOTB] FreeIPA	json	Предназначен для обработки событий, поступающих от системы FreeIPA. Источник событий — журналы службы каталогов Free IPA.
FreeRADIUS	[OOTB] FreeRADIUS syslog	Syslog	Предназначен для обработки событий системы FreeRADIUS, поступающих по Syslog. Нормализатор поддерживает события от FreeRADIUS версии 3.0.
Gardatech GardaDB	[OOTB] Gardatech GardaDB syslog	Syslog	Предназначен для обработки событий системы Gardatech GardaDB, поступающих по syslog в формате, схожим с CEF.
Gardatech Perimeter	[OOTB] Gardatech Perimeter syslog	Syslog	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, поступающих по syslog.
Gigamon GigaVUE	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
HAProxy	[OOTB] HAProxy syslog	Syslog	Предназначен для обработки журналов системы HAProxy. Нормализатор поддерживает события типа HTTP log, TCP log, Error log от HAProxy версии 2.8.
Huawei Eudemon	[OOTB] Huawei Eudemon	regexp	Предназначен для обработки событий, поступающих от межсетевых экранов Huawei Eudemon. Источник событий — журналы межсетевых экранов Huawei Eudemon.
Huawei USG	[OOTB] Huawei USG Basic	Syslog	Предназначен для обработки событий, поступающих от шлюзов безопасности Huawei USG по Syslog.
IBM InfoSphere Guardium	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ideco UTM	[OOTB] Ideco UTM Syslog	Syslog	Предназначен для обработки событий, поступающих от Ideco UTM по Syslog. Нормализатор поддерживает обработку событий Ideco UTM версии 14.7, 14.10.
Illumio Policy Compute Engine (PCE)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Imperva Incapsula	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Imperva SecureSphere	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Indeed PAM	[OOTB] Indeed PAM syslog	Syslog	Предназначен для обработки событий Indeed PAM (Privileged Access Manager) версии 2.6.
Indeed SSO	[OOTB] Indeed SSO xml	xml	Предназначен для обработки событий системы Indeed SSO (Single Sign-On). Нормализатор поддерживает работу с KUMA 2.1.3 и выше.
InfoWatch Traffic	[OOTB]	sql	Предназначен для обработки событий, полученных коннектором из базы данных

Monitor	InfoWatch Traffic Monitor SQL		системы InfoWatch Traffic Monitor.
Intralinks VIA	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
IPFIX	[OOTB] IPFIX	ipfix	Предназначен для обработки событий в формате IP Flow Information Export (IPFIX).
Juniper JUNOS	[OOTB] Juniper - JUNOS	regexp	Предназначен для обработки событий аудита, поступающих от сетевых устройств Juniper.
Kaspersky Anti Targeted Attack (KATA)	[OOTB] KATA	cef	Предназначен для обработки алертов или событий из журнала активности Kaspersky Anti Targeted Attack.
Kaspersky CyberTrace	[OOTB] CyberTrace	regexp	Предназначен для обработки событий Kaspersky CyberTrace.
Kaspersky Endpoint Detection and Response (KEDR)	[OOTB] KEDR telemetry	json	Предназначен для обработки телеметрии Kaspersky EDR, размеченных KATA. Источник событий — kafka, EnrichedEventTopic
Kaspersky Industrial CyberSecurity for Networks	[OOTB] KICS4Net v2.x	cef	Предназначен для обработки событий Kaspersky Industrial CyberSecurity for Networks версии 2.x.
Kaspersky Industrial CyberSecurity for Networks	[OOTB] KICS4Net v3.x	Syslog	Предназначен для обработки событий Kaspersky Industrial CyberSecurity for Networks версии 3.x.
Kaspersky Security Center	[OOTB] KSC	cef	Предназначен для обработки событий Kaspersky Security Center по Syslog.
Kaspersky Security Center	[OOTB] KSC from SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных приложения Kaspersky Security Center.
Kaspersky Security для Linux Mail Server (KLMS)	[OOTB] KLMS Syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Kaspersky Security for Linux Mail Server в формате CEF по Syslog.
Kaspersky Secure Mail Gateway (KSMG)	[OOTB] KSMG Syslog CEF	Syslog	Предназначен для обработки событий Kaspersky Secure Mail Gateway версии 2.0 в формате CEF по Syslog.
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS Syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Kaspersky Web Traffic Security в формате CEF по Syslog.
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS (KV)	Syslog	Предназначен для обработки событий Kaspersky Web Traffic Security для формата Key-Value.
Kemptechnologies LoadMaster	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Kerio Control	[OOTB] Kerio Control	Syslog	Предназначен для обработки событий межсетевых экранов Kerio Control.
KUMA	[OOTB] KUMA forwarding	json	Предназначен для обработки событий, перенаправленных из KUMA.
Libvirt	[OOTB] Libvirt syslog	Syslog	Предназначен для обработки событий Libvirt версии 8.0.0, поступающих по syslog.
Lieberman Software ERPM	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Linux	[OOTB] Linux audit and iptables Syslog	Syslog	Предназначен для обработки событий операционной системы Linux. Этот нормализатор будет удален из набора OOTB через релиз. Если вы используете этот нормализатор, вам необходимо перейти на использование нормализатора [OOTB] Linux audit and iptables Syslog v1.
Linux	[OOTB] Linux audit and iptables Syslog v1	Syslog	Предназначен для обработки событий операционной системы Linux.

Linux	[OOTB] Linux audit.log file	regexp	Предназначен для обработки журналов безопасности операционных систем семейства Linux, поступающих по Syslog.
MariaDB	[OOTB] MariaDB Audit Plugin Syslog	Syslog	Предназначен для обработки событий, поступающих от плагина аудита MariaDB Audit по Syslog.
Microsoft Active Directory Federation Service (AD FS)	[OOTB] Microsoft Products	xml	Предназначен для обработки событий Microsoft AD FS. Нормализатор поддерживает работу с данным источником событий в KUMA 3.0.2.
Microsoft Active Directory Domain Service (AD DS)	[OOTB] Microsoft Products	xml	Предназначен для обработки событий Microsoft AD DS. Нормализатор поддерживает работу с данным источником событий в KUMA 3.0.2.
Microsoft Defender	[OOTB] Microsoft Products	xml	Предназначен для обработки событий Microsoft Defender.
Microsoft DHCP	[OOTB] MS DHCP file	regexp	Предназначен для обработки событий от DHCP-сервера Microsoft. Источник событий — журналы DHCP сервера Windows.
Microsoft DNS	[OOTB] DNS Windows	regexp	Предназначен для обработки событий DNS сервера Microsoft. Источник событий — журналы DNS сервера Windows.
Microsoft Exchange	[OOTB] Exchange CSV	csv	Предназначен для обработки журнала событий системы Microsoft Exchange. Источник событий — журналы MTA сервера Exchange.
Microsoft IIS	[OOTB] IIS Log File Format	regexp	Нормализатор обрабатывает события в формате, описанном по ссылке: https://learn.microsoft.com/en-us/windows/win32/http/iis-logging. Источник событий — журналы Microsoft IIS.
Microsoft Network Policy Server (NPS)	[OOTB] Microsoft Products	xml	Нормализатор предназначен для обработки событий операционной системы Microsoft Windows. Источник событий — события Network Policy Server.
Microsoft Sysmon	[OOTB] Microsoft Products	xml	Нормализатор предназначен для обработки событий модуля Microsoft Sysmon.
Microsoft Windows	[OOTB] Microsoft Products	xml	Нормализатор предназначен для обработки событий операционной системы Microsoft Windows.
Microsoft PowerShell	[OOTB] Microsoft Products	xml	Нормализатор предназначен для обработки событий операционной системы Microsoft Windows.
Microsoft SQL Server;	[OOTB] Microsoft SQL Server xml	xml	Предназначен для обработки событий MS SQL Server версии 2008, 2012, 2014, 2016. Нормализатор поддерживает работу с KUMA 2.1.3 и выше.
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products	xml	Нормализатор предназначен для обработки событий операционной системы Microsoft Windows. Источник событий — журнал Applications and Services Logs - Microsoft - Windows - TerminalServices-LocalSessionManager - Operational
Microsoft Windows XP/2003.	[OOTB] SNMP. Windows {XP/2003}	json	Предназначен для обработки событий, поступающих от рабочих станций и серверов под управлением операционных систем Microsoft Windows XP, Microsoft Windows 2003 с использованием протокола SNMP.
MikroTik	[OOTB] MikroTik syslog	regexp	Предназначен для событий, поступающих от устройств MikroTik по Syslog.
Minerva Labs Minerva EDR	[OOTB] Minerva EDR	regexp	Предназначен для обработки событий от EDR системы Minerva.
MySQL 5.7	[OOTB] MariaDB Audit Plugin Syslog	Syslog	Предназначен для обработки событий, поступающих от плагина аудита MariaDB Audit по Syslog.
NetApp	[OOTB] NetApp syslog, [OOTB] NetApp file	regexp	[OOTB] NetApp syslog - предназначен для обработки событий системы NetApp (версия - ONTAP 9.12), поступающих по syslog. [OOTB] NetApp file - предназначен для обработки событий системы NetApp (версия - ONTAP 9.12), хранящихся в файле.
NetIQ Identity Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
NetScout Systems nGenius	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Performance Manager			
Netskope Cloud Access Security Broker	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Netwrix Auditor	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Nextcloud	[OOTB] Nextcloud syslog	Syslog	Предназначен для событий Nextcloud версии 26.0.4, поступающих по syslog. Нормализатор не сохраняет информацию из поля Trace.
Nexthink Engine	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Nginx	[OOTB] Nginx regexp	regexp	Предназначен для обработки событий журнала веб-сервера Nginx.
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
One Identity Privileged Session Management	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Open VPN	[OOTB] OpenVPN file	regexp	Предназначен для обработки журнала системы OpenVPN.
Oracle	[OOTB] Oracle Audit Trail	sql	Предназначен для обработки событий аудита БД, полученных коннектором непосредственно из базы данных Oracle.
Orion soft zVirt	[OOTB] Orion Soft zVirt syslog	regexp	Предназначен для обработки событий системы виртуализации Orion soft zVirt версии 3.1.
PagerDuty	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Networks NGFW	[OOTB] PA-NGFW (Syslog-CSV)	Syslog	Предназначен для обработки событий от межсетевых экранов Palo Alto Networks, поступающих по Syslog в формате CSV.
Palo Alto Networks PANOS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Penta Security WAPPLES	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Positive Technologies ISIM	[OOTB] PTsecurity ISIM	regexp	Предназначен для обработки событий от системы PT Industrial Security Incident Manager.
Positive Technologies Network Attack Discovery (NAD)	[OOTB] PTsecurity NAD	Syslog	Предназначен для обработки событий от PT Network Attack Discovery (NAD), поступающих по Syslog.
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	Предназначен для обработки событий системы PT Sandbox.
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF	Syslog	Предназначен для обработки событий, поступающих от системы PTsecurity (Web Application Firewall).
PostgreSQL pgAudit	[OOTB] PostgreSQL pgAudit Syslog	Syslog	Предназначен для обработки событий плагина аудита pgAudit для базы данных PostgreSQL, поступающих по Syslog.
PowerDNS	[OOTB] PowerDNS syslog	Syslog	Предназначен для обработки событий PowerDNS Authoritative Server версии 4.5, поступающих по Syslog.
Proofpoint Insider Threat Management	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Proxmox	[OOTB] Proxmox file	regexp	Предназначен для событий системы Proxmox версии 7.2-3, хранящихся в файле. Нормализатор поддерживает обработку событий в журналах access и pveam.
PT NAD	[OOTB] PT NAD json	json	Предназначен для обработки событий, поступающий от PT NAD в формате json. Нормализатор поддерживает обработку событий PT NAD версий 11.1, 11.0.
QEMU - журналы гипервизора	[OOTB] QEMU - Hypervisor file	regexp	Предназначен для обработки событий гипервизора QEMU, хранящихся в файле. Поддерживаются версии QEMU 6.2.0, Libvirt 8.0.0.
QEMU - журналы виртуальных машин	[OOTB] QEMU - Virtual Machine file	regexp	Предназначен для обработки событий из журналов виртуальных машин гипервизора QEMU версии 6.2.0, хранящихся в файле.
Radware DefensePro AntiDDoS	[OOTB] Radware DefensePro AntiDDoS	Syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по Syslog.
Reak Soft Blitz Identity Provider	[OOTB] Reak Soft Blitz Identity Provider file	regexp	Предназначен для обработки событий системы Reak Soft Blitz Identity Provider версии 5.16, хранящихся в файле.
Recorded Future Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
RedCheck Desktop	[OOTB] RedCheck Desktop file	regexp	Предназначен для обработки журналов системы RedCheck Desktop 2.6, хранящихся в файле.
RedCheck WEB	[OOTB] RedCheck WEB file	regexp	Предназначен для обработки журналов системы RedCheck Web 2.6, хранящихся в файлах.
ReversingLabs N1000 Appliance	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Rubicon Communications pfSense	[OOTB] pfSense Syslog	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана pfSense, поступающих по Syslog.
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана pfSense. Syslog-заголовок этих событий не содержит имени устройства.
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Sendmail	[OOTB] Sendmail syslog	Syslog	Предназначен для обработки событий Sendmail версии 8.15.2, поступающих по syslog.
SentinelOne	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Snort	[OOTB] Snort 3 json file	json	Предназначен для обработки событий Snort версии 3 в формате JSON.
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall	Syslog	Предназначен для обработки событий, поступающих по Syslog от межсетевого экрана Sonicwall TZ.
Sophos XG	[OOTB] Sophos XG	regexp	Предназначен для обработки событий от межсетевого экрана Sophos XG.
Squid	[OOTB] Squid access Syslog	Syslog	Предназначен для обработки событий прокси-сервера Squid, поступающих по протоколу Syslog.
Squid	[OOTB] Squid access.log file	regexp	Предназначен для обработки событий журнала Squid прокси-сервера Squid. Источник событий — журналы access.log
S-Terra VPN Gate	[OOTB] S-Terra	Syslog	Предназначен для обработки событий от устройств S-Terra VPN Gate.
Suricata	[OOTB] Suricata json file	json	Пакет содержит нормализатор для событий Suricata версии 7.0.1, хранящихся в файле в формате JSON. Нормализатор поддерживает обработку следующих типов событий: flow, anomaly, alert, dns, http, ssl, tls, ftp, ftp_data, ftp, smb, rdp, pgsql, modbus, quic, dhcp, bittorrent_dht, rfb.
ThreatConnect Threat Intelligence	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Platform			
ThreatQuotient	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
TrapX DeceptionGrid	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro Control Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro Deep Security	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro NGFW	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Unbound	[OOTB] Unbound Syslog	Syslog	Предназначен для обработки событий, поступающих по Syslog от DNS-сервера Unbound.
UserGate	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы UserGate по Syslog.
Varonis DatAdvantage	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Veriato 360	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
ViPNet TIAS	[OOTB] Vipnet TIAS syslog	Syslog	Предназначен для обработки событий системы ViPNet TIAS версии 3.8, поступающих по Syslog.
VMware ESXi	[OOTB] VMware ESXi syslog	regexp	Предназначен для обработки событий VMware ESXi (поддержка ограниченного количества событий от ESXi с версиями 5.5, 6.0, 6.5, 7.0), поступающих по Syslog.
VMWare Horizon	[OOTB] VMWare Horizon - Syslog	Syslog	Предназначен для обработки событий, поступающих от системы VMWare Horizon версии 2106 по Syslog.
VMware Carbon Black EDR	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Vormetric Data Security Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Votiro Disarmer for Windows	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Wallix AdminBastion	[OOTB] Wallix AdminBastion syslog	regexp	Предназначен для событий, поступающих от системы Wallix AdminBastion по Syslog.
WatchGuard - Firebox	[OOTB] WatchGuard Firebox	Syslog	Предназначен для обработки событий межсетевых экранов WatchGuard Firebox, поступающих по Syslog.
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Winchill Fracas	[OOTB] PTC Winchill Fracas	regexp	Предназначен для обработки событий системы регистрации сбоев Winchill Fracas.
Zabbix	[OOTB] Zabbix SQL	sql	Предназначен для обработки событий Zabbix версии 6.4.
ZEEK IDS	[OOTB] ZEEK IDS json file	json	Предназначен для обработки журналов системы ZEEK IDS в формате JSON. Нормализатор поддерживает события от ZEEK IDS версии 1.8.
Zettaset BDEncrypt	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Zscaler Nanolog Streaming Service (NSS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

АйТи Бастион – СКДПУ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы АйТи Бастион - СКДПУ по Syslog.
А-реал Интернет Контроль Сервер (ИКС)	[OOTB] A-real IKS syslog	regexp	Предназначен для обработки событий системы А-реал Интернет Контроль Сервер (ИКС), поступающих по Syslog. Нормализатор поддерживает события от A-real IKS версии 7.0 и выше.
Веб-сервер Apache	[OOTB] Apache HTTP Server file	regexp	Предназначен для обработки событий Apache HTTP Server версии 2.4, хранящихся в файле. Нормализатор поддерживает обработку событий журнала Application в форматах Common или Combined Log, и журнала Error. Ожидаемый формат журнала Error: "[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i"
Веб-сервер Apache	[OOTB] Apache HTTP Server syslog	Syslog	Предназначен для обработки событий системы Apache HTTP Server, поступающих по syslog. Нормализатор поддерживает обработку событий Apache HTTP Server версии 2.4 журнала Access в формате Common или Combined Log, и журнала Error. Ожидаемый формат журнала Error: "[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i"
Веб-сервер Lighttpd	[OOTB] Lighttpd syslog	Syslog	Предназначен для обработки событий Access системы Lighttpd, поступающих по syslog. Нормализатор поддерживает обработку событий Lighttpd версии 1.4. Ожидаемый формат событий журнала Access: $remote_addr $http_request_host_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"
ИВК Кольчуга-К	[OOTB] Kolchuga-K Syslog	Syslog	Предназначен для обработки событий, поступающих от системы ИВК Кольчуга-К, версии ЛКНВ.466217.002 по Syslog.
ИнфоТеКС ViPNet IDS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы ИнфоТеКС ViPNet IDS по Syslog.
ИнфоТеКС ViPNet Coordinator	[OOTB] VipNet Coordinator Syslog	Syslog	Предназначен для обработки событий от системы ViPNet Coordinator, поступающих по Syslog.
Код безопасности - Континент	[OOTB] [regexp] Continent IPS/IDS & TLS	regexp	Предназначен для обработки журнала событий устройств Континент IPS/IDS.
Код безопасности - Континент	[OOTB] Continent SQL	sql	Предназначен для получения событий системы Континент из базы данных.
Код Безопасности SecretNet 7	[OOTB] SecretNet SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы SecretNet.
Конфидент - Dallas Lock	[OOTB] Конфидент Dallas Lock	regexp	Предназначен для обработки событий, поступающих от системы защиты информации Dallas Lock версии 8.
КриптоПро Ngate	[OOTB] Ngate Syslog	Syslog	Предназначен для обработки событий, поступающих от системы КриптоПро Ngate по Syslog.
НТ Мониторинг и аналитика	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы НТ Мониторинг и аналитика по Syslog.
Прокси-сервер BlueCoat	[OOTB] BlueCoat Proxy v0.2	regexp	Предназначен для обработки событий прокси-сервера BlueCoat. Источник событий — журнал событий прокси-сервера BlueCoat.
СКДПУ НТ Шлюз доступа	[OOTB] Bastion SKDPU-GW	Syslog	Предназначен для обработки событий системы СКДПУ НТ Шлюз доступа, поступающих по Syslog.
Солар Дозор	[OOTB] Solar Dozor Syslog	Syslog	Предназначен для обработки событий, поступающих от системы Солар Дозор версии 7.9 по Syslog. Нормализатор поддерживает обработку событий в пользовательском формате и не поддерживает обработку событий в формате CEF.
-	[OOTB] Syslog header	Syslog	Предназначен для обработки событий, поступающих по Syslog. Нормализатор выполняет парсинг Syslog-заголовка события, поле message события не затрагивается. В случае необходимости вы можете выполнить парсинг поля message другими нормализаторами.

Правила агрегации

Правила агрегации позволяют объединить однотипные повторяющиеся события и заменить их одним общим событием. В правилах агрегации поддерживается работа с полями стандартной схемы событий KUMA и с полями расширенной схемы событий. Таким образом можно уменьшить количество схожих событий, передаваемых в хранилище и/или коррелятор, снизить нагрузку на сервисы, сэкономить место для хранения данных и сэкономить лицензионную квоту (EPS). Агрегационное событие создается по достижении порога по времени или порога по числу событий, смотря что произойдет раньше.

Для правил агрегации можно настроить фильтр и применять его только к событиям, которые соответствуют заданным условиям.

Можно настроить правила агрегации в разделе **Ресурсы - Правила агрегации**, а затем выбрать созданное правило агрегации в раскрывающемся списке в настройках коллектора. Также можно настроить правила агрегации прямо в настройках коллектора.

Доступные параметры правил агрегации

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Предел событий	Ограничение по количеству событий. После накопления заданного количества событий с идентичными полями коллектор создает агрегационное событие и начинает накопление событий для следующего агрегированного события. По умолчанию указано значение `100`.
Время ожидания событий	Обязательный параметр. Ограничение по времени в секундах. По истечении указанного срока накопление базовых событий прекращается, коллектор создает агрегированное событие и начинает получать события для следующего агрегированного события. По умолчанию указано значение `60`.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.
Группирующие поля	Обязательный параметр. В раскрывающемся списке перечислены поля нормализованных событий, значения которых должны совпадать. Например, для сетевых событий это могут быть SourceAddress, DestinationAddress, DestinationPort. В итоговом агрегационном событии эти поля будут заполнены значениями базовых событий.
Уникальные поля	В раскрывающемся списке перечислены поля, спектр значений которых нужно сохранить в агрегированном событии. Например, если поле DestinationPort указать не в **Группирующие поля**, а в **Уникальные поля**, то агрегированное событие объединит базовые события подключения к разным портам, а поле DestinationPort агрегированного события будет содержать список всех портов, к которым выполнялись подключения.
Поля суммы	В раскрывающемся списке можно выбрать поля, значения которых при агрегации будут просуммированы и записаны в одноименные поля агрегированного события.
Фильтр	Блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Не используйте в правилах агрегации фильтры с операндом **TI** или операторами **TIDetect**, **inActiveDirectoryGroup** и **hasVulnerability**. Поля Active Directory, для которых используется оператор **inActiveDirectoryGroup,** появляются на этапе обогащения, то есть после выполнения правил агрегации. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В поставку OSMP включены перечисленные в таблице ниже правила агрегации.

Предустановленные правила агрегации

Название правила агрегации	Описание
[OOTB] Netflow 9	Правило сработает при достижении 100 событий или по истечении 10 секунд. Агрегация событий выполняется по полям: • DestinationAddress • DestinationPort • SourceAddress • TransportProtocol • DeviceVendor • DeviceProduct Поля DeviceCustomString1 и BytesIn суммируются.

Правила обогащения

Обогащение событий – это дополнение событий информацией, которая может быть использована для выявления инцидента и при проведении расследования.

Правила обогащения позволяют добавлять в поля события дополнительную информацию путем преобразования данных, уже размещенных в полях, или с помощью запроса данных из внешних систем. Например, в событии есть имя учетной записи пользователя. С помощью правила обогащения вы можете добавить сведения об отделе, должности и руководителе этого пользователя в поля события.

Правила обогащения можно использовать в следующих сервисах и функциях KUMA:

- Коллектор.
- Коррелятор.
- Нормализатор.

Доступные параметры правил обогащения перечислены в таблице ниже.

Вкладка Основные параметры

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип источника	Обязательный параметр. Раскрывающийся список для выбора типа входящих событий. В зависимости от выбранного типа отображаются дополнительные параметры: • **константа** Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения: • В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено. • В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные. Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа. Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива. • **dictionary**

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- table

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **entropy** используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа float. Результатом преобразования является число. Вычисление информационной энтропии позволяет обнаруживать DNS-туннели или скомпрометированные пароли, например, когда пользователь вводит пароль вместо учетной записи и этот пароль регистрируется в виде обычного текста.

- **lower** – используется для перевода всех символов значения в нижний регистр

- **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле Символы. Это поле появляется при выборе данного типа преобразования. Например, если для значения Microsoft-Windows-Sysmon выполнить преобразование trim со значением Micromon, то получается значение soft-Windows-Sys.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле Константа. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле Константа. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

- **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
- **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- dns;

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10.

Доступные параметры:

- **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
- **Рабочие процессы** – максимальное количество запросов в один момент времени. По умолчанию указано значение `1`.
- **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Срок жизни кеша** – время жизни значений, хранящихся в кеше. По умолчанию указано значение `60`.
- **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

- cybertrace;

Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
- **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. По умолчанию указано значение `1000`.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение `30`.
- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - **ip**
  - **url**
  - **hash**

  В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- cybertrace-http

Этот тип обогащения используется для добавления в поля события сведений с помощью REST API из потоков данных CyberTrace.

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
- **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. По умолчанию указано значение 30.
- **Ключевые поля** (обязательно) – это список полей событий, используемых для обогащения событий данными из CyberTrace.
- **Максимальное количество событий в очереди обогащения** – максимальное количество событий, хранящихся в очереди обогащения для повторной отправки. По умолчанию указано значение 1000000000. При достижении 1 000 000 событий, полученных с сервера CyberTrace, обогащение событий прекращается до тех пор, пока количество полученных событий станет меньше 500 000.

Когда значение метрики Queue достигает 1 000 000 полученных событий, обогащение событий прекращается и события записываются в Хранилище необогащенными до тех пор, пока количество событий в очереди не станет меньше 500 000.

- часовой пояс

Этот тип обогащения используется в коллекторах и коррелляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

> Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

> При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:
>
> | Формат времени в обрабатываемом событии | Пример |
> | --- | --- |
> | +-чч:мм | -07:00 |
> | +-ччмм | -0700 |
> | +-чч | -07 |
>
> Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

- геоданные.

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

   С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. Можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события, нажав эту кнопку.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ✕.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.
   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

Отладка	Переключатель, с помощью которого можно включить логирование операций сервиса. По умолчанию логирование выключено.
Описание	Описание ресурса: до 4000 символов в кодировке Unicode.
Фильтр	Блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Предустановленные правила обогащения

В поставку OSMP включены перечисленные в таблице ниже правила обогащения.

Предустановленные правила обогащения

Название правила обогащения	Описание
[OOTB] KATA alert	Используется для обогащения событий, поступивших от KATA в виде гиперссылки на алерт. Гиперссылка размещается в поле DeviceExternalId.

Правила корреляции

Правила корреляции используются для распознавания определенных последовательностей обрабатываемых событий и выполнения определенных действий после распознавания: например, создание корреляционных событий или алертов, взаимодействие с активным листом.

Правила корреляции можно использовать в следующих сервисах и функциях KUMA:

- Коррелятор.

- Правило уведомления.
- Связи правил сегментации.
- Ретроспективная проверка.

Доступные параметры правила корреляции зависят от выбранного типа. Типы правил корреляции:

- standard – используется для поиска корреляций между несколькими событиями. Правила этого типа могут создавать корреляционные события.

  Этот тип правил используется для определения сложных закономерностей в последовательности событий. Для более простых комбинаций следует использовать другие типы правил корреляции, которые требуют меньше ресурсов.

- simple – используется для создания корреляционных событий при обнаружении определенного события.
- operational – используется для операций с активными листами и контекстными таблицами. Этот тип правил не может создавать корреляционные события.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Если правило корреляции используется в коррелляторе и по нему был создан алерт, то при изменении правила корреляции существующий алерт не будет изменен, даже если перезапустить сервис коррелятора. Например, если у правила корреляции было изменено название, название алерта останется прежним. Если существующий алерт закрыть, то новый алерт будет создан уже с учетом изменений правила корреляции.

Правила корреляции типа standard

Правила корреляции типа **standard** используются для определения сложных закономерностей в обрабатываемых событиях.

Поиск закономерностей происходит с помощью контейнеров

Контейнеры правила корреляции – это временные хранилища данных, которые используются ресурсами правила корреляции при определении необходимости создания корреляционных событий. Эти контейнеры выполняет следующие функции:

- Группируют события, которые были отобраны фильтрами в группе настроек **Селекторы** ресурса правила корреляции. События группируются по полям, которые указываются пользователем в поле **Группирующие поля**.
- Определяют момент, когда должно сработать правило корреляции, меняя соответствующим образом события, сгруппированные в контейнере.
- Выполняют действия, указанные в группе настроек **Действия**.
- Создают корреляционные события.

Доступные состояния контейнера:

- `Пусто` – в контейнере нет событий. Это может произойти только в момент своего создания при срабатывании правила корреляции.
- `Частичное совпадение` – в контейнере есть некоторые из ожидаемых событий (события восстановления не учитываются).
- `Полное совпадение` – в корзине есть все ожидаемые события (события восстановления не учитываются). При достижении этого состояния:
  - Срабатывает правило корреляции
  - События удаляются из контейнера
  - Счетчик срабатываний контейнера обновляется
  - Контейнера переводится в состояние `Пусто`
- `Ложное совпадение` – такое состояние контейнера возможно в следующих случаях:
  - когда было достигнуто состояние `Полное совпадение`, но объединяющий фильтр возвратил значение false.
  - когда при установленном флажке **Обнуление** были получены события восстановления.

  Когда это условие достигается, правило корреляции не срабатывает. События удаляются из контейнера, счетчик срабатываний обновляется, контейнер переводится в состояния `Пусто`.

Окно правила корреляции содержит следующие вкладки:

- **Общие** – используется для указания основных параметров правила корреляции. На этой вкладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа правил.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер.

Доступные параметры зависят от выбранного типа правил.

- **Корреляторы** - используется для привязки корреляторов. Доступна только для созданных правил корреляции, открытых на редактирование.

Вкладка **Общие**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.

- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **standard**, если хотите создать правило корреляции типа standard.

- **Группирующие поля** (обязательно) – поля событий, которые должны быть сгруппированы в контейнере. Хеш-код значений выбранных полей используется в качестве ключа контейнера. Если срабатывает селектор (см. ниже), отобранные поля копируются в корреляционное событие.

  Если в разных селекторах корреляционного правила используются поля, которые имеют разные значения в событиях, эти поля не нужно указывать в разделе **Группирующие поля**.

- **Уникальные поля** – поля событий, которые должны быть отправлены в контейнер. Если задан этот параметр, в контейнер будут отправляться только уникальные поля. Хеш-код значений отобранных полей используется в качестве ключа контейнера.

  Вы можете использовать локальные переменные в разделах **Группирующие поля** и **Уникальные поля**. Для обращения к переменной необходимо перед ее именем указать символ "$".
  Для ознакомления с примерами использования локальных переменных в этих разделах используйте правило, поставляемое с KUMA: R403_Обращение на вредоносные ресурсы с устройства с выключенной защитой или устаревшей антивирусной базой.

- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. По умолчанию указано значение 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Время жизни контейнера, сек.** (обязательно) – время жизни контейнера в секундах. Значение по умолчанию – 86400 секунд (24 часа). Этот таймер запускается при создании контейнера (когда он получает первое событие). Время жизни не обновляется, и когда оно истекает, срабатывает триггер **По истечении времени жизни контейнера** из группы настроек **Действия**, а контейнер удаляется. Триггеры **На каждом срабатывании правила** и **На последующих срабатываниях правила** могут срабатывать более одного раза в течение времени жизни контейнера.

- **Политика хранения базовых событий** – этот раскрывающийся список используется, чтобы определить, какие базовые события должны быть сохранены в корреляционном событии:

  - **first** (значение по умолчанию) – поместить в корреляционное событие первое базовое событие из коллекции событий, инициировавшей создание корреляционного события.

  - **last** – поместить в корреляционное событие последнее базовое событие из коллекции событий, инициировавшей создание корреляционного события.

- **all** – поместить в корреляционное событие все базовые события из коллекции событий, инициировавшей создание корреляционного события.

- **Уровень важности** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию – **Низкий**.

- **Сортировать по** – в этом раскрывающемся списке можно выбрать поле события, по которому селекторы правила корреляции будут отслеживать изменение ситуации. Это может пригодиться, если, например, вы захотите настроить правило корреляции на срабатывание при последовательном возникновении нескольких типов событий.

- **Описание** – описание ресурса. До 4000 символов в кодировке Unicode.

Вкладка **Селекторы**

В правиле типа **standard** может быть несколько селекторов. Селекторы можно добавлять с помощью кнопки **Добавить селектор** и удалять с помощью кнопки **Удалить селектор**. Вы можете перемещать селекторы с помощью кнопки ⣿.

Для каждого селектора доступны две вкладки **Параметры** и **Локальные переменные**.

Вкладка **Параметры** содержит следующие параметры:

- **Название** (обязательно) – уникальное имя группы событий, удовлетворяющих условиям селектора. Имя должно содержать от 1 до 128 символов Юникода.

- **Порог срабатывания селектора (количество событий)** (обязательно) – количество событий, которое необходимо получить для срабатывания селектора. По умолчанию указано значение 1.

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

[Фильтрация по данным из поля события Extra]

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

Последовательность условий, заданных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.

Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.

Фильтр селектора 1:

Условие 1. DeviceProduct = Microsoft Windows

Условие 2. DeviceEventClassID = 4624

Фильтр селектора 2:

Условие 1. DeviceEventClassID = 4624

Условие 2. DeviceProduct = Microsoft Windows

Последовательность условий, заданная в Фильтре селектора 2, более предпочтительна, поскольку оказывает меньшую нагрузку на систему.

- **Обнуление** – этот флажок должен быть установлен, если правило корреляции НЕ должно срабатывать при получении селектором определенного количества событий. По умолчанию флажок снят.

Выбрав вкладку **Локальные переменные**, с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

В селекторе корреляционного правила могут быть использованы регулярные выражения, соответствующие стандарту RE2.

Применение регулярных выражений в правилах корреляции создает большую нагрузку в сравнении с другими операциями. Поэтому при разработке правил корреляции мы рекомендуем ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Для использования регулярного выражения необходимо применить оператор сравнения `match`. Регулярное выражение должно быть размещено в константе. Применение capture-групп в регулярных выражениях не обязательно. Для срабатывания корреляционного правила текст поля, сопоставляемый с regexp, должен полностью совпасть с регулярным выражением.

Для ознакомления с синтаксисом и примерами корреляционных правил, в селекторах которых есть регулярные выражения, используйте следующие правила, поставляемые с KUMA:

- R105_04_Подозрительные PowerShell-команды. Подозрение на обфускацию.
- R333_Подозрительное создание файлов в директории автозапуска.

Вкладка **Действия**

В правиле типа **standard** может быть несколько триггеров.

- **На первом срабатывании правила** – этот триггер срабатывает, когда контейнер регистрирует первое в течение срока своей жизни срабатывание селектора.
- **На последующих срабатываниях правила** – этот триггер срабатывает, когда контейнер регистрирует в течение срока своей жизни второе и последующие срабатывания селектора.
- **На каждом срабатывании правила** – этот триггер срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора.
- **По истечении времени жизни контейнера** – этот триггер срабатывает по истечении времени жизни контейнера и используется в связке с селектором с установленным флажком **Обнуление**. То есть триггер срабатывает, если в течение заданного времени ситуация, обнаруженная правилом корреляции, не разрешается.

Каждый триггер представлен в виде группы настроек со следующими доступными параметрами:

- **В дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на пост-обработку: на внешнее обогащение вне корреляционного правила, для реагирования и в точки назначения.
- **В коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться цепочкой правил текущего коррелятора. Это позволяет достичь иерархической корреляции.

  Если установлены флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции сначала отправляется на постобработку, а затем в селекторы текущего правила корреляции.
- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции. Если вы не хотите создавать алерт при срабатывании правила корреляции, но все же хотите отправить событие корреляции в хранилище, установите флажки **Выводить** и **Нет алертов**. Если вы установите только флажок **Нет алертов**, событие корреляции не сохраняется в хранилище.
- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения. Эти правила обогащения хранятся в правиле корреляции, в котором они были

созданы. Можно создать несколько правил обогащения. Вы можете добавлять или удалять правила обогащения с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.

- **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

  Доступные типы обогащения:

  - **константа**

    Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

    - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено.
    - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива.

  - **dictionary**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

    Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

    Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

    Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

    Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

    Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **table**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.
- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра Тип источника данных выбран тип "Событие", а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом "Массив строк", а целевым полем является поле с типом "Строка", значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем "Массив строк" и целевое поле полем "Массив строк", значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **Отладка** – с помощью этого переключателя можно включить логирование операций сервиса.
- **Описание** – описание ресурса. До 4000 символов в кодировке Unicode.

- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько. Вы можете добалять или удалять правила категоризации с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию активу.
    - **Удалить** – отвязать актив от категории.
  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.
  - **Идентификатор категории** – в раскрывающемся списке отображается дерево категорий и вы можете выбрать категорию, над которой будет совершена операция. Список раскрывается, если нажать на строку.
- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. Вы можете добавлять или удалять операции с активными листами с помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом**.

Доступные параметры:

- **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.
- **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
  - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
  - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
  - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
  - **Удалить** – удалить запись из активного листа.
- **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в Консоли KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.
  - Левое поле используется для указания поля активного листа.

    Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.
  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.
  - Группа параметров Обновление контекстных таблиц – используется для назначения триггера на одну или несколько операций с контекстными таблицами. С помощью кнопок Добавить действие с контекстной таблицей и Удалить действие с контекстной таблицей можно добавлять и удалять операции с контекстными таблицами.
  - Доступные параметры:
  - Название (обязательно) – этот раскрывающийся список используется для выбора ресурсов контекстной таблицы.
  - Операция (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить.
  - Сложить – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей типа число и число с плавающей точкой.

- Установить – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.

- Получить – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа.

- Объединить – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.

- Удалить – удалить запись из контекстной таблицы.

- Ключевые поля (обязательно) – это список полей события, используемых для создания записи контекстной таблицы. Этот список также используется в качестве ключа записи контекстной таблицы. В качестве значения ключевого поля можно указать поле события или локальную переменную, объявленную на вкладке Селекторы.

- Составной ключ записи контекстной таблицы зависит только от значения полей и не зависит от порядка их отображения в Консоли KUMA.

- Сопоставление (требуется для всех операций, кроме Удалить) – используется для сопоставления полей контекстной таблицы с полями событий или переменными. Можно установить более одного правила сопоставления. Одно поле контекстной таблицы можно указать несколько раз.

- Левое поле используется для указания поля контекстной таблицы.

- Поле не должно содержать название поля, которое уже используется в сопоставлении, табуляцию, специальные символы или только цифры. Максимальное количество символов – 128. Название не может начинаться с символа нижнего подчеркивания.

- Средний раскрывающийся список используется для выбора полей событий или локальной переменной.

- Правое поле можно использовать для назначения константы полю контекстной таблицы, если была выбрана операция Установить. Объединить или Сложить. Максимальное количество символов – 1024.

Вкладка **Корреляторы**

- **Добавить** – Используется при редактировании созданного корреляционного правила. С помощью кнопки **Добавить** вы можете выбрать коррелятор из списка в открывшемся окне **Корреляторы**. После того, как вы нажмете **ОК**, правило будет привязано к выбранному коррелятору. Вы можете выбрать одновременно несколько корреляторов. Правило будет добавлено последним в очередь для выполнения. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Коррелятор** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок **Вверх** или **Вниз** установите необходимый порядок выполнения правил.

- **Удалить** – Используется, чтобы отвязать корреляционное правило от коррелятора.

Правила корреляции типа simple

Правила корреляции типа **simple** используются для определения простых последовательностей событий.

Окно правила корреляции содержит следующие вкладки параметров:

- **Общие** – используется для указания основных параметров правила корреляции. На этой вкладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа правила.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа правил.
- **Корреляторы** - используется для привязки корреляторов. Доступна только для созданных правил корреляции, открытых на редактирование.

Вкладка **Общие**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **simple**, если хотите создать правило корреляции типа simple.
- **Наследуемые поля** (обязательно) – поля событий, по которым отбираются события. При срабатывания селектора (см. ниже) эти поля будут записаны в корреляционное событие.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. По умолчанию указано значение 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Уровень важности** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию – `Низкий`.
- **Описание** – описание ресурса. До 4000 символов в кодировке Unicode.

Вкладка **Селекторы**

В правиле типа **simple** может быть только один селектор, для которого доступны вкладки **Параметры** и **Локальные переменные**.

Вкладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

Последовательность условий, заданных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.

Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.

Фильтр селектора 1:

Условие 1. DeviceProduct = Microsoft Windows

Условие 2. DeviceEventClassID = 4624

Фильтр селектора 2:

Условие 1. DeviceEventClassID = 4624

Условие 2. DeviceProduct = Microsoft Windows

Последовательность условий, заданная в Фильтре селектора 2, более предпочтительна, поскольку оказывает меньшую нагрузку на систему.

Выбрав вкладку **Локальные переменные**, с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Вкладка **Действия**

В правиле типа **simple** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- **В дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на постобработку: на обогащение, для реагирования и в точки назначения.

- **В коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться цепочкой правил текущего коррелятора. Это позволяет достичь иерархической корреляции.

  Если установлены флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции сначала отправляется на постобработку, а затем в селекторы текущего правила корреляции.

- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции. Если вы не хотите создавать алерт при срабатывании правила корреляции, но все же хотите отправить событие корреляции в хранилище, установите флажки **Выводить** и **Нет алертов**. Если вы установите только флажок **Нет алертов**, событие корреляции не сохраняется в хранилище.

- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения. Эти правила обогащения хранятся в правиле корреляции, в котором они были созданы. Можно создать несколько правил обогащения. Вы можете добавлять или удалять правила обогащения с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.

  - **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

    Доступные типы обогащения:

    - **константа**

      Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

      - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов в кодировке Unicode. Если оставить это поле пустым, существующее значение поля события будет удалено.

      - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

      Если вы используете функции обогащения событий для полей расширенной схемы с типом "Строка", "Число" или "Число с плавающей точкой" с помощью константы, в поле будет добавлена константа.

      Если вы используете функции обогащения событий для полей расширенной схемы с типом "Массив строк", "Массив чисел" или "Массив чисел с плавающей точкой" с помощью константы, константа будет добавлена к элементам массива.

    - **dictionary**

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

Когда в раскрывающемся списке **Название словаря** выбран этот тип обогащения, вам нужно выбрать словарь, который предоставит значения. В блоке параметров **Ключевые поля** вам нужно нажать на кнопку **Добавить поле** и выбрать поля событий, значения которых будут использоваться для выбора записи словаря.

Если вы используете обогащение событий, у которого в качестве параметра Тип источника данных выбран тип "Словарь", а в параметре Ключевые поля обогащения указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку согласно правилам сериализации одного значения в формате TSV.

Пример: В параметре Ключевые поля обогащения используется поле расширенной схемы SA.StringArrayOne. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c". В качестве ключа в словарь будет передано значение: ['a','b','c'].

Если в параметре Ключевые поля обогащения используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом "|".

Пример: В параметре Ключевые поля обогащения используются два поля: поле расширенной схемы SA.StringArrayOne и поле Code. Поле расширенной схемы SA.StringArrayOne, содержит 3 элемента "a", "b" и "c", строковое поле Code, содержит последовательность символов "myCode". В качестве ключа в словарь будет передано значение: ['a','b','c']|myCode.

- **table**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  Когда этот тип обогащения выбран в раскрывающемся списке **Название словаря**, выберите словарь, который предоставит значения. В группе параметров **Ключевые поля** нажмите на кнопку **Добавить поле** и выберите поля событий, значения которых используются для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить, нажав на кнопку ✕.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.
- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, такая строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, такая строка будет обрезана до размера этого поля события.

Преобразования при использовании расширенной схемы событий

Возможность использования преобразования зависит от типа используемого поля расширенной схемы событий:

- для дополнительное поле с типом "Строка" доступны все типы преобразований.
- для полей с типами "Число", "Число с плавающей точкой" доступны следующие виды преобразований: regexp, substring, replace, trim, append, prepend, replaceWithRegexp, decodeHexString, decodeBase64String, decodeBase64URLString.
- для полей с типами "Массив строк", "Массив чисел" и "Массив чисел с плавающей точкой" доступны следующие виды преобразований: append, prepend.

При использовании обогащения событий, у которых в качестве параметра Тип источника данных выбран тип "Событие", а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходным полем было поле с типом "Массив строк", а целевым полем является поле с типом "Строка", значения будут размещены в целевом поле в формате TSV.

  Пример: в поле расширенной схемы событий SA.StringArray, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий DeviceCustomString1. В результате выполнения операции в поле DeviceCustomString1 будет находиться: ["string1", "string2", "string3"].

- Если исходное поле является полем "Массив строк" и целевое поле полем "Массив строк", значения исходного поля добавляются к значениям целевого поля и помещаются в целевое поле с запятыми (","), которые используются в качестве символа-разделителя.

  Пример: в поле расширенной схемы событий SA.StringArrayOne, находятся значения "string1", "string2", "string3". Выполняются операция обогащения событий. Результат выполнения операции был занесен в поле схемы событий SA.StringArrayTwo. В результате выполнения операции в поле SA.StringArrayTwo будут находиться значения "string1", "string2", "string3".

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Чтобы преобразовать данные в поле массива в шаблоне в формат TSV, вам нужно использовать функцию toString.

Если вы используете обогащения событий, у которого в качестве параметра Тип источника данных выбран тип "Шаблон", в котором целевым полем является поле с типом Строка, а исходным полем является поле расширенной схемы событий, содержащее массив строк, в шаблоне может быть использован один из примеров, приведенных далее.

Пример:

{{.SA.StringArrayOne}}

Пример:

{{- range $index, $element := . SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **Отладка** – с помощью этого переключателя можно включить логирование операций сервиса.
- **Описание** – описание ресурса. До 4000 символов в кодировке Unicode.
- Блок параметров **Фильтр** – позволяет выбрать, какие события будут отправляться на обогащение. Настройка происходит, как описано выше.

- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько. Вы можете добалять или удалять правила категоризации с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию активу.
    - **Удалить** – отвязать актив от категории.
  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.
  - **Идентификатор категории** – в раскрывающемся списке отображается дерево категорий и вы можете выбрать категорию, над которой будет совершена операция. Список раскрывается, если нажать на строку.

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. Вы можете добавлять или удалять операции с активными листами с помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом**.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
    - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
    - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
    - **Удалить** – удалить запись из активного листа.
  - **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

    > Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в Консоли KUMA.

  - **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.
    - Левое поле используется для указания поля активного листа.

      > Поле не должно содержать специальные символы или только цифры.

    - Средний раскрывающийся список используется для выбора полей событий.
    - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров Обновление контекстных таблиц – используется для назначения триггера на одну или несколько операций с контекстными таблицами. С помощью кнопок Добавить действие с контекстной таблицей и Удалить действие с контекстной таблицей можно добавлять и удалять операции с контекстными таблицами.

- Доступные параметры:

- Название (обязательно) – этот раскрывающийся список используется для выбора ресурсов контекстной таблицы.

- Операция (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить.

- Сложить – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей типа число и число с плавающей точкой.

- Установить – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.

- Получить – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа.

- Объединить – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.

- Удалить – удалить запись из контекстной таблицы.

- Ключевые поля (обязательно) – это список полей события, используемых для создания записи контекстной таблицы. Этот список также используется в качестве ключа записи контекстной таблицы. В качестве значения ключевого поля можно указать поле события или локальную переменную, объявленную на вкладке Селекторы.

- Составной ключ записи контекстной таблицы зависит только от значения полей и не зависит от порядка их отображения в Консоли KUMA.

- Сопоставление (требуется для всех операций, кроме Удалить) – используется для сопоставления полей контекстной таблицы с полями событий или переменными. Можно установить более одного правила сопоставления. Одно поле контекстной таблицы можно указать несколько раз.

- Левое поле используется для указания поля контекстной таблицы.

- Поле не должно содержать название поля, которое уже используется в сопоставлении, табуляцию, специальные символы или только цифры. Максимальное количество символов – 128. Название не может начинаться с символа нижнего подчеркивания.

- Средний раскрывающийся список используется для выбора полей событий или локальной переменной.

- Правое поле можно использовать для назначения константы полю контекстной таблицы, если была выбрана операция Установить. Объединить или Сложить. Максимальное количество символов – 1024.

Вкладка Коррелляторы

- **Добавить** – Используется при редактировании созданного корреляционного правила. С помощью кнопки **Добавить** вы можете выбрать коррелятор из списка в открывшемся окне **Коррелляторы**. После того, как вы нажмете **OK**, правило будет привязано к выбранному коррелятору. Вы можете выбрать одновременно несколько корреляторов. Правило будет добавлено последним в очередь для выполнения. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Коррелятор** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок Вверх или Вниз установите необходимый порядок выполнения правил.

- **Удалить** – Используется, чтобы отвязать корреляционное правило от коррелятора.

Правила корреляции типа operational

Правила корреляции типа **operational** используются для работы с активными листами.

Окно правила корреляции содержит следующие вкладки:

- **Общие** – используется для указания основных параметров правила корреляции. На этой вкладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа правил.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа правил.
- **Корреляторы** - используется для привязки корреляторов. Доступна только для созданных правил корреляции, открытых на редактирование.

Вкладка **Общие**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **operational**, если хотите создать правило корреляции типа operational.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. По умолчанию указано значение 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Описание** – описание ресурса. До 4000 символов в кодировке Unicode.

Вкладка **Селекторы**

В правиле типа **operational** может быть только один селектор, для которого доступны вкладки **Параметры** и **Локальные переменные**.

Вкладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.
  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    Значение этого типа указывается вручную.

    Чтобы работать со значением из поля Extra на глубине 3 и ниже, следует использовать кавычки ``. Например, `Extra.lev1.lev2.lev3`.
- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

На вкладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Вкладка **Действия**

В правиле типа **operational** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. Вы можете добавлять или удалять операции с активными листами с помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом**.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:

- **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
- **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
- **Удалить** – удалить запись из активного листа.

- **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в Консоли KUMA.

- **Сопоставление** (требуется для операции **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.
  - Левое поле используется для указания поля активного листа.

    Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.
  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров **Обновление контекстных таблиц** – используется для назначения триггера на одну или несколько операций с контекстными таблицами. С помощью кнопок **Добавить действие с контекстной таблицей** и **Удалить действие с контекстной таблицей** можно добавлять и удалять операции с контекстными таблицами.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов контекстной таблицы.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить.
    - **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей типа число и число с плавающей точкой.
    - **Установить** – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.
    - **Объединить** – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.
    - **Удалить** – удалить запись из контекстной таблицы.

  - **Ключевые поля** (обязательно) – это список полей события, используемых для создания записи контекстной таблицы. Этот список также используется в качестве ключа записи контекстной таблицы.

В качестве значения ключевого поля можно указать поле события или локальную переменную, объявленную на вкладке **Селекторы**.

Составной ключ записи контекстной таблицы зависит только от значения полей и не зависит от порядка их отображения в Консоли KUMA.

- **Сопоставление** (требуется для всех операций, кроме **Удалить**) – используется для сопоставления полей контекстной таблицы с полями событий или переменными. Можно установить более одного правила сопоставления. Одно поле контекстной таблицы можно указать несколько раз.

  - Левое поле используется для указания поля контекстной таблицы.

    Поле не должно содержать название поля, которое уже используется в сопоставлении, табуляцию, специальные символы или только цифры. Максимальное количество символов – 128. Название не может начинаться с символа нижнего подчеркивания.

  - Средний раскрывающийся список используется для выбора полей событий или локальной переменной.

  - Правое поле можно использовать для назначения константы полю контекстной таблицы. Максимальное количество символов – 1024.

Вкладка Корреляторы

- **Добавить** – Используется при редактировании созданного корреляционного правила. С помощью кнопки **Добавить** вы можете выбрать коррелятор из списка в открывшемся окне **Корреляторы**. После того, как вы нажмете **OK**, правило будет привязано к выбранному коррелятору. Вы можете выбрать одновременно несколько корреляторов. Правило будет добавлено последним в очередь для выполнения. Если вы хотите переместить правило в очереди выполнения, перейдите в **Ресурсы** → **Коррелятор** → <выбранный коррелятор> → **Редактирование коррелятора** → **Корреляция**, установите флажок рядом с нужным правилом и с помощью кнопок Вверх или Вниз установите необходимый порядок выполнения правил.

- **Удалить** – Используется, чтобы отвязать корреляционное правило от коррелятора.

Переменные в корреляторах

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными *переменными*. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменные можно объявить в корреляторе (*глобальные переменные*) или в правиле корреляции (*локальные переменные*), присвоив им какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Область применения переменных:

- При поиске группирующих или уникальных значений полей в правилах корреляции.

- В селекторах правил корреляции в фильтрах условий, при которых должно срабатывать правило корреляции.

- При обогащении корреляционных событий. В качестве типа источника следует выбирать **Событие**.

- При наполнении активных листов значениями.

К переменным можно обращаться так же, как к полям события, предваряя их название символом $.

Локальные переменные в группирующих и уникальных полях

Вы можете использовать локальные переменных в разделах **Группирующие поля** и **Уникальные поля** правил корреляции типа standard. Для использования локальной переменной необходимо перед ее именем указывать символ "$".

Вы можете ознакомиться с примером использования локальных переменных в разделах **Группирующие поля** и **Уникальные поля** в правиле, поставляемом в KUMA: R403_Обращение на вредоносные ресурсы с устройства с отключенной защитой или устаревшей антивирусной базой.

Локальные переменные в селекторе

Чтобы использовать локальную переменную в селекторе:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Селекторы**, выберите существующий фильтр или создайте новый и нажмите на кнопку **Добавить условие.**
4. В качестве операнда выберите **поле события**.
5. В качестве значения поля события укажите локальную переменную и укажите символ "$" перед именем переменной.
6. Укажите остальные параметры фильтра.
7. Нажмите на кнопку **Сохранить**.

Вы можете ознакомиться с примером использования локальных переменных в правиле, поставляемом с KUMA: R403_Обращение на вредоносные ресурсы с устройства с отключенной защитой или устаревшей антивирусной базой.

Локальные переменные в обогащении событий

Вы можете использовать правила корреляции типа standard и simple для обогащения событий с помощью локальных переменных.

Обогащение текстом и числами

Обогащение событий можно выполнять с помощью текста (строк). Для этого могут быть использованы функции, позволяющие модифицировать строки: to_lower, to_upper, str_join, append, prepend, substring, tr, replace, str_join.

Обогащение событий можно выполнять с помощью чисел. Для этого могут быть использованы функции: сложение (оператор "+"), вычитание (оператор "-"), умножение (оператор "*"), деление (оператор "/"), round, ceil, floor, abs, pow.

Также для работы с данными в локальных переменных могут быть использованы регулярные выражения.

Применение регулярных выражений в правилах корреляции создает большую нагрузку в сравнении с другими операциями. Поэтому при разработке правил корреляции мы рекомендуем ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Обогащение временных отметок

Обогащение событий можно выполнять с помощью временных отметок (даты и времени). Для этого могут быть использованы функции, позволяющие получать или модифицировать временные метки: now, extract_from_timestamp, parse_timestamp, format_timestamp, truncate_timestamp, time_diff.

Операции с активными списками и таблицами

Вы можете выполнять обогащение событий с помощью локальных переменных и данных, находящихся в активных списках и таблицах.

Для обогащения событий данными из активного списка необходимо воспользоваться функциями active_list, active_list_dyn.

Для обогащения событий данными из таблицы необходимо воспользоваться функциями table_dict, dict.

Вы можете создавать условные операторы при помощи функции conditional в локальных переменных. Таким образом переменная может вернуть одно из значений в зависимости от того, какие данные поступили для обработки.

Использование локальной переменной для обогащения событий

Чтобы использовать локальную переменную для обогащения событий:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Действия** и в группе параметров **Обогащение** в раскрывающемся списке **Тип источника данных** выберите **событие**.
4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое необходимо передать значение локальной переменной.
5. В раскрывающемся списке **Исходное поле** выберите локальную переменную. Перед именем локальной переменной укажите символ "$".
6. Укажите остальные параметры правила.
7. Нажмите на кнопку **Сохранить**.

Локальные переменные в обогащении активных листов

Вы можете использовать локальные переменные для обогащения активных листов.

Чтобы выполнить обогащение активного списка при помощи локальной переменной:

1. Добавьте локальную переменную в правило.

2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".

3. В окне **Правила корреляции** перейдите на вкладку **Действия** и в группе параметров **Обновление активных листов** добавьте локальную переменную в поле **Ключевые поля**. Перед именем локальной переменной укажите символ "$".

4. В группе параметров **Сопоставление** укажите соответствие между полями события и полями активного списка.

5. Нажмите на кнопку **Сохранить**.

Свойства переменных

Локальные и глобальные переменные

Свойства глобальных и локальных переменных различаются.

Глобальные переменные:

- Глобальные переменные объявляются на уровне коррелятора и действуют только в пределах этого коррелятора.
- К глобальным переменным коррелятора можно обращаться из всех правил корреляции, которые в нем указаны.
- В правилах корреляции типа standard одна и та же глобальная переменная в каждом селекторе может принимать разные значения.
- Невозможно переносить глобальные переменные между разными корреляторами.

Локальные переменные:

- Локальные переменные объявляются на уровне правила корреляции и действуют только в пределах этого правила.
- В правилах корреляции типа standard областью действия локальной переменной является только тот селектор, в котором переменная была объявлена.
- Локальные переменные можно объявлять в любых типах правил корреляции.
- Невозможно переносить локальные переменные между правилами или селекторами.
- Локальная переменная не может быть использована в качестве глобальной переменной.

Переменные в разных типах правил корреляции

- В правилах корреляции типа **operational** на вкладке **Действия** можно указывать все доступные или объявленные в этом правиле переменные.
- В правилах корреляции типа **standard** на вкладке **Действия** можно указывать только переменные, указанные в этих правилах на вкладке **Общие** в поле **Группирующие поля**.

- В правилах корреляции типа **simple** на вкладке **Действия** можно указывать только переменные, указанные в этих правилах на вкладке **Общие** в поле **Наследуемые поля**.

Требования к переменным

Добавляя функцию переменной необходимо сначала указать название функции, а затем в круглых скобках перечислить ее параметры. Основные математические операции (сложение, вычитание, умножение, деление) являются исключением для этого требования. Когда используются эти операции, скобки используются для обозначения значимости операций.

Требования к названиям функций:

- Должно быть уникально в рамках коррелятора.
- Имя должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

Особенности указания функций переменных:

- Последовательность указания параметров имеет значение.
- Параметры передаются через запятую: `,`.
- Строковые параметры передаются в одинарных кавычках: `'`.
- Наименования полей событий и переменные указываются без кавычек.
- При обращении к переменной как параметру перед ее названием необходимо добавлять символ `$`.
- Ставить пробел между параметрами необязательно.
- Во всех функциях, где в качестве параметров допускается использование переменной, допускается создавать вложенные функции.

Функции переменных

Операции с активными листами и словарями

Функции "active_list" и "active_list_dyn"

Функции позволяют получать информацию из активного листа и динамически формировать имя поля активного листа и ключа.

Необходимо указать параметры в следующей последовательности:

1. Название активного листа.
2. Выражение, возвращающее название поля активного листа.
3. Одно или несколько выражений, из результатов которых будет составлен ключ.

Пример использования	Результат выполнения
`active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2),`	Получение значения поля

`to_lower(DeviceCustomString1))`	активного листа.

С помощью этих функций из переменной можно обратиться к активному листу общего тенанта. Для этого после названия активного листа необходимо добавить суффикс @Shared (регистр имеет значение). Например, active_list('exampleActiveList@Shared', 'score', SourceAddress,SourceUserName).

Функция "table_dict"

Получение информации о значении в указанном столбце словаря типа таблица.

Необходимо указать параметры в следующей последовательности:

1. Название словаря.
2. Название столбца словаря.
3. Одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример использования	Результат выполнения
`table_dict('exampleTableDict', 'office', SourceUserName)`	Получение данных из словаря `exampleTableDict` из строки с ключом `SourceUserName` из столбца `office`.
`table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))`	Получение данных из словаря `exampleTableDict` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре из столбца `office`.

С помощью этой функции из переменной можно обратиться к словарю общего тенанта. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `table_dict('exampleTableDict@Shared', 'office', SourceUserName)`.

Функция "dict"

Получение информации о значении в указанном столбце словаря типа словарь.

Необходимо указать параметры в следующей последовательности:

1. Название словаря.
2. Одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример использования	Результат выполнения
`dict('exampleDictionary', SourceAddress)`	Получение данных из словаря `exampleDictionary` из строки с ключом `SourceAddress`.
`dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))`	Получение данных из словаря `exampleDictionary` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре.

С помощью этой функции из переменной можно обратиться к словарю общего тенанта. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `dict('exampleDictionary@Shared', SourceAddress)`.

Операции с контекстными таблицами

Функция "context_table"

Возвращает значение указанного поля в базовом типе (например, целое число,массив целых чисел).

Необходимо указать параметры в следующей последовательности:

1. Название контекстной таблицы. Название не должно быть пустым.
2. Выражение, возвращающее название поля контекстной таблицы.
3. Выражение, возвращающее название ключевого поля 1 контекстной таблицы.
4. Выражение, возвращающее значение ключевого поля 1 контекстной таблицы.

Функция должна содержать минимум 4 параметра.

Пример использования	Результат выполнения
`context_table('tbl1', 'list_field1', 'key1', 'key1_val')`	`Получение значения указанного поля. В случае отсутствия контекстной таблицы или поля контекстной таблицы будет получена пустая строка.`

Функция "len"

Возвращает длину строки и массива.

Функция возвращает длину массива, если переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает длину полученной строки.

Примеры использования
`len(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`len(DeviceCustomString1)`

Функция "distinct_items"

Возвращает список уникальных элементов массива.

Функция возвращает список уникальных элементов массива, если переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;

- массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает строку, состоящую из уникальных символов исходной строки.

Примеры использования
`distinct_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`distinct_items(DeviceCustomString1)`

Функция "sort_items"

Возвращает отсортированный список элементов массива.

Необходимо указать параметры в следующей последовательности:

1. Выражение, возвращающее объект сортировки.
2. Сортировка возможных значений: `asc`, `desc`. Если параметр не указан, значение по умолчанию – `asc`.

Функция возвращает отсортированный список элементов массива, если переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк.

Функция возвращает список элементов массива в исходном порядке, если был передан массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает строку отсортированных символов.

Примеры использования
`sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')`
`sort_items(DeviceCustomString1)`

Функция "item"

Возвращает элемент массива с указанным индексом или символ строки с указанным индексом, если передан массив целых чисел, чисел с плавающей точкой, строк или булевых значений.

Необходимо указать параметры в следующей последовательности:

1. Выражение, возвращающее объект индексирования.
2. Выражение, возвращающее индекс элемента или символа.

Функция должна содержать минимум 2 параметра.

Функция возвращает элемент массива с указанным индексом или символ строки с указанным индексом,если индекс находится в диапазоне массива и переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа и индекс находится в диапазоне массива, данные приводятся к строковому типу и функция возвращает символ строки по индексу. Если передан массив другого типа и индекс не находится в диапазоне массива, функция возвращает пустую строку.

Примеры использования
`item(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 1)`
`item(DeviceCustomString1, 0)`

Операции со строками

Функция "len"

Возвращает число символов в строке. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Строку можно передать строкой, названием поля или переменной.

Примеры использования
`len('SomeText')`
`len(Message)`
`len($otherVariable)`

Функция "to_lower"

Перевод символов в строке в нижний регистр. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Строку можно передать строкой, названием поля или переменной.

Примеры использования
`to_lower(SourceUserName)`
`to_lower('SomeText')`
`to_lower($otherVariable)`

Функция "to_upper"

Перевод символов в строке в верхний регистр. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка". Строку можно передать строкой, названием поля или переменной.

Примеры использования
`to_upper(SourceUserName)`
`to_upper('SomeText')`
`to_upper($otherVariable)`

Функция "append"

Добавление символов в конец строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`append(Message, '123')`	Строка из поля `Message`, в конце которой добавлена строка `123`.
`append($otherVariable, 'text')`	Строка из переменной `otherVariable`, в конце которой добавлена строка `text`.
`append(Message, $otherVariable)`	Строка из поля `Message`, в конце которой добавлена строка из переменной `otherVariable`.

Функция "prepend"

Добавление символов в начало строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`prepend(Message, '123')`	Строка из поля `Message`, в начало которой добавлена строка `123`.
`prepend($otherVariable, 'text')`	Строка из переменной `otherVariable`, в начало которой добавлена строка `text`.
`prepend(Message, $otherVariable)`	Строка из поля `Message`, в начало которой добавлена строка из переменной `otherVariable`.

Функция "substring"

Возвращает подстроку из строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Позиция начала подстроки (натуральное число или 0).
3. Позиция конца подстроки (необязательно).

Строки можно передать строкой, названием поля или переменной. Если номер позиции больше, чем длина строки исходных данных, возвращается пустая строка.

Примеры использования	Результат использования
`substring(Message, 2)`	Возвращает часть строки из поля `Message`: от 3 символа до конца.
`substring($otherVariable, 2, 5)`	Возвращает часть строки из переменной `otherVariable`: от 3 до 6 символа.
`substring(Message, 0, len(Message) - 1)`	Возвращает всю строку из поля `Message`, кроме последнего символа.

Функция "tr"

Убирает из начала и конца строки указанные символы. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка, которую следует удалить из начала и конца исходной строки (необязательно).

Строки можно передать строкой, названием поля или переменной. Если строку на удаление не указать, в начале и в конце исходной строки будут удалены пробелы.

Примеры использования	Результат использования
`tr(Message)`	В начале и в конце строки из поля `Message` удалены пробелы.
`tr($otherVariable, '_')`	Если переменной `otherVariable` соответствует значение `_test_`, будет возвращена строка `test`.
`tr(Message, '@example.com')`	Если в поле события `Message` находится строка `user@example.com`, будет возвращена строка `user`.

Функция "replace"

Заменяет все вхождения последовательности символов A в строке на последовательность символов B. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка поиска: последовательность символов, подлежащая замене.
3. Строка замены: последовательность символов, на которую необходимо заменить строку поиска.

Строки можно передать выражением.

Примеры использования	Результат использования
`replace(Name, 'UserA', 'UserB')`	Возвращается строка из поля события `Name`, в которой все вхождения `UserA` заменены на `UserB`.
`replace($otherVariable, ' text ', '_text_')`	Возвращается строка из переменной `otherVariable`, в которой все вхождения `' text '` заменены на `'_text_'`.

Функция "regexp_replace"

Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка поиска: регулярное выражение.
3. Строка замены: последовательность символов, на которую необходимо заменить строку поиска, и идентификаторы групп захвата регулярного выражения. Строку можно передать выражением.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` необходимо указывать выражение `^example\\\\`.

Примеры использования	Результат использования
`regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')`	Возвращается строка из поля события `SourceAddress`, в которой перед IP-адресами вставлен текст `newIP`. Также последние цифры адреса заменены на `10`.

Функция "regexp_capture"

Получение из исходной строки результата, удовлетворяющего условию регулярного выражения. Поддерживается для стандартных полей и полей расширенной схемы событий типа "строка".

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка поиска: регулярное выражение.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` необходимо указывать выражение `^example\\\\`.

Примеры использования	Примеры значений	Результат использования
`regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})')`	`Message = 'Access from 192.168.1.1 session 1'` `Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'`	`'192.168.1.1'` `'45.45.45.45'`

Операции с метками времени

Функция now

Получение временной метки в формате epoch. Запускается без аргументов.

Примеры использования
`now()`

Функция "extract_from_timestamp"

Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных с временем в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение атомарного представления времени. Параметр регистрозависимый.

   Возможные варианты обозначения атомарного времени:

   - y – год в виде числа.
   - M – месяц, числовое обозначение.
   - d – число месяца.
   - wd – день недели: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
   - h – часы в 24-часовом формате.
   - m – минуты.
   - s – секунды.
3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Примеры использования
`extract_from_timestamp(Timestamp, 'wd')`

`extract_from_timestamp(Timestamp, 'h')`
`extract_from_timestamp($otherVariable, 'h')`
`extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')`

Функция "parse_timestamp"

Представление времени из формата RFC3339 (например, "2022-05-24 00:00:00", "2022-05-24 00:00:00+0300) в формат epoch.

Примеры использования
`parse_timestamp(Message)`
`parse_timestamp($otherVariable)`

Функция "format_timestamp"

Представление времени из формата epoch в формат RFC3339.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение формата времени: RFC3339.
3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Примеры использования
`format_timestamp(Timestamp, 'RFC3339')`
`format_timestamp($otherVariable, 'RFC3339')`
`format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')`

Функция "truncate_timestamp"

Округление времени в формате epoch. После округления время возвращается в формате epoch. Время округляется в меньшую сторону.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Параметр округления:
   - 1s – округление до секунд;
   - 1m – округление до минут;
   - 1h – округление до часов;
   - 24h – округление до суток.

3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Примеры использования	Примеры округляемых значений	Результат использования
`truncate_timestamp(Timestamp, '1m')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654631760000 (7 June 2022 г., 19:56:00)
`truncate_timestamp($otherVariable, '1h')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654628400000 (7 June 2022 г., 19:00:00)
`truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654560000000 (7 June 2022 г., 0:00:00)

Функция "time_diff"

Получение интервала времени между двумя метками времени в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Время конца отрезка. Поле события, имеющего тип timestamp, или переменная.
2. Время начала отрезка. Поле события, имеющего тип timestamp, или переменная.
3. Представление временного интервала:
   - ms – в миллисекундах;
   - s – в секундах;
   - m – в минутах;
   - h – в часах;
   - d – в днях.

Примеры использования
`time_diff(EndTime, StartTime, 's')`
`time_diff($otherVariable, Timestamp, 'h')`
`time_diff(Timestamp, DeviceReceiptTime, 'd')`

Математические операции

Представлены как простейшими математическими операциями, так и функциями.

Простейшие математические операции

Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Операции:

- сложение;
- вычитание;

- умножение;
- деление;
- деление по модулю.

Использование круглых скобок определяет последовательность действий

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- вещественные числа.

  При делении по модулю в качестве аргументов можно использовать только натуральные числа.

Ограничения использования:

- деление на ноль возвращает ноль;
- математические операции между числами и строками возвращают ноль;
- целые числа, полученные в результате операций, возвращаются без точки.

Примеры использования (Type=3; otherVariable=2; Message=text)	Результат использования
`Type + 1`	4
`$otherVariable - Type`	-1
`2 * 2.5`	5
`2 / 0`	0
`Type * Message`	0
`(Type + 2) * 2`	10
`Type % $otherVariable`	1

Функция "round"

Округление чисел. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)	Результат использования
`round(DeviceCustomFloatingPoint1)`	8
`round(DeviceCustomFloatingPoint2)`	8
`round($otherVariable)`	7

Функция "ceil"

Округление чисел в большую сторону. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	Результат использования
ceil(DeviceCustomFloatingPoint1)	8
ceil($otherVariable)	9

Функция "floor"

Округление чисел в меньшую сторону. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	Результат использования
floor(DeviceCustomFloatingPoint1)	7
floor($otherVariable)	8

Функция "abs"

Получение числа по модулю. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomNumber1=-7; otherVariable=-2)	Результат использования
abs(DeviceCustomFloatingPoint1)	7
abs($otherVariable)	2

Функция "pow"

Возведение числа в степень. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Параметры необходимо указать в следующей последовательности:

1. База – вещественные числа.
2. Степень – натуральные числа.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования
`pow(DeviceCustomNumber1, DeviceCustomNumber2)`
`pow($otherVariable, DeviceCustomNumber1)`

Функция "str_join"

Позволяет объединить несколько строк в одну с использованием разделителя. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Параметры необходимо указать в следующей последовательности:

1. Разделитель. Строка.
2. Строка1, строка2, строкаN. Минимум 2 выражения.

Примеры использования	Результат использования
`str_join('|', to_lower(Name), to_upper(Name), Name)`	Строка.

Функция "conditional"

Позволяет получить одно значения в случае выполнения условия и другое значение, если условие не выполнится. Поддерживаются для полей расширенной схемы событий с типом "целое число" и "число с плавающей точкой".

Параметры необходимо указать в следующей последовательности:

1. Условие. Строка. Синтаксис аналогичен условиям в SQL Where. В условии можно использовать функции переменных KUMA и ссылаться на другие переменные.
2. Значение при выполнении условия. Выражение.
3. Значение при невыполнении условия. Выражение.

Поддерживаемые операторы:

- AND
- OR
- NOT
- =
- !=
- <
- <=
- >
- >=
- LIKE (передается регулярное выражение RE2, а не SQL-выражение)
- ILIKE (передается регулярное выражение RE2, а не SQL-выражение)
- BETWEEN
- IN
- IS NULL (проверка на пустое значение, например 0 или пустую строку)

Примеры использования (значение зависит от аргументов 2 и 3)
`conditional('SourceUserName = \\'root\\' AND DestinationUserName = SourceUserName', 'match', 'no match')`
`conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no match')`
`conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no match')`

Операции для полей расширенной схемы событий

Для полей расширенной схемы событий типа "строка" поддерживаются следующие виды операций:

- Функция "len"
- Функция "to_lower"
- Функция "to_upper"
- Функция "append"
- Функция "prepend"
- Функция "substring"
- Функция "tr"
- Функция "replace"
- Функция "regexp_replace"

- Функция "regexp_capture"

Для полей расширенной схемы событий с типом "целое число" или "число с плавающей точкой" поддерживаются следующие виды математических операций:

- Простые математические операции:
- Функция "round"
- Функция "ceil"
- Функция "floor"
- Функция "abs"
- Функция "pow"
- Функция "str_join"
- Функция "conditional"

Для полей расширенной схемы событий с типом "массив чисел", "массив чисел с плавающей точкой" и "массив строк" поддерживаются следующие виды математических операций:

- item(SA.someStringArray, i) - получение i-го элемента из поля someStringArray[i].
- SA.someStringArray , returns ["string1", "string2", "string1"] - получение массива значений из поля someStringArray.
- len(SA.someStringArray) – функция позволяет получить количество элементов в массиве someStringArray.
- distinct_items(SA.someStringArray), returns ["string1", "string2"] - функция позволяет получить уникальные записей из массиве someStringArray.
- to_string(SA.someStringArray) - функция формирует строку массива в формате TSV.
- sort_items(<type>.someStringArray); вместо <type> -- необходимо указать тип массива: sa для массива строка, fa для массива чисел с плавающей точкой, na для массива целых чисел. Пример: sort_items (SA.StringArray, DESC).

Для полей с типом "массив целых чисел" и "массив чисел с плавающей точкой" поддерживаются следующие функции:

- math_min – возвращает минимальный элемент массива. Пример: math_min(NA.NumberArray), math_min(FA.FloatArray).
- math_max – возвращает максимальный элемент массива. Пример: math_max(NA.NumberArray), math_max(FA.FloatArray).
- math_avg – возвращает среднее значение массива. Пример: math_avg(NA.NumberArray), math_avg(FA.FloatArray).

Объявление переменных

Для объявления переменных их необходимо добавить в коррелятор или правило корреляции.

Чтобы добавить глобальную переменную в существующий коррелятор:

1. В Консоли KUMA в разделе **Ресурсы** → **Коррелляторы** выберите набор ресурсов нужного коррелятора.

   Откроется мастер установки коррелятора.

2. Выберите шаг мастера установки **Глобальные переменные**.

3. Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.
     - Имя должно содержать от 1 до 128 символов Юникода.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     Описание функций переменных.

   Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

4. Выберите шаг мастера установки **Проверка параметров** и нажмите **Сохранить**.

Глобальная переменная добавлена в коррелятор. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Чтобы добавить локальную переменную в существующее правило корреляции:

1. В Консоли KUMA в разделе **Ресурсы** → **Правила корреляции** выберите нужное правило корреляции.

   Откроется окно параметров правила корреляции. Параметры правила корреляции можно также открыть из коррелятора, в которое оно было добавлено, перейдя на шаг мастера установки **Корреляция**.

2. Откройте вкладку **Селекторы**.

3. В селекторе откройте вкладку **Локальные переменные**, нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.
     - Имя должно содержать от 1 до 128 символов Юникода.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

- В окне **Значение** введите функцию переменной.

  Описание функций переменных.

Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

Для правил корреляции типа standard повторите этот шаг для каждого селектора, в которым вы хотите объявить переменные.

4. Нажмите на кнопку **Сохранить**.

Локальная переменная добавлена в правило корреляции. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Добавленные переменные можно изменить или удалить. Если правило корреляции обращается к необъявленной переменной (например, если ее название было изменено), в качестве результата возвращается пустая строка.

Если вы измените название переменной, вам потребуется вручную изменить название этой переменной во всех правилах корреляции, где вы ее использовали.

Предустановленные правила корреляции

В поставку OSMP включены перечисленные в таблице ниже правила корреляции.

Предустановленные правила корреляции

Название правила корреляции	Описание
[OOTB] KATA alert	Используется для обогащения событий KATA.
[OOTB] Successful Bruteforce	Срабатывает после выявления успешной попытки аутентификации после множества неуспешных попыток аутентификации. Правило работает на основе событий демона sshd.
[OOTB][AD] Account created and deleted within a short period	Выявляет факты создания и последующего удаления учетных записей на устройствах на базе ОС Microsoft Windows.
[OOTB][AD] An account failed to log on from different hosts	Выявляет множественные неуспешные попытки аутентификации на различных устройствах.
[OOTB][AD] Granted TGS without TGT (Golden Ticket)	Выявляет подозрения на атаку типа "Golden Ticket". Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD][Technical] 4768. TGT Requested	Техническое правило, используется для формирования активного списка – [OOTB][AD] List of requested TGT. EventID 4768. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] Membership of sensitive group was modified	Работает на базе событий ОС Microsoft Windows.
[OOTB][AD] Multiple accounts failed to log on from the same host	Срабатывает после выявления множественных неуспешных попыток аутентификации на одном устройстве от имени разных учетных записей.
[OOTB][AD] Possible Kerberoasting attack	Выявляет подозрения на атаки типа "Kerberoasting". Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] Successful authentication with the same account on multiple hosts	Выявляет подключения на разных устройствах под одной учетной записью. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] The account added and deleted from the group in a short period	Выявляет добавление и последующее удаление пользователя из группы. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][Net] Possible port scan	Выявляет подозрения на сканирование порта. Правило работает на основе событий Netflow, Ipfix.

Фильтры

Фильтры позволяют выбрать события на основе заданных вами условий.

В сервисе коллектора фильтры используются для того, чтобы выбрать события, которые вы хотите передавать в KUMA. То есть если событие удовлетворяет условию фильтра, событие будет передано в KUMA для дальнейшей обработки.

Фильтры можно использовать в следующих сервисах и функциях KUMA:

- Коллектор.
- Коррелятор.
- Хранилище.
- Агенты KUMA.
- Правила корреляции.
- Правила обогащения.
- Правила агрегации.
- Точки назначения.
- Правила реагирования.
- Правила сегментации.

Можно использовать отдельные фильтры или встроенные фильтры, которые хранятся в сервисе или ресурсе, где они были созданы.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Доступные параметры фильтра:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода. Встроенные фильтры создаются в других ресурсах или сервисах и не имеют имен.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Описание – вы можете добавить до 4000 символов в кодировке Unicode, описывающих фильтр.
- Блок параметров **Условия** – здесь вы можете сформулировать критерии фильтрации, создав условия фильтрации и группы фильтров, а также добавив существующие фильтры.

  Для формирования критериев фильтрации вы можете использовать *режим конструктора* или *режим исходного кода*. По умолчанию используется режим конструктора.

  В режиме конструктора вы можете создавать или изменять критерии фильтрации с помощью раскрывающихся списков с вариантами условий фильтра и операторов.

  В режиме исходного кода вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

Вы можете переключаться между режимами при формировании критериев фильтрации. Чтобы переключиться в режим исходного кода, нажмите на кнопку **Код**. При переключении между режимами созданные фильтры условий сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, перейдите на вкладку **Конструктор** и вернитесь снова на вкладку **Код**. Отобразится код фильтра.

Формирование условий в режиме конструктора

Вы можете формировать критерии фильтрации в режиме конструктора с помощью следующих кнопки:

- **Добавить условие** – добавление строки с полями для определения условия.
- **Добавить группу –** добавление группы фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить группы, условия и существующие фильтры. Условия, помещенные в подгруппу **НЕ**, объединяются оператором **И**.

Для замены в сформированном условии оператора вам необходимо нажать на оператор, который вы хотите заменить, и в раскрывающемся списке выбрать новый оператор.

Для удаления в сформированном условии оператора необходимо нажать на оператор, который вы хотите удалить, и нажать на клавишу **Backspace**.

Для изменения последовательности условий фильтра вам необходимо нажать на кнопку ⣿ и перетащить условие на новое место.

Условия, группы и фильтры можно удалить, нажав на кнопку ✕.

Параметры условий:

- **Если** (обязательно) – в этом раскрывающемся списке можно указать, требуется ли использовать инвертированную функцию оператора
- **Левый операнд** и **Правый операнд** (обязательно) – используются для указания значений, которые будет обрабатывать оператор. Доступные типы зависят от выбранного оператора.

  Операнды фильтров

- **Поле события** – используется для присвоения операнду значения поля события. Дополнительные параметры:
  - **поле события** (обязательно) – этот раскрывающийся список используется для выбора поля, из которого следует извлечь значение операнда.
- **Активный лист** – используется для присвоения операнду значения записи активного листа. Дополнительные параметры:
  - **название активного листа** (обязательно) – этот раскрывающийся список используется для выбора активного листа.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для создания записи активного листа и служащих ключом записи активного листа.
  - **поле** (требуется, если не выбран оператор **inActiveList**) – используется для ввода имени поля активного листа, из которого следует извлечь значение операнда.
- **Контекстная таблица** – используется для присвоения операнду значения контекстной таблицы. Дополнительные параметры:
  - **название контекстной таблицы** (обязательно) – этот раскрывающийся список используется для выбора контекстной таблицы.
  - **ключевые поля** (обязательно) – это список полей событий или локальных переменных, используемых для создания записи контекстной таблицы и служащих ключом записи контекстной таблицы.
  - **поле** – используется для ввода имени поля контекстной таблицы, из которого следует извлечь значение операнда.
  - **индекс** – используется для ввода индекса списочного поля таблицы, из которого следует извлечь значение операнда.
- **Словарь** – используется для присвоения значения операнду значения из ресурса словарь. Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.
- **Константа** – используется для присвоения операнду пользовательского значения. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите константу, которую хотите присвоить операнду.
- **Таблица** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря типа **Таблица**.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.

- **Список** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:

  - **значение** (обязательно) – здесь вы вводите список констант, которые хотите назначить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

- **TI** – используется для чтения данных CyberTrace об угрозах (TI) из событий. Дополнительные параметры:

  - **поток** (обязательно) – в этом поле указывается категория угрозы CyberTrace.

  - **ключевые поля** (обязательно) – этот раскрывающийся список используется для выбора поля события с индикаторами угроз CyberTrace.

  - **поле** (обязательно) – в этом поле указывается поле фида CyberTrace с индикаторами угроз.

- **Оператор** (обязательно) – используется для выбора оператора условия.

  В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **inSubnet**, **inActiveList**, **inCategory**, **InActiveDirectoryGroup, hasBit**, **inDictionary**. По умолчанию флажок снят.

  Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Доступные типы операндов зависят от того, является ли операнд левым (L) или правым (R).

Доступные типы операндов для левого (L) и правого (R) операндов

Оператор	Тип "поле события"	Тип "активный лист"	Тип "словарь"	Тип "контекстная таблица"	Тип "таблица"	Тип "TI"	Тип "константа"	Тип "список"
=	L,R	L,R	L,R	L,R	L,R	L,R	R	R
>	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
>=	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
<	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
<=	L,R	L,R	L,R	L,R (только при поиске значения таблицы по индексу)	L,R	L	R	—
inSubnet	L,R	L,R	L,R	L,R	L,R	L,R	R	R
contains	L,R	L,R	L,R	L,R	L,R	L,R	R	R
startsWith	L,R	L,R	L,R	L,R	L,R	L,R	R	R
endsWith	L,R	L,R	L,R	L,R	L,R	L,R	R	R
match	L	L	L	L	L	L	R	R
hasVulnerability	L	L	L	L	L	—	—	—
hasBit	L	L	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—	—	—
inDictionary	—	—	—	—	—	—	—	—
inCategory	L	L	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—	—	—
inActiveDirectoryGroup	L	L	L	L	L	—	R	R
TIDetect	—	—	—	—	—	—	—	—

Вы можете использовать при работе с фильтрами горячие клавиши. Описание горячих клавиш приведено в таблице ниже.

Горячие клавиши и их функциональность

Клавиша	Функциональность
e	Вызывает фильтр по полю события
d	Вызывает фильтр по полю словаря
a	Вызывает фильтр по полю активного листа
c	Вызывает фильтр по полю контекстной таблицы
t	Вызывает фильтр по полю таблицы
f	Вызывает фильтр
t+i	Вызывает фильтр с использованием TI
Ctrl+Enter	Завершение редактирования условия

Работа с полями типа "строка", "число" и "число с плавающей точкой" расширенной схемы событий в фильтрах не отличается от работы с полями схемы событий KUMA.

При использовании фильтров с полями расширенной схемы событий с типами полей "Массив строк", "Массив целых чисел" и "Массив чисел с плавающей точкой" возможно использование следующих операций:

- Операция "contains" вернет значение True, если указанная подстрока присутствует в массиве, иначе вернет False.
- Операция "match" – поиск в строке по регулярному выражению.
- Операция "intersec".

При использовании фильтров с полями расширенной схемы событий с типами полей "Массив целых чисел" и "Массив чисел с плавающей точкой" возможно использование следующих операций сравнения чисел: <,>, =, >=, <=.

Для обращения к конкретному элементу массива в фильтре необходимо использовать следующий синтаксис: NA.<Имя массива>.<номер элемента>

Нумерация элементов массива начинается с 0.

Пример:

NA.ArrayOne.0 – обращение к первому элементу массива чисел ArrayOne.

FA.ArrayTwo.2 – обращение к третьему элементу массива чисел с плавающей точкой ArrayTwo.

Формирование условий в режиме исходного кода

Режим редактора кода позволяет быстро редактировать условия, выделять и копировать блоки кода.

В правой части конструктора отображается навигатор, позволяющий переместиться ко коду фильтра.

Перенос строк выполняется автоматически по логическим операторам И, ИЛИ, НЕ или запятым, являющимися разделителем элементов списка значений.

Для ресурсов, использованных в фильтре, автоматически указывается их наименование. Поля, содержащие наименования связанных ресурсов, нельзя отредактировать. Имена категорий общих ресурсов не отображаются в фильтре, если у вас нет роли "Доступ к общим ресурсам".

В поставку OSMP включены перечисленные в таблице ниже фильтры.

Предустановленные фильтры

Название фильтра	Описание
[OOTB][AD] A member was added to a security-enabled global group (4728)	Выбирает события добавления пользователя в группу безопасности (security-enabled global group) Active Directory.
[OOTB][AD] A member was added to a security-enabled universal group (4756)	Выбирает события добавления пользователя в группу безопасности (security-enabled universal group) Active Directory.
[OOTB][AD] A member was removed from a security-enabled global group (4729)	Выбирает события удаления пользователя из группы безопасности (security-enabled global group) Active Directory.
[OOTB][AD] A member was removed from a security-enabled universal group (4757)	Выбирает события удаления пользователя из группы безопасности (security-enabled universal group) Active Directory.
[OOTB][AD] Account Created	Выбирает события создания учетной записи в ОС Windows.

[OOTB][AD] Account Deleted	Выбирает события удаления учетной записи в ОС Windows.
[OOTB][AD] An account failed to log on (4625)	Выбирает события неуспешной попытки входа в ОС Windows.
[OOTB][AD] Successful Kerberos authentication (4624, 4768, 4769, 4770)	Выбирает события успешной попытки входа в ОС Windows и события с идентификаторами 4769, 4770, регистрирующиеся на контроллерах домена.
[OOTB][AD][Technical] 4768. TGT Requested	Выбирает события Microsoft Windows с идентификатором 4768.
[OOTB][Net] Possible port scan	Выбирает события, которые могут говорить о проведении сканирования портов.
[OOTB][SSH] Accepted Password	Выбирает события успешного подключения с использование пароля по протоколу SSH.
[OOTB][SSH] Failed Password	Выбирает события попыток подключения с использование пароля по протоколу SSH.

Активные листы

Активный лист – это контейнер для данных, которые используются коррелятором KUMA при анализе событий по правилам корреляции.

Например, если у вас есть список IP-адресов с плохой репутацией, вы можете:

1. Создать корреляционное правило типа operational и добавить в активный лист эти IP-адреса.
2. Создать корреляционное правило типа standard и указать активный лист в качестве условия фильтрации.
3. Создать коррелятор с этим правилом.

   В этом случае KUMA выберет все события, которые содержат IP-адреса, внесенные в активный лист, и создаст корреляционное событие.

Вы можете наполнять активные листы автоматически с помощью корреляционных правил типа simple или импортировать файл с данными для активного листа.

Вы можете добавлять, копировать и удалять активные листы.

Активные листы можно использовать в следующих сервисах и функциях KUMA:

- Правила корреляции.
- Панель мониторинга.

Один и тот же активный лист может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

В активный лист добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, дублировать, удалять и экспортировать записи в активном листе коррелятора.

В процессе корреляции при удалении записей из активных листов в корреляторах создаются служебные события. Эти события существуют только в корреляторах, они не перенаправляются в другие точки назначения. Правила корреляции можно настроить на отслеживание этих событий, чтобы с их помощью распознавать угрозы. Поля служебных событий удаления записи из активного листа описаны ниже.

Поле события	Значение или комментарий

`ID`	Идентификатор события
`Timestamp`	Время удаления записи, срок жизни которой истек.
`Name`	`"active list record expired"`
`DeviceVendor`	`"Лаборатория Касперского".`
`DeviceProduct`	`"KUMA"`
`ServiceID`	Идентификатор коррелятора.
`ServiceName`	Название коррелятора.
`DeviceExternalID`	Идентификатор активного листа
`DevicePayloadID`	Ключ записи, чей срок жизни истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи
`S.<active list field>`	Запись активного листа в следующем формате: S.<поле активного листа> = <значение активного листа>

Просмотр таблицы активных листов

Чтобы просмотреть таблицу активных листов коррелятора:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя активного листа.
- **Записи** – количество записей в активном листе.
- **Размер на диске** – размер активного листа.
- **Каталог** – путь к активному листу на сервере коррелятора KUMA.

Добавление активного листа

Чтобы добавить активный лист:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. Нажмите на кнопку **Добавить активный лист**.

4. Выполните следующие действия:

   a. В поле **Название** введите имя активного листа.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   c. В поле **Срок жизни** укажите время, в течение которого в активном листе будет храниться добавленная в него запись.

      По истечении указанного времени запись удаляется. Время указывается в секундах.

      По умолчанию указано значение 0. Если в поле указано значение 0, запись хранится 36000 дней (около 100 лет).

   d. В поле **Описание** укажите любую дополнительную информацию.

      Вы можете использовать до 4000 символов в кодировке Unicode.

      Поле не является обязательным.

5. Нажмите на кнопку **Сохранить**.

Активный лист будет добавлен.

Просмотр параметров активного листа

Чтобы просмотреть параметры активного листа:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. В столбце **Название** выберите активный лист, параметры которого вы хотите просмотреть.

Откроется окно с параметрами активного листа. В нем отображается следующая информация:

- **Идентификатор** – идентификатор активного листа.
- **Название** – уникальное имя ресурса.
- **Тенант** – название тенанта, которому принадлежит ресурс.
- **Срок жизни** – время, в течение которого в активном листе будет храниться добавленная в него запись. Значение указывается в секундах.
- **Описание** – любая дополнительная информация о ресурсе.

Изменение параметров активного листа

Чтобы изменить параметры активного листа:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. В столбце **Название** выберите активный лист, параметры которого вы хотите изменить.

4. Укажите значения для следующих параметров:

   - **Название** – уникальное имя ресурса.
   - **Срок жизни** – время, в течение которого в активном листе будет храниться добавленная в него запись. Значение указывается в секундах.

     Если в поле указано значение 0, запись хранится бессрочно.
   - **Описание** – любая дополнительная информация о ресурсе.

   Поля **Идентификатор** и **Тенант** недоступны для редактирования.

Дублирование параметров активного листа

Чтобы скопировать активный лист:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. Установите флажок рядом с активным листом, который вы хотите скопировать.
4. Нажмите на кнопку **Дублировать**.
5. Укажите нужные вам параметры.
6. Нажмите на кнопку **Сохранить**.

Активный лист будет скопирован.

Удаление активного листа

Чтобы удалить активный лист:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. Установите флажки рядом с активными листами, которые вы хотите удалить.
   Если вы хотите удалить все листы, установите флажок рядом со столбцом **Название**.

   Должен быть установлен хотя бы один флажок.
4. Нажмите на кнопку **Удалить**.
5. Нажмите на кнопку **ОК**.

Активные листы будут удалены.

Просмотр записей в активном листе

Чтобы просмотреть список записей в активном листе:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

Откроется таблица записей для выбранного листа.

Таблица содержит следующие данные:

- **Ключ** – значение ключа записи.
- **Повторы записи** – общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте активных листов в KUMA.
- **Срок действия** – дата и время, когда запись должна быть удалена.

  Если при создании активного листа в поле **Срок жизни** было указано значение 0, записи этого активного листа хранятся 36000 дней (около 100 лет).
- **Создано** – время создания активного листа.
- **Последнее обновление** – время последнего обновления активного листа.

Поиск записей в активном листе

Чтобы найти запись в активном листе:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. В поле **Поиск** введите значение ключа записи или несколько знаков из ее ключа.

В таблице записей активного листа отобразятся только те записи, в ключе которых есть введенные символы.

Добавление записи в активный лист

Чтобы добавить запись в активный лист:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив нужного коррелятора.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. Нажмите на кнопку **Добавить**.

   Откроется окно **Создать запись**.
7. Укажите значения для следующих параметров:

   a. В поле **Ключ** введите имя записи.

   Вы можете указать несколько значений, используя символ "|".

   > Поле **Ключ** не может быть пустым. Если поле остается пустым, при попытке сохранить изменения KUMA возвращает ошибку.

   b. В поле **Значение** укажите значения для полей в столбце **Поле**.

   KUMA берет названия полей из корреляционных правил, к которым привязан активный лист. Эти названия недоступны для редактирования. Вы можете удалить эти поля при необходимости.

   c. Если вы хотите добавить дополнительное значение, нажмите на кнопку **Добавить элемент**.

   d. В столбце **Поле** укажите название поля.

   Название должно соответствовать следующим требованиям:

   - Название уникально.
   - Не содержит табуляцию.
   - Не содержит специальные символы, кроме символа нижнего подчеркивания.
   - Максимальное количество символов – 128.

   > Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.

   e. В столбце **Значение** укажите значение для этого поля.

Оно должно соответствовать следующим требованиям:

- Не содержит табуляцию.
- Не содержит специальные символы, кроме символа нижнего подчеркивания.
- Максимальное количество символов – 1024.

Поле не является обязательным.

8. Нажмите на кнопку **Сохранить**.

Запись добавлена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Дублирование записей в активном листе

Чтобы дублировать запись в активном листе:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. Установите флажок для записи, которую вы хотите скопировать.
7. Нажмите на кнопку **Дублировать**.
8. Укажите нужные вам параметры.

   Поле **Ключ** не может быть пустым. Если поле остается пустым, при попытке сохранить изменения KUMA возвращает ошибку.

   Редактирование названий полей в столбце **Поле** для записей, добавленных в активный лист ранее, недоступно. Вы можете менять названия только для записей, добавленных в момент редактирования. Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.
9. Нажмите на кнопку **Сохранить**.

Запись будет скопирована. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Изменение записи в активном листе

Чтобы изменить запись в активном листе:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. Нажмите на название записи в столбце **Ключ**.
7. Укажите требуемые значения.
8. Нажмите на кнопку **Сохранить**.

Запись будет изменена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Ограничения, действующие при редактировании записи:

- Название записи недоступно для редактирования. Вы можете изменить его, выполнив импорт аналогичных данных с другим названием.
- Редактирование названий полей в столбце **Поле** для записей, добавленных в активный лист ранее, недоступно. Вы можете менять названия только для записей, добавленных в момент редактирования. Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.
- Значения в столбце **Значение** должны соответствовать следующим требованиям:
  - Не содержит буквы русского алфавита.
  - Не содержит пробелы и табуляцию.
  - Не содержит специальные символы, кроме символа нижнего подчеркивания.
  - Максимальное количество символов – 128.

Удаление записей в активном листе

Чтобы удалить записи из активного листа:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.
   Откроется окно со списком записей для выбранного листа.
6. Установите флажки для записей, которые вы хотите удалить.
   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

   > Должен быть установлен хотя бы один флажок.

7. Нажмите на кнопку **Удалить**.
8. Нажмите на кнопку **OK**.

Записи будут удалены.

Импорт данных в активный лист

Чтобы импортировать данные в активный лист:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.
   Отобразится таблица **Активные листы коррелятора**.
5. Наведите курсор мыши на строку с требуемым активным листом.
6. Нажмите на ... слева от названия активного листа.
7. Выберите **Импортировать**.
   Откроется окно импорта активного листа.
8. В поле **Файл** выберите файл, который требуется импортировать.
9. В раскрывающемся списке **Формат** выберите формат файла:
   - **csv**
   - **tsv**
   - **internal**
10. В поле **Ключевое поле** введите название столбца с ключами записей активного листа.
11. Нажмите на кнопку **Импортировать**.

Данные из файла будут импортированы в активный лист. Записи, внесенные в лист ранее, сохраняются.

При импорте данные из файла не проходят проверку на допустимые символы. Если вы будете использовать эти данные в веб-виджетах, при наличии недопустимых символов в данных веб-виджеты будут отображаться некорректно.

Экспорт данных из активного листа

Чтобы экспортировать активный лист:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. Наведите курсор мыши на строку с требуемым активным листом.
6. Нажмите на ... слева от нужного активного листа.
7. Нажмите на кнопку **Экспортировать**.

Активный лист будет загружен в формате JSON с использованием настроек вашего браузера. Название загруженного файла соответствует названию активного листа.

Предустановленные активные листы

В поставку OSMP включены перечисленные в таблице ниже активные листы.

Предустановленные активные листы

Имя активного листа	Описание
[OOTB][AD] End-users tech support accounts	Активный список используется в качестве фильтра при работе корреляционного правила [OOTB][AD] Successful authentication with same user account on multiple hosts. В активный список могут быть добавлены учетные записи сотрудников технической поддержки. Записи не удаляются из активного списка.
[OOTB][AD] List of requested TGT. EventID 4768	Активный список наполняется правилом [OOTB][AD][Technical] 4768. TGT Requested, также данный активный список используется в селекторе правила [OOTB][AD] Granted TGS without TGT (Golden Ticket). Записи удаляются из списка через 10 часов после внесения.
[OOTB][AD] List of sensitive groups	Активный список используется в качестве фильтра при работе корреляционного правила [OOTB][AD] Membership of sensitive group was modified. В активный список могут быть добавлены критичные доменные группы, членство в которых необходимо отслеживать. Записи не удаляются из активного списка.
[OOTB][Linux] CompromisedHosts	Активный список наполняется правилом [OOTB] Successful Bruteforce потенциально скомпрометированными устройствами под управлением операционной системой Linux. Записи удаляются из списка через 24 часов после внесения.

Словари

Описание параметров

Словари – это ресурсы, в которых хранятся данные, которые могут использоваться другими ресурсами и сервисами KUMA.

Словари могут использоваться в следующих сервисах и функциях KUMA:

- Коллектор.
- Правила корреляции.
- Нормализаторы.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Описание** – вы можете добавить до 4000 символов в кодировке Unicode, описывающих ресурс.
- **Тип** (обязательно) – тип словаря. От выбранного типа зависит формат данных, которые может содержать словарь:
  - В тип **Словарь** можно добавлять пары ключ–значение.

    Не рекомендуется добавлять в словари этого типа более 50 000 записей.

    > При добавлении в словарь строк с одинаковыми ключами каждая новая строка будет записана поверх уже существующий строки с тем же самым ключом. В итоге в словарь будет добавлена только одна строка.

  - В тип **Таблица** можно добавлять данные в виде сложных таблиц. С этим типом словарей можно взаимодействовать с помощью REST API.
- Блок параметров **Значения** – содержит таблицу с данными словаря:

  Для типа **Словарь** в блоке отображается перечень пар **Ключ** – **Значение**. Вы можете нажать на кнопку +, чтобы добавить строки в таблицу. Вы можете удалить строки с помощью на кнопки ×, которая отображается при наведении курсора мыши на нужную строку. В поле **Ключ** допустимо указать уникальное значение: максимум 128 символов в кодировке Unicode, первый символ не может быть $. В поле **Значение** допустимо указать значение: максимум 255 символов в кодировке Unicode, первый символ не может быть $. Допускается добавить одну или несколько пар **Ключ** – **Значение**.

  - Для типа **Таблица** в блоке отображается таблица с данными. Вы можете нажать на кнопку +, чтобы добавить строки или столбцы в таблицу. Удалить строки и столбцы можно, нажав на кнопки ×, которые отображаются при наведении курсора мыши на нужную строку или заголовок нужного столбца. Заголовки столбцов доступны для редактирования.

  Если словарь содержит больше 5000 записей, они не отображаются в Консоли KUMA. Для просмотра содержимого таких словарей содержимое необходимо экспортировать в формат CSV. Если CSV-файл отредактировать и снова импортировать в KUMA, словарь будет обновлен.

Импорт и экспорт словарей

Вы можете импортировать или экспортировать данные словарей в формате CSV (в кодировке UTF-8) с помощью кнопок **Импортировать CSV** и **Экспортировать CSV**.

Формат CSV-файла зависит от типа словаря:

- Тип **Словарь**:

  `{КЛЮЧ},{ЗНАЧЕНИЕ}\n`

- Тип **Таблица**:

  `{Заголовок столбца 1},{Заголовок столбца N},{Заголовок столбца N+1}\n`

  `{Ключ1},{ЗначениеN},{ЗначениеN+1}\n`

  `{Ключ2},{ЗначениеN},{ЗначениеN+1}\n`

  Ключи должны быть уникальными как для CSV-файла, так и для словаря. В таблицах ключи указываются в первом столбце. Ключ должен содержать от 1 до 128 символов в кодировке Unicode.

  Значения должны содержать от нуля до 256 символов в кодировке Unicode.

При импорте содержимое словаря перезаписывается загружаемым файлом. При импорте в словарь также изменяется название ресурса, чтобы отразить имя импортированного файла.

При экспорте, если ключ или значение содержат символы запятой или кавычек (, и "), они заключаются в кавычки ("). Кроме того, символ кавычки (") экранируется дополнительной кавычкой ("").

Если в импортируемом файле обнаружены некорректные строки (например, неверные разделители), то при импорте в словарь такие строки будут проигнорированы, а при импорте в таблицу процесс импорта будет прерван.

Взаимодействие со словарями через API

Вы можете использовать REST API для чтения содержимого словарей **табличного типа**. Вы также можете изменить их, даже если эти ресурсы используются активными сервисами. Это позволяет, например, настроить обогащение событий данными из динамически изменяемых таблиц, выгружаемых из сторонних приложений.

Предустановленные словари

В поставку OSMP включены перечисленные в таблице ниже словари.

Предустановленные словари

название словаря;	Тип	Описание
[OOTB] Ahnlab. Severity	dictionary	Содержит таблицу соответствия между идентификатором приоритета и его названием.
[OOTB] Ahnlab. SeverityOperational	dictionary	Содержит значения параметра SeverityOperational и соответствующее ему описание.
[OOTB] Ahnlab. VendorAction	dictionary	Содержит таблицу соответствия между идентификатором выполняемой операции и ее названием.
[OOTB] Cisco ISE Message Codes	dictionary	Содержит коды событий Cisco ISE и соответствующие им имена.
[OOTB] DNS. Opcodes	dictionary	Содержит таблицу соответствия между десятичными кодами операций DNS и их описаниями, зарегистрированными IANA.
[OOTB] IANAProtocolNumbers	dictionary	Содержит номера портов транспортных протоколов (TCP, UDP) и соответствующие им имена сервисов, зарегистрированные IANA.
[OOTB] Juniper - JUNOS	dictionary	Содержит идентификаторы событий JUNOS и соответствующие им описания.
[OOTB] KEDR. AccountType	dictionary	Содержит идентификатор типа учетной записи и соответствующее ему наименование типа.
[OOTB] KEDR. FileAttributes	dictionary	Содержит идентификаторы атрибутов файлов, хранимые файловой системой, и

		соответствующие им описания.
[OOTB] KEDR. FileOperationType	dictionary	Содержит идентификаторы операций с файлами из API KATA и соответствующие им названия операции.
[OOTB] KEDR. FileType	dictionary	Содержит идентификаторы измененного файла из API KATA и соответствующие им описания типов файлов.
[OOTB] KEDR. IntegrityLevel	dictionary	Содержит SID параметра INTEGRITY LEVEL операционной системы Microsoft Windows и соответствующие им описания.
[OOTB] KEDR. RegistryOperationType	dictionary	Содержит идентификаторы операций с реестром из API KATA и соответствующие им значения.
[OOTB] Linux. Sycall types	dictionary	Содержит идентификаторы системных вызовов ОС Linux и соответствующие им названия.
[OOTB] MariaDB Error Codes	dictionary	Словарь содержит коды ошибок СУБД MariaDB и используется нормализатором [OOTB] MariaDB Audit Plugin syslog для обогащения событий.
[OOTB] Microsoft SQL Server codes	dictionary	Содержит идентификаторы ошибок MS SQL Server и соответствующие им описания.
[OOTB] MS DHCP Event IDs Description	dictionary	Содержит идентификаторы событий DHCP сервера Microsoft Windows и соответствующие им описания.
[OOTB] S-Terra. Dictionary MSG ID to Name	dictionary	Содержит идентификаторы событий устройств S-Terra и соответствующие им имена событий.
[OOTB] S-Terra. MSG_ID to Severity	dictionary	Содержит идентификаторы событий устройств S-Terra и соответствующие им значения Severity.
[OOTB] Syslog Priority To Facility and Severity	table	Таблица содержит значения **Priority** и соответствующие ему значения полей **Facility and Severity**.
[OOTB] VipNet Coordinator Syslog Direction	dictionary	Содержит идентификаторы направления (последовательность специальных символов), используемые в ViPNet Coordinator для обозначения направления, и соответствующие им значения.
[OOTB] Wallix EventClassId - DeviceAction	dictionary	Содержит идентификаторы событий Wallix AdminBastion и соответствующие им описания.
[OOTB] Windows.Codes (4738)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4738, и соответствующие им имена.
[OOTB] Windows.Codes (4719)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4719, и соответствующие им имена.
[OOTB] Windows.Codes (4663)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4663, и соответствующие им имена.
[OOTB] Windows.Codes (4662)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4662, и соответствующие им имена.
[OOTB] Windows. EventIDs and Event Names mapping	dictionary	Содержит идентификаторы событий ОС Windows и соответствующие имена событий.
[OOTB] Windows. FailureCodes (4625)	dictionary	Содержит идентификаторы из полей **Failure Information\Status** и **Failure Information\Sub Status** события 4625 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. ImpersonationLevels (4624)	dictionary	Содержит идентификаторы из поля **Impersonation level** событий с идентификатором 4624 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. KRB ResultCodes	dictionary	Содержит коды ошибок Kerberos v5 и соответствующие им описания.
[OOTB] Windows. LogonTypes (Windows all events)	dictionary	Содержит идентификаторы типов входов пользователя и соответствующие им наименования.
[OOTB] Windows_Terminal Server. EventIDs and Event Names mapping	dictionary	Содержит идентификаторы событий Microsoft Terminal Server и соответствующие им имена.
[OOTB] Windows. Validate Cred. Error Codes	dictionary	Содержит идентификаторы типов входов пользователя и соответствующие им наименования.
[OOTB] ViPNet Coordinator Syslog Direction	dictionary	Содержит идентификаторы направления (последовательность специальных символов), используемые в ViPNet Coordinator для обозначения направления, и соответствующие им значения.
[OOTB] Syslog Priority To Facility	table	Содержит значения Priority и соответствующие ему значения полей Facility and Severity.

and Severity

Правила реагирования

Правила реагирования запускают для заданных событий автоматическое выполнение задач Kaspersky Security Center, действия по реагированию для Kaspersky Endpoint Detection and Response, KICS for Networks, Active Directory и запуск пользовательского скрипта.

Автоматическое выполнение задач Kaspersky Security Center, Kaspersky Endpoint Detection and Response, KICS for Networks и Active Directory по правилам реагирования доступно при интеграции с перечисленными приложениями.

Можно настроить правила реагирования в разделе **Ресурсы - Реагирование**, а затем выбрать созданное правило реагирования в раскрывающемся списке в настройках коррелятора. Также можно настроить правила реагирования прямо в настройках коррелятора.

Правила реагирования для Kaspersky Security Center

Вы можете настроить правила реагирования для автоматического запуска задач антивирусной проверки и обновления на активах Kaspersky Security Center.

При создании и изменении правил реагирования для Kaspersky Security Center вам требуется задать значения для следующих параметров.

Параметры правила реагирования

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр, доступен при интеграции KUMA с Kaspersky Security Center. Правила реагирования **osmptasks**.
Задаче Open Single Management Platform	Обязательный параметр. Название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, их названия должны начинаться со слова "KUMA". Например, `KUMA antivirus check` (без учета регистра и без кавычек). С помощью KUMA можно запустить следующие типы задач Kaspersky Security Center: • Обновление. • Поиск вирусов.
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения: • SourceAssetID • DestinationAssetID • DeviceAssetID
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

Описание	Описание правила реагирования. Вы можете добавить до 4000 символов в кодировке Unicode.
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если правила реагирования принадлежат общему тенанту, то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от Сервера администрирования Kaspersky Security Center, к которому подключен главный тенант.

Если в правиле реагирования выбрана задача, которая отсутствует на Сервере администрирования Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

Правила реагирования для пользовательского скрипта

Вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий, и настроить правила реагирования для автоматического запуска этого скрипта. В этом случае приложение запустит скрипт при получении событий, соответствующих правилам реагирования.

Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts. Пользователю `kuma` этого сервера требуются права на запуск скрипта.

При создании и изменении правил реагирования для произвольного скрипта вам требуется задать значения для следующих параметров.

Параметры правила реагирования

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр. Тип правила реагирования, **script**.
Время ожидания	Количество секунд, в течение которого должно завершиться выполнение скрипта. Если это время превышено, выполнение скрипта прерывается.
Название скрипта	Обязательный параметр. Имя файла скрипта. Если ресурс реагирования прикреплен к сервису коррелятора, но в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.
Аргументы скрипта	Параметры или значения полей событий, которые необходимо передать скрипту. Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь. Параметры можно обрамлять кавычками ("). Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт. Пример: `-n "\"usr\": {{.SourceUserName}}"`
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов в кодировке Unicode.
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила реагирования для KICS for Networks

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

При создании и изменении правил реагирования для KICS for Networks вам требуется задать значения для следующих параметров.

Параметры правила реагирования

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр. Тип правила реагирования, **kics**.
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно выполнить действия по реагированию. Возможные значения: • SourceAssetID

	• DestinationAssetID • DeviceAssetID
Задача KICS for Networks	Действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию: • **Изменить статус актива на Разрешенное**. • **Изменить статус актива на Неразрешенное**. При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов в кодировке Unicode.
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила реагирования для Kaspersky Endpoint Detection and Response

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах Kaspersky Endpoint Detection and Response. Например, вы можете настроить автоматическую изоляцию актива от сети.

При создании и изменении правил реагирования для Kaspersky Endpoint Detection and Response вам требуется задать значения для следующих параметров.

Параметры правила реагирования

Параметр	Описание
Поле события	Обязательный параметр. Определяет поле события для актива, для которого нужно выполнить действия по реагированию. Возможные значения: • SourceAssetID • DestinationAssetID • DeviceAssetID
Тип задач	Действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию: • Включить сетевую изоляцию. При выборе этого типа реагирования вам нужно задать значения для параметра:

- **Срок действия изоляции** – количество часов, в течение которых будет действовать сетевая изоляция актива. Вы можете указать от 1 до 9999 часов. При необходимости вы можете **добавить исключение для сетевой изоляции**.

  Чтобы добавить исключение для сетевой изоляции:

  a. Нажмите на кнопку **Добавить исключение**.

  b. Выберите направление сетевого трафика, которое не должно быть заблокировано:

  - Входящее.
  - Исходящее.
  - Входящее/Исходящее.

  c. В поле **IP актива** введите IP-адрес актива, сетевой трафик которого не должен быть заблокирован.

  d. Если вы выбрали **Входящее** или **Исходящее**, укажите порты подключения в полях **Удаленные порты** и **Локальные порты**.

  e. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить исключение** и повторите действия по заполнению полей **Направление трафика**, **IP актива**, **Удаленные порты** и **Локальные порты**.

  f. Если вы хотите удалить исключение, нажмите на кнопку **Удалить** под нужным вам исключением.

  При добавлении исключений в правило сетей изоляции Kaspersky Endpoint Detection and Response может некорректно отображать значения портов в информации о правиле. Это не влияет на работоспособность приложения. Подробнее о просмотре правила сетевой изоляции см. в *справке Kaspersky Anti Targeted Attack Platform*.

- Выключить сетевую изоляцию.
- Добавить правило запрета. При выборе этого типа реагирования вам нужно задать значения для следующих параметров:
  - **Поля события для получения хеш-суммы** – поля событий, из которых KUMA извлекает SHA256- или MD5-хеши файлов, выполнение которых требуется запретить.
    Выбранные поля событий, а также значения, выбранные в **Поле события**, требуется добавить в распространяемые поля правила корреляции.
  - **Хеш файла №1** – SHA256- или MD5-хеш файла, который требуется запретить.

  Хотя бы одно из указанных выше полей должно быть заполнено.

- Удалить правило запрета.
- Запустить приложение. При выборе этого типа реагирования вам нужно задать значения для следующих параметров:
  - **Путь к файлу** – путь к файлу процесса, который вы хотите запустить.
  - **Аргументы командной строки** – параметры, с которыми вы хотите запустить файл.
  - **Текущая директория** – директория, в которой на момент запуска располагается файл.

  При срабатывании правила реагирования для пользователей с ролью Главный администратор в разделе **Диспетчер задач** консоли приложения отобразится задача **Запустить приложение**. В столбце Создал **таблицы задач** для этой задачи отображается **Задача по расписанию**. Вы можете просмотреть результат выполнения задачи.

	Все перечисленные операции выполняются на активах с Kaspersky Endpoint Agent для Windows. На активах с Kaspersky Endpoint Agent для Linux выполняется только запуск приложения. На программном уровне возможность создания правил запрета и сетевой изоляции для активов с Kaspersky Endpoint Agent для Linux не ограничена. KUMA и Kaspersky Endpoint Detection and Response не уведомляют о неуспешном применении этих правил.
Рабочие процессы	Количество процессов, которые сервис может запускать одновременно. По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание правила реагирования. Вы можете добавить до 4000 символов в кодировке Unicode.
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. **Создание фильтра в ресурсах**

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила реагирования через Active Directory

Правила реагирования через Active Directory определяют действия, которые будут применяться к учетной записи в случае срабатывания правила.

При создании и изменении правил реагирования через Active Directory вам требуется задать значения для следующих параметров.

Параметры правила реагирования

Параметр	Описание
Name	Обязательный параметр. Уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр. Тип правила реагирования, **Реагирование через Active Directory**.
Источник идентификатора аккаунта	Поле события, откуда будет взято значение идентификатора учетной записи Active Directory. Возможные значения: • SourceAccountID • DestinationAccountID

Команда Active Directory	Команда, которая будет применяться к учетной записи при срабатывании правила реагирования. Доступные значения: • **Добавить учетную запись в группу** Группа Active Directory, из которой или в которую требуется переместить учетную запись. В обязательном поле **Отличительное имя** необходимо указать полный путь к группе. Например, CN = HQ Team, OU = Groups, OU = ExchangeObjects, DC = avp, DC = ru. В рамках одной операции можно указать только одну группу. • **Удалить учетную запись из группы** Группа Active Directory, из которой или в которую требуется переместить учетную запись. В обязательном поле **Отличительное имя** необходимо указать полный путь к группе. Например, CN = HQ Team, OU = Groups, OU = ExchangeObjects, DC = avp, DC = ru. В рамках одной операции можно указать только одну группу. • Сбросить пароль учетной записи Если в вашем домене Active Directory для учетных записей допускается установка флажка **User cannot change password**, использование в качестве реагирования сброса пароля учетной записи приведет к коллизии требований к учетной записи: пользователь не сможет аутентифицироваться. Администратору домена потребуется снять один из флажков для затронутой учетной записи: **User cannot change password** или **User must change password at next logon**. • Блокировать учетную запись
Фильтр	Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр. Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает *False*.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указать, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence. То есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

По умолчанию флажок снят.

e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

f. Вы можете добавить несколько условий или группу условий.

5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.

6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Коннекторы

Коннекторы используются для установления соединений между сервисами KUMA, активного и пассивного получения событий.

В приложении доступны следующие типы коннекторов:

- tcp – используется для пассивного получения событий по протоколу TCP. Доступен для агентов Windows и Linux.
- udp – используется для пассивного получения событий по протоколу UDP. Доступен для агентов Windows и Linux.
- netflow – используется для пассивного получения событий в формате NetFlow.

- sflow – используется для пассивного получения событий в формате SFlow.
- nats-jetstream – используется для взаимодействия с брокером сообщений NATS. Доступен для агентов Windows и Linux.
- kafka – используется для коммуникации с шиной данных Apache Kafka. Доступен для агентов Windows и Linux.
- http – используется для получения событий по протоколу HTTP. Доступен для агентов Windows и Linux.
- sql – используется для выборки данных из СУБД.

  Приложение поддерживает работу со следующими типами баз данных SQL:

  - SQLite.
  - MSSQL.
  - MySQL.
  - PostgreSQL.
  - Cockroach.
  - Oracle.
  - Firebird.
  - ClickHouse.
- file – используется для получения данных из текстового файла. Доступен для агентов Linux.
- 1c-log и 1c-xml – используются для получения данных из журналов 1С. Доступен для агентов Linux.
- diode – используется для однонаправленной передачи данных в промышленных ICS-сетях с использованием диодов данных.
- ftp – используется для получения данных по протоколу File Transfer Protocol. Доступен для агентов Windows и Linux.
- nfs – используется для получения данных по протоколу Network File System. Доступен для агентов Windows и Linux.
- wmi – используется для получения данных с помощью Windows Management Instrumentation. Доступен для агентов Windows.
- wec – используется для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС устройства под управлением Windows. Доступен для агентов Windows.
- snmp – используется для получения данных с помощью Simple Network Management Protocol. Доступен для агентов Windows и Linux.
- snmp-trap – используется для получения данных с помощью "ловушек" Simple Network Management Protocol (SNMP Trap). Доступен для агентов Windows и Linux.
- kata/edr – используется для получения данных KEDR по API.

- vmware – используется для получения данных VMware vCenter по API.
- elastic – используется для получения данных Elasticsearch.
- etw – используется для получения расширенных журналов событий DNS-сервера.

Просмотр параметров коннектора

Чтобы просмотреть параметры коннектора:

1. В Консоли KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.
2. В структуре папок выберите папку, в которой располагается нужный вам коннектор.
3. Выберите коннектор, параметры которого вы хотите просмотреть.

Параметры коннекторов отображаются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Подробное описание параметров каждого коннектора см. в разделе *Параметры коннекторов*.

Добавление коннектора

Вы можете включить отображение непечатаемых символов для всех полей ввода, кроме поля **Описание**.

Чтобы добавить коннектор:

1. В Консоли KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.
2. В структуре папок выберите папку, в которой должен располагаться коннектор.

   Корневые папки соответствуют тенантам. Для того, чтобы коннектор был доступен определенному тенанту, его следует создать в папке этого тенанта.

   Если в дереве папок отсутствует требуемая папка, вам нужно создать ее.

   По умолчанию добавляемые коннекторы создаются в папке **Общий**.
3. Нажмите на кнопку **Добавить коннектор**.
4. Укажите параметры для выбранного типа коннектора.

   Параметры, которые требуется указать для каждого типа коннектора, приведены в разделе *Параметры коннекторов*.
5. Нажмите на кнопку **Сохранить**.

Параметры коннекторов

Этот раздел содержит описание параметров всех поддерживаемых KUMA типов коннекторов.

Тип tcp

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **tcp**.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
- **Auditd** – переключатель механизма, который группирует записи журнала событий auditd, полученные от коннектора, в одно событие. Auditd поддерживает только разделитель \n. Если переключатель включен, поле **Разделитель** недоступно. Если в коннекторе агента включен переключатель **Auditd**, в коннекторе коллектора, которому агент отправляет события, должен быть установлен разделитель \n.
- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то по умолчанию используется значение: `\n`.
- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.
- **TTL буфера событий** – время жизни буфера для группировки записей в одно событие auditd. Поле доступно, если переключатель **Auditd** включен. Обратный отсчет начинается с момента получения первой строки события или сразу после истечения предыдущего TTL. Возможные значения: от 50 мс до 3000 мс. По умолчанию указано значение 2000 мс.
- **Заголовок транспорта** – для событий auditd необходимо указать регулярное выражение, которое используется для определения частей журнала событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы record_type_name, record_type_value и event_sequence_number. Если многострочное событие auditd содержит префикс, то префикс сохраняется для первой записи, а для следующих записей префикс опускается.

  Вы можете вернуться к исходному значению, нажав на кнопку **Установить значение по умолчанию**.
- **Режим TLS** – режим шифрования TLS с использованием сертификатов в формате pem x509:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации сертификата.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

- **Нестандартный PFX** – использовать шифрование. Если выбран этот параметр, сертификат должен быть сгенерирован с закрытым ключом в формате контейнера PKCS#12 в доверенном центре сертификации. Затем сертификат нужно экспортировать из хранилища и загрузить его в Консоли KUMA в виде PFX-секрета. **Добавить PFX-секрет**.

  1. Если вы загрузили PFX-сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

     Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

  2. Если вы хотите добавить новый сертификат, справа от списка **Секрет** нажмите на кнопку +.

     Откроется окно **Секрет**.

  3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

  4. По кнопке **Загрузить PFX** выберите файл, в который вы экспортировали сертификат с закрытым ключом, в формате PKCS#12-контейнера.

  5. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.

  6. Нажмите на кнопку **Сохранить**.

  Сертификат будет добавлен и отобразится в списке **Секрет**.

  При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип udp

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип коннектора, **udp**.

- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

- **Auditd** – переключатель механизма, который группирует записи журнала событий auditd, полученные от коннектора, в одно событие. Auditd поддерживает только разделитель \n. Если переключатель включен, поле **Разделитель** недоступно. Если в коннекторе агента включен переключатель **Auditd**, в коннекторе коллектора, которому агент отправляет события, должен быть установлен разделитель \n.

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Количество обработчиков** – количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий правил реагирования. Вы можете определить количество обработчиков по формуле: (<количество ядер процессора>/2)+2.

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

- **TTL буфера событий** – время жизни буфера для группировки записей в одно событие auditd. Поле доступно, если переключатель **Auditd** включен. Обратный отсчет начинается с момента получения первой строки события или сразу после истечения предыдущего TTL. Возможные значения: от 50 мс до 3000 мс. По умолчанию указано значение 2000 мс.

- **Заголовок транспорта** – для событий auditd необходимо указать регулярное выражение, которое используется для определения частей журнала событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы record_type_name, record_type_value и event_sequence_number. Если многострочное событие auditd содержит префикс, то префикс сохраняется для первой записи, а для следующих записей префикс опускается.

  Вы можете вернуться к исходному значению, нажав на кнопку **Установить значение по умолчанию**.

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип netflow

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **netflow**.

  - **URL** (обязательно) – URL, с которым необходимо установить связь.

  - **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:

  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. По умолчанию указано значение 1.
- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.
- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип sflow

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **sflow**.
- **URL** (обязательно) – URL, с которым требуется установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
- **Рабочие процессы** – используется для установки количества рабочих процессов для коннектора. По умолчанию указано значение 1.
- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.
- **Отладка** – переключатель, с помощью которого можно включить логирование ресурса. По умолчанию положение **Выключено**.

Тип nats-jetstream

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **nats-jetstream**.
- **URL** (обязательно) – URL, с которым необходимо установить связь.
- **Топик** (обязательно) – тема сообщений NATS. Должно содержать символы в кодировке Unicode.

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Идентификатор группы** – параметр GroupID для сообщений NATS. Имя должно содержать от 1 до 255 символов Юникода. Значение по умолчанию – `default`.

- **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. По умолчанию указано значение 1.

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

- **Идентификатор кластера** – идентификатор кластера NATS.

- **Режим TLS** – использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации сертификата.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды:

   ```
   openssl genrsa -out ca.key 2048
   ```

2. Создать сертификат для только что созданного ключа.

   Пример команды:

   ```
   openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя устройства центра сертификации>" -out ca.crt
   ```

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды:

   ```
   openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя устройства сервера KUMA>" -out server.csr
   ```

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды:

   ```
   openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. Полученный сертификат `server.crt` следует загрузить в Консоль KUMA в секрет типа **certificate**, который затем нужно выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

Для использования сертификатов KUMA на сторонних устройствах необходимо изменить расширение файла сертификата с CERT на CRT. В противном случае может возвращаться ошибка x509: certificate signed by unknown authority.

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип kafka

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **kafka**.

- **URL** – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port.

- **Топик** – тема сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".

- **Авторизация** – необходимость агентам проходить авторизацию при подключении к коннектору:

  - **выключена** (по умолчанию).

  - **PFX**.

    Если выбран этот параметр, сертификат должен быть сгенерирован с закрытым ключом в формате контейнера PKCS#12 в доверенном центре сертификации. Затем сертификат нужно экспортировать из хранилища и загрузить его в Консоли KUMA в виде PFX-секрета.

    Добавить PFX-секрет

    1. Если вы загрузили PFX-сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

       Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

    2. Если вы хотите добавить новый сертификат, справа от списка **Секрет** нажмите на кнопку +.

       Откроется окно **Секрет**.

    3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

    4. По кнопке **Загрузить PFX** выберите файл, в который вы экспортировали сертификат с закрытым ключом, в формате PKCS#12-контейнера.

    5. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.

    6. Нажмите на кнопку **Сохранить**.

    Сертификат будет добавлен и отобразится в списке **Секрет**.

  - **обычная**.

    При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

    Добавить секрет

1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

   Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

   Секрет будет добавлен и отобразится в списке **Секрет**.

- **Идентификатор группы** – параметр GroupID для сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Размер одного сообщения в запросе** – размер сообщения в запросе следует указывать в байтах. Значение по умолчанию – 16 МБ.

- **Максимальное время ожидания одного сообщения** – время ожидания сообщения заданного размера. Значение по умолчанию – 5 секунд.

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

- **Режим TLS** – использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации сертификата.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды:

   ```
   openssl genrsa -out ca.key 2048
   ```

2. Создать сертификат для только что созданного ключа.

   Пример команды:

   ```
   openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя устройства центра сертификации>" -out ca.crt
   ```

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды:

   ```
   openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя устройства сервера KUMA>" -out server.csr
   ```

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды:

   ```
   openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. Полученный сертификат `server.crt` следует загрузить в Консоль KUMA в секрет типа **certificate**, который затем нужно выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

Для использования сертификатов KUMA на сторонних устройствах необходимо изменить расширение файла сертификата с CERT на CRT. В противном случае может возвращаться ошибка x509: certificate signed by unknown authority.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип kata/edr

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **kata/edr**.
- **URL** (обязательно) – URL, по которому доступно получение телеметрии с сервера KATA/EDR. В URL указывается устройство и порт, по умолчанию порт 443. Если KATA/EDR развернута в кластере, можно

указать несколько URL, чтобы обеспечить высокую доступность подключения.

- **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения к серверу KATA/EDR. Вы можете выбрать ресурс секрета в раскрывающемся списке или создать его, нажав на кнопку +. При создании секрета вы можете указать пользовательский сертификат и закрытый ключ или автоматически сгенерировать новый самоподписанный сертификат и закрытый ключ. Выбранный секрет можно изменить, нажав на кнопку .

- **Внешний ID** – идентификатор для внешних систем. KUMA генерирует идентификатор и заполняет это поле автоматически.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- **Кодировка символов** – параметр исходной кодировки символов для конвертации в UTF-8. Мы рекомендуем применять конвертацию только в том случае, если в полях нормализованного события отображаются недопустимые символы. Значение по умолчанию: не выбрано.

- **Максимальное количество событий** – максимальное количество событий в одном запросе. По умолчанию используется значение, заданное на сервере KATA/EDR.

- **Время ожидания получения событий** – время ожидания получения событий от сервера KATA/EDR в секундах. По умолчанию указано значение 0 – это означает, что используется значение, заданное на сервере KATA/EDR.

- **Время ожидания ответа** – время ожидания ответа от сервера KATA/EDR в секундах. Значение по умолчанию: 1800 сек, отображается как 0.

- **Фильтр KEDRQL** – фильтр запросов к серверу KATA/EDR. Подробнее о языке запросов см. в Справке KEDR.

Тип http

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **http**.

  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.

  - **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации.
    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке приложения и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

    При использовании TLS невозможно указать IP-адрес в качестве URL.
  - **Прокси-сервер** – раскрывающийся список, в котором можно выбрать ресурс прокси-сервера.
  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип sql

KUMA поддерживает работу с несколькими **типами баз данных**.

Приложение поддерживает работу со следующими типами баз данных SQL:

- SQLite.
- MSSQL.
- MySQL.
- PostgreSQL.
- Cockroach.
- Oracle.
- Firebird.

При создании коннектора вам требуется задать значения для общих параметров коннектора и индивидуальных параметров подключения к базе данных.

Для коннектора на вкладке **Основные параметры** вам требуется задать значения следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тип** (обязательно) – тип коннектора, **sql**.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Запрос по умолчанию** (обязательно) – SQL-запрос, который выполняется при подключении к базе данных.

- **Переподключаться к БД каждый раз при отправке запроса** – по умолчанию флажок снят.

- **Период опроса, мс** – период выполнения SQL-запросов. Значение указывается в секундах. Значение по умолчанию – 10 секунд.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Для подключения к базе данных вам нужно задать значения следующих параметров на вкладке **Основные параметры** в разделе **Подключение**:

- В раскрывающемся списке **Тип базы данных** вы можете выбрать тип базы данных, к которой вы хотите подключиться. После выбора типа базы данных в поле **URL** отображается префикс, соответствующий протоколу обмена данными. Например, для базы данных ClickHouse поле **URL** содержит префикс clickhouse://.

- Если установлен флажок **Секрет отдельно**, в окне отображается обязательное поле **URL**, в котором можно указать URL подключения, и раскрывающийся список **Секрет** с секретами типа "credentials". Таким образом вы сможете просматривать информацию о подключении без необходимости повторно создавать большое количество подключений, если изменился пароль учетной записи, которую вы использовали для подключений. Если флажок снят, для выбора или создания секрета типа "urls" доступно только поле **URL**. По умолчанию флажок снят.

- **URL** (обязательно) – секрет, в котором хранится список URL-адресов для подключения к базе данных.

  - Поле для выбора или создания секрета типа "urls", в котором хранится список URL для подключения к базе данных. Поле доступно, если снят флажок Секрет отдельно.

    При необходимости вы можете **изменить** или **создать секрет**.

1. Нажмите на кнопку +.

   Откроется окно секрета.

2. Укажите значения для следующих параметров:

   a. **Название** – имя добавляемого секрета.

   b. **Тип** – **urls**.

      Значение установлено по умолчанию, его редактирование недоступно.

   c. **URL** – URL-адрес базы данных.

      Вам требуется учитывать, что для подключения к каждому типу базы данных используется свой формат URL-адреса.

      Доступные форматы URL-адресов:

      - Для SQLite:
        - `sqlite3://file:<file_path>`

        В качестве плейсхолдера используется знак вопроса: ?.

      - Для MsSQL:
        - `sqlserver://<user>:<password>@<server:port>/<instance_name>?database=<database>` (рекомендуется)
        - `sqlserver://<user>:<password>@<server>?database=<database>&encrypt=disable`

        В качестве плейсхолдера используются символы @p1.

      - Для MySQL:
        - `mysql://<user>:<password>@tcp(<server>:<port>)/<database>`

        В качестве плейсхолдера используются символы %s.

      - Для PostgreSQL:
        - `postgres://<user>:<password>@<server>/<database>?sslmode=disable`

        В качестве плейсхолдера используются символы $1.

      - Для Cockroach:
        - `postgres://<user>:<password>@<server>:<port>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Firebird:
  - `firebirdsql://<user>:<password>@<server>:<port>/<database>`

В качестве плейсхолдера используется знак вопроса: ?.

d. **Описание** – любая дополнительная информация.

3. При необходимости нажмите на кнопку **Добавить** и укажите дополнительный URL-адрес.

   В этом случае при недоступности одного URL-адреса приложение подключается к следующему URL-адресу, указанному в списке адресов.

4. Нажмите на кнопку **Сохранить**.

1. Нажмите на кнопку .

   Откроется окно секрета.

2. Укажите значения для параметров, которые требуется изменить.

   Вы можете изменить значения для следующих параметров:

   a. **Название** – имя добавляемого секрета.

   b. **URL** – URL-адрес базы данных.

      Вам требуется учитывать, что для подключения к каждому типу базы данных используется свой формат URL-адреса.

      Доступные форматы URL-адресов:

      - Для SQLite:
        - `sqlite3://file:<file_path>`

        В качестве плейсхолдера используется знак вопроса: ?.

      - Для MsSQL:
        - `sqlserver://<user>:<password>@<server:port>/<instance_name>?database=<database>` (рекомендуется)
        - `sqlserver://<user>:<password>@<server>?database=<database>&encrypt=disable`

        В качестве плейсхолдера используются символы @p1.

      - Для MySQL:
        - `mysql://<user>:<password>@tcp(<server>:<port>)/<database>`

        В качестве плейсхолдера используется символ `?`.

      - Для PostgreSQL:
        - `postgres://<user>:<password>@<server>/<database>?sslmode=disable`

        В качестве плейсхолдера используются символы $1.

      - Для Cockroach:
        - `postgres://<user>:<password>@<server>:<port>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Firebird:
  - `firebirdsql://<user>:<password>@<server>:<port>/<database>`

В качестве плейсхолдера используется знак вопроса: ?.

c. **Описание** – любая дополнительная информация.

3. При необходимости нажмите на кнопку **Добавить** и укажите дополнительный URL-адрес.

   В этом случае при недоступности одного URL-адреса приложение подключается к следующему URL-адресу, указанному в списке адресов.

4. Нажмите на кнопку **Сохранить**.

При создании подключений могут некорректно обрабатываться строки с учетными данными, содержащими специальные символы. Если при создании подключения возникает ошибка, но вы уверены в том, что значения параметров корректны, укажите специальные символы в процентной кодировке.

Коды специальных символов

!	#	$	%	&	'	(	)	*	+
%21	%23	%24	%25	%26	%27	%28	%29	%2A	%2B
,	/	:	;	=	?	@	[	]	\
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5D	%5C

Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.

- Поле для указания URL подключения. URL используется вместе с секретом типа "credentials". Поле доступно, если установлен флажок **Секрет отдельно**.

- **Секрет** – раскрывающийся список для выбора существующего секрета или создания секрета типа "credentials". Раскрывающийся список доступен, когда установлен флажок **Секрет отдельно**.

- **Авторизация** – тип авторизации при подключении к указанному URL. Доступны следующие значения:
  - **Выключена** – значение по умолчанию.
  - Если выбрано значение **Обычная**, вам нужно указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.
  - Если выбрано значение **PublicPKI**, необходимо указать секрет, содержащий закрытый ключ PEM в кодировке base64 и открытый ключ.

- Режим **TLS** – использование шифрования TLS. Доступные значения:

- Выключено – шифрование TLS не используется.
- Включено – шифрование используется, но без проверки сертификата.
- Нестандартный CA – используется шифрование с проверкой сертификата, который должен быть подписан центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке "Нестандартный CA", который отображается при выборе этого пункта.

  Создание сертификата, подписанного центром сертификации

  *Для использования этого режима **TLS** необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):*

  1. Создать ключ, который будет использоваться центром сертификации.

     Пример команды:

     ```
     openssl genrsa -out ca.key 2048
     ```

  2. Создать сертификат для только что созданного ключа.

     Пример команды:

     ```
     openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя устройства центра сертификации>" -out ca.crt
     ```

  3. Создать приватный ключ и запрос на его подписание в центре сертификации.

     Пример команды:

     ```
     openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя устройства сервера KUMA>" -out server.csr
     ```

  4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

     Пример команды:

     ```
     openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
     ```

  5. Полученный сертификат server.crt следует загрузить в Консоль KUMA в секрет типа **certificate**, который затем нужно выбрать в раскрывающемся списке **Нестандартный CA**.

  При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Столбец идентификатора** (обязательно) – название столбца, содержащего идентификатор для каждой строки таблицы.
- **Начальное значение идентификатора** (обязательно) – значение в столбце идентификатора, по которому будет определена строка, с которой требуется начать считывание данных из SQL-таблицы.
- **Запрос** – поле для дополнительного SQL-запроса. Запрос, указанный в этом поле, выполняется вместо запроса по умолчанию.
- **Период опроса, мс** – период выполнения SQL-запросов. Интервал, указанный в этом поле, используется вместо интервала, указанного по умолчанию для коннектора.

  Значение указывается в секундах. Значение по умолчанию – 10 секунд.

Для коннектора на вкладке **Дополнительные параметры** вам требуется задать значения следующих параметров:

- **Кодировка символов** – кодировка символов. Значение по умолчанию – `UTF-8`.

  KUMA конвертирует ответы SQL в кодировку UTF-8. Вы можете настроить SQL-сервер на отправку ответов в кодировке UTF-8 или выбрать их кодировку на стороне KUMA.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

В рамках одного коннектора вы можете **создать подключение** для нескольких поддерживаемых баз данных.

Чтобы создать подключение для нескольких баз данных SQL:

1. Нажмите на кнопку **Добавить подключение**.
2. Задайте значение для параметров **URL**, **Столбец идентификатора**, **Начальное значение идентификатора**, **Запрос**, **Интервал запросов, сек**.
3. Повторите шаги 1–2 для каждого требуемого подключения.

Если коллектор с коннектором типа sql не удается запустить, необходимо проверить, пуст ли state-файл /opt/kaspersky/kuma/collector/<идентификатор коллектора>/sql/state-<идентификатор файла>.

Если state-файл пуст, необходимо его удалить и выполнить перезапуск коллектора.

Поддерживаемые типы SQL и особенности их использования

Поддерживаются следующие типы SQL:

- MSSQL.

  Примеры URL:

  - `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}` – (рекомендуемый вариант)
  - `sqlserver://{user}:{password}@{server}?database={database}`

  В качестве плейсхолдера в SQL-запросе используются символы `@p1`.

  Если вам требуется подключиться с доменными учетными данными, укажите имя учетной записи в формате `<домен>%5C<пользователь>`. Например: `sqlserver://domain%5Cuser:password@ksc.example.com:1433/SQLEXPRESS?database=KAV`.

- MySQL.

  Пример URL: `mysql://{user}:{password}@tcp({server}:{port})/{database}`

  В качестве плейсхолдера в SQL-запросе используются символ `?`.

- PostgreSQL.

  Пример URL: `postgres://{user}:{password}@{server}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- CockroachDB.

  Пример URL: `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- SQLite3.

  Пример URL: `sqlite3://file:{file_path}`

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

  При обращении к SQLite3, если начальное значение идентификатора используется в формате datetime, в SQL-запрос нужно добавить преобразование даты с помощью функции sqlite datetime. Например, select * from connections where datetime(login_time) > datetime(?, 'utc') order by login_time. В этом примере `connections` – это таблица SQLite, а значение переменной `?` берется из поля **Начальное значение идентификатора**, и его следует указывать в формате {date}T{time}Z (например, - 2021-01-01T00:10:00Z).

- Oracle DB.

  Начиная с версии 2.1.3 KUMA использует новый драйвер для подключения к oracle. При обновлении KUMA переименует секрет для подключения в oracle-deprecated и коннектор продолжит работу. Если после запуска коллектора с типом драйвера oracle-deprecated не удается получить события, создайте новый секрет с драйвером oracle и используйте его для подключения.

  Рекомендуется использовать новый драйвер.

  Пример URL секрета с новым драйвером oracle:

  oracle://{user}:{password}@{server}:{port}/{service_name}

  oracle://{user}:{password}@{server}:{port}/?SID={SID_VALUE}

  Пример URL секрета с прежним драйвером oracle-deprecated:

  oracle-deprecated://{user}/{password}@{server}:{port}/{service_name}

  В качестве плейсхолдера в SQL-запросе используется переменная `:val`.

  При обращении к Oracle DB, если начальное значение идентификатора используется в формате datetime, нужно учитывать тип поля в самой базе данных и при необходимости добавить дополнительные преобразования строки со временем в запросе для обеспечения корректной работы sql коннектора. Например, если в базе создана таблица Connections, в которой есть поле login_time, возможны следующие преобразования:

  - Если у поля login_time тип TIMESTAMP, то в зависимости от настроек базы в поле login_time может лежать значение в формате YYYY-MM-DD HH24:MI:SS (например, 2021-01-01 00:00:00). Тогда в поле **Начальное значение идентификатора** следует указать значение 2021-01-01T00:00:00Z, а в запросе произвести преобразование с помощью функции to_timestamp. Например:

    ```
    select * from connections where login_time > to_timestamp(:val, 'YYYY-MM-DD"T"HH24:MI:SS"Z"')
    ```

  - Если у поля login_time тип TIMESTAMP WITH TIME ZONE, то в зависимости от настроек базы в поле login_time может лежать значение в формате YYYY-MM-DD"T"HH24:MI:SSTZH:TZM (например, 2021-01-01T00:00:00+03:00). Тогда в поле **Начальное значение идентификатора** следует указать значение 2021-01-01T00:00:00+03:00, а в запросе произвести преобразование с помощью функции to_timestamp_tz. Например:

    ```
    select * from connections_tz where login_time > to_timestamp_tz(:val, 'YYYY-MM-DD"T"HH24:MI:SSTZH:TZM')
    ```

    Подробнее о функциях to_timestamp и to_timestamp_tz см. в официальной документации Oracle.

  Для обращения к Oracle DB необходимо установить пакет Astra Linux libaio1.

- Firebird® SQL.

  Пример URL:

  `firebirdsql://{user}:{password}@{server}:{port}/{database}`

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

  Если возникает проблема подключения к firebird на Windows, используйте полный путь до файла с базой данных. Например:

  `firebirdsql://{user}:{password}@{server}:{port}/C:\Users\user\firebird\db.FDB`

- ClickHouse.

  Этот коннектор работает с ClickHouse только по TCP-порту 9000 по умолчанию без шифрования TLS и по порту 9440 по умолчанию в режиме TLS. Если на сервере ClickHouse настроен режим шифрования TLS и в коннекторе выбран режим "Выключено" (или наоборот), подключение с базой данных не устанавливается.

  Если вы хотите подключиться к KUMA ClickHouse, в параметрах коннектора SQL укажите тип секрета PublicPki, который содержит закрытый ключ PEM в кодировке base64 и открытый ключ.

  В параметрах SQL-коннектора для подключения ClickHouse необходимо указать режим **TLS**. Значение **Выключено** не разрешено, если для аутентификации используется сертификат. Если вы выбрали **Нестандартный CA**, в поле **Столбец идентификатора** укажите идентификатор секрета типа "certificate".

  Также нужно указать тип **Авторизации**:

  - Если указано значение **Выключено**, значение **Столбец идентификатора** не задано.
  - Тип **Обычная** используется, когда установлен флажок **Секрет отдельно** и идентификатор секрета типа "credentials" указан в поле **Столбец идентификатора**.
  - Тип **PublicPki** используется, когда установлен флажок **Секрет отдельно** и в поле **Столбец идентификатора** указан идентификатор секрета типа "PublicPki".

  Флажок **Секрет отдельно** позволяет указать URL отдельно, а не как часть секрета.

В SQL-запросах поддерживается последовательный запрос сведений из базы данных. Например, если в поле **Запрос** указать запрос `select * from <название таблицы с данными> where id > <плейсхолдер>`, то при первом обращении к таблице в качестве значения плейсхолдера будет использоваться значение поля **Начальное значение идентификатора**. При этом в сервисе, в котором используется SQL-коннектор, сохраняется идентификатор последней прочитанной записи, и во время следующего обращения к базе данных в качестве значения плейсхолдера в запросе будет использоваться идентификатор этой записи.

Примеры SQL-запросов

SQLite, Firebird – `select * from table_name where id > ?`

MsSQL – `select * from table_name where id > @p1`

MySQL – `select * from table_name where id > ?`

PostgreSQL, Cockroach – `select * from table_name where id > $1`

Oracle – `select * from table_name where id > :val`

Тип файла

Тип **file** используется для получения данных из любого текстового файла. Одна строка файла считается одним событием. Разделители между строк: \n. Этот тип коннектора доступен для агентов Linux и Windows.

Для чтения файлов Windows необходимо создать коннектор типа "file" и вручную установить агент на устройстве под управлением Windows. В одном Windows-агенте вы можете настроить несколько подключений разных типов, но должно быть только одно подключение типа "file". Windows-агент не должен читать свои файлы в папке, в которой установлен агент. Коннектор будет работать даже с файловой системой FAT. Если диск дефрагментирован, коннектор повторно считывает все файлы, поскольку все индексные дескрипторы файлов сбрасываются.

Не рекомендуется запускать агент под учетной записью администратора. Права на чтение для папок и файлов должны быть настроены для учетной записи пользователя агента. Не рекомендуется устанавливать агент на важные системы. Предпочтительнее отправлять журналы событий и читать их на выделенных устройствах с помощью агента.

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **file**.
  - **Путь к файлу** (обязательно) – полный путь к файлу, с которым требуется выполнять взаимодействие. Например, `/var/log/*som?[1-9].log or c:\folder\logs.*.` Следующие пути недопустимы:
    - `` `(?i)^[a-zA-Z]:\\Program Files` ``
    - `` `(?i)^[a-zA-Z]:\\Program Files \(x86\)` ``
    - `` `(?i)^[a-zA-Z]:\\Windows` ``
    - `` `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` ``

    Шаблоны масок для файлов и директорий

Маски:

- '*' – соответствует любой последовательности символов;
- '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
- '?' – соответствует любому одиночному символу.

Диапазоны символов:

- [0-9] – числа;
- [a-zA-Z] – буквы латинского алфавита.

Примеры:

- /var/log/*som?[1-9].log
- /mnt/dns_logs/*/dns.log
- /mnt/proxy/access*.log

Ограничения при использовании префиксов к путям файлов

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/

- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

Ограничение количества отслеживаемых файлов по маске

Количество одновременно отслеживаемых файлов по маске может быть ограничено параметром Ядра max_user_watches. Чтобы просмотреть значение параметра, выполните следующую команду:

```
cat /proc/sys/fs/inotify/max_user_watches
```

Если количество файлов для отслеживания превышает значение параметра max_user_watches, коллектор больше не сможет считывать события из файлов и в журнале коллектора появится следующая ошибка:

```
Failed to add files for watching {"error": "no space left on device"}
```

Чтобы коллектор продолжил корректно работать, вы можете настроить правильную ротацию файлов, чтобы количество файлов не превышало значение параметра max_user_watches, или увеличить значение max_user_watches.

Чтобы увеличить значение параметра:

```
sysctl fs.inotify.max_user_watches=<количество файлов>
```

```
sysctl -p
```

Также вы можете добавить значение параметра max_user_watches в sysctl.conf, чтобы значение сохранялось всегда.

После того, как вы увеличите значение параметра max_user_watches, коллектор успешно продолжит работу.

- **Auditd** – переключатель механизма, который группирует записи журнала событий auditd, полученные от коннектора, в одно событие. Auditd поддерживает только разделитель \n. Если переключатель включен, поле **Разделитель** недоступно. Если в коннекторе агента включен переключатель **Auditd**, в коннекторе коллектора, которому агент отправляет события, должен быть установлен разделитель \n.
- **Для Windows** – переключатель, который включает получение журнала событий Windows от Windows-агента. В этом случае переключатель **Auditd** должен быть выключен. По умолчанию переключатель **Для Windows** выключен.
- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:
  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.
  - **Размер буфера** – параметр, который позволяет указать размер буфера в байтах для накопления событий в оперативной памяти перед их отправкой на хранение или для дальнейшей обработки.

    Значение по умолчанию – 1 048 576 байт (1 МБ).

    Возможные значения: положительное целое число, меньшее или равное 67 108 864 байта (64 МБ).

- **Количество обработчиков** – параметр, который используется для задания количества служб, обрабатывающих очередь. Вы можете определить количество обработчиков по формуле: (<количество ядер процессора>/2)+2.

- **Период опроса, мс** – параметр, позволяющий установить период, по истечении которого коннектор повторно считывает директорию с файлами. Значение указано в миллисекундах. Коннектор ожидает указанное время, если в файле нет изменений. Если файл постоянно изменяется и интервал опроса равен 5000 миллисекунд, пятисекундный интервал для повторного чтения файлов в директории не соблюдается, а вместо этого они постоянно перечитываются. Если в файле нет изменений, коннектор ждет пять секунд. Если в веб-интерфейсе задано значение 0, используется значение по умолчанию – 700 мс. Рекомендуется установить значение для параметра **Период опроса** ниже значения параметра **TTL буфера событий**. Иначе это может отрицательно повлиять на параметр **Auditd**.

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – UTF-8.

- **TTL буфера событий** – время жизни буфера для группировки записей в одно событие auditd. Поле доступно, если переключатель **Auditd** включен. Обратный отсчет начинается с момента получения первой строки события или сразу после истечения предыдущего TTL. Возможные значения: от 700 мс до 3000 мс. По умолчанию указано значение 2000 мс.

- **Заголовок транспорта** – для событий auditd необходимо указать регулярное выражение, которое используется для определения частей журнала событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы record_type_name, record_type_value и event_sequence_number. Если многострочное событие auditd содержит префикс, то префикс сохраняется для первой записи, а для следующих записей префикс опускается.

  Вы можете вернуться к исходному значению, нажав на кнопку **Установить значение по умолчанию**.

Тип 1c-xml

Тип **1c-xml** используется для получения данных из журналов регистрации программы 1С. При обработке коннектором многострочные события преобразовываются в однострочные. Коннектор этого типа доступен для Linux-агентов.

При создании этого типа коннектора требуется указать значения для следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **1c-xml**.

  - **URL** (обязательно) – полный путь до директории с файлами, с которыми требуется выполнять взаимодействие. Например, `/var/log/1c/logs/`.

    Ограничения при использовании префиксов к путям файлов

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/

- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

  - **Размер буфера** – параметр, который позволяет указать размер буфера в байтах для накопления событий в оперативной памяти перед их отправкой на хранение или для дальнейшей обработки.

    Значение по умолчанию – 1 048 576 байт (1 МБ).

    Возможные значения: положительное целое число, меньшее или равное 67 108 864 байта (64 МБ).

  - **Интервал опроса, мс** – параметр, позволяющий установить интервал, с которым коннектор повторно считывает каталог с файлами. Значение указано в миллисекундах. Коннектор ожидает указанное время, если в файле нет изменений. Если файл постоянно изменяется и интервал опроса равен 5000 миллисекунд, пятисекундный интервал для повторного чтения файлов в директории не соблюдается, а вместо этого они постоянно перечитываются. Если в файле нет изменений, коннектор ждет пять секунд. Если в веб-интерфейсе задано значение 0, используется значение по умолчанию – 700 мс.

  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Схема работы коннектора:

1. Происходит поиск всех файлов с журналами 1С с расширением XML внутри указанной директории. Журналы помещаются в директорию или вручную, или через приложение, написанное на языке 1С, например, с помощью функции ВыгрузитьЖурналРегистрации(). Коннектор поддерживает журналы, полученные только таким образом. Подробнее о том, как получить журналы 1С, см. в официальной документации 1С.

2. Файлы отсортированы по времени последнего изменения в порядке возрастания. Все файлы, измененные перед последним чтением, сбрасываются.

   Сведения об обработанных файлах хранятся в файле /<рабочая директория коллектора>/1c_xml_connector/state.ini и имеют следующий формат: "offset=<число>\ndev=<число>\ninode=<число>".

3. В каждом непрочитанном файле определяются события.

4. События из файла принимаются на обработку по очереди. Многострочные события преобразовываются в однострочные события.

Ограничения коннектора:

- Установка коллектора с коннектором 1c-xml на ОС Windows не поддерживается. Чтобы обеспечить передачу файлов с журналами 1С для обработки коллектором KUMA, выполните следующие действия:

  1. На сервере Windows предоставьте доступ для чтения по сети к папке с журналами 1С.

  2. На сервере Linux примонтируйте сетевую папку с журналами 1С на сервере Linux (см. список поддерживаемых ОС).

3. На сервере Linux установите коллектор, который будет обрабатывать файлы с журналами 1С из примонтированной сетевой папки.

- Не читаются файлы с некорректным форматом событий. Например, если теги события в файле на русском языке, коллектор не прочитает такие события.

  Пример корректного XML файла с событием.

```
<?xml version="1.0" encoding="UTF-8"?>
<v8e:EventLog xmlns:v8e="http://v8.1c.ru/eventLog"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <v8e:Event>
                <v8e:Level>Information</v8e:Level>
                <v8e:Date>2022-12-07T01:55:44+03:00</v8e:Date>
                <v8e:ApplicationName>generator.go</v8e:ApplicationName>

<v8e:ApplicationPresentation>generator.go</v8e:ApplicationPresentation>
                <v8e:Event>Test event type: Count test</v8e:Event>
                <v8e:EventPresentation></v8e:EventPresentation>
                <v8e:User>abcd_1234</v8e:User>
                <v8e:UserName>TestUser</v8e:UserName>
                <v8e:Computer>Test OC</v8e:Computer>
                <v8e:Metadata></v8e:Metadata>
                <v8e:MetadataPresentation></v8e:MetadataPresentation>
                <v8e:Comment></v8e:Comment>
                <v8e:Data>
                        <v8e:Name></v8e:Name>
                        <v8e:CurrentOSUser></v8e:CurrentOSUser>
                </v8e:Data>
                <v8e:DataPresentation></v8e:DataPresentation>
                <v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus>
                <v8e:TransactionID></v8e:TransactionID>
                <v8e:Connection>0</v8e:Connection>
                <v8e:Session></v8e:Session>
                <v8e:ServerName>kuma-test</v8e:ServerName>
                <v8e:Port>80</v8e:Port>
                <v8e:SyncPort>0</v8e:SyncPort>
        </v8e:Event>
</v8e:EventLog>
```

  Пример обработанного события.

```
<v8e:Event><v8e:Level>Information</v8e:Level><v8e:Date>2022-12-
07T01:55:44+03:00</v8e:Date><v8e:ApplicationName>generator.go</v8e:ApplicationName><v8e:ApplicationPresentation>generator.go
</v8e:ApplicationPresentation><v8e:Event>Test event type: Count
test</v8e:Event><v8e:EventPresentation></v8e:EventPresentation><v8e:User>abcd_1234</v8e:User><v8e:UserName>TestUser</v8e:Use
rName><v8e:Computer>Test
OC</v8e:Computer><v8e:Metadata></v8e:Metadata><v8e:MetadataPresentation></v8e:MetadataPresentation><v8e:Comment></v8e:Commen
t><v8e:Data><v8e:Name></v8e:Name><v8e:CurrentOSUser></v8e:CurrentOSUser></v8e:Data><v8e:DataPresentation></v8e:DataPresentat
ion><v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus><v8e:TransactionID></v8e:TransactionID><v8e:Connection>0</v8
e:Connection><v8e:Session></v8e:Session><v8e:ServerName>kuma-
test</v8e:ServerName><v8e:Port>80</v8e:Port><v8e:SyncPort>0</v8e:SyncPort></v8e:Event>
```

- Если дополнить уже прочитанный коннектором файл новыми событиями и если этот файл не является последним прочитанным файлом в директории, все события из файла будут обработаны заново.

Тип 1c-log

Тип **1c-log** используется для получения данных из технологических журналов программы 1С. Разделители между строк: \n. Из многострочной записи о событии коннектор принимает только первую строку. Коннектор этого типа доступен для Linux-агентов.

При создании этого типа коннектора требуется указать значения для следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **1c-log**.
- **URL** (обязательно) – полный путь до директории с файлами, с которыми требуется выполнять взаимодействие. Например, `/var/log/1c/logs/`.

  Ограничения при использовании префиксов к путям файлов

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/

- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

  - **Размер буфера** – параметр, который позволяет указать размер буфера в байтах для накопления событий в оперативной памяти перед их отправкой на хранение или для дальнейшей обработки.

    Значение по умолчанию – 1 048 576 байт (1 МБ).

    Возможные значения: положительное целое число, меньшее или равное 67 108 864 байта (64 МБ).

  - **Интервал опроса, мс** – параметр, позволяющий установить интервал, с которым коннектор повторно считывает каталог с файлами. Значение указано в миллисекундах. Коннектор ожидает указанное время, если в файле нет изменений. Если файл постоянно изменяется и интервал опроса равен 5000 миллисекунд, пятисекундный интервал для повторного чтения файлов в директории не соблюдается, а вместо этого они постоянно перечитываются. Если в файле нет изменений, коннектор ждет пять секунд. Если в веб-интерфейсе задано значение 0, используется значение по умолчанию – 700 мс.

  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

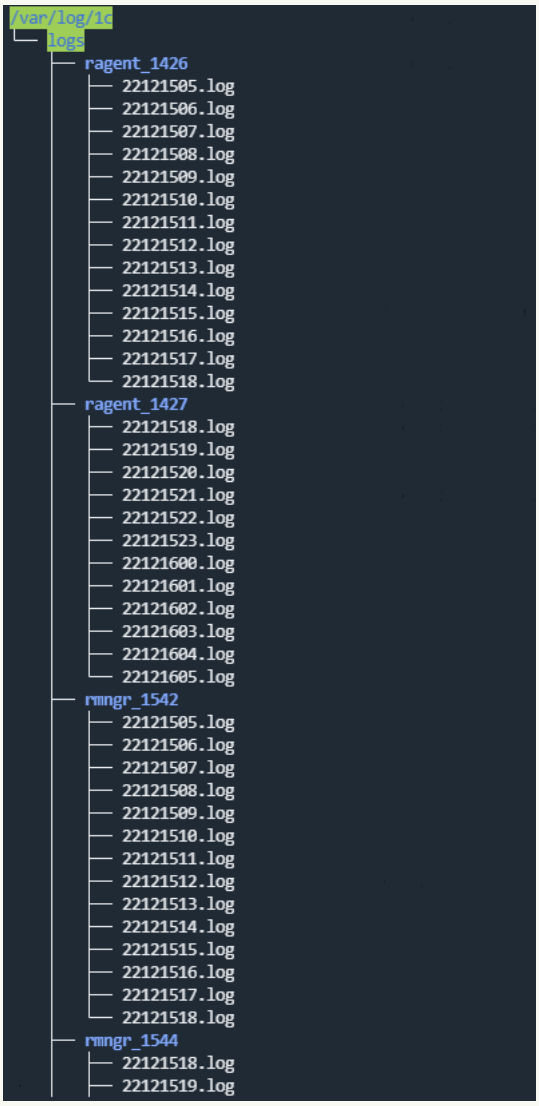
Схема работы коннектора:

1. Происходит поиск всех файлов технологических журналов 1С.

   Требования к файлам журналов:

   - Файлы с расширением LOG создаются в директории журналов (по умолчанию `/var/log/1c/logs/`) в поддиректории каждого процесса.

     Пример поддерживаемый структуры технологических журналов 1с



- События записываются в файл в течение часа, после чего создается следующий файл журнала.
- Название файлов имеет следующий формат: `<ГГ><ММ><ДД><ЧЧ>.log`. Например, `22111418.log` – файл, созданный в 2022 году, в 11 месяце, 14 числа в 18 часов.
- Каждое событие начинается с времени события в формате <мм>:<сс>.<микросекунды>-<длительность_в_микросекундах>.

2. Отбрасываются уже обработанные файлы.

   Сведения об обработанных файлах хранятся в файле /<рабочая директория коллектора>/1c_log_connector/state.json.

3. Принимаются на обработку новые события, при этом время события приводится к формату RFC3339.

4. Обрабатывается следующий в очереди файл.

Ограничения коннектора:

- Установка коллектора с коннектором 1c-log на ОС Windows не поддерживается. Чтобы обеспечить передачу файлов с журналами 1С для обработки коллектором KUMA, выполните следующие действия:

  1. На сервере Windows предоставьте доступ для чтения по сети к папке с журналами 1С.

2. На сервере Linux примонтируйте сетевую папку с журналами 1С на сервере Linux (см. список поддерживаемых ОС).

3. На сервере Linux установите коллектор, который будет обрабатывать файлы с журналами 1С из примонтированной сетевой папки.

- Из многострочной записи о событии на обработку принимается только первая строка.
- Нормализатор обрабатывает только следующие типы событий:
  - ADMIN
  - ATTN
  - CALL
  - CLSTR
  - CONN
  - DBMSSQL
  - DBMSSQLCONN
  - DBV8DBENG
  - EXCP
  - EXCPCNTX
  - HASP
  - LEAKS
  - LIC
  - MEM
  - PROC
  - SCALL
  - SCOM
  - SDBL
  - SESN
  - SINTEG
  - SRVC
  - TLOCK
  - TTIMEOUT

- VRSREQUEST
- VRSRESPONSE

Тип diode

Используется для передачи событий с помощью диода данных.

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **diode**.
  - **Директория с событиями от диода данных** (обязательно) – полный путь до директории на сервере коллектора KUMA, в которую диод данных перемещает файлы с событиями из изолированного сегмента сети. После считывания коннектором файлы удаляются из директории. Путь может содержать до 255 символов в кодировке Unicode.

    Ограничения при использовании префиксов к путям

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/

- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то по умолчанию используется значение: `\n`.

  Этот параметр должен совпадать для коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:

  - **Рабочие процессы** – количество служб, обрабатывающих очередь запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

  - **Интервал запросов, сек** – регулярность считывания файлов из директории с событиями от диода данных. По умолчанию указано значение 2. Значение указывается в секундах.

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

    Этот параметр должен совпадать для коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип ftp

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **ftp**.

  - **URL** (обязательно) – Действительный URL файла или маски файлов, который начинается со схемы 'ftp://'. Для маски файлов допустимо использование * ? [...].

    Шаблоны масок для файлов

Маски:

- '*' – соответствует любой последовательности символов;
- '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
- '?' – соответствует любому одиночному символу.

Диапазоны символов:

- [0-9] – числа;
- [a-zA-Z] – буквы латинского алфавита.

Примеры:

- /var/log/*som?[1-9].log
- /mnt/dns_logs/*/dns.log
- /mnt/proxy/access*.log

Если в URL не содержится порт ftp сервера, подставляется 21 порт.

- **Учетные данные для URL** – для указания логина и пароля к FTP серверу. При отсутствии логина и пароля строка остается пустой.
- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.
  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип nfs

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **nfs**.
- **URL** (обязательно) – путь до удаленной директории в формате nfs://host/path.
- **Маска имени файла** (обязательно) – маска, по которой фильтруются файлы с событиями. Допустимо использование масок "`*`", "`?`", "`[...]`".

- **Интервал запросов, сек.** – интервал опроса. Промежуток времени, через который перечитываются файлы с удаленной системы. Значение указывается в секундах. По умолчанию указано значение 0.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

Вкладка **Дополнительные параметры**:

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип vmware

При создании этого типа коннектора вам требуется указать значения следующих параметров:

Вкладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип коннектора, **vmware**.

- **URL** (обязательно) – URL, по которому доступен API VMware. В URL указывается устройство и порт. Может быть указан только один URL.

- **Учетные данные VMware** (обязательно) – секрет, где хранится логин и пароль для подключения к API VMware.

- **Время ожидания, сек** – время ожидания между запросом, который не вернул события, и новым запросом. Значение указывается в секундах. Значение по умолчанию – 5 секунд. Если значение равно 0, используется значение по умолчанию.

- **Количество запрашиваемых событий** – количество запрашиваемых событий из API VMware за один запрос. По умолчанию указано значение 100. Максимальное значение: 1000.

- **Начальная временная метка** – дата и время, начиная с которого события будут считываться из API VMware. По умолчанию: с момента запуска коллектора. При запуске после остановки коллектора, считывание событий будет происходить с последней сохраненной даты.

Вкладка **Дополнительные параметры**:

- **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – UTF-8.

- **Режим TLS** – режим шифрования TLS с использованием сертификатов в формате pem x509:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации сертификатов.

  - **Нестандартный CA** – при выборе этого варианта требуется добавить в коллектор секрет с сертификатом. Не самоподписанный сертификат. Сертификат сервера должен быть подписан

сертификатом, указанным в настройке коллектора.

- **Нестандартный CA** (обязательно, если для параметра Режим TLS выбрано значение Нестандартный CA) – секрет, где будет храниться сертификат.

Тип wmi

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **wmi**.
  - **URL** (обязательно) – URL создаваемого коллектора, например `kuma-collector.example.com:7221`.

    При создании коллектора для получения данных с помощью Windows Management Instrumentation автоматически создается агент, который будет получать необходимые данные на удаленном устройстве и перенаправлять их в сервис коллектора. В поле **URL** требуется указать адрес этого коллектора. URL-адрес известен заранее, если вы уже знаете, на каком сервере вы планируете установить службу. Это поле также можно заполнить после завершения работы мастера установки, скопировав данные URL в разделе **Ресурсы** → **Активные службы**.
  - **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.
  - **Учетные данные по умолчанию** – раскрывающийся список, в котором выбирать значение не требуется. Учетные данные для подключения к устройствам необходимо указывать в таблице **Удаленные устройства** (см. ниже).
  - В таблице **Удаленные устройства** перечисляются удаленные активы Windows, к которым требуется установить подключение. Доступные столбцы:
    - **Устройство** (обязательно) – IP-адрес или имя устройства, с которого необходимо принимать данные. Например, "machine-1".
    - **Домен** (обязательно) – название домена, в котором расположено удаленное устройство. Например, "example.com".
    - **Тип журналов** – раскрывающийся список для выбора названия журналов Windows, которые требуется получить. По умолчанию в списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами, введя их название в поле **Журналы Windows**, а затем нажав **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов.

      Журналы, доступные по умолчанию:
      - Application
      - ForwardedEvents
      - Security
      - Операционная система

- HardwareEvents

Если в одном из подключений WMI используется хотя бы один журнал с неверным названием, в этом случае агент, использующий коннектор, не будет получать события из всех журналов данного подключения, даже если названия остальных журналов указаны верно. При этом подключения WMI-агента, в которых все названия журналов указаны правильно, будет работать корректно.

- **Секрет** – учетные данные для доступа к удаленному активу Windows с правами на чтение журналов. Если оставить это поле пустым, то будут использоваться учетные данные из секрета, выбранного в раскрывающемся списке **Учетные данные, используемые по умолчанию**. Учетная запись в секрете должна быть указана без домена. Значение домена для доступа к устройству берется из столбца **Домен** таблицы **Удаленные устройства**.

  Вы можете выбрать ресурс секрета в раскрывающемся списке или создать его, нажав на кнопку +. Выбранный секрет можно изменить, нажав на кнопку ✎.

- Вкладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Получение событий с удаленного устройства

Условия для получения событий с удаленного устройства Windows с агентом KUMA:

- Для запуска агента KUMA на удаленном устройстве необходимо использовать учетную запись с правами Log on as a service.

- Для получения событий от агента KUMA необходимо использовать учетную запись с правами Event Log Readers. Для серверов домена может быть создана одна такая учетная запись, чтобы через групповую политику ее права на чтение логов можно было распространить на все серверы и рабочие станции домена.

- На удаленных устройствах Windows необходимо открыть следующие TCP-порты 135, 445, 49152-65535.

- На удаленных устройствах требуется запустить следующие службы:

  - Remote Procedure Call (RPC)

  - RPC Endpoint Mapper

Тип wec

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип коннектора, **wec**.
- **URL** (обязательно) – URL создаваемого коллектора, например `kuma-collector.example.com:7221`.

  При создании коллектора для получения данных с помощью Windows Event Collector автоматически создается агент, который будет получать необходимые данные на удаленном устройстве и перенаправлять их в сервис коллектора. В поле **URL** требуется указать адрес этого коллектора. URL-адрес известен заранее, если вы уже знаете, на каком сервере вы планируете установить службу. Это поле также можно заполнить после завершения работы мастера установки, скопировав данные URL в разделе **Ресурсы** → **Активные службы**.
- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.
- **Журналы Windows** (обязательно) – в этом раскрывающемся списке необходимо выбрать названия журналов Windows, которые требуется получить. По умолчанию в списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами, введя их название в поле **Журналы Windows**, а затем нажав **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов.

  Преднастроенные журналы:

  - Application
  - ForwardedEvents
  - Security
  - Операционная система
  - HardwareEvents

  Если неверно указать название хотя бы одного журнала, в этом случае агент, использующий коннектор, не будет получать события из всех журналов, даже если названия остальных журналов указаны верно.

- Вкладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.
  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Для запуска агента KUMA на удаленном устройстве необходимо использовать сервисную учетную запись с правами Log on as a service. Для получения событий из журнала ОС сервисная учетная запись также должна обладать правами Event Log Readers.

Вы можете создать одну учетную запись с правами Log on as a service и Event Log Readers, а затем права этой учетной записи на чтение журналов распространить на все серверы и рабочие станции домена с помощью групповой политики.

Мы рекомендуем запретить для сервисной учетной записи возможность интерактивного входа.

Тип snmp

Для обработки событий, полученных по SNMP, необходимо использовать нормализатор типа json.

Доступен для Windows- и Linux-агентов. Поддерживаемые версии протокола:

- snmpV1
- snmpV2
- snmpV3

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **snmp**.
  - **Версия SNMP** (обязательно) – в этом раскрывающемся списке можно выбрать версию используемого протокола.
  - **Устройство** (обязательно) – имя устройства или его IP-адрес. Доступные форматы: hostname, IPv4, IPv6.
  - **Порт** (обязательно) – порт для подключения к устройству. Обычно используются значения 161 или 162.

  С помощью параметров **Версия SNMP**, **Устройство** и **Порт** определяется одно подключение к SNMP-ресурсу. Вы можете создать несколько таких соединений в одном коннекторе, добавив новые с помощью кнопки **SNMP-ресурс**. Удалить соединения можно, нажав на кнопку .
  - **Секрет** (обязательно) – раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения через Simple Network Management Protocol. Тип секрета должен соответствовать версии SNMP. При необходимости секрет можно создать в окне создания коннектора, нажав на кнопку . Выбранный секрет можно изменить, нажав на кнопку .
  - **Данные источника** – это таблица, где можно задать правила именования получаемых данных, по которым идентификаторы объектов (OID) будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные столбцы таблицы:
    - **Название параметра** (обязательно) – произвольное название для типа данных. Например, "Имя узла" или "Время работы узла".
    - **OID** (обязательно) – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий. Например, "1.3.6.1.2.1.1.5".
    - **Ключ** (обязательно) – уникальный идентификатор, возвращается в ответ на запрос к активу со значением запрошенного параметра. Например, "sysName". К этому ключу можно обращаться при нормализации данных.
    - **MAC-адрес** – если эта функция включена, KUMA правильно декодирует данные, в которых OID содержит информацию об MAC-адресе в формате OctetString. После декодирования MAC-адрес преобразуется в строковое значение формата XX:XX:XX:XX:XX:XX.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`.

  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Тип snmp-trap

Коннектор типа **snmp-trap** используется в агентах и коллекторах для пассивного приема SNMP-Trap сообщений. В коннекторе сообщения принимаются и подготавливаются к нормализации путем сопоставления идентификаторов SNMP-объектов с временными ключами. Затем сообщение необходимо передать в JSON-нормализатор, где временные ключи будут сопоставлены с полями KUMA и будет создано событие.

Для обработки событий, полученных по SNMP, необходимо использовать нормализатор типа json.

Доступен для Windows- и Linux-агентов. Поддерживаемые версии протокола:

- snmpV1

- snmpV2

При создании этого типа коннектора вам требуется указать значения следующих параметров:

- Вкладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **snmp-trap**.

  - **Версия SNMP** (обязательно) – в этом раскрывающемся списке необходимо выбрать версию используемого протокола: **snmpV1** или **snmpV2**.

    Например, Windows по умолчанию использует версию **snmpV2**.

  - **URL** (обязательно) – URL, на котором будут ожидаться сообщения SNMP Trap. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

  С помощью параметров **Версия SNMP** и **URL** определяется одно соединение для приема событий SNMP Trap. Таких соединений в одном коннекторе можно создать несколько, добавляя новые с помощью кнопки **SNMP-ресурс**. Удалить соединения можно, нажав на кнопку ✕.

  - **Данные источника** – это таблица, где можно задать правила именования получаемых данных, по которым идентификаторы объектов (OID) будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор.

С помощью кнопки **Применить значения OID для WinEventLog** таблицу можно заполнить сопоставлениями для значений OID, поступающих в журналах WinEventLog. Если в поступающих событиях необходимо определить и нормализовать больше данных, дополните таблицу строками с перечнем OID-объектов и их ключей.

Доступные столбцы таблицы:

- **Название параметра** – произвольное название для типа данных. Например, "`Имя узла`" или "`Время работы узла`".
- **OID** (обязательно) – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий. Например, "`1.3.6.1.2.1.1.1`".
- **Ключ** (обязательно) – уникальный идентификатор, возвращается в ответ на запрос к активу со значением запрошенного параметра. Например, "`sysDescr`". К этому ключу можно обращаться при нормализации данных.
- **MAC-адрес** – если эта функция включена, KUMA правильно декодирует данные, в которых OID содержит информацию об MAC-адресе в формате OctetString. После декодирования MAC-адрес преобразуется в строковое значение формата XX:XX:XX:XX:XX:XX.

Данные обрабатываются по принципу списка разрешенных: объекты, которые не указаны в таблице, не будут переданы в нормализатор для дальнейшей обработки.

- **Описание** – описание ресурса: до 4000 символов в кодировке Unicode.

- Вкладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию – `UTF-8`. При получении snmp-trap событий из Windows с русской локализацией мы рекомендуем изменить кодировку символов в коннекторе типа snmp-trap на Windows 1251, если в событии получены недопустимые символы.
  - **Отладка** – переключатель, с помощью которого можно указать, будет ли включено логирование ресурса. По умолчанию положение **Выключено**.

Настройка источника SNMP-trap сообщений для Windows
Настройка устройства Windows для отправки SNMP-trap сообщений в коллектор KUMA происходит в несколько этапов:

1. Настройка и запуск служб SNMP и SNMP Trap
2. Настройка службы Event to Trap Translator

События от источника SNMP-trap сообщений должен принимать коллектор KUMA, в котором используется коннектор типа snmp-trap и нормализатор типа json.

Настройка и запуск служб SNMP и SNMP Trap
Чтобы настроить и запустить службы SNMP и SNMP Trap в Windows 10:

1. Откройте раздел **Settings** → **Apps** → **Apps and features** → **Optional features** → **Add feature** → **Simple Network Management Protocol (SNMP)** и нажмите **Install**.
2. Дождитесь завершения установки и перезагрузите компьютер.
3. Убедитесь, что служба SNMP запущена. Если какие-то из перечисленных ниже служб не запущены, включите их:

- **Services** → **SNMP Service**.
- **Services** → **SNMP Trap**.

4. Нажмите правой кнопкой мыши **Сервисы** → **SNMP-службы** и в контекстном меню выберите **Свойства**. Задайте следующие параметры:
   - На вкладке **Log On** установите флажок **Local System account**.
   - На вкладке **Agent** заполните поля **Contact** (например, укажите `User-win10`) и Location (например, укажите `ekaterinburg`).
   - На вкладке **Traps**:
     - В поле **Community Name** введите **community public** и нажмите **Add to list**.
     - В поле **Trap destination** нажмите **Add**, укажите IP-адрес или устройство сервера KUMA, на котором развернут коллектор, ожидающий SNMP-события, и нажмите **Add**.
   - На вкладке **Security**:
     - Установите флажок **Send authentication trap**.
     - В таблице **Accepted community names** нажмите **Add**, а затем введите **Community Name public**, указав в качестве **Community rights** значение **READ WRITE**.
     - Установите флажок **Accept SNMP packets from any hosts**.
5. Нажмите **Apply** и подтвердите выбор.
6. Нажмите правой кнопкой мыши на службу **Services** → **SNMP Service** и выберите **Restart**.

Чтобы настроить и запустить службы SNMP и SNMP Trap в Windows XP:

1. Откройте раздел **Start** → **Control Panel** → **Add or Remove Programs** → **Add/Remove Windows Components** → **Management and Monitoring Tools** → **Details**.
2. Выберите **Simple Network Management Protocol** и **WMI SNMP Provider**, затем нажмите **OK** → **Next**.
3. Дождитесь завершения установки и перезагрузите компьютер.
4. Убедитесь, что служба SNMP запущена. Если какие-то из перечисленных ниже служб не запущены, включите их, выбрав для параметра **Startup type** значение **Automatic**:
   - **Services** → **SNMP Service**.
   - **Services** → **SNMP Trap**.
5. Нажмите правой кнопкой мыши **Сервисы** → **SNMP-службы** и в контекстном меню выберите **Свойства**. Задайте следующие параметры:
   - На вкладке **Log On** установите флажок **Local System account**.
   - На вкладке **Agent** заполните поля **Contact** (например, укажите `User-win10`) и Location (например, укажите `ekaterinburg`).

- На вкладке **Traps**:
  - В поле **Community Name** введите **community public** и нажмите **Add to list**.
  - В поле **Trap destination** нажмите **Add**, укажите IP-адрес или устройство сервера KUMA, на котором развернут коллектор, ожидающий SNMP-события, и нажмите **Add**.
- На вкладке **Security**:
  - Установите флажок **Send authentication trap**.
  - В таблице **Accepted community names** нажмите **Add**, а затем введите **Community Name public**, указав в качестве **Community rights** значение **READ WRITE**.
  - Установите флажок **Accept SNMP packets from any hosts**.

6. Нажмите **Apply** и подтвердите выбор.
7. Нажмите правой кнопкой мыши на службу **Services** → **SNMP Service** и выберите **Restart**.

Изменение порта службы snmptrap

При необходимости вы можете изменить порт службы snmptrap.

Чтобы изменить порт службы snmptrap:

1. Откройте папку C:\Windows\System32\drivers\etc.
2. Откройте файл **services** с помощью приложения Notepad от имени администратора.
3. В разделе файла **service name** для службы **snmptrap** укажите порт коннектора snmp-trap, добавленный в коллектор KUMA.
4. Сохраните файл.
5. Откройте панель управления и выберите **Administrative Tools** → **Services**.
6. Нажмите на службу **SNMP Service** правой кнопкой мыши и выберите **Restart**.

Настройка службы Event to Trap Translator
Чтобы настроить службу Event to Trap Translator, с помощью которой события Windows переводятся в SNMP-trap сообщения:

1. Наберите в командной строке `evntwin` и нажмите **Enter**.
2. В переключателе **Configuration type** выберите **Custom**, а затем нажмите на кнопку **Edit**.
3. В блоке параметров **Источники событий** нажмите на кнопку **Добавить**, найдите и добавьте события, которые вы хотите отправить в коллектор KUMA с установленным коннектором SNMP Trap.
4. Нажмите на кнопку **Settings**, в открывшемся окне установите флажок **Don't apply throttle** и нажмите **OK**.
5. Нажмите **Apply** и подтвердите выбор.

Предустановленные коннекторы

В поставку OSMP включены перечисленные в таблице ниже коннекторы.

Предустановленные коннекторы

Название коннектора	Комментарий
[OOTB] Continent SQL	Получает события из СУБД АПКШ Континент. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] InfoWatch Trafic Monitor SQL	Получает события из СУБД системы InfoWatch Trafic Monitor. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC MSSQL	Получает события из СУБД MS SQL приложения Kaspersky Security Center. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC MySQL	Получает события из СУБД MySQL приложения Kaspersky Security Center. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC PostgreSQL	Получает события из СУБД PostgreSQL приложения Kaspersky Security Center версии 15.0. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Oracle Audit Trail SQL	Получает события аудита из СУБД Oracle. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] SecretNet SQL	Получает события из СУБД системы SecretNet SQL. Для использования необходимо настроить параметры соответствующего типа секрета.

Секреты

Секреты используются для безопасного хранения конфиденциальной информации, такой как логины и пароли, которые должны использоваться KUMA для взаимодействия с внешними службами. Если секрет хранит данные учетной записи, такие как логин и пароль, то при подключении коллектора к источнику событий учетная запись пользователя, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

Секреты можно использовать в следующих сервисах и функциях KUMA:

- Коллектор (при использовании шифрования TLS).
- Коннектор (при использовании шифрования TLS).
- Точки назначения (при использовании шифрования TLS или авторизации).
- Прокси-серверы.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Имя должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип секрета.

  При выборе в раскрывающемся списке типа секрета отображаются параметры для настройки выбранного типа секрета. Эти параметры описаны ниже.
- **Описание** – вы можете добавить до 4000 символов в кодировке Unicode.

В зависимости от типа секрета доступны различные поля для заполнения. Вы можете выбрать один из следующих типов секрета:

- **credentials** – тип секрета используется для хранения данных учетных записей, с помощью которых осуществляется подключение к внешним службам, например к SMTP-серверам. При выборе этого типа секрета требуется заполнить поля **Пользователь** и **Пароль**. При использовании в ресурсе **Секрет** типа credentials для подключения коллектора к источнику событий, например СУБД, учетная запись пользователя, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

- **token** – тип секрета используется для хранения токенов для API-запросов. Токены используются, например, при подключении к IRP-системам. При выборе этого типа секрета требуется заполнить поле **Токен**.

- **ktl** – тип секрета используется для хранения данных учетной записи Kaspersky Threat Intelligence Portal. При выборе этого типа секрета требуется заполнить следующие поля:

  - **Пользователь** и **Пароль** (обязательные поля) – имя пользователя и пароль вашей учетной записи Kaspersky Threat Intelligence Portal.

  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – позволяет загрузить ключ сертификата Kaspersky Threat Intelligence Portal.

  - **Пароль PFX-файла** (обязательно) – пароль для доступа к ключу сертификата Kaspersky Threat Intelligence Portal.

- **urls** – тип секрета используется для хранения URL для подключения к базам SQL и прокси-серверам. В поле **Описание** требуется описать, для какого именно подключения вы используете секрет **urls**.

  Вы можете указать URL в следующих форматах: hostname:port, IPv4:port, IPv6:port, :port.

- **pfx** – тип секрета используется для импорта PFX-файла с сертификатами. При выборе этого типа секрета требуется заполнить следующие поля:

  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – используется для загрузки PFX-файла. Файл должен содержать сертификат и ключ. В PFX-файлы можно включать сертификаты, подписанными центрами сертификации, для проверки сертификатов сервера.

  - **Пароль PFX-файла** (обязательно) – используется для ввода пароля для доступа к ключу сертификата.

- **kata/edr** – тип секрета используется для хранения файла сертификата и закрытого ключа, требуемых при подключении к серверу Kaspersky Endpoint Detection and Response. При выборе этого типа секрета вам требуется загрузить следующие файлы:

  - Файл сертификата – сертификат сервера KUMA.

    Файл должен иметь формат PEM. Вы можете загрузить только один файл сертификата.

  - Закрытый ключ шифрования соединения – RSA-ключ сервера KUMA.

    Ключ должен быть без пароля и с заголовком PRIVATE KEY. Вы можете загрузить только один файл ключа.

    Вы можете сгенерировать файлы сертификата и ключа по кнопке ⭳.

- **snmpV1** – тип секрета используется для хранения значения **Уровень доступа** (например, `public` или `private`), которое требуется при взаимодействии по протоколу Simple Network Management Protocol.

- **snmpV3** – тип секрета используется для хранения данных, требуемых при взаимодействии по протоколу Simple Network Management Protocol. При выборе этого типа секрета требуется заполнить следующие поля:

- **Пользователь** – имя пользователя, указывается без домена.
- **Уровень безопасности** – уровень безопасности пользователя:
  - **NoAuthNoPriv** – сообщения отправляются без аутентификации и без обеспечения конфиденциальности.
  - **AuthNoPriv** – сообщения посылаются с аутентификацией, но без обеспечения конфиденциальности.
  - **AuthPriv** – сообщения посылаются с аутентификацией и обеспечением конфиденциальности.

  В зависимости от выбранного уровня могут отобразиться дополнительные параметры.
- **Пароль** – пароль аутентификации пользователя SNMP. Это поле становится доступно при выборе уровней безопасности **AuthNoPriv** и **AuthPriv**.
- **Протокол аутентификации** – доступны следующие протоколы: MD5, SHA, SHA224, SHA256, SHA384, SHA512. Это поле становится доступно при выборе уровней безопасности **AuthNoPriv** и **AuthPriv**.
- **Протокол шифрования** – протокол, используемый для шифрования сообщений. Доступны следующие протоколы: DES, AES. Это поле становится доступно при выборе уровня безопасности **AuthPriv**.
- **Пароль обеспечения безопасности** – пароль шифрования, который был указан при создании пользователя SNMP. Это поле становится доступно при выборе уровня безопасности **AuthPriv**.

- **certificate** – тип секрета используется для хранения файлов сертификатов. Файлы загружаются в ресурс с помощью кнопки **Загрузить файл сертификата**. Поддерживаются открытые ключи сертификата X.509 в Base64.

Предустановленные секреты

В поставку OSMP включены перечисленные в таблице ниже секреты.

Предустановленные секреты

Название секрета	Описание
[OOTB] Continent SQL connection	Хранит конфиденциальные данные и параметры подключения к БД АПКШ Континент. Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MSSQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL Kaspersky Security Center (KSC). Для использования необходимо указать логин и пароль БД.
[OOTB] KSC MySQL Connection	Хранит конфиденциальные данные и параметры подключения к БД MySQL Kaspersky Security Center (KSC). Для использования необходимо указать логин и пароль БД.
[OOTB] Oracle Audit Trail SQL Connection	Хранит конфиденциальные данные и параметры подключения к БД Oracle. Для использования необходимо указать логин и пароль БД.
[OOTB] SecretNet SQL connection	Хранит конфиденциальные данные и параметры подключения к БД MS SQL системы SecretNet. Для использования необходимо указать логин и пароль БД.

Контекстные таблицы

Контекстная таблица – это контейнер для массива данных, которые используются коррелляторами KUMA при анализе событий по правилам корреляции. Вы можете создать контекстные таблицы в разделе **Ресурсы**. Данные контекстной таблицы хранятся только в коррелляторе, в который она была добавлена с помощью фильтров или действий в корреляционных правилах.

Вы можете наполнять контекстные таблицы автоматически с помощью корреляционных правил типа simple и operational или импортировать файл с данными для контекстной таблицы.

Вы можете добавлять, копировать и удалять контекстные таблицы, а также изменять их настройки.

Контекстные таблицы можно использовать в следующих сервисах и функциях KUMA:

- Правила корреляции.
- Панель мониторинга.

Одна и та же контекстная таблица может использоваться в разных коррелляторах. При этом для каждого коррелятора создается своя сущность контекстной таблицы. Таким образом, содержимое контекстных таблиц, используемых разными коррелляторами, различается, даже если идентификатор и название контекстных таблиц одинаковые.

В контекстную таблицу добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, удалять, импортировать и экспортировать записи в контекстной таблице коррелятора.

В процессе корреляции при удалении записей из контекстных таблиц в коррелляторах создаются служебные события. Эти события существуют только в коррелляторах, они не перенаправляются в другие точки назначения. Служебные события отправляются на обработку правилами корреляции того коррелятора, где работает контекстная таблица. Правила корреляции можно настроить на отслеживание этих событий, чтобы с их помощью распознавать угрозы.

Поля служебных событий удаления записи из контекстной таблицы описаны ниже.

Поле события	Значение или комментарий
`ID`	Идентификатор события.
`Timestamp`	Время удаления записи, срок жизни которой истек.
`Name`	`"context table record expired"`
`DeviceVendor`	`"Лаборатория Касперского".`
`DeviceProduct`	`"KUMA"`
`ServiceID`	Идентификатор коррелятора.
`ServiceName`	Название коррелятора.
`DeviceExternalID`	Идентификатор контекстной таблицы.
`DevicePayloadID`	Ключ записи, срок жизни которой истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи.
`FileName`	Название контекстной таблицы.

`S.<поле контекстной таблицы>`
`SA.<поле контекстной таблицы>`
`N.<поле контекстной таблицы>`
	В зависимости от типа записи, выпавшей из контекстной таблицы, запись записывается в соответствующий тип события:
	Например, `S.<поле контекстной таблицы>=<значение поля контекстной таблицы>`.
	`SA.<поле контекстной таблицы>=<массив значений поля контекстной таблицы>`
	
	Записи контекстной таблицы логического типа имеют следующий формат:

NA.< поле контекстной таблицы > F.< поле контекстной таблицы > FA.< поле контекстной таблицы >	S.<поле контекстной таблицы> = true/false SA.<поле контекстной таблицы> = false,true,false

Просмотр списка контекстных таблиц

Чтобы просмотреть список контекстных таблиц коррелятора:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, для которого вы хотите просмотреть контекстные таблицы, выберите пункт **Смотреть контекстные таблицы**.

   Отобразится список **Контекстные таблицы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя контекстной таблицы.
- **Размер на диске** – размер контекстной таблицы.
- **Директория** – путь к контекстной таблице на сервере коррелятора KUMA.

Добавление контекстной таблицы

Чтобы добавить контекстную таблицу:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. В окне **Контекстные таблицы** нажмите на кнопку **Добавить**.

   Откроется окно **Создание контекстной таблицы**.
4. В поле **Название** введите имя контекстной таблицы.
5. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
6. В поле **Срок жизни** укажите время, в течение которого в контекстной таблице будет храниться добавленная в него запись.

   По истечении указанного времени запись удаляется. Время указывается в секундах. Максимальное значение – `31536000` (1 год).

   По умолчанию указано значение `0`. Если в поле указано значение 0, время хранения записи неограничено.
7. В поле **Описание** укажите любую дополнительную информацию.

   Вы можете использовать до 4000 символов в кодировке Unicode.

   Поле не является обязательным.
8. В разделе **Схема** укажите состав полей контекстной таблицы и тип данных полей.

В зависимости от типа данных поле может быть или не быть ключевым. Хотя бы одно поле в таблице должно быть ключевым полем. Имена всех полей должны быть уникальными.

Для добавления строки таблицы нажмите на кнопку **Добавить** и заполните поля таблицы:

a. В поле **Название** введите название поля. Максимальная длина – 128 символов.

b. В раскрывающемся списке **Тип** выберите тип данных поля.

Возможные типы данных поля

Возможные типы данных поля контекстной таблицы

Тип данных поля	Может быть ключевым полем	Комментарий
Целое число	Да	—
Число с плавающей точкой	Да	—
Строка	Да	—
Логический оператор	Да	—
Timestamp	Да	Для поля этого типа проверяется, что значение поля больше или равно нулю. Другие операции не предусмотрены.
IP-адрес	Да	Для поля этого типа проверяется, что значение поля соответствует формату IPv4, IPv6. Другие операции не предусмотрены.
Список целых чисел	Нет	—
Список чисел с плавающей точкой	Нет	—
Список строк	Нет	—
Список логических типов	Нет	—
Список временных меток	Нет	Для поля этого типа проверяется, что каждый элемент списка больше или равен нулю. Другие операции не предусмотрены.
Список IP-адресов	Нет	Для поля этого типа проверяется, что каждый элемент списка соответствует формату IPv4, IPv6. Другие операции не предусмотрены.

c. Если вы хотите сделать поле ключевым, установите флажок **Ключевое поле**.

В таблице может быть несколько ключевых полей. Ключевые поля задаются при создании контекстной таблицы, уникально идентифицируют запись таблицы и не могут изменяться.

Если ключевых полей в контекстной таблице несколько, каждая запись таблицы уникально идентифицируется несколькими полями (составной ключ).

9. Добавьте нужное количество строк контекстной таблицы.

После сохранения контекстной таблицы схему поменять нельзя.

10. Нажмите на кнопку **Сохранить**.

Контекстная таблица будет добавлена.

Просмотр параметров контекстной таблицы

Чтобы просмотреть параметры контекстной таблицы:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. В окне **Контекстные таблицы** в списке выберите контекстную таблицу, параметры которой вы хотите просмотреть.

Откроется окно с параметрами контекстной таблицы. В нем отображается следующая информация:

- **Название** – уникальное имя ресурса.
- **Тенант** – название тенанта, которому принадлежит ресурс.
- **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Значение указывается в секундах.
- **Описание** – любая дополнительная информация о ресурсе.
- **Схема** – упорядоченный список полей и их типов данных с отметкой ключевых полей.

Изменение параметров контекстной таблицы

Чтобы изменить параметры контекстной таблицы:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. В окне **Контекстные таблицы** в списке выберите контекстную таблицу, параметры которой вы хотите изменить.
4. Укажите значения для следующих параметров:
   - **Название** – уникальное имя ресурса.
   - **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Значение указывается в секундах.
   - **Описание** – любая дополнительная информация о ресурсе.
   - **Схема** – упорядоченный список полей и их типов данных с отметкой ключевых полей. Если контекстная таблица не используется в корреляционном правиле, вы можете поменять состав полей.

     Если вы хотите изменить схему в контекстной таблице, которая уже используется в корреляционном правиле, выполните шаги инструкции ниже.

   Поле **Тенант** недоступно для редактирования.
5. Нажмите на кнопку **Сохранить**.

Чтобы изменить параметры контекстной таблицы, ранее используемой коррелятором:

1. Выполните экспорт данных из таблицы.
2. Скопируйте и сохраните путь к файлу с данными таблицы на диске коррелятора. Путь указан в столбце **Директория** в окне **Контекстные таблицы коррелятора**. Этот путь понадобится вам в дальнейшем для удаления файла с диска коррелятора.

3. Удалите из коррелятора контекстную таблицу.
4. Измените необходимые параметры контекстной таблицы.
5. Удалите файл с данными таблицы на диске коррелятора по пути из шага 2.
6. Добавьте в коррелятор контекстную таблицу, в которой вы изменили параметры.
7. Перезапустите коррелятор: в разделе **Ресурсы** → **Активные сервисы** в списке сервисов установите флажок рядом с нужным коррелятором, на панели инструментов нажмите на значок с тремя точками и в открывшемся меню выберите **Перезапустить**.
8. Адаптируйте в экспортированной таблице (см. шаг 1) поля, чтобы они соответствовали полям таблицы, которую вы загрузили в коррелятор на шаге 6.
9. Импортируйте адаптированные данные в контекстную таблицу.

Дублирование параметров контекстной таблицы

Чтобы скопировать контекстную таблицу:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. Установите флажок рядом с контекстной таблицей, которую вы хотите копировать.
4. Нажмите на кнопку **Дублировать**.
5. Укажите нужные вам параметры.
6. Нажмите на кнопку **Сохранить**.

Контекстная таблица будет скопирована.

Удаление контекстной таблицы

Вы можете удалить только те контекстные таблицы, которые не используются ни в одном в корреляторе.

Чтобы удалить контекстную таблицу:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Контекстные таблицы**.
3. Установите флажки рядом с контекстными таблицами, которые вы хотите удалить.

   Если вы хотите удалить все контекстные таблицы, установите флажок рядом со столбцом **Название**.

   > Должен быть установлен хотя бы один флажок.

4. Нажмите на кнопку **Удалить**.
5. Нажмите на кнопку **ОК**.

Контекстные таблицы будут удалены.

Просмотр записей контекстной таблицы

Чтобы просмотреть список записей контекстной таблицы:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, контекстную таблицу которого вы хотите просмотреть, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
4. В столбце **Название** выберите нужную контекстную таблицу.

Откроется список записей для выбранной контекстной таблицы.

Список содержит следующие данные:

- **Ключ** – композитный ключ записи. Формируется из одного и более значений ключевых полей, разделенных символом "|". Если одно из значений ключевого поля отсутствует, то разделяющий символ все равно отображается.

  Например, ключ записи состоит из трех полей: `DestinationAddress`, `DestinationPort`, `SourceUserName`. При отсутствии значений в последних двух полях ключ записи будет отображаться следующим образом: `43.65.76.98| | `.
- **Повторы записи** – общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте контекстных таблиц в KUMA.
- **Срок действия** – дата и время, когда запись должна быть удалена.

  Если при создании контекстной таблицы в поле **Срок жизни** было указано значение 0, записи этой контекстной таблицы хранятся 36000 дней (около 100 лет).
- **Обновлено** – дата и время обновления контекстной таблицы.

Поиск записей в контекстной таблице

Чтобы найти запись в контекстной таблице:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите найти запись, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
4. В столбце **Название** выберите нужную вам контекстную таблицу.

   Откроется окно со списком записей для выбранной контекстной таблицы.
5. В поле **Поиск** введите значение ключа записи или несколько знаков из ее ключа.

В списке записей контекстной таблицы отобразятся только те записи, в ключе которых есть введенные символы.

Если под условие вашего поискового запроса попадают записи с пустыми значениями в ключе, в разделе **Панель мониторинга** на веб-виджете отобразится текст <По вашему запросу ничего не найдено>. Мы рекомендуем уточнить условия поискового запроса.

Добавление записи в контекстную таблицу

Чтобы добавить запись в контекстную таблицу:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите добавить запись, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
4. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.
5. Нажмите на кнопку **Добавить**.

   Откроется окно **Создать запись**.
6. В поле **Значение** укажите значения для полей в столбце **Поле**.

   KUMA берет названия полей из корреляционных правил, к которым привязана контекстная таблица. Эти названия недоступны для редактирования. Состав полей изменить невозможно.

   Если вы укажете не все значения полей, отсутствующие поля, включая ключевые, будут заполнены значениями по умолчанию. Из итоговой совокупности полей будет сформирован ключ записи, и запись будет добавлена в таблицу. Если такой ключ в таблице уже существует, отобразится ошибка.

   Список значений полей по умолчанию

Тип поля	Значение по умолчанию
Целое число	0
Число с плавающей точкой	0.0
Строка	""
Логический оператор	false
IP-адрес	"0.0.0.0"
Timestamp	0
Список целых чисел	[]
Список чисел с плавающей точкой	[]
Список строк	[]
Список логических типов	[]
Список временных меток	[]
Список IP-адресов	[]

7. Нажмите на кнопку **Сохранить**.

Запись добавлена.

Изменение записи в контекстной таблице

Чтобы изменить запись в контекстной таблице:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, контекстную таблицу которого вы хотите изменить, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
4. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.
5. Нажмите на строку записи, которую вы хотите изменить.
6. Укажите требуемые значения в столбце **Значение**.
7. Нажмите на кнопку **Сохранить**.

Запись будет изменена.

Ограничения, действующие при редактировании записи:

- Значение ключевого поля записи недоступно для редактирования. Вы можете изменить его с помощью операций экспорта и импорта записи.
- Редактирование названий полей в столбце **Поле** недоступно.
- Значения в столбце **Значение** должны соответствовать следующим требованиям:
  - больше или равно 0 для полей типов **Временная метка** и **Список временных меток**;
  - соответствует формату IPv4 или IPv6 для полей типов **IP-адрес** и **Список IP-адресов**;
  - равно **true** или **false** для поля типа **Логический тип**.

Удаление записи из контекстной таблицы

Чтобы удалить записи из контекстной таблицы:

1. В Консоли KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. В контекстном меню коррелятора, из контекстной таблицы которого вы хотите удалить запись, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
4. В столбце **Название** выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.
5. Установите флажки для записей, которые вы хотите удалить.

   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

   Должен быть установлен хотя бы один флажок.

6. Нажмите на кнопку **Удалить**.

7. Нажмите на кнопку **ОК**.

Записи будут удалены.

Импорт данных в контекстную таблицу

Чтобы импортировать данные в контекстную таблицу:

1. В Консоли KUMA выберите раздел **Ресурсы**.

2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите импортировать данные, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.

4. Установите флажок рядом с нужной контекстной таблицей и нажмите на кнопку **Импортировать**.

   Откроется окно импорта данных в контекстную таблицу.

5. Нажмите **Добавить** и выберите файл, который требуется импортировать.

6. В раскрывающемся списке **Формат** выберите формат файла:

   - **csv**
   - **tsv**
   - **internal**

7. Нажмите на кнопку **Импортировать**.

Данные из файла будут импортированы в контекстную таблицу. Записи, внесенные в контекстную таблицу ранее, сохраняются.

При импорте KUMA проверяет уникальность ключа каждой записи. Если запись уже существует, то в ее поля записываются новые значения, полученные слиянием прежних значений со значениями полей импортируемой записи.

Если записи в контекстной таблице не существовало, то создается новая запись.

При импорте данные из файла не проходят проверку на допустимые символы. Если вы будете использовать эти данные в веб-виджетах, при наличии недопустимых символов в данных веб-виджеты будут отображаться некорректно.

Аналитика

KUMA предоставляет обширную аналитику по данным, доступным приложению из следующих источников:

- События в хранилище

- Алерты
- Активы
- Учетные записи, импортированные из Active Directory
- Сведения из коллекторов о количестве обработанных событий
- Метрики

Вы можете настроить и получать аналитику в Консоли KUMA в разделах **Панель мониторинга**, **Отчеты** и **Состояние источников**. Для построения аналитики используются только данные из тенантов, к которым у пользователя есть доступ.

Формат даты зависит от языка локализации, выбранного в параметрах приложения. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Панель мониторинга

В разделе **Панель мониторинга** вы можете контролировать состояние безопасности сети вашей организации.

Панель мониторинга представляет собой набор веб-виджетов, которые отображают аналитику данных безопасности сети. Вы можете просматривать данные только для тех тенантов, к которым у вас есть доступ.

Набор веб-виджетов, используемых на панели мониторинга, называется *макетом*. Вы можете создавать макеты вручную или воспользоваться преднастроенными макетами. Параметры веб-виджетов в преднастроенных макетах можно редактировать при необходимости. По умолчанию на панели мониторинга отображается преднастроенный макет Alerts Overview.

Создавать, редактировать и удалять макеты могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик 2-го уровня и Аналитик 1-го уровня. Пользователи с учетными записями всех ролей могут просматривать макеты и назначать макеты по умолчанию. Если макет назначен по умолчанию, этот макет отображается для учетной записи при каждом переходе в раздел **Панель мониторинга**. Выбранный макет по умолчанию сохраняется для текущей учетной записи пользователя.

Информация на панели мониторинга обновляется в соответствии с расписанием, заданным в параметрах макета. При необходимости вы можете обновить данные принудительно.

Для удобства представления данных на панели мониторинга вы можете включить режим ТВ. В этом случае вы перейдете в режим полноэкранного просмотра панели мониторинга в FullHD-разрешении. В режиме ТВ вы также можете настроить отображение слайд-шоу для выбранных макетов.

Создание макета панели мониторинга

Чтобы создать макет:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.

2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите **Создать макет**.

   Откроется окно **Новый макет**.

3. В раскрывающемся списке **Тенанты** выберите тенанты, которым будет принадлежать созданный макет и данные которых будут использоваться для заполнения веб-виджетов макета.

   Выбор тенантов в этом раскрывающемся списке не имеет значения, если вы хотите создать универсальный макет (см. ниже).

4. В раскрывающемся списке **Период** выберите период, за который требуется аналитика:

   - **1 час**
   - **1 день** (это значение выбрано по умолчанию)
   - **7 дней**
   - **30 дней**
   - **За период** – получать аналитику за выбранный период. Период устанавливается с помощью календаря, который отображается при выборе этого параметра.

     > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

5. В раскрывающемся списке **Обновлять каждые** выберите частоту обновления данных в веб-виджетах макета:

   - **1 минута**
   - **5 минут**
   - **15 минут**
   - **1 час** (это значение выбрано по умолчанию)
   - **24 часа**

6. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет и настройте его параметры.

   В макет можно добавить несколько веб-виджетов.

   Вы также можете перетаскивать веб-виджеты по окну и изменять их размер с помощью кнопки ↘, которая появляется при наведении курсора мыши на веб-виджет.

   Добавленные в макет веб-виджеты можно редактировать или удалять, нажав на значок ⚙, а затем выбрав требуемое действие: **Изменить** или **Удалить**.

   - Добавление веб-виджетов

Чтобы добавить веб-виджет:

1. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет.

   Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

2. Настройте параметры веб-виджета и нажмите на кнопку **Добавить**.

- Редактирование веб-виджетов

Чтобы изменить веб-виджет:

1. Наведите указатель мыши на нужный веб-виджет и нажмите на появляющийся значок ⚙.

2. В раскрывающемся списке выберите значение **Изменить**.

   Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

3. Измените параметры веб-виджета и нажмите **Сохранить**.

7. В поле **Имя макета** введите уникальное имя для этого макета. Имя должно содержать от 1 до 128 символов Юникода.

8. При необходимости нажмите на значок ⚙ справа от поля названия макета и установите флажки напротив дополнительных параметров макета:

   - **Универсальный** – если вы установите этот флажок, веб-виджеты макета будут отображать данные тенантов, которые вы выбрали в разделе **Выбранные тенанты** в меню слева. Это означает, что данные в веб-виджетах макета будут изменяться в зависимости от выбранных вами тенантов без необходимости изменять параметры макета. Для универсальных макетов **тенанты**, выбранные в раскрывающемся списке, не учитываются.

     Если этот флажок снят, веб-виджеты макета отображают данные от тенантов, выбранных в раскрывающемся списке **Тенанты** в параметрах макета. Если какой-либо из выбранных в макете тенантов недоступен для вас, их данные не будут отображаться в веб-виджетах макета.

     Вы не можете использовать веб-виджет Активные листы в универсальных макетах.

     Универсальные макеты могут создавать и редактировать только Главные администраторы. Такие макеты могут просматривать все пользователи.

   - **Показать данные, связанные с CII** – если вы установите этот флажок, веб-виджеты макета также будут отображать данные об активах, алертах и инцидентах, связанных с критической информационной инфраструктурой (КИИ). В этом случае эти макеты будут доступны для просмотра только пользователям, в параметрах которых установлен флажок **Доступ к средствам CII**.

     Если этот флажок снят, веб-виджеты макета не будут отображать данные об активах, алертах и инцидентах, связанных с CII, даже если у пользователя есть доступ к объектам CII.

9. Нажмите на кнопку **Сохранить**.

Новый макет создан и отображается в Консоли KUMA в разделе **Панель мониторинга**.

Выбор макета панели мониторинга

Чтобы выбрать макет панели мониторинга:

1. Раскройте список в верхнем правом углу окна **Панель мониторинга**.
2. Выберите соответствующий макет.

Выбранный макет отобразится в Консоли KUMA в разделе **Панель мониторинга**.

Выбор макета панели мониторинга по умолчанию

Чтобы установить макет в панели мониторинга по умолчанию:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. Раскройте список в верхнем правом углу окна **Панель мониторинга**.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок ☆.

Выбранный макет будет отображаться на панели мониторинга по умолчанию.

Изменение макета панели мониторинга

Чтобы изменить макет панели мониторинга:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок ✎.

   Откроется окно **Настройка макета**.
5. Внесите необходимые изменения. Параметры, доступные для изменения, такие же, как и параметры, доступные при создании макета.
6. Нажмите на кнопку **Сохранить**.

Макет панели мониторинга будет отредактирован и отобразится в Консоли KUMA в разделе **Панель мониторинга**.

Если макет был удален или присвоен другому тенанту, пока вы вносили в него изменения, при нажатии на кнопку **Сохранить** отобразится ошибка. Макет не сохранен. Обновите страницу Консоли KUMA, чтобы в раскрывающемся списке просмотреть перечень доступных макетов.

Удаление макета панели мониторинга

Чтобы удалить макет:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок и подтвердите действие.

Макет удален.

Включение и отключение режима ТВ

Рекомендуется для отображения аналитики в режиме ТВ создать отдельного пользователя с минимально необходимым набором прав.

Чтобы включить режим ТВ:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку .
   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Включено**.
4. Чтобы настроить показ веб-виджетов в режиме слайд-шоу, выполните следующие действия:
   a. Переведите переключатель **Слайд-шоу** в положение **Включено**.
   b. В поле **Время ожидания** укажите, через сколько секунд должно происходить переключение макетов.
   c. В раскрывающемся списке **Очередь** выберите веб-виджеты для просмотра. Если макет не выбран, в режиме слайд-шоу по очереди отображаются все доступные пользователю макеты.
   d. Если требуется, измените порядок показа макетов, перетащив их с помощью кнопки .
5. Нажмите на кнопку **Сохранить**.

Режим ТВ включен. Чтобы вернуться к работе с Консолью KUMA, нужно выключить режим ТВ.

Чтобы отключить режим ТВ:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку .
   Откроется окно **Параметры**.

3. Переведите переключатель **Режим ТВ** в положение **Выключено**.

4. Нажмите на кнопку **Сохранить**.

Режим ТВ выключен. В левой части экрана отобразится панель с разделами Консоли KUMA.

Когда вы вносите изменения в макеты, выбранные для слайд-шоу, эти изменения будут автоматически применены к активным сеансам слайд-шоу.

Преднастроенные макеты панели мониторинга

KUMA поставляется с набором предустановленных макетов. По умолчанию для преднастроенных макетов указан период обновления **Никогда**. Вы можете изменять эти макеты при необходимости.

Предустановленные макеты

Название макета	Описание веб-виджетов в составе макета
Network Overview (Обзор сетевой активности)	• Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внутренним IP-адресам активов. • На веб-виджете отображается не более 10 IP-адресов. • Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внешним IP-адресам активов. • Netflow top hosts for remote control (Топ активов, на которые были обращения на порты для удаленного управления) – количество событий, связанных с обращением на один из следующих портов: 3389, 22, 135. Данные сгруппированы по именам активов. • Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика) – количество байт, переданное на внутренние порты активов. Данные сгруппированы по номерам портов. • Top Log Sources by Events count (Топ источников событий) – 10 источников, от которых было получено наибольшее количество событий.
[OOTB] KATA & EDR	• KATA. Top-10 detections by type – визуализирует 10 самых распространенных типов событий, выявленных решением KATA. • KATA. Top-10 detections by file type – визуализирует 10 самых распространенных типов файлов, выявленных решением KATA. • KATA. Top-10 user names in detections – визуализирует 10 самых распространенных имен пользователей, выявленных решением KATA. • KATA. Top-10 IDS detections – визуализирует 10 самых распространенных угроз, выявленных модулем IDS решением KATA. • KATA. Top-10 URL detections – визуализирует 10 самых распространенных подозрительных URL-адресов, выявленных решением KATA. • KATA. Top-10 AV detections – визуализирует 10 самых распространенных угроз, выявленных модулем антивируса системы KATA. • EDR. Top-10 MITRE technique detections – визуализирует 10 самых распространенных техник матрицы MITRE, выявленных решением EDR. • EDR. Top-10 MITRE tactic detections – визуализирует 10 самых распространенных тактик матрицы MITRE, выявленных решением EDR.
[OOTB] KSC	• KSC. Top-10 users with the most KAV alerts – визуализирует 10 самых распространенных имен пользователей, присутствующих в событиях, связанных с выявлением вредоносного программного обеспечения, сведения о

	которых содержатся в приложении Kaspersky Security Center. • KSC. Top-10 most common threats – визуализирует 10 самых распространенных типов вредоносного программного обеспечения, сведения о которых содержатся в приложении Kaspersky Security Center. • KSC. Number of devices that received AV database updates – визуализирует количество устройств, на которых были установлены обновления антивирусных баз данных, сведения о которых содержатся в приложении Kaspersky Security Center. • KSC. Number of devices on which the virus was found – визуализирует количество устройств, на которых было выявлено вредоносное программное обеспечение, сведения о которых содержатся в приложении Kaspersky Security Center. • KSC. Malware detections by hour – визуализирует распределение по часам количества вредоносного программного обеспечения, сведения о которых содержатся в приложении Kaspersky Security Center.
[OOTB] KSMG	• KSMG. Top-10 senders of blocked emails – визуализирует 10 самых распространенных отправителей писем, заблокированных решением KSMG. • KSMG. Top-10 events by action – визуализирует 10 самых распространенных действий, выполненных решением KSMG. • KSMG. Top-10 events by outcome – визуализирует 10 самых распространенных результатов действий, выполненных решением KSMG. • KSMG. Blocked emails by hour – визуализирует распределение по часам количества писем, заблокированных решением KSMG.
[OOTB] KWTS	• KWTS. Top-10 IP addresses with the most blocked web traffic – визуализирует 10 самых распространенных IP-адресов, трафик с которых был заблокирован решением KWTS. • KWTS. Top-10 IP addresses with the most allowed web traffic – визуализирует 10 самых распространенных IP-адресов, трафик с которых был разрешен решением KWTS. • KWTS. Top 10 requests by client application – визуализирует 10 самых распространенных приложений, использовавшихся для доступа к сетевым ресурсам, выявленных решением KWTS. • KWTS. Top-10 blocked URLs – визуализирует 10 самых распространенных URL-адресов, трафик с которых был разрешен решением KWTS. • KWTS. System action types – визуализирует 10 самых распространенных действий, выполненных решением KWTS. • KWTS. Top-10 users with the most allowed web traffic – визуализирует 10 самых распространенных имен пользователей, трафик которых был разрешен решением KWTS.

Отчеты

В KUMA можно настроить регулярное формирование отчетов о процессах приложения.

Отчеты формируются с помощью *шаблонов отчетов*, которые созданы и хранятся на вкладке **Шаблоны** раздела **Отчеты**.

Сформированные отчеты хранятся на вкладке **Сформированные отчеты** раздела **Отчеты**.

Для возможности сохранять сформированные отчеты в форматах HTML и PDF необходимо установить требуемые пакеты на устройстве с Ядром KUMA.

При развертывании KUMA в отказоустойчивом варианте временная зона сервера Ядра приложения и время в браузере пользователя могут различаться. Это различие проявляется в расхождении времени, которое проставляется в отчетах, сформированных по расписанию, и данных, которые пользователь может экспортировать из веб-виджетов. Чтобы избежать расхождения, рекомендуется настроить расписание формирования отчетов с учетом разницы временной зоны пользователей и временем UTC.

Шаблон отчета

Шаблоны отчетов используются для указания аналитических данных, которые следует включать в отчет, а также для настройки частоты создания отчетов. Пользователи с ролью Главного администратора, Администратора тенанта, Аналитика 2-го уровня и Аналитика 1-го уровня могут создавать, изменять и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на вкладке **Сформированные отчеты**.

Шаблоны отчетов доступны на вкладке **Шаблоны** раздела **Отчеты**, где отображается таблица существующих шаблонов. Таблица имеет **следующие столбцы**.

Вы можете настроить набор столбцов таблицы и их порядок, а также изменить сортировку данных:

- Отображение столбцов можно включить или выключить в меню, открываемом с помощью значка .
- Порядок столбцов можно изменить, перетаскивая заголовки столбцов.
- Если заголовок столбца таблицы имеет зеленый цвет, на него можно нажать, чтобы сортировать таблицу по данным этого столбца.

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, которое открывается по нажатию на заголовок столбца **Название**.

  При поиске шаблонов отчетов используются регулярные выражения.

- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение `выключено`.
- **Создал** – имя пользователя, создавшего шаблон отчета.
- **Последнее обновление** – дата последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.
- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.
- **Отправить по электронной почте** – в этом столбце отображается метка напротив шаблонов отчетов, для которых настроено уведомление пользователей по почте о сформированных отчетах.
- **Тенант** – название тенанта, которому принадлежит шаблон отчета.

Вы можете нажать имя шаблона отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Создать отчет** – используйте эту команду, чтобы немедленно сформировать отчет. Созданные отчеты отображаются на вкладке **Сформированные отчеты**.
- **Изменить расписание** – используйте эту команду, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.
- **Изменить шаблон отчета** – используйте эту команду, чтобы настроить веб-виджеты и период времени, за который должна быть извлечена аналитика.
- **Дублировать шаблон отчета** – используйте эту команду, чтобы создать копию существующего шаблона отчета.
- **Удалить шаблон отчета** – используйте эту команду, чтобы удалить шаблон отчета.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В Консоли KUMA перейдите в раздел **Отчеты** → **Шаблоны**.
2. Нажмите на кнопку **Новый шаблон**.

   Откроется окно **Новый шаблон отчета**.
3. В раскрывающемся списке **Тенанты** выберите один или несколько тенантов, которым будет принадлежать создаваемый макет.
4. В раскрывающемся списке **Период** выберите период, за который требуется аналитика:
   - **Сегодня** (это значение выбрано по умолчанию)
   - **На этой неделе**
   - **В этом месяце**
   - **За период** – получать аналитику за выбранный период.

     > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

   - **Другой** – получать аналитику за последние N дней/недель/месяцев/лет.
5. В поле **Срок хранения** укажите, на протяжении какого времени следует хранить сформированные по этому шаблону отчеты.
6. В поле **Название шаблона** введите уникальное название шаблона отчета. Имя должно содержать от 1 до 128 символов Юникода.
7. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет и настройте его параметры.

   В шаблон отчета можно добавить более одного веб-виджета.

   Вы также можете перетаскивать веб-виджеты по окну и изменять их размер с помощью кнопки , которая появляется при наведении курсора мыши на веб-виджет.

Добавленные в макет веб-виджеты можно редактировать или удалять, наведя на них указатель мыши, нажав появившийся значок ⚙, а затем выбрав требуемое действие: **Изменить** или **Удалить**.

- **Добавление веб-виджетов**

  Чтобы добавить веб-виджет:

  1. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет.

     Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

  2. Настройте параметры веб-виджета и нажмите на кнопку **Добавить**.

- **Редактирование веб-виджетов**

  Чтобы изменить веб-виджет:

  1. Наведите указатель мыши на нужный веб-виджет и нажмите на появляющийся значок ⚙.

  2. В раскрывающемся списке выберите значение **Изменить**.

     Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

  3. Измените параметры веб-виджета и нажмите **Сохранить**.

8. При необходимости можно поменять логотип шаблона отчетов с помощью кнопки **Загрузить логотип**.

   Если нажать на кнопку **Загрузить логотип**, открывается окно загрузки, в котором можно указать файл изображения для логотипа. Изображение должно быть файлом .jpg, .png или .gif размером не более 3 МБ.

   Добавленный логотип будет отображаться в отчете вместо логотипа KUMA.

9. При необходимости установите флажок **Отображать данные по КИИ**, чтобы в веб-виджетах макета в том числе отображались данные об активах, алертах и инцидентах, имеющих отношение к критической информационной инфраструктуре (КИИ). В этом случае эти макеты будут доступны для просмотра только пользователям, в параметрах которых установлен флажок **Доступ к средствам CII**.

   Если этот флажок снят, веб-виджеты макета не будут отображать данные об активах, алертах и инцидентах, связанных с CII, даже если у пользователя есть доступ к объектам CII.

10. Нажмите на кнопку **Сохранить**.

Новый шаблон отчета создан и отображается в Консоли KUMA на вкладке **Отчеты → Шаблоны**. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, требуется настроить расписание.

Настройка расписания отчетов

Чтобы настроить расписание отчетов:

1. В Консоли KUMA перейдите в раздел **Отчеты → Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Изменить расписание**.

   Откроется окно **Параметры отчета**.

3. Если вы хотите, чтобы отчет формировался регулярно:

a. Включите переключатель **Расписание**.

В группе настроек **Повторять каждый** задайте периодичность создания отчетов.

Периодичность формирования отчетов можно указать по дням, неделям, месяцам или годам. В зависимости от выбранного периода требуется задать время, день недели, число месяца или дату формирования отчета.

b. В поле **Время** укажите время, когда должен быть сформирован отчет. Вы можете ввести значение вручную или с помощью значка часов.

4. Чтобы выбрать формат отчетов и указать адресатов для рассылки, настройте следующие параметры:

a. В группе настроек **Отправить** нажмите **Добавить**.

b. В открывшемся окне **Добавление адресов электронной почты** в разделе **Группы пользователей** нажмите **Добавить группу**.

c. В появившемся поле укажите адрес электронной почты и нажмите **Enter** или щелкните вне поля ввода - адрес электронной почты будет добавлен. Можно добавить несколько адресов. Отчеты будут отправлены по указанным адресам каждый раз, когда вы сформируете отчет вручную или KUMA сформирует отчет автоматически по расписанию.

> Чтобы сформированные отчеты можно было отправлять по электронной почте, следует настроить SMTP-соединение.

Если адресаты, которым отчет пришел на почту, являются пользователями KUMA, они смогут скачать отчет или просмотреть отчет по ссылкам из письма. Если адресаты не являются пользователями KUMA, переход по ссылкам будет доступен, но авторизоваться в KUMA адресаты не смогут, поэтому им будут доступны только вложения.

Мы рекомендуем просматривать отчеты в формате HTML по ссылкам в веб-интерфейсе, поскольку при некоторых значениях разрешения экрана HTML-отчет из вложения может отображаться некорректно.

Вы можете отправить письмо без вложений, тогда адресатам будут доступны отчеты только по ссылкам и только с авторизацией в KUMA, без ограничений по ролям или тенантам.

d. В раскрывающемся списке выберите формат отчета для отправки. Доступные форматы: PDF, HTML, CSV, разделенный CSV, Excel.

5. Нажмите на кнопку **Сохранить**.

Расписание отчетов настроено.

Изменение шаблона отчета

Чтобы изменить шаблон отчета:

1. В Консоли KUMA перейдите в раздел **Отчеты** → **Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Изменить шаблон отчета**.

Откроется окно **Изменить шаблон отчета**.

> Это окно также можно открыть на вкладке **Отчеты** → **Сформированные отчеты**, нажав имя существующего отчета и выбрав в раскрывающемся списке **Изменить шаблон отчета**.

3. Внесите необходимые изменения:

- Измените список тенантов, которым принадлежит шаблон отчета.
- Обновите период времени, за который вам требуется аналитика.
- **Добавьте веб-виджеты**

  Чтобы добавить веб-виджет:

  1. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет.

     Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

  2. Настройте параметры веб-виджета и нажмите на кнопку **Добавить**.

- Измените расположение веб-виджетов, перетаскивая их.
- Измените размер веб-виджетов с помощью кнопки , которая появляется при наведении указателя мыши на веб-виджет.
- **Отредактируйте веб-виджеты**

  Чтобы изменить веб-виджет:

  1. Наведите указатель мыши на нужный веб-виджет и нажмите на появляющийся значок .
  2. В раскрывающемся списке выберите значение **Изменить**.

     Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

  3. Измените параметры веб-виджета и нажмите **Сохранить**.

- Удалите веб-виджеты, наведя на них указатель мыши, а затем нажав на появившийся значок и выбрав **Удалить**.
- В поле справа от раскрывающегося списка **Добавить веб-виджет** введите уникальное имя шаблона отчета. Имя должно содержать от 1 до 128 символов Юникода.
- Измените логотип отчета, загрузив его по кнопке **Загрузить логотип**. Если в шаблоне уже есть логотип, его предварительно потребуется удалить.
- Измените срок хранения отчетов, сформированных по этому шаблону.
- При необходимости установите или снимите флажок **Отображать данные по КИИ**.

4. Нажмите на кнопку **Сохранить**.

Шаблон отчета изменен и отображается в Консоли KUMA на вкладке **Отчеты → Шаблоны**.

Копирование шаблона отчета

Чтобы создать копию шаблона отчета:

1. В Консоли KUMA перейдите в раздел **Отчеты → Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Дублировать шаблон отчета**.

   Откроется окно **Новый шаблон отчета**. Название веб-виджета изменено на `<Шаблон отчета> - копия`.

3. Внесите необходимые изменения:

   - Измените список тенантов, которым принадлежит шаблон отчета.
   - Обновите период времени, за который вам требуется аналитика.
   - **Добавьте веб-виджеты**

     Чтобы добавить веб-виджет:

     1. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет.

        Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

     2. Настройте параметры веб-виджета и нажмите на кнопку **Добавить**.

   - Измените расположение веб-виджетов, перетаскивая их.
   - Измените размер веб-виджетов с помощью кнопки ⤡, которая появляется при наведении указателя мыши на веб-виджет.
   - **Отредактируйте веб-виджеты**

     Чтобы изменить веб-виджет:

     1. Наведите указатель мыши на нужный веб-виджет и нажмите на появляющийся значок ⚙.
     2. В раскрывающемся списке выберите значение **Изменить**.

        Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

     3. Измените параметры веб-виджета и нажмите **Сохранить**.

   - Удалите веб-виджеты, наведя на них указатель мыши, а затем нажав на появившийся значок ⚙ и выбрав **Удалить**.
   - В поле справа от раскрывающегося списка **Добавить веб-виджет** введите уникальное имя шаблона отчета. Имя должно содержать от 1 до 128 символов Юникода.
   - Измените логотип отчета, загрузив его по кнопке **Загрузить логотип**. Если в шаблоне уже есть логотип, его предварительно потребуется удалить.

4. Нажмите на кнопку **Сохранить**.

Шаблон отчета создан и отображается в Консоли KUMA на вкладке **Отчеты → Шаблоны**.

Удаление шаблона отчета

Чтобы удалить шаблон отчета:

1. В Консоли KUMA перейдите в раздел **Отчеты → Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Удалить шаблон отчета**.

   Откроется окно подтверждения.

3. Если вы хотите удалить только шаблон отчета, нажмите на кнопку **Удалить**.

4. Если вы хотите удалить шаблон отчета и все отчеты, сформированные с помощью этого шаблона, нажмите **Удалить с отчетами**.

Шаблон отчета удален.

Сформированные отчеты

Все отчеты формируются с помощью шаблонов отчетов. Сформированные отчеты доступны на вкладке **Сформированные отчеты** в разделе **Отчеты** и отображаются в таблице со **следующими столбцами**:

Вы можете настроить набор столбцов таблицы и их порядок, а также изменить сортировку данных:

- Отображение столбцов можно включить или выключить в меню, открываемом с помощью значка .
- Порядок столбцов можно изменить, перетаскивая заголовки столбцов.
- Если заголовок столбца таблицы имеет зеленый цвет, на него можно нажать, чтобы сортировать таблицу по данным этого столбца.

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

- **Период** – период времени, за который была извлечена аналитика отчета.

- **Последний отчет** – дата и время создания отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

- **Тенант** – название тенанта, которому принадлежит отчет.

- **Пользователь** – имя пользователя, который сформировал отчет вручную. Если отчет был сформирован по расписанию, значение будет пустым.

Вы можете нажать на название отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Открыть отчет** – используйте эту команду, чтобы открыть окно с данными отчета.

- **Сохранить как** – используйте эту команду, чтобы сохранить сформированный отчет в нужном формате. Доступные форматы: HTML, PDF, CSV, разделенный CSV, Excel.

- **Создать отчет** – используйте эту команду, чтобы немедленно сформировать отчет. Обновите окно браузера, чтобы увидеть вновь созданный отчет в таблице.

- **Изменить шаблон отчета** – используйте эту команду, чтобы настроить веб-виджеты и период времени, за который должна быть извлечена аналитика.

- **Удалить отчет** – используйте эту команду, чтобы удалить отчет.

Просмотр отчетов

Чтобы просмотреть отчет:

1. В Консоли KUMA перейдите в раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Открыть отчет**.

   Откроется новая вкладка браузера с веб-виджетами, отображающими аналитику отчетов. Если веб-виджет отображает данные о событиях, алертах, инцидентах или активных листах, при нажатии на его заголовок открывается соответствующий раздел Консоли KUMA с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из веб-виджета. К веб-виджетам применяются ограничения по умолчанию.

   Чтобы скачать данные, отображаемые на каждом веб-виджете в формате CSV в кодировке UTF-8, нажмите на кнопку **CSV**. Название скачиваемого файла имеет формат <название веб-виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

   Если вы хотите просмотреть полные данные, выгрузите отчет в формате CSV с указанными параметрами из запроса.
3. При необходимости сохраните отчет в выбранном формате, нажав на кнопку **Сохранить как**.

Создание отчетов

Вы можете создать отчет вручную или настроить расписание, чтобы отчеты создавались автоматически.

Чтобы создать отчет вручную:

1. В Консоли KUMA перейдите в раздел **Отчеты** → **Шаблоны**.
2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Создать отчет**.

   > Отчет также можно создать на вкладке **Отчеты** → **Сформированные отчеты**, нажав имя существующего отчета и выбрав в раскрывающемся списке **Создать отчет**.

   Отчет создается и помещается на вкладку **Отчеты** → **Сформированные отчеты**.

Чтобы создавать отчеты автоматически, настройте расписание отчетов.

Сохранение отчетов

Чтобы сохранить отчет в нужном формате:

1. В Консоли KUMA перейдите в раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Сохранить как**. Затем выберите нужный формат: HTML, PDF, CSV, разделенный CSV, Excel.

   Отчет сохраняется в папку загрузки, настроенную в вашем браузере.

Отчет также можно сохранить в выбранном формате при просмотре.

Удаление отчетов

Чтобы удалить отчет:

1. В Консоли KUMA перейдите в раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Удалить отчет**.

   Откроется окно подтверждения.
3. Нажмите на кнопку **OK**.

Веб-виджеты

С помощью веб-виджетов вы можете осуществлять мониторинг работы приложения.

Веб-виджеты организованы в группы, каждая из которых связана с типом аналитики, которую она предоставляет. В KUMA доступны следующие группы веб-виджетов и веб-виджеты:

- **События** – веб-виджет для создания аналитики на основе событий.
- **Активные листы** – веб-виджет для создания аналитики на основе активных листов корреляторов.
- Активы – группа для аналитики об активах из обработанных событий. Эта группа включает следующие веб-виджеты:
  - **Затронутые активы** – таблица с информацией об уровне важности активов и количестве незакрытых алертов, с которыми они связаны.
  - **Категории затронутых активов** – категории активов, привязанных к незакрытым алертам.
  - **Количество активов** – количество активов, добавленных в KUMA.
  - **Активы в инцидентах по тенантам** – количество активов в незакрытых инцидентах. Сгруппированы по тенантам.
  - **Активы в алертах по тенантам** – количество активов в незакрытых алертах, сгруппированных по тенантам.
- Источники событий – группа для аналитики об источниках событий. В группу входят следующие веб-виджеты:
  - **Топ источников событий по количеству алертов** – количество незакрытых алертов, сгруппированных по источникам событий.
  - **Топ источников событий по условному рейтингу** – количество событий, для которых существует незакрытый алерт, сгруппированных по источникам событий. Группировка осуществляется по источнику событий.

    В некоторых случаях количество алертов, созданных источниками, может быть искажено. Для получения точной статистики рекомендуется в правиле корреляции указать поле события Device Product в качестве уникального, а также включить хранение всех базовых событий в корреляционном событии. Правила корреляции с такими параметрами являются более ресурсоемкими.

- Пользователи – группа для аналитики о пользователях из обработанных событий. В группу входят следующие веб-виджеты:

  - **Затронутые пользователи в алертах** – количество учетных записей, связанных с незакрытыми алертами.

  - **Количество пользователей AD** – количество учетных записей в Active Directory, полученных по LDAP в течение указанного в веб-виджете периода.

В таблице событий, в области сведений о событиях, в окне алертов и в веб-виджетах имена активов, учетных записей и служб отображаются вместо идентификаторов в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID. При экспорте событий в файл идентификаторы сохраняются, но в файл добавляются столбцы с именами. Идентификаторы также отображаются при наведении курсора мыши на названия активов, учетных записей или служб.

Поиск полей с идентификаторами возможен только по идентификаторам.

Основные принципы работы с веб-виджетами

Принцип отображения данных на веб-виджете зависит от типа графика. В KUMA доступны следующие типы графиков:

- Круговая диаграмма ( ).
- Счетчик ( ).
- Таблица ( ).
- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).
- Линейная диаграмма.

Основные принципы работы со всеми веб-виджетами

В левом верхнем углу веб-виджетов отображается название веб-виджета. По ссылке с названием веб-виджета о событиях, алертах, инцидентах или активных листах вы можете перейти в соответствующий раздел Консоли KUMA.

Под названием веб-виджета отображается список тенантов, для которых представлены данные.

В правом верхнем углу веб-виджета указан период, за который отображаются данные на веб-виджете (30д). Вы можете просмотреть даты периода и время последнего обновления, наведя указатель мыши на этот значок.

Слева от значка периода отображается кнопка **CSV**. Вы можете скачать данные, которые отображаются на веб-виджете, в формате CSV (кодировка UTF-8). Название скачиваемого файла имеет формат <название веб-виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

Веб-виджет отображает данные за период, выбранный в параметрах веб-виджета или макета, только для тенантов, указанных в параметрах веб-виджета или макета.

Основные принципы работы с графиками типа "Круговая диаграмма"

Под списком тенантов отображается круговая диаграмма. Вы можете перейти в раздел Консоли KUMA с соответствующими данными, щелкнув левой кнопкой мыши по выбранному разделу диаграммы. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в веб-виджете.

Под значком периода отображается количество событий, активных листов, активов, алертов или инцидентов, сгруппированных по выбранным критериям за период отображения данных на веб-виджетах.

Примеры:

- На веб-виджете **Алерты по статусу** под значком периода отображается количество алертов, сгруппированных по статусам **Новый**, **Открыт**, **Назначен** или **Эскалирован**.
  Если вы хотите просмотреть в легенде алерты только со статусами **Открыт** и **Назначен**, вы можете снять флажки слева от статусов **Новый** и **Эскалирован**.

- На веб-виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, Name AS `value` FROM `events` GROUP BY Name ORDER BY `metric` DESC LIMIT 10`, под значком периода отображается 10 событий, сгруппированных по имени и отсортированных в порядке убывания.
  Если вы хотите просмотреть в легенде события с определенными именами, вы можете снять флажки слева от имен событий, которые не должны отображаться в легенде.

Основные принципы работы с графиками типа "Счетчик"

На графиках этого типа отображается сумма выбранных данных.

Пример:
На веб-виджете **Количество активов** отображается общее количество активов, добавленных в KUMA.

Основные принципы работы с графиками типа "Таблица"

На графиках этого типа данные отображаются в виде таблицы.

Пример:
На веб-виджете **События**, для которого указан SQL-запрос `SELECT TenantID, Timestamp, Name, DeviceProduct, DeviceVendor FROM `events` LIMIT 10`, отображается таблица событий со столбцами **TenantID**, **Timestamp**, **Name**, **DeviceProduct**, **DeviceVendor**. Таблица содержит 10 строк.

Основные принципы работы с графиками типа "Столбчатая диаграмма"

Под списком тенантов отображается столбчатая диаграмма. Вы можете перейти в Консоли KUMA в раздел **События**, нажав левой кнопкой мыши по выбранному разделу диаграммы. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в веб-виджете. Справа от диаграммы эти данные представлены в виде таблицы.

Пример:
На веб-виджете **Netflow top internal IPs**, для которого указан SQL-запрос `SELECT sum(BytesIn) AS metric, DestinationAddress AS value FROM `events` WHERE (DeviceProduct = 'netflow' OR DeviceProduct = 'sflow') AND (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16')) GROUP BY DestinationAddress ORDER BY metric DESC LIMIT 10`, на оси X диаграммы отображается сумма трафика в байтах, на оси Y диаграммы отображаются адреса портов назначения. Данные сгруппированы по адресам назначения в порядке убывания суммы трафика.

Основные принципы работы с графиками типа "Календарная диаграмма"

Под списком тенантов отображается календарная диаграмма. Вы можете перейти в Консоли KUMA в раздел **События** с соответствующими данными, нажав левой кнопкой мыши по выбранному разделу диаграммы. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в веб-виджете. Справа от диаграммы эти данные представлены в виде таблицы.

Пример:
На веб-виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, Timestamp AS `value` FROM `events` GROUP BY Timestamp ORDER BY `metric` DESC LIMIT 250`, на оси X диаграммы отображается дата создания события, на оси Y диаграммы отображается примерное количество событий. События сгруппированы по дате создания в порядке убывания.

Основные принципы работы с графиками типа "Линейная диаграмма"

Под списком тенантов отображается линейная диаграмма. Вы можете перейти в Консоли KUMA в раздел **События** с соответствующими данными, нажав левой кнопкой мыши по выбранному разделу диаграммы. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в веб-виджете. Справа от диаграммы эти данные представлены в виде таблицы.

Пример:
На веб-виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY `value` ASC LIMIT 250`, на оси X диаграммы представлен примерный номер порта, на оси Y диаграммы отображаются количество событий. Данные сгруппированы по номеру порта в порядке возрастания.

Особенности отображения данных в веб-виджетах

Ограничение отображаемых данных

Для удобства восприятия информации в KUMA заданы ограничения на отображение данных в веб-виджетах в зависимости от их типа:

- Круговая диаграмма – отображается не более 20 отсеков.
- Столбчатая диаграмма – отображается не более 40 столбцов.
- Таблица – отображается не более 500 записей.
- Календарная диаграмма – отображается не более 365 дней.

Данные, выходящие за указанные ограничения, отображаются в веб-виджете в категории **Остальное**.

Все данные, по которым построена аналитика в веб-виджете, можно скачать в формате CSV.

Суммирование данных

Формат отображения итоговой суммы данных на календарной, столбчатой и круговой диаграммах зависит от языка локализации:

- Английская локализация: порядки разделяются запятыми, дробная часть отделяется точкой.
- Русская локализация: порядки разделяются пробелами, дробная часть отделяется запятой.

Создание веб-виджета

Вы можете создать веб-виджет в макете панели мониторинга во время создания или изменения макета.

Чтобы создать веб-виджет:

1. Создайте макет или переключитесь в режим редактирования для выбранного макета.
2. Нажмите на кнопку **Добавить веб-виджет**.
3. В раскрывшемся списке выберите тип веб-виджета.

   Откроется окно с параметрами веб-виджета.
4. Измените параметры веб-виджета.
5. Если вы хотите увидеть, как данные будут отображаться в веб-виджете, нажмите на кнопку **Предварительный просмотр**.
6. Нажмите на кнопку **Добавить**.

Веб-виджет появится на макете в панели мониторинга.

Изменение веб-виджета

Чтобы изменить веб-виджет:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на кнопку .

   Откроется окно **Настройка макета**.
5. На веб-виджете, который вы хотите отредактировать, нажмите на кнопку .
6. Выберите **Изменить**.

   Откроется окно с параметрами веб-виджета.
7. Измените параметры веб-виджета.
8. Нажмите на кнопку **Сохранить** в окне свойств веб-виджета.
9. Нажмите на кнопку Сохранить в окне **Настройка макета**.

Веб-виджет изменен.

Удаление веб-виджета

Чтобы удалить веб-виджет:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на кнопку .
   Откроется окно **Настройка макета**.
5. На веб-виджете, который вы хотите удалить, нажмите на кнопку .
6. Выберите пункт **Удалить**.
7. В отобразившемся окне подтверждения нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Сохранить**.

Веб-виджет удален.

Параметры веб-виджетов

Этот раздел содержит описание параметров всех доступных в KUMA веб-виджетов.

Веб-виджет "События"

Вы можете использовать веб-виджет **События** для получения необходимой аналитики на основе SQL-запросов.

При создании этого веб-виджета вам требуется указать значения для следующих параметров:

Вкладка :

- **График** – тип графика. Доступны следующие типы графиков:
  - **Круговая диаграмма**.
  - **Столбчатая диаграмма**.
  - **Счетчик**.
  - **Линейная диаграмма**.
  - **Таблица**.
  - **Календарная диаграмма**.
- **Тенант** – тенант, по которому отображаются данные на веб-виджете.
  Вы можете выбрать несколько тенантов.
  По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.
- **Период** – период, за который отображаются данные на веб-виджете. Доступны следующие периоды:
  - **Как на макете** – отображаются данные за период, выбранный для макета.
    Это значение используется по умолчанию.

- **1 час** – отображаются данные за предыдущий час.
- **1 день** – отображаются данные за предыдущий день.
- **7 дней** – отображаются данные за предыдущие 7 дней.
- **30 дней** – отображаются данные за предыдущие 30 дней.
- **В течение периода** – отображаются данные за выбранный период времени.

  При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

  > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

- **Показывать данные за предыдущий период** – включение отображения данных сразу за два периода: за текущий и за предыдущий.
- **Хранилище** – хранилище, в котором выполняется поиск событий.
- Поле SQL-запроса () – в этом поле вы можете ввести запрос для фильтрации и поиска событий вручную.

  Также вы можете составить запрос в конструкторе запросов, нажав на кнопку  .

  Как создать запрос в конструкторе запросов

Чтобы создать запрос в конструкторе запросов:

1. Укажите значения для следующих параметров:

   a. **SELECT** – поля событий, которые следует возвращать. Количество доступных полей зависит от выбранного типа графика.

   - В раскрывающемся списке слева выберите поля событий, данные по которым должны отображаться на веб-виджете.
   - Среднее поле показывает, для чего выбранное поле используется в веб-виджете: **metric** (метрики) или **value** (значение).

     Если вы выбрали тип графика **Таблица**, в средних полях нужно указать названия столбцов, используя символы ANSII-ASCII.

   - В раскрывающемся списке справа вы можете выбрать операцию, которую следует произвести над данными:
     - **count** – подсчет событий. Эта операция доступна только для поля события **ID**. Используется по умолчанию для линейных, круговых и столбчатых диаграмм, а также для счетчиков. Является единственно возможным вариантом для календарных диаграмм.
     - **max** – максимальное значение поля **события** из выборки событий.
     - **min** – минимальное значение поля **события** из выборки событий.
     - **avg** – среднее значение поля **события** из выборки событий.
     - **sum** – сумма значений полей событий из выборки событий.

   b. **SOURCE** – тип источника данных. Для выбора доступно только значение **events** (события).

   c. **WHERE** – условия фильтрации событий.

   - В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.
   - В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.
   - В раскрывающемся списке справа введите значение условия. В зависимости от выбранного типа поля может потребоваться ввести значение вручную, выбрав его из раскрывающегося списка или в календаре.

   Вы можете добавить условия поиска, нажав на кнопку **Добавить условие** или удалить их, нажав на кнопку ✕.

   Вы можете добавить группы условий, нажав на кнопку **Добавить группу**. По умолчанию группы условий добавляются с оператором **AND**, но при необходимости вы можете изменить значение. Доступные значения: **AND**, **OR**, **NOT**. Группы условий можно удалить, нажав на кнопку **Удалить группу**.

   d. **GROUP BY** – поля событий или псевдонимы, по которым следует группировать возвращаемые данные. Этот параметр недоступен для графиков типа **Счетчик**.

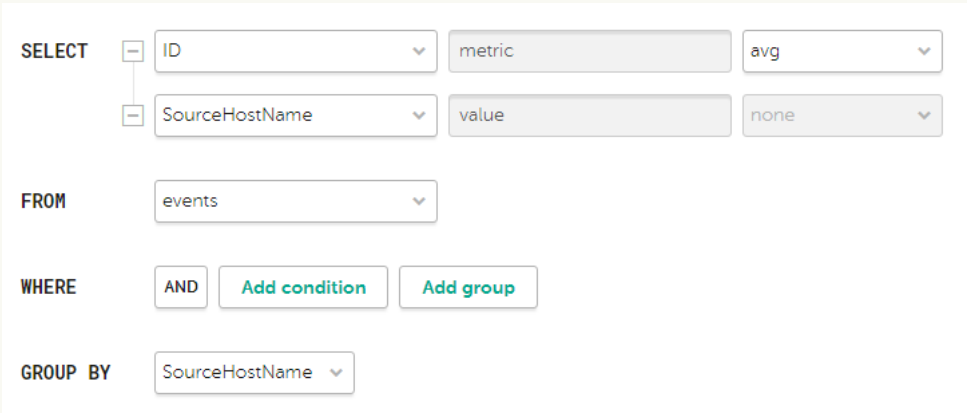
e. **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

- В раскрывающемся списке слева выберите значение, которое будет использоваться для сортировки.
- В раскрывающемся списке справа выберите порядок сортировки: **ASC** – по возрастанию, **DESC** – по убыванию.
- Для графиков типа **Таблица** можно добавить условия сортировки с помощью кнопки **Добавить столбец**.

f. **LIMIT** – максимальное количество точек данных для веб-виджета. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

2. Нажмите **Применить**.

[Пример условий поиска в конструкторе запросов]



Параметры условия поиска для веб-виджета, показывающие среднее количество байтов, полученных с одного устройства

Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов веб-виджета с аналитикой по событиям, кроме таблиц.

Псевдонимы в веб-виджетах типа **Таблица** могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: `"Псевдоним с пробелом"`, `` `Другой псевдоним` ``.

При отображении данных за предыдущий период сортировка по параметру `count(ID)` может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`.

В веб-виджетах типа **Счетчик** необходимо для значений функции `SELECT` указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`.

Вкладка :

Вкладка отображается, если на вкладке в поле **График** вы выбрали одно из следующих значений: **Столбчатая диаграмма**, **Линейная диаграмма**, **Календарная диаграмма**.

- **Минимальное значение Y** и **Максимальное значение Y** – масштаб оси Y.
- **Минимальное значение X** и **Максимальное значение X** – масштаб оси X.

  На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на веб-виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

- **Толщина линии** – толщина линии на графике. Поле отображается для типа графика "Линейная диаграмма".
- **Размер указателя** – размер указателя на графике. Поле отображается для типа графика "Линейная диаграмма".

Вкладка :

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Цвет** – раскрывающийся список, в котором вы можете выбрать цвет отображения информации:
  - **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый;**
  - **красный;**
  - **синий;**
  - **желтый.**
- **Горизонтальный** – использование горизонтальной гистограммы вместо вертикальной.

  При включении этого параметра горизонтальная прокрутка при большом количестве данных не будет отображаться и вся имеющаяся информация будет отражена в заданном размере веб-виджета. Если данных для отображения много, рекомендуется увеличить размер веб-виджета.

- **Итоговые значения** – суммы значений.
- **Легенда** – легенда для аналитики.

  По умолчанию переключатель включен.

- **Пустые значения в легенде** – отображение параметров с нулевым значением в легенде для аналитики.

  По умолчанию переключатель выключен.

- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено.

- **Длительность отрезков периода** (доступно для графика типа **Календарная диаграмма**) – длительность отрезков, на которые требуется делить период.

Веб-виджет "Активные листы"

Вы можете использовать веб-виджет **Активные листы** для получения аналитики на основе SQL-запросов.

При создании этого веб-виджета вам требуется указать значения для следующих параметров:

Вкладка :

- **График** – тип графика. Доступны следующие типы графиков:
  - **Столбчатая диаграмма**.
  - **Круговая диаграмма**.
  - **Счетчик**.
  - **Таблица**.
- **Тенант** – тенант, по которому отображаются данные на веб-виджете.

  Вы можете выбрать несколько тенантов.

  По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.
- **Коррелятор** – название коррелятора, содержащего активный лист, по которому вы хотите получать данные.
- **Активный лист** – название активного листа, по которому вы хотите получать данные.

  > Один и тот же активный лист может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

- Поле SQL-запроса – в этом поле вы можете ввести запрос для фильтрации и поиска данных активного листа вручную.

  Структура запроса аналогична той, которая используется при поиске событий.

  При создании запроса по активным листам вам нужно учитывать следующие особенности:

  - Для функции FROM требуется указать значение `records`.
  - Если вы хотите получать данные по полям, названия которых содержат пробелы и символы кириллицы, в запросе такие названия требуется выделять кавычками:
    - в функции SELECT псевдонимы следует выделять двойными или косыми кавычками: "псевдоним", `другой псевдоним`;
    - в функции ORDER BY псевдонимы следует выделять косыми кавычками: `другой псевдоним`;
    - значения полей событий выделяются прямыми кавычками: WHERE DeviceProduct = 'Microsoft'.

  Название полей событий выделять кавычками не требуется.

Если название поля активного листа начинается или заканчивается пробелами, в веб-виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов.

Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции LIKE '%значение поля%'.

- Вы можете использовать в запросе служебные поля _key (поле с ключами записей активного листа) и _count (сколько раз эта запись была добавлена в активный лист), а также пользовательские поля.
- Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов веб-виджета с аналитикой по активным листам, кроме таблиц.
- Если в SQL-запросе используется функция преобразования даты и времени (например, fromUnixTimestamp64Milli) и при этом обрабатываемое поле не содержит даты и времени, в веб-виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Например: SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250.
- Если задать большие значения для функции LIMIT, это может привести к ошибкам в работе браузера.
- Если в качестве типа графика вы выбрали Счетчик, необходимо для значений функции SELECT указывать способ обработки данных: count, max, min, avg, sum.
- **Вы можете получать в веб-виджете названия тенантов, а не их идентификаторы.**

  Если вы хотите, чтобы в веб-виджетах по активным листам отображались названия тенантов, а не их идентификаторы, настройте в корреляционных правилах коррелятора функцию наполнения активного листа сведениями об использующем его тенанте. Процесс настройки состоит из следующих этапов:

  1. Экспорт списка тенантов.
  2. Создание словаря типа **Таблица** и импорт в него полученного ранее списка тенантов.
  3. Добавление в корреляционное правило локальной переменной с функцией **dict** для распознания имени тенанта по идентификатору.

     Пример:

     - Переменная: `TenantName`.
     - Значение: `dict('<Название ранее созданного словаря с тенантами>', TenantID)`.
  4. Добавьте действие с активными листами в правило корреляции. Это действие запишет значение ранее созданной переменной в формате "ключ-значение" в активный лист с помощью функции **Установить**. В качестве ключа следует задать поле активного листа (например, `Tenant`), а в поле **Value** обратиться к ранее созданной переменной (например, `$TenantName`).

  В результате срабатывания этого правила в активный лист будет помещаться название тенанта, опознанного функцией **dict** по идентификатору среди словаря тенантов. При создании веб-виджетов по активным листам можно получить название тенанта, обратившись к названию поля активного листа (в примере выше это `Тенант`).

  Описанный метод можно применять и к другим полям событий с идентификаторами.

Особенности использования псевдонимов в SQL-функциях: и SELECT допустимо использовать двойные и косые кавычки: ", `.

Если в качестве типа графика вы выбрали Счетчик, псевдонимы могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: "Псевдоним с пробелом", `Другой псевдоним`.

При отображении данных за предыдущий период сортировка по параметру count(ID) может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250.

Примеры запросов для получения аналитики по активным листам:

- `SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250`
  Запрос, который возвращает ключ активного листа с названием поля "Источник событий" и значением этого поля "Екатеринбург".
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация count по полю _key) и все варианты значений пользовательского поля Status. В веб-виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля Status.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Запрос для таблицы, которая возвращает значения пользовательских полей Name и Status, а также служебного поля _count у тех записей активного листа, в которых значения пользовательского поля Description соответствует запросу ILIKE '%ftp%'. В веб-виджете отображается таблица со столбцами Status, Name и Number.

Вкладка :

Вкладка отображается, если на вкладке в поле **График** вы выбрали значение **Столбчатая диаграмма**.

- **Минимальное значение Y** и **Максимальное значение Y** – масштаб оси Y.
- **Минимальное значение X** и **Максимальное значение X** – масштаб оси X.

На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на веб-виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Вкладка :

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Цвет** – раскрывающийся список, в котором вы можете выбрать цвет отображения информации:
  - **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый;**
  - **красный;**

- **синий;**
- **желтый.**

- **Горизонтальный** – использование горизонтальной гистограммы вместо вертикальной.

  При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.

- **Итоговые значения** – суммы значений.

- **Легенда** – легенда для аналитики.

  По умолчанию переключатель включен.

- **Пустые значения в легенде** – отображение параметров с нулевым значением в легенде для аналитики.

  По умолчанию переключатель выключен.

Веб-виджет "Контекстные таблицы"

Вы можете использовать веб-виджет **Контекстные таблицы** для получения аналитики на основе SQL-запросов.

При создании этого веб-виджета вам требуется указать значения для следующих параметров:

Вкладка :

- **График** – тип графика. Доступны следующие типы графиков:
  - **Столбчатая диаграмма**.
  - **Круговая диаграмма**.
  - **Счетчик**.
  - **Таблица**.

- **Тенант** – тенант, по которому отображаются данные на веб-виджете.

  Вы можете выбрать несколько тенантов.

  По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.

- **Коррелятор** – название коррелятора, содержащего контекстную таблицу, по которой вы хотите получать данные.

- **Контекстная таблица** – название контекстной таблицы, по которой вы хотите получать данные.

  > Одна и та же контекстная таблица может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность контекстной таблицы. Таким образом, содержимое контекстных таблиц, используемых разными корреляторами, различается, даже если идентификатор и название контекстных таблиц одинаковые.

- **Поле SQL-запроса** – в этом поле вы можете ввести запрос для фильтрации и поиска данных контекстной таблицы вручную. По умолчанию для каждого типа графика в поле указан запрос, который получает схему контекстной таблицы и ключ по ключевым полям.

  Структура запроса аналогична той, которая используется при поиске событий.

При создании запроса по контекстным таблицам вам нужно учитывать следующие особенности:

- Для функции FROM требуется указать значение `records`.
- Вы можете получить данных только по полям, указанным в схеме контекстной таблицы.
- Вы можете использовать поддерживаемые функции ClickHouse.
- Если вы хотите получать данные по полям, названия которых содержат пробелы и символы кириллицы, в запросе такие названия требуется выделять кавычками:
  - в функции SELECT псевдонимы следует выделять двойными или косыми кавычками: "псевдоним", `другой псевдоним`;
  - в функции ORDER BY псевдонимы следует выделять косыми кавычками: `другой псевдоним`;
  - значения полей событий выделяются прямыми кавычками: WHERE DeviceProduct = 'Microsoft'.

  Название полей событий выделять кавычками не требуется.

  > Если название поля активного листа начинается или заканчивается пробелами, в веб-виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов.

  Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции LIKE '%значение поля%'.
- Вы можете использовать в запросе служебное поле _count (сколько раз эта запись была добавлена в контекстную таблицу), а также пользовательские поля.
- Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов веб-виджета с аналитикой по активным листам, кроме таблиц.
- Если в SQL-запросе используется функция преобразования даты и времени (например, fromUnixTimestamp64Milli) и при этом обрабатываемое поле не содержит даты и времени, в веб-виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Например: SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250.
- Если задать большие значения для функции LIMIT, это может привести к ошибкам в работе браузера.
- Если в качестве типа графика вы выбрали **Счетчик**, необходимо для значений функции SELECT указывать способ обработки данных: count, max, min, avg, sum.
- **Вы можете получать в веб-виджете названия тенантов, а не их идентификаторы.**

Если вы хотите, чтобы в веб-виджетах по активным листам отображались названия тенантов, а не их идентификаторы, настройте в корреляционных правилах коррелятора функцию наполнения активного листа сведениями об использующем его тенанте. Процесс настройки состоит из следующих этапов:

1. Экспорт списка тенантов.
2. Создание словаря типа **Таблица** и импорт в него полученного ранее списка тенантов.
3. Добавление в корреляционное правило локальной переменной с функцией **dict** для распознания имени тенанта по идентификатору.

   Пример:

   - Переменная: `TenantName`.
   - Значение: `dict('<Название ранее созданного словаря с тенантами>', TenantID)`.
4. Добавьте действие с активными листами в правило корреляции. Это действие запишет значение ранее созданной переменной в формате "ключ-значение" в активный лист с помощью функции **Установить**. В качестве ключа следует задать поле активного листа (например, `Tenant`), а в поле **Value** обратиться к ранее созданной переменной (например, `$TenantName`).

В результате срабатывания этого правила в активный лист будет помещаться название тенанта, опознанного функцией **dict** по идентификатору среди словаря тенантов. При создании веб-виджетов по активным листам можно получить название тенанта, обратившись к названию поля активного листа (в примере выше это `Тенант`).

Описанный метод можно применять и к другим полям событий с идентификаторами.

Особенности использования псевдонимов в SQL-функциях и SELECT: допустимо использовать двойные и косые кавычки: ", `.
При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: "Псевдоним с пробелом", Значения следует выделять прямыми одинарными кавычками: 'Значение с пробелом'.
При отображении данных за предыдущий период сортировка по параметру count(ID) может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250.

Примеры запросов для получения аналитики по активным листам:

- SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250
  Запрос, который возвращает ключ активного листа с названием поля "Источник событий" и значением этого поля "Екатеринбург".
- SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250
  Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация count по полю _key) и все варианты значений пользовательского поля Status. В веб-виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля Status.
- SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250
  Запрос для таблицы, которая возвращает значения пользовательских полей Name и Status, а также служебного поля _count у тех записей активного листа, в которых значения пользовательского поля Description соответствует запросу ILIKE '%ftp%'. В веб-виджете отображается таблица со столбцами Status, Name и Number.

Вкладка :

Вкладка отображается, если на вкладке в поле **График** вы выбрали значение **Столбчатая диаграмма**.

- **Минимальное значение Y** и **Максимальное значение Y** – масштаб оси Y.
- **Минимальное значение X** и **Максимальное значение X** – масштаб оси X.
- На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на веб-виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Вкладка :

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Цвет** – раскрывающийся список, в котором вы можете выбрать цвет отображения информации:
  - **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый;**
  - **красный;**
  - **синий;**
  - **желтый.**
- **Горизонтальный** – использование горизонтальной гистограммы вместо вертикальной.

  При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
- **Итоговые значения** – суммы значений.
- **Легенда** – легенда для аналитики.

  По умолчанию переключатель включен.
- **Пустые значения в легенде** – отображение параметров с нулевым значением в легенде для аналитики.

  По умолчанию переключатель выключен.

Другие веб-виджеты

В этом разделе описываются параметры всех веб-виджетов, кроме веб-виджетов **События** и **Активные листы**.

Набор параметров, доступных для виджета, зависит от типа графика, который отображается на виджете. В KUMA доступны следующие типы графиков:

- Круговая диаграмма ().
- Счетчик ().
- Таблица ().

- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).
- Линейная диаграмма.

Параметры для круговых диаграмм

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Тенант** – тенант, по которому отображаются данные на веб-виджете.

  Вы можете выбрать несколько тенантов.

  По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.
- **Период** – период, за который отображаются данные на веб-виджете. Доступны следующие периоды:
  - **Как на макете** – отображаются данные за период, выбранный для макета.

    Это значение используется по умолчанию.
  - **1 час** – отображаются данные за предыдущий час.
  - **1 день** – отображаются данные за предыдущий день.
  - **7 дней** – отображаются данные за предыдущие 7 дней.
  - **30 дней** – отображаются данные за предыдущие 30 дней.
  - **В течение периода** – отображаются данные за выбранный период времени.

    При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

    > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.
- **Итоговые значения** – суммы значений.
- **Легенда** – легенда для аналитики.

  По умолчанию переключатель включен.
- **Пустые значения в легенде** – отображение параметров с нулевым значением в легенде для аналитики.

  По умолчанию переключатель выключен.
- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено.

Параметры для счетчиков

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Тенант** – тенант, по которому отображаются данные на веб-виджете.

  Вы можете выбрать несколько тенантов.

  По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.
- **Период** – период, за который отображаются данные на веб-виджете. Доступны следующие периоды:
  - **Как на макете** – отображаются данные за период, выбранный для макета.

    Это значение используется по умолчанию.
  - **1 час** – отображаются данные за предыдущий час.
  - **1 день** – отображаются данные за предыдущий день.
  - **7 дней** – отображаются данные за предыдущие 7 дней.
  - **30 дней** – отображаются данные за предыдущие 30 дней.
  - **В течение периода** – отображаются данные за выбранный период времени.

    При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

    > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

Параметры для таблиц

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Тенант** – тенант, по которому отображаются данные на веб-виджете.

  Вы можете выбрать несколько тенантов.

  По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.
- **Период** – период, за который отображаются данные на веб-виджете. Доступны следующие периоды:
  - **Как на макете** – отображаются данные за период, выбранный для макета.

    Это значение используется по умолчанию.
  - **1 час** – отображаются данные за предыдущий час.
  - **1 день** – отображаются данные за предыдущий день.
  - **7 дней** – отображаются данные за предыдущие 7 дней.

- **30 дней** – отображаются данные за предыдущие 30 дней.
- **В течение периода** – отображаются данные за выбранный период времени.

  При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

  > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

- **Показывать данные за предыдущий период** – включение отображения данных сразу за два периода: за текущий и за предыдущий.
- **Цвет** – раскрывающийся список, в котором вы можете выбрать цвет отображения информации:
  - **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый;**
  - **красный;**
  - **синий;**
  - **желтый.**
- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено.

Параметры для столбчатых и календарных диаграмм

Вкладка :

- **Минимальное значение Y** и **Максимальное значение Y** – масштаб оси Y.
- **Минимальное значение X** и **Максимальное значение X** – масштаб оси X.

  > На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на веб-виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено.

Вкладка :

- **Название** – название веб-виджета.
- **Описание** – описание веб-виджета.
- **Тенант** – тенант, по которому отображаются данные на веб-виджете.

  Вы можете выбрать несколько тенантов.

По умолчанию данные отображаются по тенантам, которые были выбраны в параметрах макета.

- **Период** – период, за который отображаются данные на веб-виджете. Доступны следующие периоды:
  - **Как на макете** – отображаются данные за период, выбранный для макета.

    Это значение используется по умолчанию.
  - **1 час** – отображаются данные за предыдущий час.
  - **1 день** – отображаются данные за предыдущий день.
  - **7 дней** – отображаются данные за предыдущие 7 дней.
  - **30 дней** – отображаются данные за предыдущие 30 дней.
  - **В течение периода** – отображаются данные за выбранный период времени.

    При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

    > Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.
- **Показывать данные за предыдущий период** – включение отображения данных сразу за два периода: за текущий и за предыдущий.
- **Цвет** – раскрывающийся список, в котором вы можете выбрать цвет отображения информации:
  - **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый;**
  - **красный;**
  - **синий;**
  - **желтый.**
- **Горизонтальный** – использование горизонтальной гистограммы вместо вертикальной.

  При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
- **Итоговые значения** – суммы значений.
- **Легенда** – легенда для аналитики.

  По умолчанию переключатель включен.
- **Пустые значения в легенде** – отображение параметров с нулевым значением в легенде для аналитики.

  По умолчанию переключатель выключен.
- **Длительность отрезков периода** (доступно для графика типа **Календарная диаграмма**) – длительность отрезков, на которые требуется делить период.

Отображение названий тенантов в веб-виджетах типа "Активный лист"

Если вы хотите, чтобы в виджетах типа "Активные листы" отображались названия тенантов, а не их идентификаторы, настройте в корреляционных правилах коррелятора функцию наполнения активного листа сведениями об использующем его тенанте.

Процесс настройки состоит из следующих этапов:

1. Экспорт списка тенантов.
2. Создание словаря типа **Таблица**.
3. Импорт списка тенантов, полученного на шаге 1, в словарь, созданный на шаге 2 этой инструкции.
4. Добавление в корреляционное правило локальной переменной с функцией **dict** для распознания имени тенанта по идентификатору.

   Пример:

   - Переменная: `TenantName`.
   - Значение: `dict('<Название ранее созданного словаря с тенантами>', TenantID)`.
5. Добавление в корреляционное правило действия **Установить**, с помощью которого значение ранее созданной переменной будет записываться в активный лист в формате <ключ> – <значение>. В качестве ключа следует задать поле активного листа (например, `Tenant`), а в поле **Value** указать переменную (например, `$TenantName`).

В результате срабатывания этого правила в активный лист будет помещаться название тенанта, опознанного функцией **dict** по идентификатору в словаре тенантов. При создании виджетов по активным листам в виджете вместо идентификатора тенанта будет отображаться название тенанта.

Работа с Open Single Management Platform

Open Single Management Platform (далее OSMP) – это технологическая платформа, которая позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности и обеспечивает кросс-программные сценарии. Для управления OSMP используется веб-интерфейс OSMP (далее Консоль OSMP).

С помощью Консоли OSMP вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- просматривать информацию о безопасности сети вашей организации;
- настраивать обнаружения, поиск и реагирование на угрозы;
- управлять политиками, сформированными для активов вашей сети;
- управлять задачами приложений, установленных на устройствах сети;
- управлять пользователями и ролями;
- настраивать перенос данных в Open Single Management Platform;
- устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями;
- опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически;
- управлять интеграцией Open Single Management Platform с другими приложениями.

Консоль OSMP – это многоязыковой веб-интерфейс. Вы можете изменить язык интерфейса в любое время без повторного открытия приложения.

Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к приложению Open Single Management Platform.

Сервер администрирования

Компоненты Open Single Management Platform позволяют осуществлять удаленное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*). Серверы администрирования должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- с именем `kladminserver_srv`;

- с автоматическим типом запуска при старте операционной системы;
- с учетной записью `ksc` либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Полный список параметров установки см. в разделе: Установка Open Single Management Platform.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов приложений;
- удаленная установка приложений на клиентские устройства и удаление приложений;
- обновление баз и модулей приложений "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе приложений "Лаборатории Касперского";
- распространение лицензионных ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

Правило именования Серверов администрирования в интерфейсе приложения

В интерфейсе консоли консоль OSMP Серверы администрирования могут иметь следующие имена:

- Имя устройства Сервера администрирования, например: "*имя_устройства*" или "Сервер администрирования: *имя_устройства"*.
- IP-адрес устройства Сервера администрирования, например: "*IP_адрес*" или "Сервер администрирования: *IP_адрес*".
- Подчиненные Серверы администрирования и виртуальные Серверы администрирования имеют собственные имена, которые вы указываете при подключении виртуального или подчиненного Сервера администрирования к главному Серверу администрирования.
- Если вы используете консоль OSMP, установленную на устройство под управлением Linux, то приложение отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов.

Вы можете подключиться к Серверу администрирования с помощью консоли OSMP.

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Корневой Сервер администрирования может действовать только как главный Сервер. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования*.

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить на каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.
- Использование Open Single Management Platform поставщиками услуг. Поставщику услуг достаточно установить Open Single Management Platform. Для управления большим числом клиентских устройств различных организаций поставщик услуг может включать в иерархию Серверов администрирования подчиненные Серверы администрирования (включая виртуальные Серверы).

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент приложения Open Single Management Platform, предназначенный для управления антивирусной защитой сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки приложения "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.
- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Open Single Management Platform перезапускает главный Сервер администрирования и все виртуальные Серверы.
- Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

Веб-сервер

Веб-сервер Open Single Management Platform (далее также *Веб-сервер*) – это компонент Open Single Management Platform, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных инсталляционных пакетов.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере. Вы можете передать ссылку пользователю любым удобным способом, например, по электронной почте. По полученной ссылке пользователь может загрузить инсталляционный пакет на локальное устройство.

Агент администрирования

Взаимодействие между Сервером администрирования и устройствами обеспечивается *Агентом администрирования* – компонентом Open Single Management Platform. Агент администрирования требуется установить на все устройства, на которых управление работой приложений "Лаборатории Касперского" выполняется с помощью Open Single Management Platform.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Агент администрирования Kaspersky Security Center";
- с автоматическим типом запуска при старте операционной системы;
- с помощью учетной записи LocalSystem.

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*. Вы можете установить Агент администрирования следующими способами:

- Инсталляционный пакет в хранилище Сервера администрирования (необходимо, чтобы был установлен Сервер администрирования).
- Инсталляционный пакет находится на веб-серверах "Лаборатории Касперского".

Во время установки Сервера администрирования, серверная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования. Для управления устройством с Сервером администрирования рекомендуется установить Агент администрирования для Linux на это устройство. В этом случае Агент администрирования для Linux устанавливается и работает независимо от серверной версии Агента администрирования, которая была установлена вместе с Сервером администрирования.

Названия процессов, которые запускает Агент администрирования:

- klnagent64.service (для 64-разрядной операционной системы);
- klnagent.service (для 32-разрядной операционной системы).

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (*периодический сигнал*) равным 15 минут на 10 000 управляемых устройств.

Группы администрирования

Группа администрирования (далее также *группа*) – это набор управляемых устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым Open Single Management Platform.

Для всех управляемых устройств в группе администрирования устанавливаются:

- Единые параметры работы приложений – с помощью групповых политик.
- Единый режим работы всех приложений – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей приложений, проверку устройства по требованию и включение постоянной защиты.

Управляемое устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и управляемые устройства. Можно переводить устройства из одной группы в другую, не перемещая их физически. Например, если сотрудник предприятия перешел с позиции бухгалтера на позицию разработчика, вы можете перевести компьютер этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, устройство будут автоматически переданы параметры приложений, необходимые для разработчика.

Управляемое устройство

Управляемое устройство – это устройство с операционной системой Linux, Windows или macOS, на котором установлен Агент администрирования. Вы можете управлять такими устройствами с помощью задач и политик для приложений, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

Вы можете настроить управляемое устройство, чтобы оно выполняло функции точки распространения и шлюза соединений.

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 20 000 устройств.

Нераспределенное устройство

Нераспределенное устройство – это устройство в сети, которое не включено ни в одну из групп администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливать на них приложения.

Когда в сети обнаруживается новое устройство, оно помещается в группу администрирования **Нераспределенные устройства**. Можно настроить правила автоматического распределения устройств по группам администрирования в момент обнаружения.

Рабочее место администратора

Устройства, на которых установлен Сервер Консоли OSMP, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

Веб-плагин управления

Веб-плагин управления – это специальный компонент, используемый для удаленного управления приложениями "Лаборатории Касперского" с помощью Консоли OSMP. Веб-плагин управления также называется *плагином управления*. Плагин управления представляет собой интерфейс между Консолью OSMP и определенным приложением "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для приложения.

Плагин управления предоставляет следующие возможности:

- Интерфейс для создания и изменения задач и параметров приложения.
- Интерфейс для создания и изменения политик и профилей политик для удаленной централизованной настройки приложений "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных приложениями.
- Функции Консоли OSMP для отображения оперативных данных и событий приложения, а также статистики, полученной от клиентских устройств.

Политики

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

Профили политик

Может возникнуть необходимость создать несколько копий одной политики для разных групп администрирования; может также возникнуть необходимость централизованно изменить параметры этих политик. Эти копии могут различаться одним или двумя параметрами. Например, все бухгалтеры в организации работают под управлением одной и той же политики, но старшим бухгалтерам разрешено использовать флеш-накопители USB, а младшим бухгалтерам не разрешено. В этом случае применение политик к устройствам только через иерархию групп администрирования может оказаться неудобным.

Чтобы избежать создания нескольких копий одной политики, Open Single Management Platform позволяет создавать *профили политик*. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

Задачи

Open Single Management Platform управляет работой программ безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения, только если для этого приложения установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;

- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором с помощью Консоли OSMP, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

> Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи.

Результаты выполнения задач сохраняются в системном журнале событий и журнале событий Open Single Management Platform как централизованно на Сервере администрирования, так и локально на каждом устройстве.

> Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область действия задачи

Область задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал) или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

  Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

Взаимосвязь политики и локальных параметров приложения

Вы можете при помощи политик устанавливать одинаковые значения параметров работы приложения для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров приложения. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт замком).

Значение параметра, которое использует приложение на клиентском устройстве, определяется наличием замка () у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же заданное политикой значение.

- Если запрет не наложен, то на каждом клиентском устройстве приложение использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры приложения.

Таким образом, при выполнении задачи на клиентском устройстве приложение использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами приложения, если в политике не был установлен запрет на изменение параметра;

- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры приложения изменяются после первого применения политики в соответствии с параметрами политики.

Точка распространения

Точка распространения (ранее называлась "агент обновлений") – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в сети. Точка распространения может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для точки распространения должна быть создана задача обновления.

  Точки распространения ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.

- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования.

  Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, точку распространения можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

  Наличие точки распространения, работающей в режиме шлюза соединений не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

- Осуществлять удаленную установку приложений "Лаборатории Касперского" и других поставщиков программного обеспечения, в том числе установку на клиентские устройства без Агента администрирования.

  Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.

- Выступать в роли прокси-сервера, участвующего в Kaspersky Security Network (KSN).

  Можно включить прокси-сервер KSN на стороне точки распространения, чтобы устройство исполняло роль прокси-сервера KSN. В этом случае на устройстве запустится служба прокси-сервера KSN.

Передача файлов от Сервера администрирования точке распространения осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены точками распространения вручную администратором или автоматически Сервером администрирования. Полный список точек распространения для указанных групп администрирования отображается в отчете со списком точек распространения.

Областью действия точки распространения является группа администрирования, для которой она назначена администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп администрирования назначено несколько точек распространения, Агент администрирования управляемого устройства подключается к наиболее близкой по иерархии точке распространения.

Если точки распространения назначаются автоматически Сервером администрирования, то Сервер назначает точки распространения по широковещательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковещательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковещательным доменам. Широковещательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковещательные домены каждые два часа. После того как точки распространения назначены по широковещательным доменам, их невозможно назначить снова по группам администрирования.

Если администратор вручную назначает точки распространения, их можно назначать группам администрирования или сетевым местоположениям.

Агенты администрирования с активным профилем соединения не участвуют в определении широковещательного домена.

Open Single Management Platform присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов. Адреса многоадресной IP-рассылки, уже присвоенные в прошлых версиях приложения, изменены не будут.

Если на одном участке сети или в группе администрирования назначаются две точки распространения или более, одна из них становится активной точкой распространения, остальные назначаются резервными. Активная точка распространения загружает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные точки распространения обращаются за обновлениями только к активной точке распространения. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между точками распространения. Если активная точка распространения по каким-либо причинам становится недоступной, одна из резервных точек распространения назначается активной. Сервер администрирования назначает точку распространения резервной автоматически.

Статус точки распространения (*Активный*/*Резервный*) отображается флажком в отчете утилиты klnagchk.

Для работы точки распространения требуется не менее 4 ГБ свободного места на диске. Если объем свободного места на диске точки распространения меньше 2 ГБ, Open Single Management Platform создает проблему безопасности с уровнем важности *Предупреждение*. Проблема безопасности будет опубликована в свойствах устройства в разделе **Проблемы безопасности**.

При работе задач удаленной установки на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть больше размера всех устанавливаемых инсталляционных пакетов.

При работе задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть как минимум в два раза больше размера всех устанавливаемых патчей.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Шлюз соединения

Шлюз соединения – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

Шлюз соединения может принимать соединения от 10 000 устройств.

Существует два варианта использования шлюзов соединения:

- Рекомендуется установить шлюз соединения в демилитаризованной зоне (DMZ). Для других Агентов администрирования, установленных на автономных устройствах, необходимо специально настроить подключение к Серверу администрирования через шлюз соединения.

  Шлюз соединения не изменяет и не обрабатывает данные, передаваемые от Агентов администрирования на Сервер администрирования. Шлюз соединения не записывает эти данные в буфер и, следовательно, не может принимать данные от Агента администрирования и затем передавать их на Сервер администрирования. Если Агент администрирования пытается подключиться к Серверу администрирования через шлюз соединения, но шлюз соединения не может подключиться к Серверу администрирования, Агент администрирования воспринимает это как недоступный Сервер администрирования. Все данные остаются на Агенте администрирования (не на шлюзе соединения).

  Шлюз соединения не может подключиться к Серверу администрирования через другой шлюз соединения. Это означает, что Агент администрирования не может одновременно быть шлюзом соединения и использовать шлюз соединения для подключения к Серверу администрирования.

  Все шлюзы соединения включены в список точек распространения в свойствах Сервера администрирования.

- Вы также можете использовать шлюзы соединения в сети. Например, автоматически назначаемые точки распространения также становятся шлюзами соединений в своей области действия. Однако во внутренней сети шлюзы соединения не дают значительных преимуществ. Они уменьшают количество сетевых подключений, принимаемых Сервером администрирования, но не уменьшают объем входящих данных. Даже без шлюзов соединения все устройства могли подключаться к Серверу администрирования.

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования Kaspersky Security Center.

Настройка подключения Консоли OSMP к Серверу администрирования

Вы можете настроить подключение Консоли OSMP к Серверу администрирования через свойства Сервера администрирования или с помощью параметров политики Сервера администрирования.

Чтобы задать порты подключения с помощью свойств Сервера администрирования:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

3. При необходимости укажите **SSL-порт для Kaspersky Security Center Web Console** или укажите другие порты подключения к Серверу администрирования.

Основные параметры подключения выбранного Сервера указаны.

Чтобы задать порты подключения с помощью свойств политики Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на название политики Сервера администрирования и перейдите на вкладку **Параметры приложения**.

3. При необходимости укажите **SSL-порт для Kaspersky Security Center Web Console** или укажите другие порты подключения к Серверу администрирования.

> Если вы выключите параметр **Открыть порт для Kaspersky Security Center Web Console** и этот параметр политики будет применен к устройству, вы не сможете подключиться к Серверу администрирования с помощью Консоли OSMP. В этом случае соединение будет прервано. Если у вас есть Сервер администрирования, на котором не применяется эта политика, вы можете повторно подключиться к этому Серверу администрирования с помощью Консоли OSMP.

Основные параметры подключения выбранного Сервера указаны.

Настройка параметров доступа к интернету

Подключение к интернету необходимо для правильной работы компонентов Open Single Management Platform и может использоваться для определенных интеграций как с "Лабораторией Касперского", так и со сторонними производителями. Например, доступ для Сервера администрирования к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Open Single Management Platform и управляемых приложений "Лаборатории Касперского".

В параметрах интеграции некоторых приложений "Лаборатории Касперского" есть возможность включить или выключить использование прокси-сервера. Например, такая возможность доступна при настройке интеграции с Kaspersky Threat Intelligence Portal.

Чтобы указать параметры доступа к интернету:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры доступа к сети интернет**.

3. Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

   - **Адрес**

     Адрес прокси-сервера для подключения Open Single Management Platform к интернету.

   - **Номер порта**

     Номер порта, по которому будет выполняться подключение Open Single Management Platform к прокси-серверу.

   - **Не использовать прокси-сервер для локальных адресов**

     При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

   - **Аутентификация на прокси-сервере**

     Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере. Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

   - **Имя пользователя**

     Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

   - **Пароль**

     Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

Сертификаты для работы с Open Single Management Platform

В этом разделе содержится информация о сертификатах OSMP и описание, как выпустить и заменить сертификаты для Консоли OSMP, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с консолью OSMP.

О сертификатах Open Single Management Platform

Open Single Management Platform использует следующие типы сертификатов для обеспечения безопасного взаимодействия между компонентами приложения:

- сертификат Сервера администрирования;

- сертификат Сервера Консоли OSMP;
- сертификат Консоли OSMP.

По умолчанию Open Single Management Platform использует самоподписанные сертификаты (то есть выданные самим Open Single Management Platform). Если требуется, вы можете заменить самоподписанные сертификаты пользовательскими сертификатами, в соответствии со стандартами безопасности вашей организации. После того как Сервер администрирования проверит соответствие пользовательского сертификата всем применимым требованиям, этот сертификат приобретает такую же область действия, что и самоподписанный сертификат. Единственное отличие состоит в том, что пользовательский сертификат не перевыпускается автоматически по истечении срока действия. Вы заменяете сертификаты на пользовательские с помощью утилиты klsetsrvcert или в Консоли OSMP в свойствах Сервера администрирования, в зависимости от типа сертификата. При использовании утилиты klsetsrvcert необходимо указать тип сертификата, используя одно из следующих значений:

- C – общий сертификат для портов 13000 и 13291;
- CR – общий резервный сертификат для портов 13000 и 13291.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для следующих целей:

- Аутентификация Сервера администрирования при подключении к Консоли OSMP.
- Безопасное взаимодействие Сервера администрирования и Агента администрирования на управляемых устройствах.
- Аутентификация при подключении главных Серверов администрирования к подчиненным Серверам администрирования.

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке /var/opt/kaspersky/klnagent_srv/1093/cert/. Сертификат Сервера администрирования вы указываете при создании файла ответов для установки Консоли OSMP. Этот сертификат называется общим ("C").

Сертификат Сервера администрирования действителен 397 дней. Open Single Management Platform автоматически генерирует общий резервный сертификат ("CR") за 90 дней до истечения срока действия общего сертификата. Общий резервный сертификат впоследствии используется для замены сертификата Сервера администрирования. Когда истекает срок действия общего сертификата, общий резервный сертификат используется для поддержания связи с экземплярами Агента администрирования, установленными на управляемых устройствах. С этой целью общий резервный сертификат автоматически становится новым общим сертификатом за 24 часа до истечения срока действия старого общего сертификата.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

При необходимости можно назначить Серверу администрирования пользовательский сертификат. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата. При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы устранить эту ошибку, вам потребуется восстановить соединение после замены сертификата.

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных.

Вы также можете создать резервную копию сертификата Сервера администрирования отдельно от других параметров Сервера администрирования, чтобы перенести Сервер администрирования с одного устройства на другое без потери данных.

Мобильные сертификаты

Мобильный сертификат ("M") необходим для аутентификации Сервера администрирования на мобильных устройствах. Вы указываете мобильный сертификат в свойствах Сервера администрирования.

Также существует мобильный резервный сертификат ("MR"): он используется для замены мобильного сертификата. Open Single Management Platform автоматически генерирует этот сертификат за 60 дней до истечения срока действия общего сертификата. Когда истекает срок действия мобильного сертификата, мобильный резервный сертификат используется для поддержания связи с Агентами администрирования, установленными на управляемых мобильных устройствах. С этой целью мобильный резервный сертификат автоматически становится новым мобильным сертификатом за 24 часа до истечения срока действия старого мобильного сертификата.

Если сценарий подключения требует использования сертификата клиента на мобильных устройствах (подключение с двусторонней SSL-аутентификация), вы генерируете эти сертификаты с помощью аккредитованного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA"). Кроме того, в свойствах Сервера администрирования можно указать пользовательские сертификаты, выпущенные другим аккредитованным центром сертификации, при условии, что интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

сертификат Веб-сервера;

Веб-сервер является компонентом Сервера администрирования Kaspersky Security Center и использует специальный тип сертификата. Этот сертификат необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства. Для этого Веб-сервер может использовать различные сертификаты.

Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли OSMP.

2. Общий сертификат Сервера администрирования ("C").

Сертификат Консоли OSMP

Сервер Консоли OSMP имеет собственный сертификат. Когда вы открываете сайт, браузер проверяет, является ли ваше соединение надежным. Сертификат Web Console позволяет аутентифицировать Web Console и используется для шифрования трафика между браузером и Web Console.

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Консоли OSMP не является приватным и что сертификат Консоли OSMP недействителен. Это предупреждение появляется потому, что сертификат Консоли OSMP является самоподписанным и автоматически генерируется Open Single Management Platform. Чтобы удалить это предупреждение, можно выполнить одно из следующих действий:

- Замените сертификат Kaspersky Security Center Web Console на пользовательский сертификат (рекомендуемый параметр). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.

- Добавить сертификат Web Console в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

Требования к пользовательским сертификатам, используемым в Open Single Management Platform

В таблице ниже представлены требования к пользовательским сертификатам, предъявляемые к различным компонентам Open Single Management Platform.

Требования к сертификатам Open Single Management Platform

Тип сертификата	Требования	Комментарии
Общий сертификат, Общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера, аутентификация клиента.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом отличным от "None", но не меньше 1.
Сертификат Веб-сервера	Расширенное использование ключа (EKU): аутентификация Сервера. Контейнер PKCS #12 / PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	–
Сертификат Консоли OSMP	Контейнер PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Консолью OSMP.

Перевыпуск сертификата для Консоли OSMP

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия сертификата в Консоли OSMP равен 397 дням. Вы можете заменить существующий сертификат, полученный от доверенного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Консоли OSMP.

Автоматический перевыпуск сертификата для OSMP не поддерживается. Вам необходимо вручную перевыпустить сертификат.

Когда вы открываете Консоль OSMP, браузер может информировать вас о том, что подключение к Консоли OSMP не является приватным и что сертификат Консоли OSMP недействителен. Это предупреждение появляется потому, что сертификат Консоли OSMP является самоподписанным и автоматически генерируется Open Single Management Platform. Чтобы удалить или предотвратить это предупреждение, можно выполнить одно из следующих действий:

- Укажите пользовательский сертификат при его повторном выпуске (рекомендуемый вариант). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
- Добавьте сертификат Консоли OSMP в список доверенных сертификатов браузера после перевыпуска сертификата. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

Чтобы перевыпустить просроченный сертификат Консоли OSMP:

Переустановите Консоль OSMP, выполнив одно из следующих действий:

- Если вы хотите использовать тот же установочный файл Консоли OSMP, удалите Консоль OSMP и установите ту же версию Консоли OSMP.
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления.

Сертификат Консоли OSMP перевыпущен со сроком действия 397 дней.

Замена сертификата для Консоли OSMP

По умолчанию при установке Сервера Консоли OSMP (далее также Консоль OSMP) сертификат браузера для приложения генерируется автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

Чтобы заменить сертификат для Консоли OSMP на пользовательский сертификат:

1. Создайте новый файл ответов, необходимый для установки Консоли OSMP.
2. В файле ответов укажите путь к файлу пользовательского сертификата и файлу ключа с помощью параметра `certPath` и параметра `keyPath`.
3. Переустановите Консоль OSMP, указав новый файл ответов. Выполните одно из следующих действий:

- Если вы хотите использовать тот же установочный файл Консоли OSMP, удалите Консоль OSMP и установите ту же версию Консоли OSMP.
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления.

Консоль OSMP работает с указанным сертификатом.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Консоли OSMP, вам необходимо предварительно преобразовать его в формат PEM с помощью любой кроссплатформенной утилиты на основе OpenSSL.

Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Linux:

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Убедитесь, что файл сертификата и закрытый ключ сгенерированы в той же папке, где хранится файл PFX.

3. Консоль OSMP не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Не используйте одно и то же имя для входных и выходных файлов .pem.

   В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Консоли OSMP.

Сценарий: задание пользовательского сертификата Сервера администрирования

Вы можете назначить пользовательский сертификат Сервера администрирования, например, для лучшей интеграции с существующей инфраструктурой открытых ключей (PKI) вашей организации или для пользовательской конфигурации параметров сертификата. Целесообразно заменять сертификат сразу после инсталляции Сервера администрирования.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

Предварительные требования

Новый сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации) и должен быть выпущен доверенным центром сертификации (CA). Также новый сертификат должен включать в себя всю цепочку доверия и закрытый ключ, который должен храниться в файле с расширением pfx или p12. Для нового сертификата должны быть соблюдены требования, перечисленные ниже.

Тип сертификата: Общий сертификат, общий резервный сертификат ("C", "CR")

Требования:

- Минимальная длина ключа: 2048.
- Основные ограничения:
  - CA: Да.
  - Ограничение длины пути: Отсутствует.

    Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.
- Использование ключа:
  - Цифровая подпись.
  - Подпись сертификата.
  - Шифрование ключей.
  - Подписывание списка отзыва (CRL).
- Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера и аутентификация клиента. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации Сервера и клиента должны быть указаны в EKU.

Сертификаты, выпущенные доверенным центром сертификации (англ. certificate authority, CA), не имеют разрешения на подписывание сертификатов. Чтобы использовать такие сертификаты, убедитесь, что на точках распространения или шлюзах соединения в вашей сети установлен Агент администрирования версии 13 или выше. В противном случае вы не сможете использовать сертификаты без разрешения на подпись.

Этапы

Указание сертификата Сервера администрирования состоит из следующих этапов:

1. **Замена сертификата Сервера администрирования**

   Используйте для этой цели утилиту командной строки klsetsrvcert.

2. **Указание нового сертификата и восстановление связи Агентов администрирования с Сервером администрирования**

   При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы указать новый сертификат и восстановить соединение, используйте командную строку утилиты klmover.

Результаты

После завершения сценария сертификат Сервера администрирования будет заменен, Сервер Агент администрирования на управляемых устройствах аутентифицирует Сервер с использованием нового сертификата.

Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert

Чтобы заменить сертификат Сервера администрирования,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke ksc --action klsetsrvcert --param ksc_server_certificate=<path_to_new_certificate> --param
ksc_server_cert_pass=<password>
```

где

- `<path_to_new_certificate>` – путь к контейнеру с сертификатом и закрытому ключу в формате PKCS#12 (файл с расширением .p12 или .pfx).
- `<password>` – пароль, который используется для защиты контейнера PKCS # 12. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.

По умолчанию параметры проверки сертификата не указаны, используется пользовательский сертификат без разрешения на подпись. Вы можете заменить общий сертификат для порта 13000.

Вам не нужно загружать утилиту klsetsrvcert. Он включен в кластер Kubernetes и недоступен для прямого запуска. Утилиту klsetsrvcert можно запустить только с помощью KDT с устройства администратора.

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

После замены сертификата Сервера администрирования с помощью утилиты командной строки klsetsrvcert вам необходимо установить SSL-соединение между Агентами администрирования и Сервером администрирования, так как соединение разорвано.

Чтобы указать новый сертификат Сервера администрирования и восстановить соединение:

В командной строке выполните следующую команду:

```
klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу
сертификата>]
```

Эта утилита автоматически копируется в папку установки Агента администрирования при установке Агента администрирования на клиентское устройство.

Описание параметров утилиты klmover представлено в таблице ниже.

Значения параметров утилиты klmover

Параметр	Значение
`-address <адрес Сервера>`	Адрес Сервера администрирования для подключения. В качестве адреса можно указать IP-адрес или DNS-имя.
`-pn <номер порта>`	Номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования. По умолчанию установлен порт 14000.
`-ps <номер SSL-порта>`	Номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию установлен порт 13000. Для корневого Сервера администрирования это порт 13000, и его невозможно изменить.
`-nossl`	Использовать незашифрованное подключение к Серверу администрирования. Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.
`-cert <путь к файлу сертификата>`	Использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

Иерархия Серверов администрирования

Некоторые компании-клиенты, например MSP-клиенты, могут использовать несколько Серверов администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования на разных уровнях иерархии. Корневой Сервер администрирования может действовать только как главный Сервер.

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики, задачи, роли пользователей и инсталляционные пакеты, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты и выборки событий на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.
- Главный Сервер администрирования может использоваться в качестве источника обновлений для подчиненного Сервера администрирования.

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux. Корневой Сервер администрирования может действовать только как главный Сервер.

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер".

Чтобы добавить Сервер администрирования, доступный для подключения через Консоль OSMP, в качестве подчиненного Сервера:

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. На будущем главном Сервере администрирования нажмите на значок параметров ( ).
3. На открывшейся странице свойств нажмите на вкладку **Серверы администрирования**.
4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.
5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.
6. Заполните следующие поля:

   - **Имя подчиненного Сервера администрирования**

     Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

   - **Адрес подчиненного Сервера администрирования (необязательно)**

     Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

     Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   - **SSL-порт Сервера администрирования**

Укажите номер SSL-порта главного Сервера администрирования. По умолчанию установлен порт 13000.

- **API-порт Сервера администрирования**

  Укажите номер порта главного Сервера администрирования для получения соединений через OpenAPI. По умолчанию установлен порт 13299.

- **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**

  Выберите этот параметр, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

  Если выбран этот параметр, необходимо указать **Адрес подчиненного Сервера**.

  Если выбран этот параметр, главный Сервер администрирования инициирует подключение к подчиненному Серверу администрирования. Иначе подчиненный Сервер администрирования инициирует подключение к главному Серверу администрирования.

7. Укажите сертификат будущего подчиненного Сервера.

   Работа мастера завершена.

8. Отправьте файл сертификата будущего главного Сервера администрирования системному администратору офиса, в котором находится будущий подчиненный Сервер администрирования. (Например, вы можете записать файл на внешнее устройство или отправить его по электронной почте.)

   Файл сертификата находится на будущем главном Сервере администрирования, /var/opt/kaspersky/klnagent_srv/1093/cert/.

9. Предложите системному администратору, ответственному за будущий подчиненный Сервер администрирования, следующее:

   a. Нажмите на значок параметров ( ).

   b. На открывшейся странице свойств перейти в раздел **Иерархия Серверов администрирования** на вкладке **Общие**.

   c. Выберите параметр **Данный Сервер администрирования является подчиненным в иерархии**.

      Корневой Сервер администрирования может действовать только как главный Сервер.

   d. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.

   e. Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

   f. Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   g. Если подключение к будущему главному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.

h. Нажмите на кнопку **Сохранить**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер начинает принимать подключение от подчиненного Сервера, используя порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Просмотр списка подчиненных Серверов администрирования

Чтобы просмотреть список подчиненных (включая виртуальные) Серверов администрирования:

В главном меню нажмите на имя Сервера администрирования, которое находится рядом со значком параметров ( ).

Отобразится раскрывающийся список подчиненных (включая виртуальные) Серверов администрирования.

Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

Группы администрирования тоже отображаются, но они неактивны и недоступны для управления в этом меню.

Если вы подключены к главному Серверу администрирования в Консоли OSMP и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- Измените существующую установку Консоли OSMP, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Консоли OSMP.

  1. На устройстве, где установлена Консоль OSMP, запустите установочный файл Консоли OSMP, соответствующий дистрибутиву Linux, установленному на вашем устройстве, под учетной записью с правами администратора.

     Запустится мастер установки приложения. Для продолжения работы мастера нажмите на кнопку **Далее**.

  2. Выберите параметр **Обновить**.

  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

  6. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

- Используйте Консоль OSMP, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете

переключиться на виртуальный Сервер администрирования в Консоли OSMP.

Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования;
- включение и выключение виртуальных Серверов администрирования;
- назначение администратора виртуального Сервера администрирования;
- смена Сервера администрирования для клиентских устройств;
- удаление виртуальных Серверов администрирования.

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования.

Чтобы создать и добавить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
2. На открывшейся странице выберите вкладку **Серверы администрирования**.
3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
   Виртуальный Сервер администрирования будет управлять устройствами из выбранной группы (включая подгруппы).
4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.
5. На открывшейся странице задайте свойства нового виртуального Сервера администрирования:
   - **Имя виртуального Сервера администрирования**.
   - **Адрес подключения Сервера администрирования**
     Вы можете указать имя или IP-адрес Сервера администрирования.
6. Из списка пользователей выберите администратора виртуального Сервера администрирования. Существующую учетную запись при необходимости можно изменить перед тем, как назначить ей роль администратора; можно также создать новую учетную запись.
7. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

Если вы подключены к главному Серверу администрирования в Консоли OSMP и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- **Измените существующую установку Консоли OSMP, добавив подчиненный Сервер в список доверенных Серверов администрирования**. После этого вы сможете подключиться к виртуальному Серверу администрирования в Консоли OSMP.

  1. На устройстве, где установлена Консоль OSMP, запустите установочный файл Консоли OSMP, соответствующий дистрибутиву Linux, установленному на вашем устройстве, под учетной записью с правами администратора.

     Запустится мастер установки приложения. Для продолжения работы мастера нажмите на кнопку **Далее**.

  2. Выберите параметр **Обновить**.

  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

  6. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

- Используйте Консоль OSMP, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Консоли OSMP.

Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

Чтобы включить или выключить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

2. На открывшейся странице выберите вкладку **Серверы администрирования**.

3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.

4. В меню нажмите на кнопку **Подключить / отключить виртуальный Сервер администрирования**.

   Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что у администратора нет прав доступа на главном Сервере администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

Чтобы войти в Консоль OSMP, администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль. Консоль OSMP выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан.
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции → Права пользователей**.

Настройка прав доступа вручную

Чтобы назначить администратора виртуального Сервера администрирования:

1. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:
   a. Нажмите на значок шеврона (>) справа от текущего имени Сервера администрирования.
   b. Выберите требуемый Сервер администрирования.

2. В главном меню нажмите на значок параметров () рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Права доступа** нажмите на кнопку **Добавить**.

   Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.

4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **OK**.

   Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.

5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.

6. Настройте права администратора на виртуальном Сервере администрирования.

   Для успешной аутентификации администратор должен иметь следующие права:

   - право **Чтение** в функциональной области **Общие функции** → **Базовая функциональность**.
   - право **Чтение** в функциональной области **Общие функции** → **Виртуальные Серверы администрирования**.

Приложение сохраняет измененные права пользователя в учетной записи администратора.

Настройка прав доступа с помощью назначения пользовательских ролей

Также вы можете предоставить права доступа администратору виртуального Сервера администрирования через пользовательскую роль. Например, это может быть полезно, если вы хотите назначить несколько администраторов на один и тот же виртуальный Сервер администрирования. В этом случае вы можете назначить учетным записям администраторов одну или несколько пользовательских ролей вместо того, чтобы настраивать одни и те же права для нескольких администраторов.

Чтобы назначить администратора виртуального Сервера администрирования, назначив ему пользовательские роли:

1. На главном Сервере администрирования создайте пользовательскую роль и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования. Вы можете создать несколько ролей, например, если хотите разделить доступ к разным функциональным областям.

2. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:

   a. Нажмите на значок шеврона () справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

3. Назначьте новую роль или несколько ролей учетной записи администратора.

Приложение назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области, вы можете настроить доступ к определенным объектам на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Open Single Management Platform выберите тип задачи **Смена Сервера администрирования**.
4. Укажите имя задачи, которую вы создаете.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами.
7. Задайте параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой была установлена и запущена приложение, выполняющая эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

   - **Учетная запись**

     Учетная запись, от имени которой будет запускаться задача.

   - **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

13. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Open Single Management Platform, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

Чтобы удалить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем Сервера администрирования.

2. На открывшейся странице выберите вкладку **Серверы администрирования**.

3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.

4. В строке меню нажмите на кнопку **Удалить**.

Виртуальный Сервер администрирования удален.

Настройка журнала событий подключения к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

Чтобы настроить регистрацию событий подключения к Серверу администрирования:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

3. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл /var/opt/kaspersky/klnagent_srv/logs/sc.syslog.

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.

3. Нажмите на кнопку **Сохранить**.

Изменение учетных данных СУБД

Вам может потребоваться изменить учетные данные СУБД, например, чтобы выполнить ротацию учетных данных в целях безопасности.

Чтобы изменить учетные данные СУБД в среде Windows с помощью утилиты klsrvswch.exe:

1. Запустите утилиту klsrvswch, которая расположена в папке установки Open Single Management Platform. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

2. Нажимайте на кнопку **Далее** мастера, пока не дойдете до шага **Изменить учетные данные для доступа к СУБД**.

3. На шаге мастера **Изменить учетные данные для доступа к СУБД** выполните следующие действия:

   Шаг мастера **Изменить учетные данные для доступа к СУБД** пропускается, если используется аутентификация Windows.

   - Выберите параметр **Применить новые учетные данные**.
   - Укажите новое имя учетной записи в поле **Учетная запись**.
   - Укажите новый пароль для учетной записи в поле **Пароль**.
   - Подтвердите новый пароль в поле **Подтвердить пароль**.

   Вам нужно указать учетные данные учетной записи, которая существует в СУБД.

4. Нажмите на кнопку **Далее**.

После завершения работы мастера учетные данные СУБД изменяются.

Утилиту klsrvswch можно использовать только для изменения пароля учетной записи для аутентификации SQL. Изменение способа авторизации не поддерживается. Для изменения способа авторизации переустановите Сервер администрирования и укажите нужные параметры.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет сохранять данные Сервера администрирования в определенном состоянии и восстанавливать данные при необходимости, например, если данные Сервера администрирования повреждены.

Прежде чем создавать резервную копию данных Сервера администрирования, проверьте, добавлен ли виртуальный Сервер администрирования в группу администрирования. Если виртуальный Сервер администрирования добавляется перед резервным копированием, убедитесь, что этому виртуальному Серверу назначен администратор. Вы не можете предоставить права администратора к виртуальному Серверу администрирования после резервного копирования. Обратите внимание, если учетные данные администратора утеряны, вы не сможете назначить нового администратора виртуальному Серверу администратора.

Вы можете создать резервную копию данных Сервера администрирования, только запустив задачу *Резервное копирование Сервера администрирования*. Эта задача создается автоматически при развертывании Open Single Management Platform.

На главном Сервере администрирования создание и удаление задачи *Резервное копирование данных Сервера администрирования* недоступно.

Резервная копия сохраняется в папке `/var/spool/ksc backup`. Папка резервного копирования создается автоматически на рабочем узле, на котором установлен Сервер администрирования, при развертывании Open Single Management Platform. На главном Сервере администрирования невозможно изменить путь к папке резервного копирования.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- База данных Сервера администрирования (политики, задачи, параметры приложения, события, сохраненные на Сервере администрирования)
- Детали конфигурации структуры групп администрирования и клиентских устройств
- Хранилище дистрибутивов приложений для удаленной установки
- Сертификат Сервера администрирования

Восстановление данных Сервера администрирования возможно только с помощью утилиты KDT.

Вы можете создать резервную копию Ядра KUMA и при необходимости восстановить его из резервной копии. Также можно создавать резервные копии других компонентов Open Single Management Platform с помощью сторонних инструментов, только если вы используете СУБД, установленную на отдельном сервере вне кластера Kubernetes. Не нужно создавать резервную копию базы данных Сервера администрирования с помощью инструментов сторонних производителей.

Настройка задачи резервного копирования данных Сервера администрирования

Задача *Резервное копирование данных Сервера администрирования* создается автоматически при развертывании Open Single Management Platform и не может быть удалена. Вы можете создать резервную копию данных Сервера администрирования, только запустив задачу *Резервное копирование Сервера администрирования*.

Чтобы настроить задачу резервного копирования данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи** и выберите задачу **Создание резервной копии Сервера администрирования**.
2. Выберите задачу **Создание резервной копии Сервера администрирования**.

   Откроется окно свойств задачи.
3. При необходимости укажите общие параметры задачи в соответствии с вашими требованиями.
4. В разделе **Параметры приложения** установите защиту паролем резервного копирования и количество резервных копий, если это необходимо.

   Рекомендуется ограничить количество резервных копий данных Сервера администрирования, чтобы избежать переполнения дискового пространства, выделенного для хранения резервных копий.
5. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Задача *Резервное копирование данных Сервера администрирования* настроена.

Использование утилиты KDT для восстановления данных Сервера администрирования

Задача *Резервное копирование данных Сервера администрирования* позволяет копировать данные Сервера администрирования для резервного копирования. Для восстановления данных Сервера администрирования необходимо использовать утилиту KDT.

Чтобы восстановить данные Сервера администрирования:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

   `./kdt invoke ksc --action listBackup`

   Отобразится список резервных копий, находящихся в папке `/var/spool/ksc/backup`.
2. Выполните следующую команду:

   `./kdt invoke ksc --action restoreBackup --param ksc_file_backup='<file name>' --param ksc_backup_password="<password>"`

   где

   - `ksc_file_backup` – путь к нужному архиву резервных копий и имя архива.
   - `ksc_backup_password` – пароль архива, если резервная копия была сохранена с паролем. Если пароль не использовался, установите для переменной `ksc_backup_password` значение "".

Данные Сервера администрирования восстанавливаются из выбранного архива.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

Чтобы удалить иерархию Серверов администрирования:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем главного Сервера администрирования.

2. На открывшейся странице выберите вкладку **Серверы администрирования**.

3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.

4. В меню выберите пункт **Удалить**.

5. В открывшемся окне нажмите на кнопку **ОК** для подтверждения удаления подчиненного Сервера администрирования.

Бывший главный и бывшие подчиненные Серверы администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

Доступ к общедоступным DNS-серверам

Если доступ к серверам "Лаборатории Касперского" через системный DNS невозможен, Open Single Management Platform может использовать публичные DNS-серверы в следующем порядке:

1. Google Public DNS (8.8.8.8).

2. Cloudflare DNS (1.1.1.1).

3. Alibaba Cloud DNS (223.6.6.6).

4. Quad9 DNS (9.9.9.9).

5. CleanBrowsing (185.228.168.168).

Запросы к DNS-серверам могут содержать доменные адреса и общедоступный IP-адрес Сервера администрирования, так как приложение устанавливает TCP/UDP-соединение с DNS-сервером. Если Open Single Management Platform использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса.

Чтобы настроить использование публичного DNS с помощью утилиты klscflag:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду, чтобы выключить использование публичного DNS:

```
./kdt invoke ksc --action klscflag --param klscflag_param=" -fset -pv
".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1"
```

2. Чтобы включить использование публичного DNS, выполните следующую команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=" -fset -pv
".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0"
```

Настройка интерфейса

Вы можете настроить интерфейс Консоли OSMP на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

Чтобы настроить интерфейс Консоли OSMP в соответствии в соответствии с используемым в настоящее время набором функций:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса.**
2. Включите или выключите нужные параметры:
   - **Показать раздел "Шифрование и защита данных"**
   - **Показать EDR-алерты**
3. Нажмите на кнопку **Сохранить**.

После включения требуемых параметров консоль отображает соответствующие разделы в главном меню. Например, если вы включите параметр **Показать EDR-алерты**, в главном меню появится раздел **Мониторинг и отчеты** → **Алерты** (сначала убедитесь, что вы добавили лицензионный ключ для EDR Optimum для просмотра информации об обнаруженных угрозах на конечных устройствах).

Шифрование подключения TLS

Чтобы закрыть уязвимости в сети вашей организации, вы можете включить шифрование трафика с использованием TLS-протокола. Вы можете включить протоколы шифрования TLS и поддерживаемые наборы шифрования на Сервере администрирования. Open Single Management Platform поддерживает TLS-протокол версий 1.0, 1.1, 1.2 и 1.3. Вы можете выбрать требуемый протокол шифрования и наборы шифрования.

Open Single Management Platform использует самоподписанные сертификаты. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные доверенным центром сертификации.

Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

   ```
   ./kdt invoke ksc --action klscflag --param klscflag_param=" -fset -pv
   ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <значение> -t d"
   ```

   Используйте флаг SrvUseStrictSslSettings, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования.

   Укажите параметр <value> флага SrvUseStrictSslSettings:

   - 4 – включены только TLS-протоколы версий 1.2 и 1.3. Также включены наборы шифрования с TLS_RSA_WITH_AES_256_GCM_SHA384 (эти наборы шифрования необходимы для обратной совместимости с Kaspersky Security Center 11). Это значение по умолчанию.

     Наборы шифрования поддерживаемые TLS-протоколом 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (с набором шифрования TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-SHA256

Наборы шифрования поддерживаемые TLS-протоколом 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 – включены только TLS-протоколы версий 1.2 и 1.3. Для TLS-протоколов версий 1.2 и 1.3 поддерживаются определенные наборы шифрования, перечисленные ниже.

  Наборы шифрования поддерживаемые TLS-протоколом 1.2:

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  Наборы шифрования поддерживаемые TLS-протоколом 1.3:

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

Не рекомендуется использовать значения 0, 1, 2 или 3 для значений параметра флага SrvUseStrictSslSettings. Эти значения параметров соответствуют небезопасным версиям TLS-протокола (протоколы TLS 1.0 и TLS 1.1) и небезопасным наборам шифрования и используются только для обратной совместимости с более ранними версиями Kaspersky Security Center.

2. Перезапустите следующие службы Open Single Management Platform:

- службу Сервера администрирования;
- службу Веб-сервера;
- службу активации прокси-сервера.

Шифрование трафика с помощью TLS-протокола включено.

Вы можете использовать флаги KLTR_TLS12_ENABLED и KLTR_TLS13_ENABLED, чтобы включить поддержку TLS-протоколов 1.2 и 1.3 соответственно. Эти флаги включены по умолчанию.

Чтобы включить или выключить поддержку TLS-протоколов 1.2 и 1.3,

На устройстве администратора, на котором расположена утилита KDT, выполните одну из следующих команд:

- Чтобы включить или выключить поддержку TLS-протокола 1.2:

  ```
  ./kdt invoke --action klscflag --param klscflag_param=" -fset -pv ".core/.independent"
  -s Transport -n KLTR_TLS12_ENABLED -v <значение> -t d"
  ```

- Чтобы включить или выключить поддержку TLS-протокола 1.3:

  ```
  ./kdt invoke --action klscflag --param klscflag_param=" -fset -pv ".core/.independent"
  -s Transport -n KLTR_TLS13_ENABLED -v <значение> -t d"
  ```

Укажите параметр `<значение>` флага:

- `1` – чтобы включить поддержку TLS-протокола.
- `0` – чтобы выключить поддержку TLS-протокола.

Обнаружение устройств в сети

В этом разделе описаны поиск устройств и опрос сети.

Open Single Management Platform позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- управляемые устройства в группах администрирования Сервера администрирования и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений безопасности. При обнаружении сетевых устройств можно получить о них информацию и управлять ими с помощью политик. Регулярные опросы сети необходимы для проверки появления новых устройств и наличия обнаруженных ранее устройств в сети.

Обнаружение сетевых устройств состоит из следующих этапов:

1. **Первоначальное обнаружение устройств**

   Выполните обнаружение устройств вручную.

2. **Настройка будущих опросов**

   Убедитесь, что опрос IP-диапазонов включен и что расписание опроса соответствует требованиям вашей организации. При настройке расписания опроса опирайтесь на рекомендации для частоты опросов сети.

Также можно включить опрос Zeroconf, если в вашей сети есть IPv6-устройства.

Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена.

Вы можете выполнять опрос IP-диапазонов и опрос Zeroconf только с помощью точки распространения.

3. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. При необходимости можно настроить правила автоматического перемещения этих устройств в группу **Управляемые устройства**. Можно также настроить правила хранения.

   Если вы пропустили этап, на котором задаются правила, все новые обнаруженные устройства будут помещены в группу **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.

Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Опрос IP-диапазонов

Open Single Management Platform позволяет опрашивать IP-диапазоны только с помощью точки распространения. Точка распространения пытается выполнить обратное преобразование имен: для каждого IPv4-адреса из указанного диапазона выполнить преобразование в DNS-имя с помощью стандартных DNS-запросов. Если данная операция завершается успешно, точка распространения отправляет запрос `ICMP ECHO REQUEST` (аналог команды `ping`) на полученное имя. Если устройство отвечает, информация об этом устройстве добавляется в базу данных Open Single Management Platform. Обратное преобразование имен необходимо для исключения сетевых устройств, которые могут иметь IP-адреса, но не являются компьютерами, таких как сетевые принтеры или роутеры.

Этот способ опроса основывается на правильно настроенной локальной службе DNS. Для его использования должна быть настроена зона обратного просмотра DNS. Если эта зона не настроена, опрос IP-подсети не даст результатов.

Первоначально точка распространения получает IP-диапазоны для опроса из сетевых параметров устройства, который выполняет роль точки распространения. Если адрес устройства 192.168.0.1 и маска подсети – 255.255.255.0, сеть 192.168.0.0/24 включена в список адресов для автоматического опроса. Точка распространения выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Если включен только опрос IP-диапазонов, точка распространения обнаруживает устройства только с IPv4-адресами. Если в вашей сети есть IPv6-устройства, включите опрос Zeroconf устройств.

Опрос IP-диапазонов с помощью точки распространения

Чтобы настроить опрос IP-диапазонов с помощью точки распространения:

1. Откройте свойства точки распространения.
2. Перейдите в раздел **Опрос IP-диапазонов** и выберите параметр **Разрешить опрос диапазона**.

   Откроется окно **IP-диапазон**
3. Укажите имя нового IP-диапазона.
4. Нажмите на кнопку **Добавить** и укажите IP-диапазон с помощью адреса и маски подсети или с помощью начального и конечного IP-адреса. Также можно добавить существующую подсеть, нажав на кнопку **Обзор**.
5. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

   Варианты расписания опроса:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

   - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

     Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

     По умолчанию параметр выключен.

6. Включите параметр **Использовать Zeroconf для опроса IPv6-сетей**, чтобы точка распространения выполняла опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*).

   В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

После завершения опроса вновь обнаруженные устройства автоматически включаются в группу **Управляемые устройства**, если вы настроили и включили правила перемещения устройств. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Опрос контроллеров домена

Open Single Management Platform поддерживает опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4.

При опросе контроллера домена Сервер администрирования или точка распространения получают информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен.

Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.

Предварительные требования

Перед опросом контроллеров домена убедитесь, что включены следующие протоколы:

- Simple Authentication and Security Layer (SASL).
- Lightweight Directory Access Protocol (LDAP).

Убедитесь, что на устройстве контроллеров домена доступны следующие порты:

- 389 для SASL.
- 636 для TLS.

Опрос контроллеров домена с помощью Сервера администрирования

Чтобы опросить контроллеры домена с помощью Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.
2. Нажмите на кнопку **Параметры опроса**.

   Откроется окно **Параметры опроса контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.

4. В разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, укажите адрес и учетные данные пользователя контроллеров домена.

5. При необходимости в окне **Параметры опроса контроллеров домена** укажите расписание опроса. По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

   Доступны следующие варианты расписания опроса сети:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

   - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

     Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

     По умолчанию параметр выключен.

   Если вы измените учетные записи пользователей в группе безопасности домена, эти изменения отобразятся в Open Single Management Platform через час после опроса контроллеров домена.

6. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

7. Если требуется запустить опрос сети немедленно, нажмите на кнопку **Начать опрос**.

Опрос контроллеров домена с помощью точки распространения

Также можно опрашивать контроллеры домена с помощью точки распространения. Управляемое устройство с операционной системой Windows или Linux может выступать в роли точки распространения.

Для точки распространения с операционной системой Linux поддерживается опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba.
Для точки распространения с операционной системой Windows поддерживается только опрос контроллеров домена Microsoft Active Directory.
Опрос с помощью точки распространения с операционной системой Mac не поддерживается.

Чтобы настроить опрос контроллеров домена с помощью точки распространения:

1. Откройте свойства точки распространения.
2. Выберите раздел **Опрос контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.
4. Выберите контроллеры домена, которые вы хотите опросить.

   Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллеров домена.

   Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

   - **Опросить текущий домен**
   - **Опросить весь лес доменов**
   - **Опросить указанные домены**
5. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

После завершения опроса в разделе **Контроллеры доменов** отобразится структура домена.

Если вы настроили и включили правила перемещения устройств, новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в Консоли OSMP.

Аутентификация и подключение к контроллеру домена

При первоначальном подключении к контроллеру домена Сервер администрирования идентифицирует протокол подключения. Этот протокол используется для всех будущих подключений к контроллеру домена.

Первоначальное подключение к контроллеру домена происходит следующим образом:

1. Сервер администрирования пытается подключиться к контроллеру домена по TLS.

По умолчанию проверка сертификата не требуется. Для флага KLNAG_LDAP_TLS_REQCERT установите значение 1, чтобы принудительно выполнить проверку сертификата.

По умолчанию для доступа к цепочке сертификатов используется зависящий от операционной системы путь к центру сертификации (CA). Используйте флаг KLNAG_LDAP_SSL_CACERT, чтобы указать другой путь.

2. В случае сбоя TLS-соединения Сервер администрирования пытается подключиться к контроллеру домена по SASL (DIGEST-MD5).

3. В случае сбоя подключения по SASL (DIGEST-MD5) Сервер администрирования использует простую проверку подлинности (Simple Authentication) по незашифрованному TCP-соединению для подключения к контроллеру домена.

Вы можете использовать команды KDT для настройки флагов. Например, вы можете принудительно проверить сертификат. Для этого на устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=" -fset -pv klserver -n
KLNAG_LDAP_TLS_REQCERT -t d -v 1"
```

Настройка контроллеров домена Samba

Open Single Management Platform поддерживает контроллеры домена Linux, работающие только на Samba 4.

Контроллер домена Samba поддерживает те же расширения схемы, что и контроллер домена Microsoft Active Directory. Вы можете включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory, используя расширение схемы Samba 4. Это необязательное действие.

Рекомендуется включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory. Это обеспечит корректное взаимодействие Open Single Management Platform и контроллером домена Samba.

Чтобы включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory:

1. Выполните следующую команду, чтобы использовать расширение схемы RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Включите обновление схемы на контроллере домена Samba. Для этого добавьте следующую строку в файл `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   Если обновление схемы завершается с ошибкой, необходимо выполнить полное восстановление контроллера домена, который выполняет роль схемы master.

Если вы хотите правильно опросить контроллер домена Samba, вам нужно указать `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`.

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Open Single Management Platform обнаруживает временные виртуальные машины и добавляет данные о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Кроме того, несуществующие виртуальные машины могут отображаться в Консоли OSMP.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Open Single Management Platform реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI в свойствах инсталляционного пакета Агента администрирования, который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

Чтобы включить динамический режим VDI:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно **Свойства**.
3. В окне **Свойства** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** выберите параметр **Включить динамический режим для VDI**.

Устройство, на которое устанавливается Агент администрирования, будет являться частью VDI.

Перемещение в группу администрирования устройств, являющихся частью VDI

Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования:

1. Перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. На вкладке **Условия правила** выберите вкладку **Виртуальные машины**.
4. Установите для правила **Является виртуальной машиной** значение **Да** и для **Часть Virtual Desktop Infrastructure** значение **Да.**

5. Нажмите на кнопку **Сохранить**.

Управление клиентскими устройствами

Open Single Management Platform позволяет управлять клиентскими устройствами:

- Просматривать параметры и статусы управляемых устройств, в том числе кластеров и массивов серверов.
- Настраивать точки распространения.
- Управлять задачами.

Группы администрирования можно использовать для объединения клиентских устройств в набор, которым можно управлять как единым целым. Клиентское устройство может быть включено только в одну группу администрирования. Устройства могут быть автоматически отнесены к группе на основе **Условия правила**:

- Создание правил перемещения устройств.
- Копирование правил перемещения устройств.
- Условия для правила перемещения устройств.

Вы можете использовать выборки устройств, чтобы для фильтровать устройства по условию. Вы также можете назначать теги устройствам для создания выборок устройств, поиска устройств и распределения устройств между группами администрирования.

Параметры управляемого устройства

Чтобы просмотреть параметры управляемого устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.

Откроется окно свойств выбранного устройства.

В верхней части окна свойств отображаются следующие вкладки, на которых представлены основные группы параметров:

- **Общие**

Эта вкладка содержит следующие разделы:

- Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

  - **Имя**

    В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

  - **Описание**

    В поле можно ввести дополнительное описание клиентского устройства.

  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на устройстве и активности устройства в сети.

  - **Полное название группы**

    Группа администрирования, в состав которой входит клиентское устройство.

  - **Последнее обновление антивирусных баз**

    Дата последнего обновления баз или приложений на устройстве.

  - **Соединение с Сервером администрирования**

    Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

  - **Последнее появление в сети**

    Дата и время, когда устройство последний раз было видимо в сети.

  - **Версия Агента администрирования**

    Версия установленного Агента администрирования.

  - **Создано**

    Дата создания устройства в Open Single Management Platform.

  - **Владелец устройства**

Имя владельца устройства. Вы можете назначить или удалить пользователя в качестве владельца устройства, нажав на ссылку **Сменить владельца устройства**.

- **Не разрывать соединение с Сервером администрирования**

  Если флажок установлен, поддерживается непрерывное соединение между Сервером администрирования и клиентским устройством.

  Если флажок снят, клиентское устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  По умолчанию флажок установлен, если на устройстве установлен Сервер администрирования.

  Если на устройстве установлен только Агент администрирования, по умолчанию флажок снят.

- В разделе **Сеть** отображается следующая информация о сетевых свойствах клиентского устройства:

  - **IP-адрес**

    IP-адрес устройства.

  - **Windows-домен**

    Windows-домен или рабочая группа, в которую входит устройство.

  - **DNS-имя**

    Имя DNS-домена устройства.

  - **NetBIOS-имя**

    Имя клиентского устройства в сети Windows.

  - **IPv6-адрес**

- В разделе **Система** представлена информация об операционной системе, установленной на клиентском устройстве:

  - **Операционная система**
  - **Архитектура процессора**
  - **Имя устройства**
  - **Тип виртуальной машины**

    Производитель виртуальной машины

- **Динамическая виртуальная машина как часть VDI**

  В этой строке показано, является ли клиентское устройство динамической виртуальной машиной как часть VDI.

- В разделе **Защита** представлена следующая информация о состоянии антивирусной защиты на клиентском устройстве:

  - **Видимо в сети**

    Статус видимости клиентского устройства.

  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на устройстве и активности устройства в сети.

  - **Описание статуса**

    Статус защиты клиентского устройства и подключения к Серверу администрирования.

  - **Состояние защиты**

    Статус текущего состояния постоянной защиты клиентского устройства.

  - **Последняя полная проверка**

    Дата и время последнего поиска вирусов на клиентском устройстве.

  - **Обнаружен вирус**

    Общее количество обнаруженных на клиентском устройстве вирусов (счетчик обнаруженных вирусов) со времени установки приложения защиты (первой проверки устройства), либо со времени последнего обнуления значения этой величины.

  - **Объекты, которые не удалось вылечить**

    Количество необработанных файлов на клиентском устройстве.

    В поле не учитывается количество необработанных файлов для мобильных устройств.

  - **Статус шифрования дисков**

    Текущее состояние шифрования файлов на локальных дисках устройства.

- В разделе **Статус устройства определен приложением** отображается информация о статусе устройства, который определен управляемым приложением, установленным на клиентском

устройстве. Это состояние устройства может отличаться от того, которое определено Open Single Management Platform.

- **Приложения**

  На этой вкладке отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве. Вы можете нажать на имя приложения, чтобы просмотреть общую информацию о приложении, список событий, произошедших на устройстве, и параметры приложения.

- **Действующие политики и профили политик**

  На этой вкладке отображаются списки политик и профилей политик, которые активны на управляемом устройстве.

- **Задачи**

  В разделе **Задачи** можно управлять задачами клиентского устройства: просматривать список существующих, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры, просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. В случае отсутствия связи статус не отображается.

- **События**

  В разделе **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

- **Проблемы безопасности**

  В разделе **Инциденты** можно просматривать, редактировать и создавать инциденты для клиентского устройства. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать по этому поводу инцидент. В тексте инцидента администратор может кратко описать ситуацию и рекомендуемые действия, например, административные меры в отношении пользователя, а также добавить ссылку на пользователя.

  Инцидент, для которого выполнены необходимые действия, называется обработанным. Наличие необработанных инцидентов может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

  В разделе содержится список инцидентов, созданных для устройства. Инциденты классифицируются по уровню важности и типу. Тип инцидента определяется приложением "Лаборатории Касперского", которая создает инцидент. Обработанные инциденты можно отметить в списке, установив флажок в графе **Обработан**.

- **Теги**

В разделе **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые и переименовывать старые теги, удалять теги.

- Дополнительно

Эта вкладка содержит следующие разделы:

- **Реестр приложений**. В этом разделе можно просмотреть реестр установленных на клиентском устройстве приложений и обновлений для них, а также настроить отображение реестра приложений.

  Информация об установленных приложениях предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

  При нажатии на имя приложения открывается окно, содержащее сведения о приложении и список пакетов обновлений, установленных для этого приложения.

- **Исполняемые файлы**. В этом разделе отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

- **Точки распространения**. В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.

  - **Экспортировать в файл**

    По кнопке **Экспортировать в файл** вы можете сохранить в файле список агентов обновлений, с которыми взаимодействует устройство. По умолчанию приложение экспортирует список устройств в файл формата CSV.

  - **Свойства**

    По кнопке **Свойства** вы можете посмотреть и настроить параметры агента обновлений, с которым взаимодействует устройство.

- **Реестр оборудования**. В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

- **Применимые обновления**. В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Уязвимости в приложениях**. В этом разделе можно просмотреть список с информацией об уязвимостях сторонних приложений, установленных на клиентских устройствах.

  Чтобы сохранить уязвимости в файл, установите флажки рядом с уязвимостями, которые вы хотите сохранить, и нажмите на кнопку **Экспортировать в CSV** или на кнопку **Экспортировать в TXT**.

  Раздел содержит следующие параметры:

  - **Показывать только те уязвимости, которые можно закрыть**

    Если флажок установлен, в разделе отображаются уязвимости, которые можно закрыть патчем.

    Если флажок снят, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

    По умолчанию флажок установлен.

  - **Свойства уязвимости**

Нажмите на имя уязвимости в приложениях в списке, чтобы просмотреть свойства выбранной уязвимости в приложениях в отдельном окне. В окне свойств можно выполнить следующие действия:

- Пропустить уязвимость в приложениях на этом управляемом устройстве (в Консоли администрирования или в OSMP).
- Просмотреть список рекомендуемых исправлений для уязвимости.
- Вручную указать обновления программного обеспечения для закрытия уязвимости (в Консоли администрирования или в OSMP).
- Просмотреть экземпляр уязвимости.
- Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

- **Удаленная диагностика**. В этом разделе можно выполнять удаленную диагностику клиентских устройств.

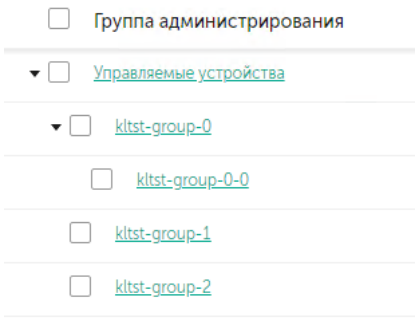
Если вы используете СУБД PostgreSQL, MariaDB или MySQL, на вкладке **События** может отображаться неполный список событий для выбранного клиентского устройства. Это происходит, когда СУБД хранит очень большое количество событий. Вы можете увеличить количество отображаемых событий, выполнив одно из следующих действий:

- Удалить ненужные события.
- Сократить срок хранения ненужных событий.

Чтобы увидеть полный список событий, зарегистрированных на Сервере администрирования для устройства, используйте Отчеты.

Создание групп администрирования

Сразу после установки Open Single Management Platform в иерархии групп администрирования присутствует только одна группа администрирования – **Управляемые устройства**. При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы (см. рисунок ниже).

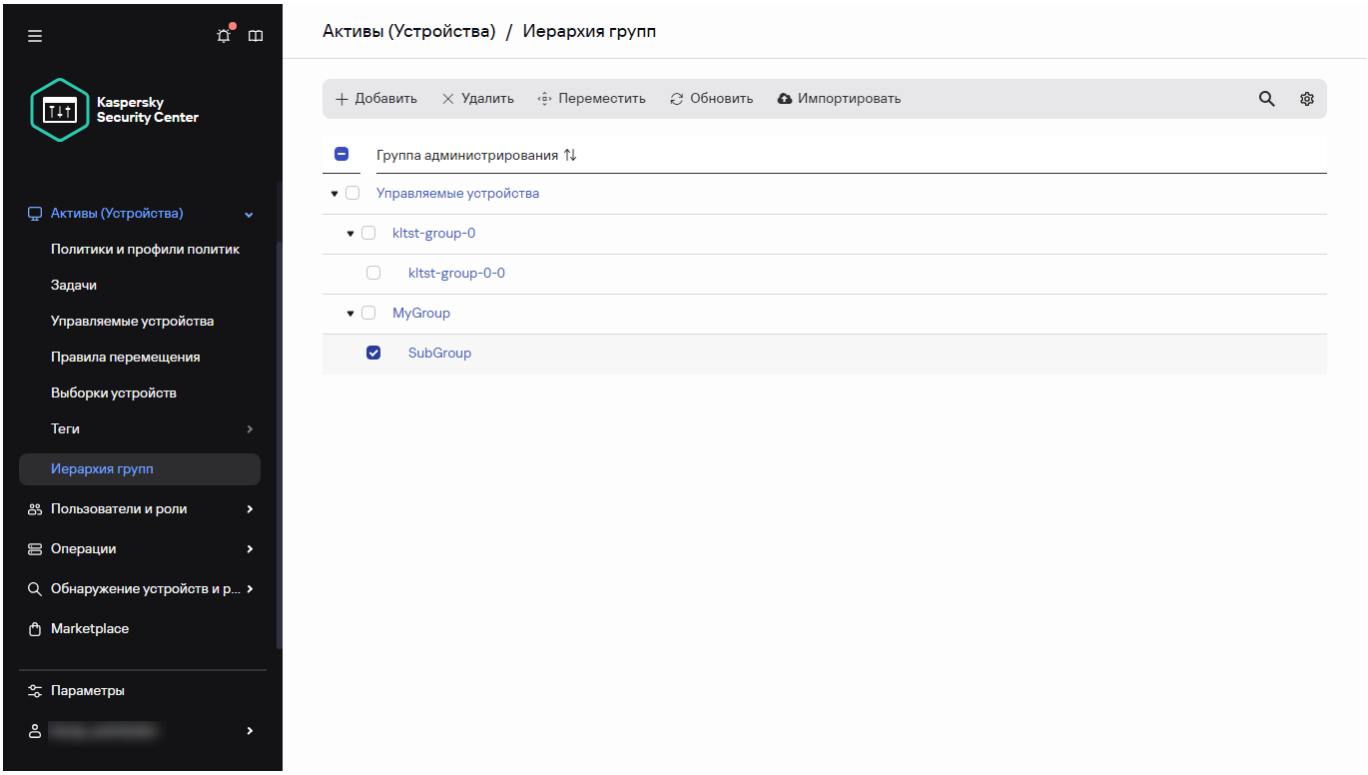


Просмотр иерархии групп администрирования

Чтобы создать группу администрирования:

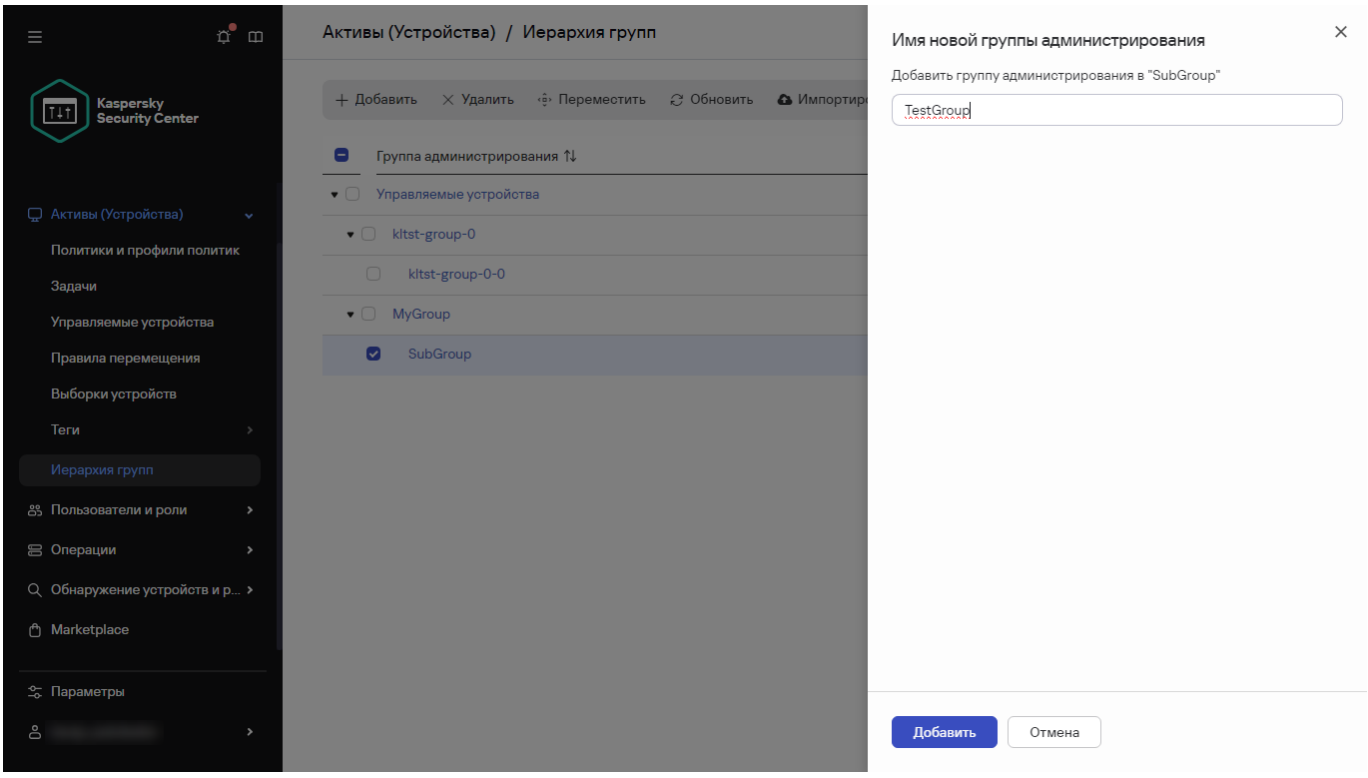
1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.



3. Нажмите на кнопку **Добавить**.

4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.



В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

Чтобы создать структуру групп администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Правила перемещения устройств

Рекомендуется автоматизировать процесс размещения устройств в группах администрирования при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Open Single Management Platform в явном виде, в разделе **Активы (Устройства)** → **Правила перемещения**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает нераспределенные устройства только один раз устройства. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу нераспределенных устройств. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила снимите флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования** заблокирован в свойствах автоматически созданных правил перемещения. Такие правила создаются при добавлении задачи Удаленная *установка приложения или создании автономного* инсталляционного пакета.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

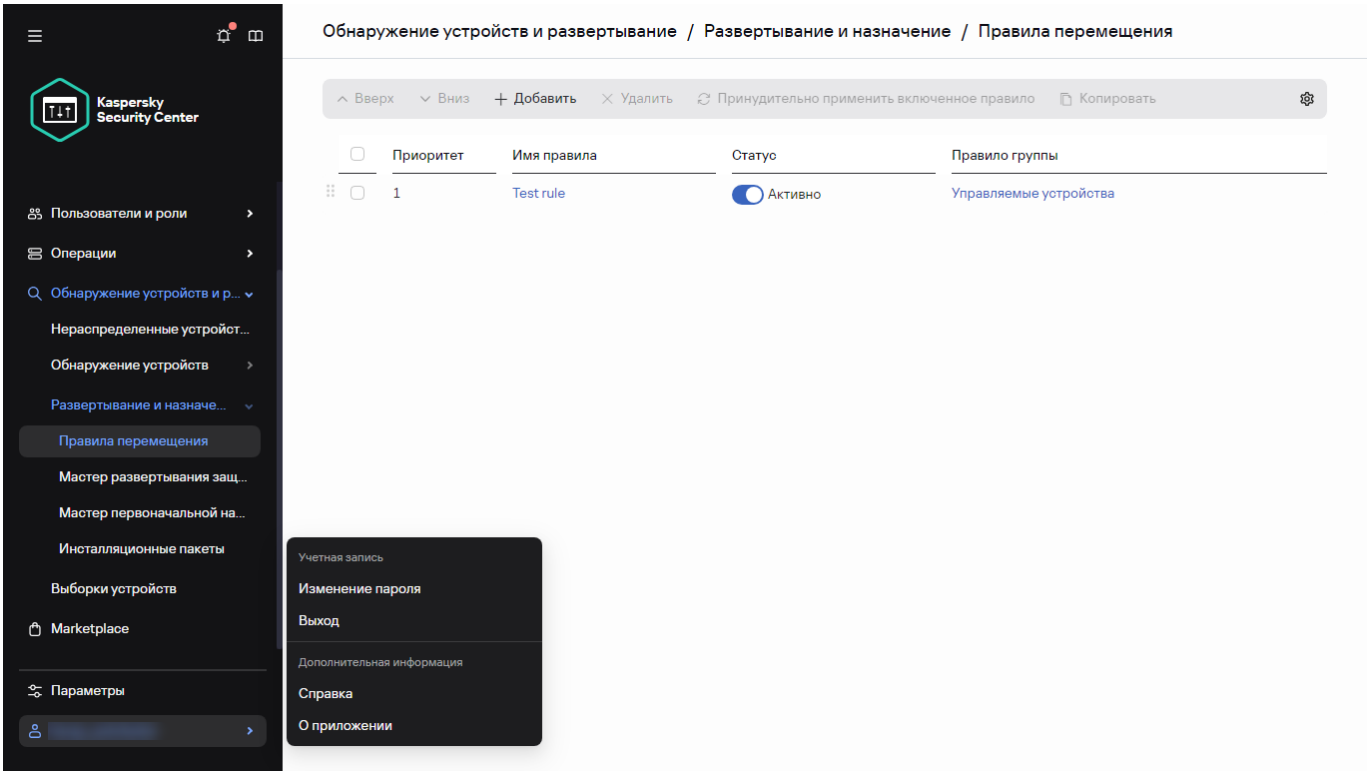
Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Open Single Management Platform (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике.

Создание правил перемещения устройств

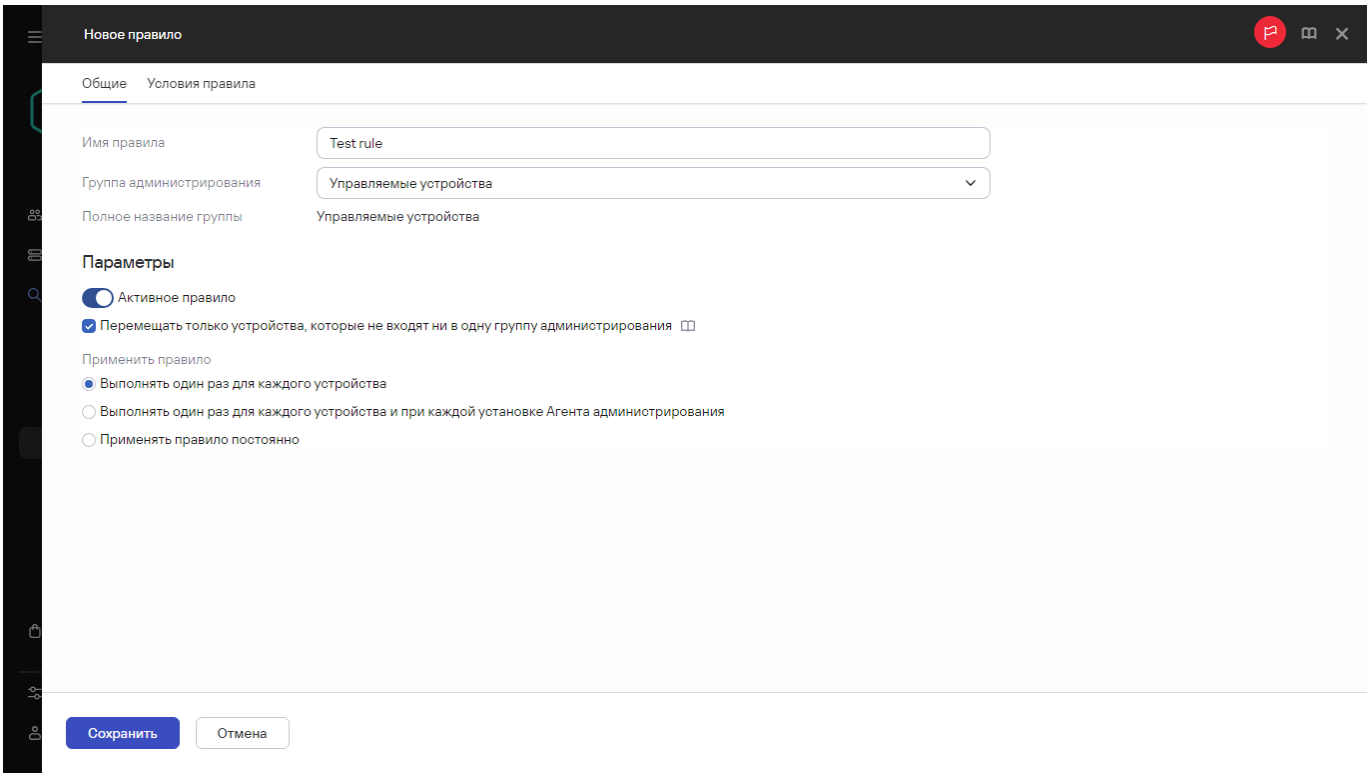
Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования.

Чтобы создать правило перемещения устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.



2. Нажмите на кнопку **Добавить**. Откроется окно **Новое правило**.



3. В открывшемся окне укажите следующие данные на вкладке **Общие**:

- **Имя правила**

  Укажите имя нового правила активации.

  Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

Вы можете выбрать один из следующих вариантов:

- **Выполнять один раз для каждого устройства**

  Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

- **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

  Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

- **Применять правило постоянно**

  Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

4. На вкладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.

5. Нажмите на кнопку **Сохранить**.

Правило перемещения создано. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет. Чтобы повысить или понизить приоритет правила перемещения, с помощью мыши переместите правило вверх или вниз по списку соответственно.

Если выбран параметр **Применять правило постоянно**, правило перемещения применяется независимо от приоритета. Такие правила применяются по расписанию, которое Сервер администрирования устанавливает автоматически.

Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

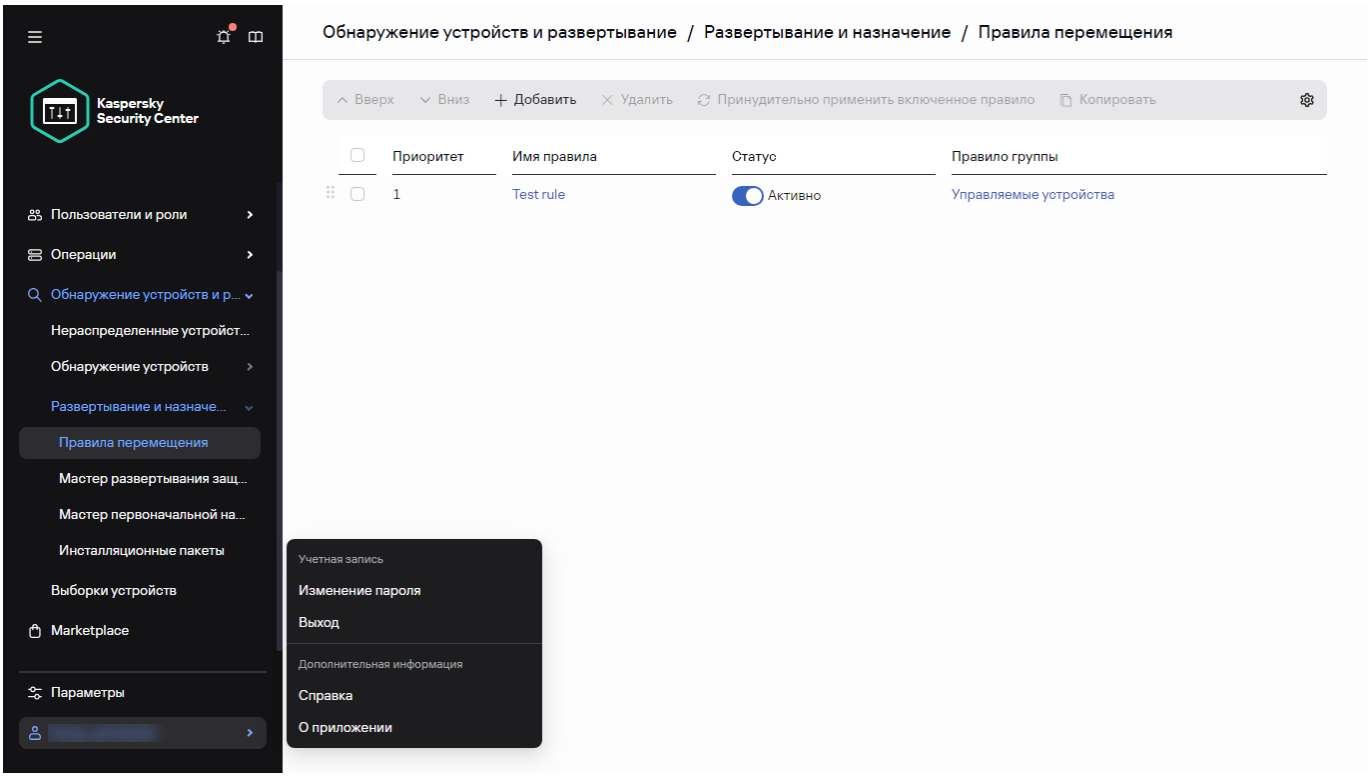
Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:

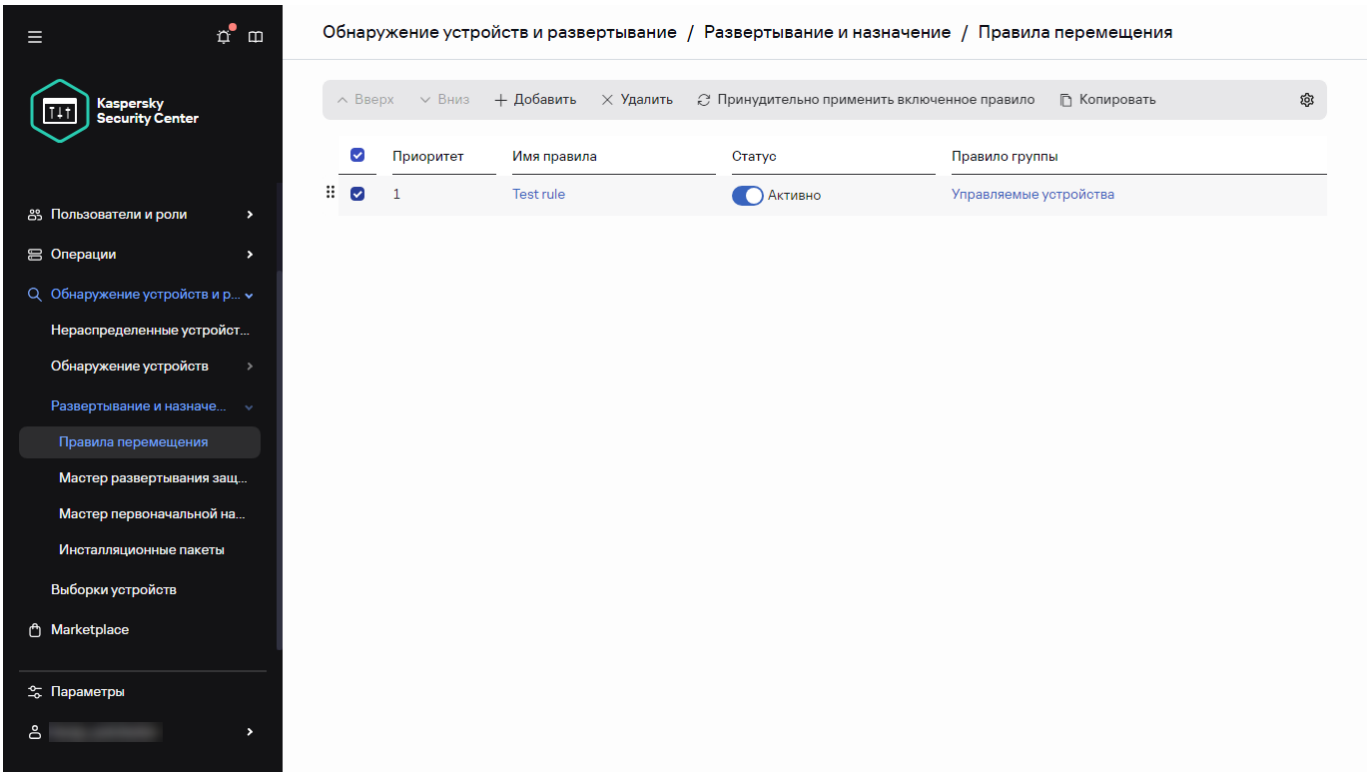
   - В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Правила перемещения**.

   Отобразится список правил перемещения устройств.



2. Установите флажок напротив правила, которое требуется скопировать.



3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне при необходимости измените данные на вкладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:

- **Имя правила**

  Укажите имя нового правила активации.

  Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

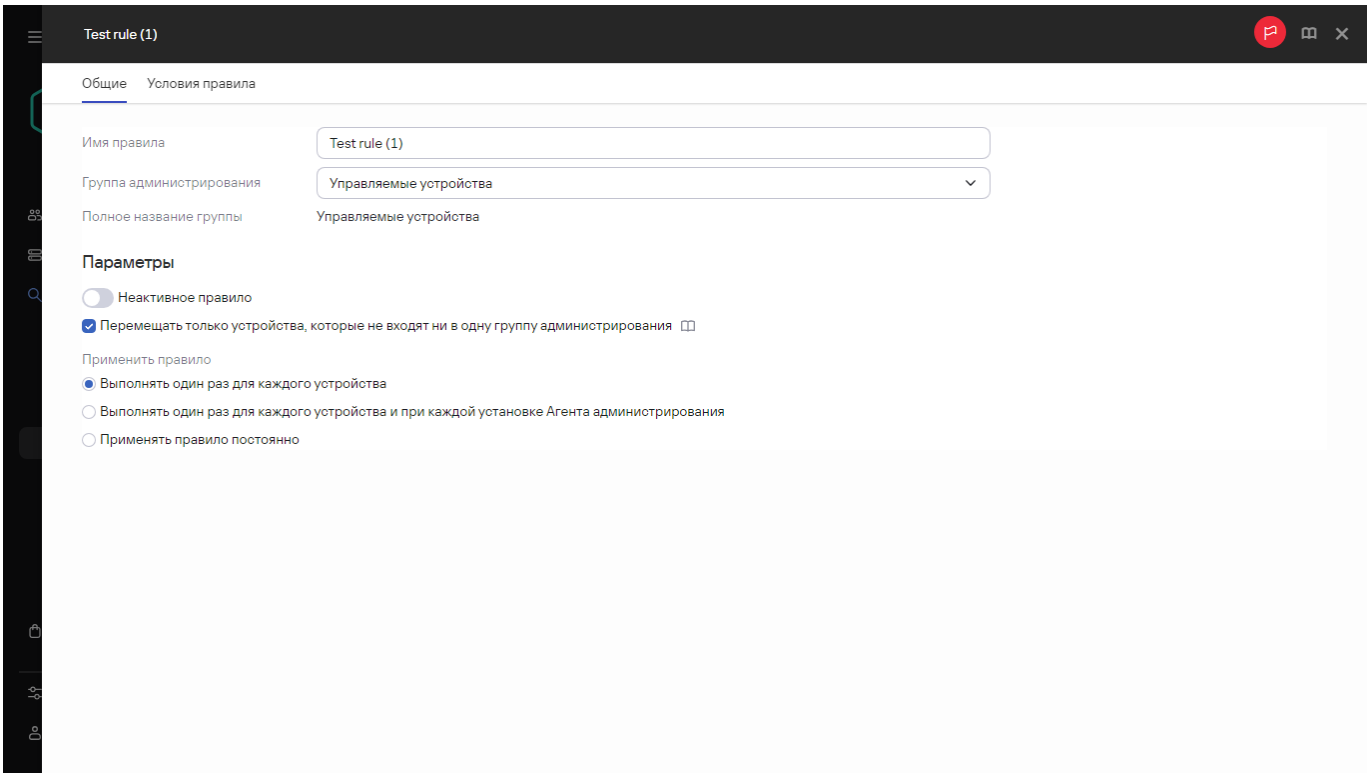
    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - **Применять правило постоянно**

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).



5. На вкладке **Условия правила** укажите критерии для устройств, которые требуется переместить автоматически.

6. Нажмите на кнопку **Сохранить**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

Условия для правила перемещения устройств

При создании или копировании правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств. Чтобы определить, какие устройства следует перемещать, можно использовать следующие критерии:

- Теги, присвоенные клиентским устройствам.
- Параметры сети. Например, вы можете перемещать устройства с IP-адресами из указанного диапазона.
- Управляемые приложения, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Информация об организационном подразделении Active Directory (OU) с клиентскими устройствами.
- Информация об облачном сегменте с клиентскими устройствами.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

Вкладка Теги

На этой вкладке можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания клиентских устройств. Для этого выберите необходимые теги. Кроме того, вы можете включить следующие параметры:

- **Применить к устройствам без выбранных тегов**

  Если этот параметр включен, все устройства с указанными тегами исключаются из правила перемещения устройств. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

  По умолчанию параметр выключен.

- **Применить, если есть хотя бы один из выбранных тегов**

  Если этот параметр включен, правило перемещения устройств применяется к клиентским устройствам хотя бы с одним из выбранных тегов. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

  По умолчанию параметр выключен.

Вкладка Сеть

На этой вкладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

- **Имя устройства в сети Windows**

  Имя устройства в сети Windows (NetBIOS-имя).

- **Windows-домен**

  Правило перемещения устройств применяется ко всем устройствам, включенным в указанный Windows-домен.

- **DNS-имя устройства**

  DNS-имя домена клиентского устройства, которое вы хотите переместить. Заполните это поле, если в вашей сети есть DNS-сервер.

  Если для базы данных, которую вы используете для Open Single Management Platform, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правило перемещения устройств не будет работать.

- **DNS-домен**

  Правило перемещения устройств применяется ко всем устройствам, включенным в указанный основной DNS-суффикс. Заполните это поле, если в вашей сети есть DNS-сервер.

- **IP-диапазон**

  Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию флажок снят.

- **IP-адрес подключения к Серверу администрирования**

  Если этот параметр включен, можно задать IP-адреса, по которым клиентские устройства подключаются к Серверу администрирования. Для этого укажите IP-диапазон, включающий все необходимые IP-адреса.

  По умолчанию параметр выключен.

- **Изменение профиля подключения**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам с измененным профилем подключения.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, профиль подключения которых не изменялся.
  - **Значение не выбрано**. Условие не применяется.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
  - **Значение не выбрано**. Условие не применяется.

Вкладка Приложения

На этой вкладке можно настроить правило перемещения устройств на основе управляемых приложений и операционных систем, установленных на клиентских устройствах:

- **Агент администрирования установлен**

Выберите одно из следующих значений:

- **Да**. Правило перемещения устройств применяется только к клиентским устройствам, на которых установлен Агент администрирования.
- **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, на которых не установлен Агент администрирования.
- **Значение не выбрано**. Условие не применяется.

- **Приложения**

  Укажите, какие управляемые приложения должны быть установлены на клиентских устройствах, чтобы к этим устройствам применялось правило перемещения устройств. Например, вы можете выбрать **Агент администрирования Kaspersky Security Center 15.2** или **Сервер администрирования Kaspersky Security Center 15.2**.

  Если вы не выберете управляемое приложение, условие не будет применяться.

- **Версия операционной системы**

  Можно выбирать клиентские устройства на основе версии операционной системы. Для этого укажите операционные системы, которые должны быть установлены на клиентских устройствах. В результате правило перемещения устройств применяется к клиентским устройствам с выбранными операционными системами.

  Если этот параметр выключен, условие не применяется. По умолчанию параметр выключен.

- **Архитектура операционной системы**

  Можно выбирать клиентские устройства по разрядности операционной системы. В поле **Архитектура операционной системы** можно выбрать одно из следующих значений:

  - **Нет данных**
  - **x86**
  - **AMD64**
  - **IA64**

  Чтобы проверить разрядность операционной системы клиентских устройств:

  1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
  2. Нажмите на кнопку **Параметры столбцов** справа ( ).
  3. Выберите параметр **Архитектура операционной системы** и нажмите на кнопку **Сохранить**.

     После этого для каждого управляемого устройства отобразится разрядность операционной системы.

- **Версия пакета обновления операционной системы**

В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Пользовательский сертификат**

  Выберите одно из следующих значений:

  - **Установлено**. Правило перемещения устройств применяется только к мобильным устройствам с мобильным сертификатом.
  - **Не установлено**. Правило перемещения устройств применяется только к мобильным устройствам без мобильного сертификата.
  - **Значение не выбрано**. Условие не применяется.

- **Номер сборки операционной системы**

  Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

- **Номер выпуска операционной системы**

  Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

Вкладка Виртуальные машины

На этой вкладке можно настроить параметры правила перемещения клиентских устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

- **Является виртуальной машиной**

В раскрывающемся списке можно выбрать одно из следующих значений:

- **Неизвестно**. Условие не применяется.
- **Нет**. Перемещаемые устройства не должны являться виртуальными машинами.
- **Да**. Перемещаемые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**
- **Часть Virtual Desktop Infrastructure**

В раскрывающемся списке можно выбрать одно из следующих значений:

- **Неизвестно**. Условие не применяется.
- **Нет**. Перемещаемые устройства не должны являться частью VDI.
- **Да**. Перемещаемые устройства должны являться частью VDI.

Вкладка Контроллеры домена

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в организационное подразделение домена. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

- **Устройство входит в следующее подразделение**

Если этот параметр включен, правило перемещения устройств применяется к устройствам из организационного подразделения контроллера домена, указанного в списке под параметром.

По умолчанию параметр выключен.

- **Включать дочерние подразделения**

Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

По умолчанию флажок снят.

- **Перемещать устройства из дочерних подразделений в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, отсутствующие в домене**
- **Устройство включено в следующую группу безопасности домена**

Если этот параметр включен, правило перемещения устройств применяется к устройствам из доменной группы безопасности, указанной в списке под параметром.

По умолчанию параметр выключен.

Вкладка Облачные сегменты

На этой вкладке можно указать, что требуется перемещать устройства, которые относятся к определенным облачным сегментам:

- **Устройство находится в облачном сегменте**

  При выборе этого параметра правило перемещения устройств применяется к клиентским устройствам, принадлежащим облачному сегменту. Вы можете выбрать нужный облачный сегмент вплоть до подсети в списке под параметром.

  По умолчанию параметр выключен.

- **Включать дочерние объекты**

  При выборе этого параметра правило перемещения устройств применяется не только к выбранному облачному сегменту, но и к дочерним объектам этого сегмента.

  По умолчанию параметр выключен.

- **Перемещать устройства в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, для которых нет соответствия в облачных сегментах**
- **Устройство обнаружено с помощью API**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API.

  - **Да**. Устройство обнаруживается с помощью AWS API. Это значит, что устройство обязательно находится в облачном окружении.
  - **Нет**. Устройство не обнаруживается с помощью AWS API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью AWS API.
    - **Значение не выбрано**. Критерий не применяется.

Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Перейдите по ссылке **Текущий путь:** `<текущий_путь>` над списком.

3. В открывшемся окне выберите группу администрирования, в которую требуется добавить устройства.

4. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.

5. Составьте список устройств, которые вы хотите добавить в группу администрирования.

   > В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Выберите, как вы хотите добавить устройства в список:

   - Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:
     - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.
     - Укажите IP-адреса устройств или IP-диапазон.
     - Укажите DNS-имя устройства.

       > Поле с именем устройства не должно содержать пробелы, отступы, а также следующие запрещенные символы: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

   - Нажмите на кнопку **Импортировать устройства из файла**, чтобы импортировать список устройств из файла формата TXT. Каждый адрес устройства (или имя устройства) должен располагаться в отдельной строке.

     > Файл не должен содержать пробелы, отступы, а также следующие запрещенные символы: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.

7. После того как вы убедитесь, что в списке нет ошибок, нажмите на кнопку **Далее**.

Мастер обрабатывает список устройств и отображает результат. После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Перемещение устройств или кластеров в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

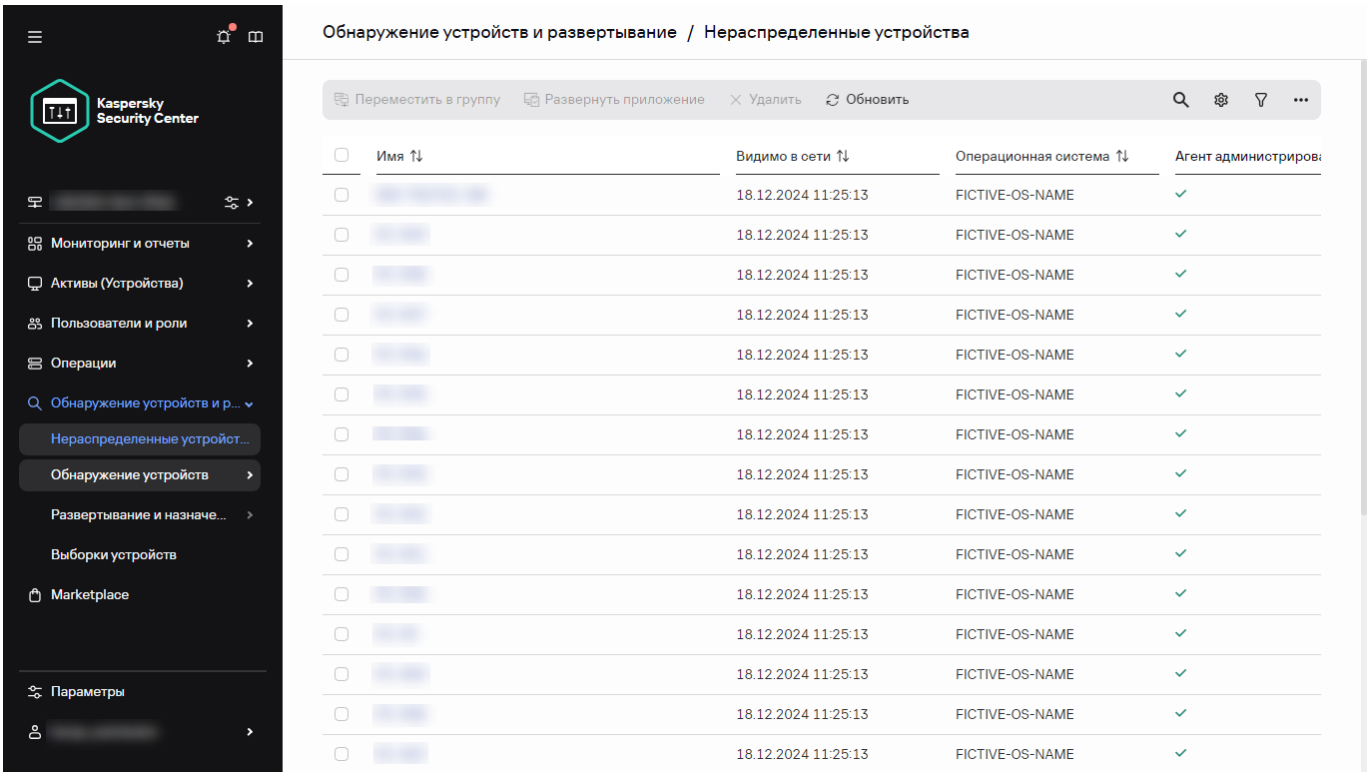
Также можно перемещать кластеры или массивы серверов из одной группы администрирования в другую. При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования. При выборе одного узла кластера на вкладке **Устройства**, кнопка **Переместить в группу** становится недоступной.

Чтобы переместить одно или несколько устройств или кластеров в состав выбранной группы администрирования:

1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:

   - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** и в открывшейся слева панели выберите группу администрирования.

   - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.



Список нераспределенных устройств

2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Управляемые устройства** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.

3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.

4. Нажмите на кнопку **Переместить в группу**.

5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.

6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

О кластерах и массивах серверов

Open Single Management Platform поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера нельзя. Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Посмотреть свойства.
- Переместить кластер или массив серверов в другую группу администрирования.

  При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования.
- Удалить

  Целесообразно удалять кластер или массив серверов только тогда, когда кластер или массив серверов больше не существует в сети организации. Если кластер по-прежнему виден в вашей сети, а Агент администрирования и приложение "Лаборатории Касперского" по-прежнему установлено на узлах кластера, Open Single Management Platform автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

Свойства кластеров или массивов серверов

Чтобы просмотреть параметры кластера или массива серверов:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → **Кластеры и массивы серверов**.

   Отображается список кластеров и массивов серверов.

2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером администрирования:

- **Имя**
- **Описание**
- **Windows-домен**

  Windows-домен или рабочая группа, содержащая кластер или массив серверов.

- **NetBIOS-имя**

  Имя кластера или массива серверов в сети Windows.

- **DNS-имя**

  Имя DNS-домена кластера или массива серверов.

Задачи

На вкладке **Задачи** вы можете управлять задачами, назначенными для кластеров и массивов серверов: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять параметры задач и просматривать результаты выполнения. Перечисленные задачи относятся к приложению "Лаборатории Касперского", установленного на узлах кластера. Open Single Management Platform получает список задач и информацию о статусе задач от узлов кластера. В случае отсутствия связи статус не отображается.

Узлы

На этой вкладке отображается список узлов, входящих в кластер или массив серверов. Вы можете нажать на имя узла, чтобы просмотреть окно свойств устройства.

Приложения "Лаборатории Касперского"

Окно свойств также может содержать дополнительные вкладки с информацией и параметрами, относящимися к приложению "Лаборатории Касперского", установленному на узлах кластера.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Open Single Management Platform выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*.

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.
- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.
- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим".

Число уникально назначенных точек распространения в сети, содержащей один сегмент, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Число уникально назначенных точек распространения в сети, содержащей несколько сегментов, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10 – 100	1

Более 100	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10 – 30	1
31 – 300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Open Single Management Platform будет сам выбирать, какие устройства назначать точками распространения.

Чтобы назначить точки распространения автоматически:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Автоматически назначать точки распространения**.

   > Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **Сохранить**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Назначение точек распространения вручную

Open Single Management Platform позволяет вручную назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Open Single Management Platform будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Чтобы вручную назначить устройство точкой распространения:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Вручную назначать точки распространения**.

4. Нажмите на кнопку **Назначить**.

5. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.

7. Нажмите на кнопку **ОК**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

8. Нажмите на добавленную точку распространения в списке, чтобы открыть окно ее свойств.

9. В окне свойств настройте параметры точки распространения:

   - В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами.

     - **SSL-порт**

Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к агенту обновлений с использованием протокола SSL.

По умолчанию номер порта – 13000.

- **Использовать многоадресную IP-рассылку**

  Если флажок установлен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

- **Адрес IP-рассылки**

  IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

  По умолчанию указан IP-адрес 225.6.7.8.

- **Номер порта IP-рассылки**

  Номер порта многоадресной рассылки.

  Номер порта по умолчанию – 15001. Если в качестве агента обновлений указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Адрес точки распространения для удаленных устройств**

  IPv4-адрес, через который удаленные устройства подключаются к точке распространения.

- **Распространять обновления**

  Если флажок установлен, обновления распространяются на клиентские устройства с помощью этого агента обновлений.

  По умолчанию флажок установлен.

- **Распространять инсталляционные пакеты**

  Если флажок установлен, инсталляционные пакеты обновления распространяются на клиентские устройства с помощью этого агента обновлений.

  По умолчанию флажок установлен.

- **Запустить push-сервер**

В Open Single Management Platform точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

- **Порт push-сервера**

  Номер порта push-сервера. Вы можете указать номер любого свободного порта.

- В разделе **Область действия** укажите группы администрирования, которым точка распространения будет распространять обновления.

- В разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения:

  - **Источник обновлений**

    Выберите источник обновлений для точки распространения:

    - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.

    - Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*.

      - Если такая задача уже существует для устройства, выберите задачу в списке.

      - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

  - **Загрузить файлы различий**

    Этот параметр включает функцию загрузки файлов различий.

    По умолчанию параметр включен.

- В разделе **Параметры подключения к интернету** можно настроить параметры доступа к сети интернет:

  - **Использовать прокси-сервер**

    Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

    По умолчанию флажок снят.

- **Адрес прокси-сервера**

  Адрес прокси-сервера.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

  Если флажок установлен, то при подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

  По умолчанию флажок снят.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

  - **Пересылать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **Игнорировать параметры прокси-сервера для подключения к KPSN**

  Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

  Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **Использовать UDP-порт**

  Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер UDP-порта. По умолчанию параметр включен.

- **UDP-порт**

  Номер UDP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Использовать HTTPS**

  Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- **Через HTTPS-порт**

  Номер HTTPS-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- В разделе **Шлюз соединения** можно настроить точку распространения как шлюз соединения для экземпляров Агента администрирования и Сервером администрирования:

  - **Шлюз соединения**

    Если прямое соединение между Сервером администрирования и Агентами администрирования не может быть установлено из-за организации вашей сети, вы можете использовать точку распространения в качестве шлюза соединения между Сервером администрирования и Агентами администрирования.

    Включите этот параметр, если требуется, чтобы точка распространения выполняла роль шлюза соединения между Агентами администрирования и Сервером администрирования. По умолчанию параметр выключен.

  - **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**

    Если Сервер администрирования находится за пределами демилитаризованной зоны (DMZ), в локальной сети, Агенты администрирования, установленные на удаленных устройствах, не могут подключаться к Серверу администрирования. Вы можете использовать точку распространения в качестве шлюза соединения с обратным подключением (Сервер администрирования устанавливает соединение с точкой распространения).

    Включите этот параметр, если требуется подключить Сервер администрирования к шлюзу соединения в демилитаризованной зоне.

  - **Открыть локальный порт для Kaspersky Security Center Web Console**

    Включите этот параметр, если вам нужен шлюз соединения в демилитаризованной зоне, чтобы открыть порт для Web Console, находящейся в демилитаризованной зоне или в интернете. Укажите номер порта, который будет использоваться для подключения Web Console к точке распространения. По умолчанию установлен порт 13299.

    Это параметр доступен, если включен параметр **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**.

  При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

  - **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт для мобильных устройств, и укажите номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13292. Мобильное устройство проверит сертификат Сервера администрирования. При установке соединения только Сервер администрирования выполняет аутентификацию.

- **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

  Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт, который будет использоваться для двусторонней аутентификации Сервера администрирования и мобильных устройств. Мобильное устройство проверит сертификат Сервера администрирования, а Сервер администрирования проверит сертификат мобильного устройства. Задайте следующие параметры:

  - Номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13293.
  - Имена DNS-доменов шлюза соединения, которые будут использоваться мобильными устройствами. Разделяйте имена доменов запятыми. Указанные имена доменов будут включены в сертификат точки распространения. Если имена доменов, используемые мобильными устройствами, не совпадают с общим именем в сертификате точки распространения, мобильные устройства не подключаются к точке распространения.

    Имя DNS-домена по умолчанию – это полное имя домена шлюза соединения.

  В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос контроллеров домена с помощью точки распространения.

  - **Опрос контроллеров домена**

    Вы можете включить обнаружение устройств для контроллеров домена.

    Если вы выбрали параметр **Включить опрос контроллеров домена**, вы можете выбрать контроллеры домена для опроса и задать расписание.

    Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллера домена.

    Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

    - **Опросить текущий домен**
    - **Опросить весь лес доменов**
    - **Опросить указанные домены**

- Настройте опрос IP-диапазонов точкой распространения.

  - **Опрос IP-диапазонов.**

Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.
  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на агенте обновлений установлен Агент администрирования.

  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на агенте обновлений, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на агенте обновлений запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
3. В открывшейся панели слева выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения.

   Для этого используйте пункт меню **Точки распространения**.
4. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Точки распространения**.

5. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить**.

6. Чтобы удалить назначенные точки распространения, выберите устройства из списка и нажмите на кнопку **Отменить назначение**.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

Включение push-сервера

В Open Single Management Platform точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве сервера push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Чтобы включить push-сервер на точке распространения:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.

   Откроется окно свойств точки распространения.

4. В разделе **Общие** включите параметр **Запустить push-сервер**.

5. В поле **Порт push-сервера** укажите номер порта. Вы можете указать номер любого свободного порта.

6. В поле **Адрес удаленного устройства** укажите IP-адрес или имя точки распространения.

7. Нажмите на кнопку **ОК**.

Push-сервер включен на выбранной точке распространения.

О статусах устройства

Open Single Management Platform присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Open Single Management Platform учитывает видимость устройства в сети (см. таблицу ниже). Если Open Single Management Platform не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический/Видим в сети*.
- *Предупреждение* или *Предупреждение/Видим в сети*.
- *OK* или *OK/Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний.

		• Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача *Синхронизация обновлений Windows Update* больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.

Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлено*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Переключатель выключен. • Переключатель включен.

Open Single Management Platform позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Open Single Management Platform с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Open Single Management Platform присваивает устройству статус, для некоторых условий (см. столбец "Описание условий" в таблице выше) учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. Откройте окно свойств одним из следующих способов:

   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.

- В контекстном меню группы администрирования выберите пункт **Свойства**.

2. В открывшемся окне **Свойства** в панели **Разделы** выберите **Статус устройства**.
3. В разделе **Установить статус 'Критический', если** установите флажок для условия из списка.

   Однако вы можете изменить параметры, которые не заблокированы в родительской политике.

4. Для выбранного условия установите необходимое вам значение.

   Вы можете установить значения для некоторых условия, но не для всех.

5. Нажмите на кнопку **OK**.

При невыполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. Откройте окно свойств одним из следующих способов:

   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.

2. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Статус устройства**.
3. В разделе **Установить статус 'Предупреждение', если** установите флажок для условия из списка.

   Однако вы можете изменить параметры, которые не заблокированы в родительской политике.

4. Для выбранного условия установите необходимое вам значение.

   Вы можете установить значения для некоторых условия, но не для всех.

5. Нажмите на кнопку **OK**.

При невыполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Выборки устройств

Выборки устройств – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Open Single Management Platform предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки невозможно удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

Просмотр списка устройств из выборки устройств

Open Single Management Platform позволяет просматривать список устройств из выборки устройств.

Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств** или в раздел **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Вы можете группировать и фильтровать данные таблицы устройств следующим образом:
   - Нажмите на значок параметров ( ) и выберите столбцы для отображения в таблице.
   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица устройств.

Вы можете выбрать одно или несколько устройств в выборке устройств и нажать на кнопку **Новая задача**, чтобы создать задачу, которая будет применена к этим устройствам.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры выборки устройств**.
3. Введите имя новой выборки.
4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:
   - **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.

- **Искать управляемые устройства** – поиск устройств, соответствующих критериям выборки, в группе **Управляемые устройства**.
- **Искать нераспределенные устройства** – поиск устройств, соответствующих критериям выборки, в группе **Нераспределенные устройства**.

Вы можете установить флажок **Включать данные подчиненных Серверов администрирования**, чтобы включить поиск устройств, отвечающих критериям выборки, на подчиненных Серверах администрирования.

5. Нажмите на кнопку **Добавить**.
6. В открывшемся окне укажите условия, которые должны быть выполнены для включения устройств в эту выборку и нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

Настройка выборки устройств

Чтобы настроить параметры выборки устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.
2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.
3. На вкладке **Общие** перейдите по ссылке **Новое условие**.
4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.
5. Нажмите на кнопку **Сохранить**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

Если флажок установлен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

По умолчанию флажок снят.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя).

- **Домен**

  Будут отображаться все устройства, входящие в указанный домен Windows.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие** или в разделе **Заметки**.

Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

- Внутри одного слова:
  - *****. Заменяет любую строку длиной 0 и более символов.

    Пример:

    Для описания слов **Сервер**, **Серверный** или **Серверная** можно использовать строку **Сервер***
  - **?**. Заменяет любой один символ.

    Пример:

    Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

    Символ ***** или **?** не может использоваться как первый символ в описании текста.
- Для связи нескольких слов:
  - Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

    Пример:

    Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.
  - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

    Пример:

    Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.
  - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

    Пример:

    Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.
  - **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

    Пример:

    Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- IP-диапазон

  Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию флажок снят.

- Под управлением другого Сервера администрирования

Выберите одно из следующих значений:

- **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
- **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
- **Значение не выбрано**. Условие не применяется.

В разделе **Контроллеры домена** можно настроить критерии включения устройств в выборку по членству в домене:

- Устройство в подразделении домена

  Если этот параметр включен, в выборку будут включаться устройства из подразделения домена, указанного в поле ввода.

  По умолчанию параметр выключен.

- Это устройство является членом группы безопасности домена

  Если этот параметр включен, в выборку будут включаться устройства из группы безопасности домена, указанной в поле ввода.

  По умолчанию параметр выключен.

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- Является точкой распространения

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут включены устройства, являющиеся агентами обновлений.
  - **Нет**. Устройства, являющиеся агентами обновлений, не будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

- Не разрывать соединение с Сервером администрирования

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
  - **Значение не выбрано**. Критерий не применяется.

- Переключение профиля подключения

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- Последнее подключение к Серверу администрирования

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- Новые устройства, обнаруженные при опросе сети

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если флажок установлен, то в выборку попадают только новые устройства, обнаруженные при опросе сети за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если флажок снят, то в выборку попадают все устройства, обнаруженные при опросе сети.

  По умолчанию флажок снят.

- Устройство в сети

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Приложение включает в выборку устройства, которые не видимы в сети в настоящий момент.
  - **Значение не выбрано**. Критерий не применяется.

Статусы устройств

В разделе **Статус управляемых устройств** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

- Статус устройства

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *OK*, *Критический*, *Предупреждение*.

- **Статус постоянной защиты**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- **Device status description**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK*, *Критический*, *Предупреждение*.

В разделе **Статусы компонентов управляемых приложений** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых приложений:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус защиты для серверов совместной работы**

  Поиск устройств по статусу компонента защиты для серверов совместной работы (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус антивирусной защиты почтовых серверов**

  Поиск устройств по статусу компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус Endpoint Sensor**

  Поиск устройств по статусу компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- **Тип платформы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Архитектура операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Неизвестно**, **x86**, **AMD64**, **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Номер сборки операционной системы**

  Этот параметр применим только для операционных систем Windows.

  Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Номер выпуска операционной системы**

  Этот параметр применим только для операционных систем Windows.

  Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

В раскрывающемся списке можно выбрать следующие элементы:

- **Не определено**.
- **Нет**. Искомые устройства не должны являться виртуальными машинами.
- **Да**. Искомые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования, которое должно быть установлено на клиентском устройстве, чтобы оно отображалось в результатах поиска.

  В поле поддерживается полнотекстовый поиск.

- **Поставщик**

  В раскрывающемся списке можно выбрать производителя оборудования, которое должно быть установлено на устройстве, чтобы устройство отображалось в результатах поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

  Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

  Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц) от**

  Минимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Частота процессора (МГц) до**

  Максимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Количество виртуальных ядер процессора от**

  Минимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Количество виртуальных ядер процессора до**

  Максимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ), от**

  Минимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ), до**

  Максимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ) от**

  Минимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ) до**

  Максимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Информация о приложениях сторонних производителей

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

- **Название приложения**

  Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

- **Версия приложения**

  Поле ввода, в котором указывается версия выбранного приложения.

- **Поставщик**

  Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

- **Статус приложения**

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если флажок установлен, поиск будет выполняться по данным об обновлении приложений, установленных на искомых устройствах. После установки флажка названия полей ввода **Название приложения** и **Версия приложения** меняются на **Имя обновления** и **Версия обновления**.

  По умолчанию флажок снят.

- **Название несовместимого приложения безопасности**

  Раскрывающийся список, в котором можно выбрать приложения защиты сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

- **Тег приложения**

  В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

  Если флажок установлен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

  Если флажок снят, критерий не применяется.

  По умолчанию флажок снят.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Windows Update с Сервера администрирования.
- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Windows Update из другого источника.

Информация о приложениях "Лаборатории Касперского"

В разделе **Приложения "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

- **Название приложения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

  В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

  Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Статус приложения**

  Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Выбор периода последнего обновления модулей**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Устройство находится под управлением Сервера администрирования**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Приложение безопасности установлено**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение защиты:

  - **Да**. Приложение включает в выборку устройства, на которых установлено приложение защиты.
  - **Нет**. Приложение включает в выборку устройства, на которых не установлено приложение защиты.
  - **Значение не выбрано**. Критерий не применяется.

В разделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию флажок снят.

- **Количество записей в базах**

  Если флажок установлен, поиск клиентских устройств выполняется по количеству записей в базах. В полях ввода можно задать нижнее и верхнее значения количества записей.

  По умолчанию флажок снят.

- **Последняя проверка**

  Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого поиск вирусов выполнялся в последний раз.

  По умолчанию флажок снят.

- **Обнаружены угрозы**

  Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию флажок снят.

В подразделе **Шифрование** можно настроить критерии включения устройств в выборку на основе выбранного алгоритма шифрования:

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56*, *AES128*, *AES192*, *AES256*.

Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Консоли OSMP.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **Статус**

  Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства, Остановлен*, *Приостановлено*, *Запускается*, *Выполняется, Сбой*, *Не установлен, Не поддерживается лицензией*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

  Статусы, отправленные приложениями:

  - *Остановлено* – компонент отключен и в данный момент не работает.
  - *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
  - *Запускается* – компонент в настоящее время находится в процессе инициализации.
  - *Выполняется* – компонент включен и работает правильно.
  - *Сбой* – во время выполнения операции компонента произошла ошибка.
  - *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.
  - *Не поддерживается лицензией* – лицензия не распространяется на выбранный компонент.

  В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, установленных на устройстве, или устройство выключено.

- **Версия**

  Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

Применить, если есть хотя бы один из выбранных тегов

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

- **Все устройства, имеющие этот тег**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Все устройства, не имеющие этого тега**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если этот параметр включен, вы можете выбрать учетную запись пользователя, для которой настроили критерий. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся выбранным пользователем.

- **Пользователь, уже выполнявший вход в систему**

  Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Владелец устройства

В разделе **Владелец устройства** вы можете настроить критерии включения устройств в выборку в соответствии с зарегистрированными владельцами устройства, их ролями и их членством в группах безопасности:

- **Владелец устройства**

Выберите имя пользователя владельца устройства из внутренней группы безопасности. Узнайте больше о пользователях и ролях пользователей в этом разделе.

В качестве владельца устройства может быть зарегистрировано не более одного пользователя.

- **Членство владельца устройства в группе безопасности Active Directory**

  Выберите внешнюю группу безопасности Active Directory, к которой принадлежит владелец устройства.

  Пользователь может быть частью группы безопасности Active Directory или частью группы, которая входит в эту группу безопасности Active Directory.

- **Роль владельца устройства**

  Выберите роль, назначенную владельцу устройства. Подробнее о ролях пользователей см. в этой статье.

- **Членство владельца устройства во внутренней группе безопасности**

  Выберите внутреннюю группу безопасности, к которой принадлежит владелец устройства.

Экспорт списка устройств из выборки устройств

Open Single Management Platform позволяет сохранять информацию об этих устройствах из выборки устройств и экспортировать ее в файл CSV или TXT.

Чтобы экспортировать список устройств из выборки устройств:

1. Откройте таблицу с устройствами из выборки устройств.
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
   - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
   - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
   - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.
3. Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

Чтобы удалить устройства из групп администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств** или **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

   В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Теги устройств

В этом разделе описаны теги устройств, приведены инструкции по их созданию и изменению, а также по назначению тегов устройствам вручную и автоматически.

Теги устройств

Open Single Management Platform позволяет назначать *теги* устройствам. Тег представляет собой строковое значение, которое можно использовать для группировки, описания или поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Если вы хотите отметить отдельное устройство, вы можете назначить тег вручную. Автоматическое назначение тегов выполняется Kaspersky Open Single Management Platform одним из следующих способов:

- В соответствии с указанными правилами назначения тегов.
- В соответствии с указанным приложением.

> Не рекомендуется использовать разные способы назначения тегов для назначения одного и того же тега. Например, если тег назначается правилом, не рекомендуется назначать этот тег устройствам вручную.

Если теги назначаются правилами, устройствам назначаются теги автоматически при соблюдении указанных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы CentOS, назначается тег `[CentOS]`. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства под управлением операционной системы CentOS и назначить им задачу.

Тег автоматически удаляется с устройства в следующих случаях:

- Устройство перестает удовлетворять условиям правила назначения тега.
- Правило назначения тега выключено или удалено.

Списки тегов и списки правил для каждого Сервера администрирования являются независимыми для всех Серверов администрирования, включая главный Сервер администрирования и подчиненные виртуальные Серверы администрирования. Правило применяется только к устройствам под управлением того Сервера администрирования, на котором оно создано.

Создание тегов устройств

Чтобы создать тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

Изменение тегов устройств

Чтобы переименовать тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.
3. В поле **Тег** измените название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

Удаление тегов устройств

Вы можете удалить только теги, назначенные вручную.

Чтобы удалить тег устройства, назначенный вручную:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.

   Отобразится список тегов.

2. Выберите теги устройства, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **Да**.

Выбранный тег устройства удален. Удаленный тег автоматически снимается со всех устройств, которым он был назначен.

При удалении тега, назначенного устройству автоматически, правило не удаляется, и тег будет назначен новому устройству, когда устройство впервые будет соответствовать условиям правила. Если вы удалите правило автоматического назначения тега, указанный в условиях правила тег, будет удален со всех устройств, которым он был назначен, но не будет удален из списка тегов. При необходимости вы можете вручную удалить тег из списка.

Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству приложением или Агентом администрирования. Для того чтобы удалить тег с вашего устройства, используйте утилиту klscflag.

Просмотр устройств, которым назначен тег

Чтобы просмотреть устройства с назначенными тегами:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.

2. Перейдите по ссылке **Просмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

   Вы будете перенаправлены в раздел **Управляемые устройства** главного меню с устройствами, отфильтрованными по тегу, для которого вы нажали ссылку **Просмотреть устройства**.

3. Если вы хотите вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

После просмотра устройств, которым назначен тег, вы можете создать и назначить новый тег или назначить существующий тег другим устройствам. В этом случае вам придется удалить фильтр по тегу, выбрать устройства и назначить тег.

Просмотр тегов, назначенных устройству

Чтобы просмотреть теги, назначенные устройству:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

2. Выберите устройство, теги которого требуется просмотреть.

3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

Отобразится список тегов, назначенных выбранному устройству. В столбце **Назначенный тег** вы можете просмотреть, как был назначен тег.

Можно назначить другой тег устройству или удалить назначенный ранее тег. Можно также просмотреть все теги устройств, которые существуют на Сервере администрирования.

Назначение тегов устройству вручную

Чтобы вручную назначить тег устройству:

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выполните одно из следующих действий:
   - Чтобы создать и добавить новый тег, выберите пункт **Создать тег** и укажите имя тега.
   - Чтобы выбрать существующий тег, выберите пункт **Назначить существующий тег** и в раскрывающемся списке выберите нужный тег.
4. Нажмите на кнопку **OK**, чтобы применить изменения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранный тег будет назначен устройству.

Удаление назначенного тега с устройства

Чтобы снять назначенный тег с устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.
4. Установите флажок напротив тега, который требуется снять.
5. В верхней части списка нажмите на кнопку **Отменить назначение тега?**.
6. В появившемся окне нажмите на кнопку **Да**.

Тег будет снят с устройства.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Вы не можете вручную удалить теги, назначенные устройству приложениями или Агентом администрирования. Для того чтобы удалить эти теги, используйте утилиту klscflag.

Просмотр правил автоматического назначения тегов устройствам

Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**, а затем перейдите по ссылке **Настроить правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству, и нажмите на кнопку **Параметры**.

Отобразится список правил автоматического назначения тегов устройствам.

Изменение правил автоматического назначения тегов устройствам

Чтобы изменить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Выберите правило, которое требуется изменить.

   Откроется окно с параметрами правила.
3. Измените основные параметры правила:

   a. В поле **Имя правила** измените название правила.

   Название не должно быть длиннее 256 символов.

   b. Выполните одно из следующих действий:

   - Включите правило, установив переключатель в положение **Правило включено**.
   - Выключите правило, установив переключатель в положение **Правило выключено**.
4. Выполните одно из следующих действий:

   - Если вы хотите добавить новое условие, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры нового условия.
   - Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры.

- Если вы хотите удалить условие, установите флажок рядом с именем условия, которое требуется удалить, и нажмите на кнопку **Удалить**.

5. В окне с параметрами условий нажмите на кнопку **ОК**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененное правило отображается в списке.

Создание правил автоматического назначения тегов устройствам

Чтобы создать правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.

2. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами нового правила.

3. Укажите основные параметры правила:

   a. В поле **Имя правила** введите название правила.

      Название не должно быть длиннее 256 символов.

   b. Выполните одно из следующих действий:

      - Включите правило, установив переключатель в положение **Правило включено**.
      - Выключите правило, установив переключатель в положение **Правило выключено**.

   c. В поле **Тег** укажите новое название тега устройства или выберите существующий тег устройства из списка.

      Название не должно быть длиннее 256 символов.

4. В поле выбора условия нажмите на кнопку **Добавить**, чтобы добавить новое условие.

   Откроется окно с параметрами нового условия.

5. Укажите название условия.

   Название не должно быть длиннее 256 символов. Название условия должно быть уникальным в рамках одного правила.

6. Настройте срабатывание правила по следующим условиям: Можно выбрать несколько условий.

   - **Сеть** – сетевые свойства устройства (например, DNS-имя устройства или принадлежность устройства к IP-подсети).

     Если для базы данных, которую вы используете для Open Single Management Platform, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

- **Приложения** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
- **Реестр приложений** – наличие на устройстве приложений различных производителей.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения.

   При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданное правило выполняется на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

В дальнейшем правило применяется в следующих случаях:

- Автоматически, регулярно, в зависимости от загрузки сервера.
- После изменения правила.
- После выполнения правила вручную.
- После того как Сервер администрирования обнаружит изменения, которые соответствуют условиям правила, в параметрах устройства или в параметрах группы, которая содержит это устройство.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства.

Выполнение правил автоматического назначения тегов устройствам

Когда выполняется правило, тег, указанный в свойствах этого правила, назначается устройству, которое соответствует условиям, указанным в свойствах правила. Можно выполнять только активные правила.

Чтобы выполнить правила автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

Удаление правил автоматического назначения тегов с устройств

Чтобы удалить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажок напротив правила, которое требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Выбранное правило будет удалено. Тег, указанный в свойствах этого правила, будет снят со всех устройств, которым он был назначен.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска. Также шифрование данных предотвращает доступ к данным неавторизованных пользователей и приложений.

Вы можете использовать функцию шифрования данных, если в вашей сети есть управляемые устройства с операционной системой Windows, на которых установлено приложение Kaspersky Endpoint Security для Windows. В этом случае на устройствах под управлением операционной системы Windows вы можете управлять следующими типами шифрования:

- шифрование диска BitLocker;
- шифрование диска Kaspersky.

С помощью этих компонентов Kaspersky Endpoint Security для Windows вы можете, например, включать или выключать шифрование, просматривать список зашифрованных жестких дисков, формировать и просматривать отчеты о шифровании.

Чтобы настроить шифрование, настройте политику Kaspersky Endpoint Security для Windows в Open Single Management Platform. Kaspersky Endpoint Security для Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в справке Kaspersky Endpoint Security для Windows.

Управление шифрованием для иерархии Серверов администрирования в настоящее время недоступно в Web Console. Используйте главный Сервер администрирования для управления зашифрованными устройствами.

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса.

Просмотр списка зашифрованных жестких дисков

В Open Single Management Platform вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

Чтобы просмотреть список зашифрованных жестких дисков,

В главном окне приложения перейдите в раздел **Операции → Шифрование и защита данных → Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security для Windows отправляет в Open Single Management Platform информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:

в главном окне приложения перейдите в раздел **Операции → Шифрование и защита данных → События шифрования**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Также можно просмотреть список событий шифрования для каждого управляемого устройства.

Чтобы просмотреть события шифрования управляемого устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
2. Нажмите на имя управляемого устройства.

3. На вкладке **Общие** перейдите в раздел **Защита**.

4. Перейдите по ссылке **Просмотреть ошибки шифрования данных**.

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.

- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.

- Отчет о правах доступа к зашифрованным жестким дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.

- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.

- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг и отчеты** → **Отчеты**. Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств

- Отчет о правах доступа к зашифрованным жестким дискам

- Отчет об ошибках шифрования файлов

*Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Показать раздел "Шифрование и защита данных"** в параметрах интерфейса включен.

2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных**.

3. Откройте один из следующих разделов:

   - **Зашифрованные жесткие диски** – формирует отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.

   - **События шифрования** – формирует отчет об ошибках шифрования файлов.

4. Выберите название отчета, который требуется сгенерировать.

Запустится процесс формирования отчета.

Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователь может запросить доступ к зашифрованному устройству, например, если Kaspersky Endpoint Security для Windows не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в справке Kaspersky Endpoint Security для Windows.

Чтобы предоставить доступ к зашифрованному жесткому диску в автономном режиме:

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в справке Kaspersky Endpoint Security для Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security для Windows.
2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

   Отобразится список зашифрованных жестких дисков.
3. Выберите диск, у которому пользователь запросил доступ.
4. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
5. В открывшемся окне выберите плагин Kaspersky Endpoint Security для Windows.
6. Следуйте инструкциям, приведенным в справке Kaspersky Endpoint Security для Windows (см. инструкции для Консоли OSMP в конце раздела).

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования на другой для конкретных клиентских устройств. Для этого используйте задачу *Смена Сервера администрирования*.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу обслуживания Сервера администрирования.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера создания задачи **Новая задача** выберите приложение **Kaspersky Security Center 15.2** и тип задачи **Смена Сервера администрирования**. Затем укажите устройства, для которых вы хотите сменить Сервер администрирования:

   - **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в справке Kaspersky Endpoint Security для Windows.

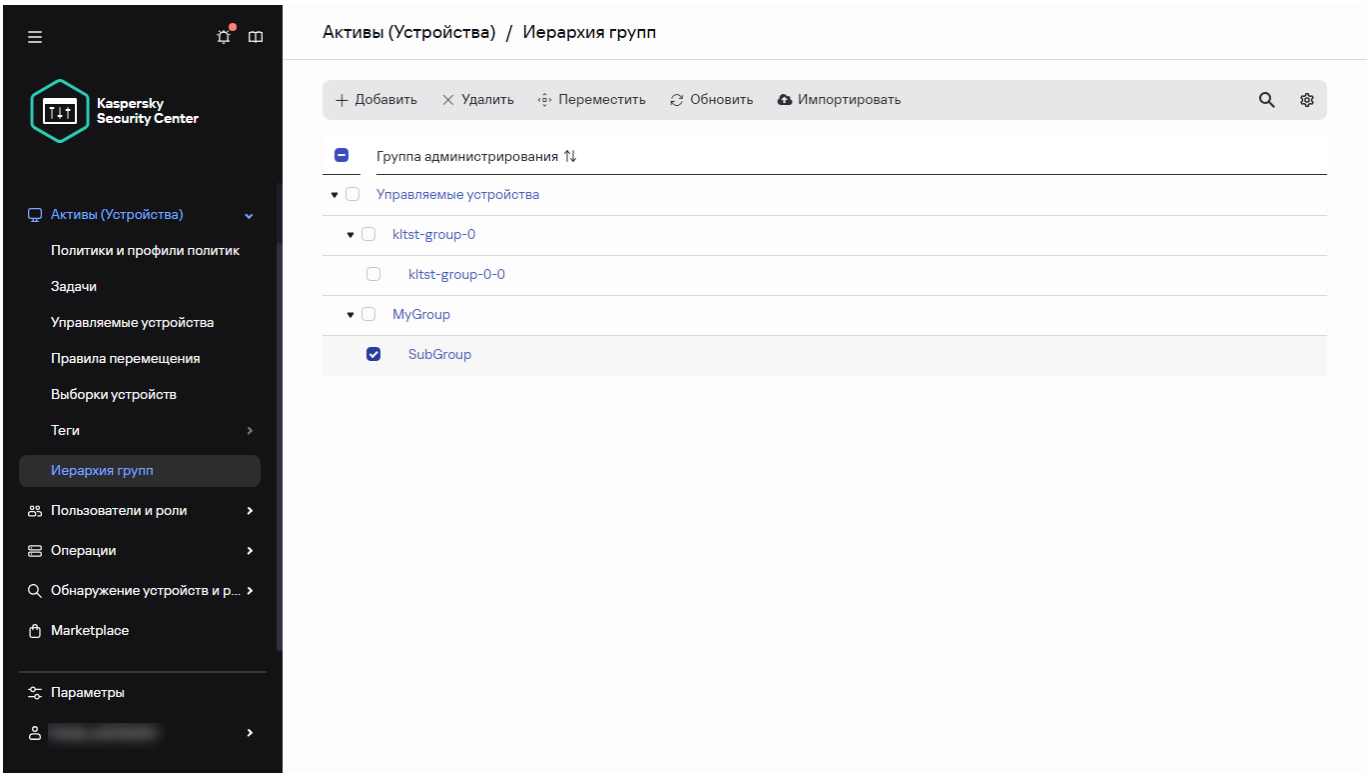
Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. Выберите имя требуемой группы администрирования.



Иерархия групп администрирования

Откроется окно свойств группы администрирования.

3. В окне свойств выберите вкладку **Параметры**.

4. В разделе **Наследование** включите или выключите следующие параметры:

- Наследовать из родительской группы

  Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств в сети** недоступны для изменения.

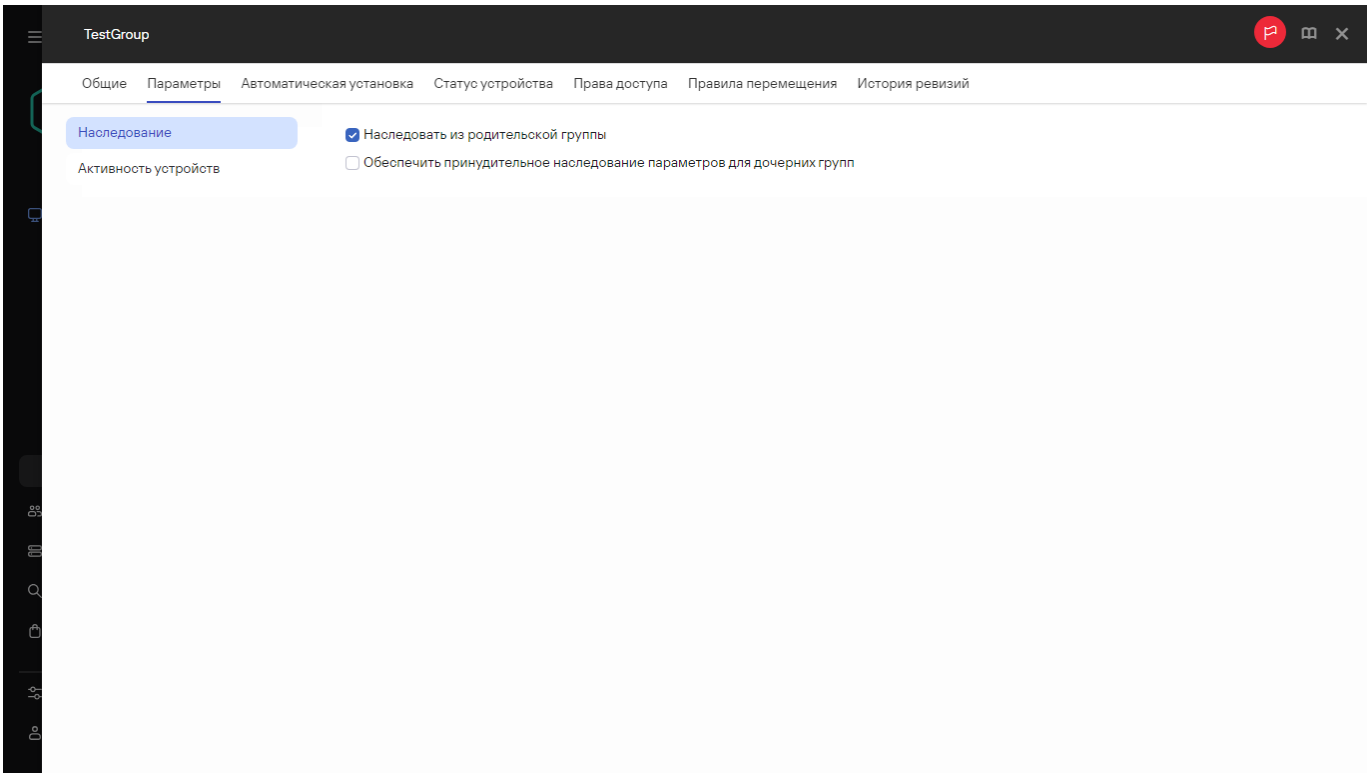
  Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

  По умолчанию параметр включен.

- Обеспечить принудительное наследование параметров для дочерних групп

  Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

  По умолчанию параметр выключен.



Свойства группы администрирования

5. В разделе **Активность устройств** включите или выключите следующие параметры:

- **Уведомлять администратора, если устройство неактивно больше (сут)**

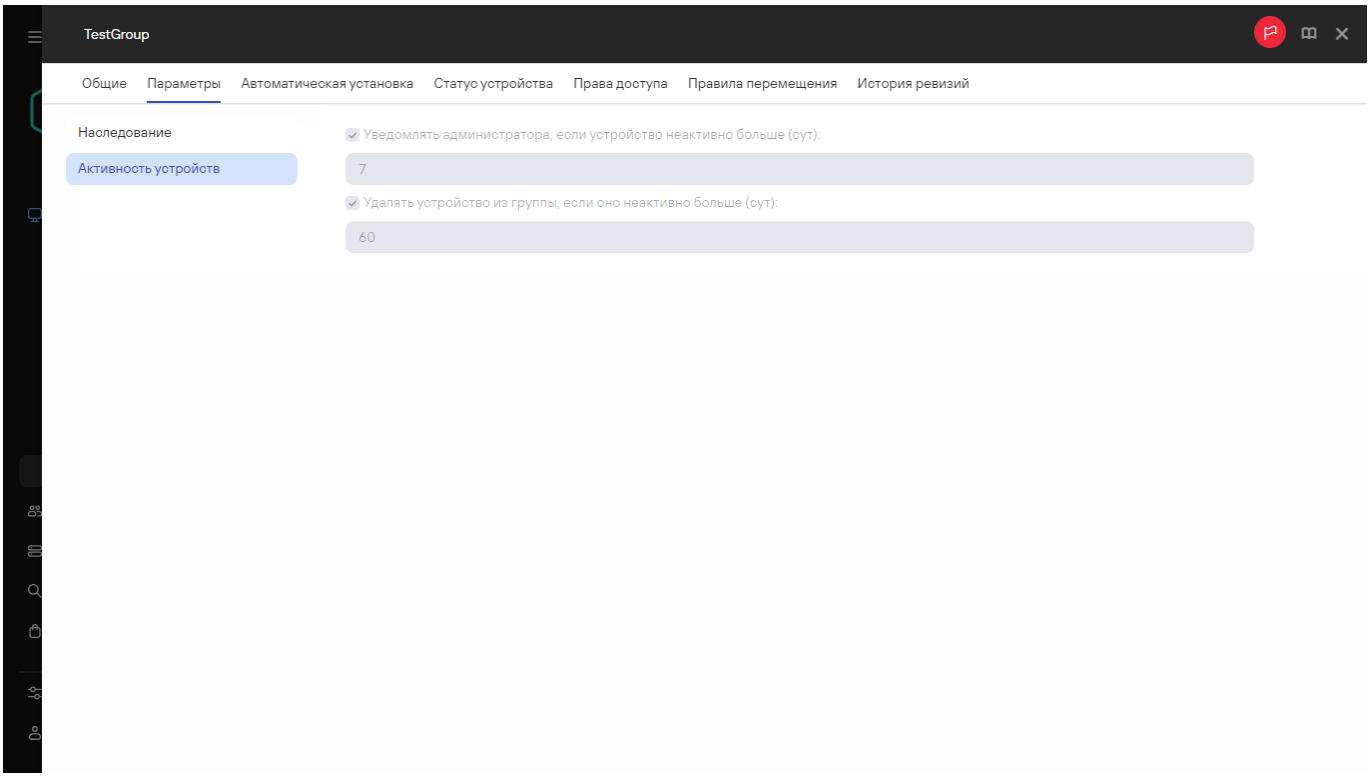
  Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

  По умолчанию параметр включен.

- **Удалять устройство из группы, если оно неактивно больше (сут)**

  Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

  По умолчанию параметр включен.



Свойства группы администрирования

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

Развертывание приложений "Лаборатории Касперского"

В этом разделе описано, как развернуть приложения "Лаборатории Касперского" на клиентских устройствах в вашей организации с помощью Консоли OSMP.

Сценарий: развертывание приложений "Лаборатории Касперского"

В этом сценарии описана процедура развертывания приложений "Лаборатории Касперского" с помощью Консоли OSMP. Можно воспользоваться мастером развертывания защиты или выполнить все необходимые шаги вручную.

Этапы

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Загрузка и создание инсталляционных пакетов**

   Загрузите пакет вручную.

   Если вы не можете установить приложения "Лаборатории Касперского" с помощью Open Single Management Platform на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные инсталляционные пакеты для приложений. Если вы используете автономные пакеты для установки приложений "Лаборатории Касперского", вам не нужно создавать и запускать задачу удаленной установки, а также создавать и настраивать задачи для Kaspersky Endpoint Security для Windows.

Также можно загрузить дистрибутивы Агента администрирования и приложений безопасности с сайта "Лаборатории Касперского". Если удаленная установка приложений по каким-либо причинам невозможна, вы можете использовать загруженные дистрибутивы для локальной установки приложений.

2. **Создание, настройка и запуск задачи удаленной установки**

   Этот шаг входит в мастер развертывания защиты. Если вы не запускали мастер развертывания защиты, вам необходимо создать и настроить эту задачу вручную.

   Вы можете вручную создать несколько задач удаленной установки для различных групп администрирования или выборок устройств. Вы можете развернуть различные версии одного приложения в этих задачах.

   Убедитесь, что все устройства в сети обнаружены, а затем запустите задачу (или задачи) удаленной установки.

   > Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

3. **Создание и настройка задач**

   Задача *Обновление* Kaspersky Endpoint Security должна быть настроена.

   Создайте эту задачу вручную и настройте ее. Убедитесь, что расписание запуска задачи соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

4. **Создание политик**

   Создайте политику для Kaspersky Endpoint Security вручную. Можно использовать установленные по умолчанию параметры политики. Также вы можете в любое время изменить заданные по умолчанию параметры политики в соответствии с вашими требованиями.

5. **Проверка результатов**

   Убедитесь, что развертывание завершилось успешно: созданы политики и задачи для каждого приложения и эти приложения установлены на управляемые устройства.

Результаты

Завершение сценария дает следующее:

- Все требуемые политики и задачи для выбранных приложений созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные приложения.

Мастер развертывания защиты

Для установки приложений "Лаборатории Касперского" можно воспользоваться мастером развертывания защиты. Мастер развертывания защиты позволяет проводить удаленную установку приложений как с использованием специально созданных инсталляционных пакетов, так и напрямую из дистрибутивов.

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет расположен: **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка приложения**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

Чтобы запустить мастер развертывания защиты вручную,

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 1. Выбор инсталляционного пакета

Выберите инсталляционный пакет приложения, которое требуется установить.

Если инсталляционный пакет требуемого приложения не содержится в списке, нажмите на кнопку **Добавить** и выберите приложение из списка.

Шаг 2. Выбор способа распространения файла ключа или кода активации

Выберите способ распространения файла ключа или кода активации:

- **Не добавлять лицензионный ключ в инсталляционный пакет**

Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

- если в свойствах ключа настроено автоматическое распространение;
- если создана задача **Добавление ключа**.

- **Добавить лицензионный ключ в инсталляционный пакет**

  Если выбран этот вариант, ключ распространяется на устройства вместе с инсталляционным пакетом.

  Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу пакетов настроен общий доступ на чтение.

Если инсталляционный пакет уже содержит файл ключа или код активации, это окно отображается, но оно содержит только информацию о лицензионном ключе.

Шаг 3. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличный от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

Шаг 4. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки приложения будет создана для группы устройств.

- **Выбор устройств для установки**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Шаг 5. Задание параметров задачи удаленной установки

В окне **Параметры задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

  Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

  Если флажок снят, доставка инсталляционных пакетов выполняется средствами Microsoft Windows.

  Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

  По умолчанию флажок установлен.

- **Средствами операционной системы с помощью точек распространения**

  Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

  Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

  По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

  Если флажок установлен, доставка файлов на клиентские устройства будет осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию флажок установлен.

Настройте дополнительный параметр:

- **Не устанавливать приложение, если оно уже установлено**

  Если флажок установлен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

  Если флажок снят, приложение будет установлено в любом случае.

  По умолчанию флажок установлен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если флажок установлен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Флажок доступен если выбран инсталляционный пакет Агента администрирования.

  По умолчанию флажок снят.

Шаг 7. Удаление несовместимых приложений перед установкой

Этот шаг присутствует, только если приложение, которое вы разворачиваете, несовместимо с другими приложениями.

Выберите этот параметр, если вы хотите, чтобы приложение Open Single Management Platform автоматически удаляло несовместимые приложения с приложением, которое вы устанавливаете.

Отображается список несовместимых приложений.

Если этот параметр не выбран, приложение будет установлено только на устройствах, на которых нет несовместимых приложений.

Шаг 8. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

- **Не перемещать устройства**

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Перемещать нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

Шаг 9. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

Если выбран этот вариант, можно указать учетную запись, от имени которой будет запускаться инсталлятор приложения. Учетную запись можно указать в случае если Агент администрирования не установлен на устройствах, для которых назначена задача.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

Если ни одна учетная запись не добавлена, задача запускается под той учетной записью, под которой работает служба Сервера администрирования.

Шаг 10. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки приложения** была успешно создана и настроена.

По умолчанию вариант **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, **Задача удаленной установки приложения** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, **Задача удаленной установки приложения** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **OK**, чтобы завершить последний шаг мастера развертывания защиты.

Добавление плагина управления для приложений "Лаборатории Касперского"

Для удаленного администрирования приложений "Лаборатории Касперского" с помощью Консоли OSMP необходимо установить веб-плагины управления. Установка веб-плагина управления возможна после развертывания Open Single Management Platform.

Чтобы установить веб-плагин управления для приложения "Лаборатории Касперского":

1. Переместите архив веб-плагина управления на устройстве администратора, на котором расположена утилита KDT.
2. При необходимости экспортируйте текущую версию конфигурационного файла на устройство администратора.

   Вам не нужно экспортировать конфигурационный файл, если параметры установки не добавлены или не изменены.
3. Выполните следующую команду, чтобы установить плагин:

   ```
   ./kdt apply -k <путь_к_архиву_плагина> -i <путь_к_конфигурационному_файлу>
   ```

   В команде укажите путь к архиву плагина и путь к текущему конфигурационному файлу. Вам не нужно указывать путь к конфигурационному файлу в команде, если параметры установки не добавлены или не изменены.

Веб-плагин управления установлен. Перезагрузите Консоль OSMP, чтобы отобразился добавленный плагин.

Вы можете просмотреть список компонентов, относящихся к OSMP (включая веб-плагины управления), с помощью KDT. Также вы можете просмотреть версию Консоли OSMP и список установленных веб-плагинов управления. Для этого в главном меню Консоли OSMP перейдите в параметры своей учетной записи и выберите пункт **О приложении**.

Удаление веб-плагина управления

Вы можете удалить веб-плагины управления приложениями "Лаборатории Касперского", которые предоставляют дополнительные возможности Open Single Management Platform. Плагины служб Open Single Management Platform используются для корректной работы Open Single Management Platform и не могут быть удалены (например, плагин Incident Response Platform).

Чтобы удалить веб-плагин управления:

1. При необходимости выполните следующую команду, чтобы получить название плагина, который вы хотите удалить:

   ```
   ./kdt status
   ```

   Отобразится список компонентов.

2. На устройстве администратора выполните следующую команду. Укажите название плагина, который вы хотите удалить:

   ```
   ./kdt remove --cnab <имя_плагина>
   ```

Указанный веб-плагин управления удален KDT.

Просмотр списка компонентов, интегрированных в Open Single Management Platform

Вы можете просмотреть список компонентов, интегрированы в OSMP (включая веб-плагины управления), с помощью KDT.

Чтобы просмотреть список компонентов,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt state
```

Список компонентов, интегрированных в OSMP (включая веб-плагины управления), отображается в окне командной строки.

Просмотр названий, параметров и пользовательских действий компонентов Open Single Management Platform

KDT позволяет просматривать список параметров и список настраиваемых действий компонента Open Single Management Platform. Если для компонента доступны пользовательские действия, вы также можете просмотреть описание и параметры указанного пользовательского действия с помощью KDT.

Пользовательское действие – это действие, позволяющее выполнять дополнительные операции, специфичные для компонента Open Single Management Platform (кроме установки, обновления, удаления). Например, восстановление данных Сервера администрирования и увеличение объема дискового пространства, используемого Сервером администрирования и его журналом событий, выполняется с помощью пользовательских действий.

Пользовательское действие запускается с помощью KDT следующим образом:

```
./kdt invoke <название_компонента> --action <пользовательское_действие> --param
<парметр_пользовательского_действия>
```

Чтобы просмотреть список компонентов Open Single Management Platform,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt describe
```

Отобразится список компонентов Open Single Management Platform.

Чтобы просмотреть список параметров и список пользовательских действий компонента Open Single Management Platform,

на устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя компонента Open Single Management Platform:

```
./kdt describe <название_компонента>
```

Отображаются списки параметров и пользовательских действий, доступных для указанного компонента.

Чтобы просмотреть описание и список параметров настраиваемого действия,

на устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя компонента Open Single Management Platform и его команду:

```
./kdt describe <название_компонента> <название_действия>
```

Отображаются описание и список параметров пользовательского действия указанного компонента.

Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создать инсталляционные пакеты приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского.

Чтобы загрузить и создать инсталляционный пакет для приложения "Лаборатории Касперского":

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах для приложений "Лаборатории Касперского" в списке экранных уведомлений. Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

   Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех приложений, которые совместимы с текущей версией Open Single Management Platform.

4. Выберите требуемый инсталляционный пакет, например, Kaspersky Endpoint Security для Linux.

   Откроется окно с информацией об инсталляционном пакете.

   > Вы можете загрузить и использовать инсталляционный пакет, который включает в себя криптографические инструменты, реализующие надежное шифрование, если он соответствует применимым законам и правилам. Чтобы загрузить инсталляционный пакет Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить и создать инсталляционный пакет** отображается кнопка **Загрузить дистрибутив**.

   Начинается загрузка инсталляционного пакета на Сервер администрирования. Вы можете закрыть окно мастера или перейти к следующему шагу инструкции. Если вы закроете мастер, процесс загрузки продолжится в фоновом режиме.

   Если вы хотите отслеживать процесс загрузки инсталляционного пакета:

   a. В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты → В процессе ()**.

   b. Следите за ходом операции в столбцах **Ход загрузки** и **Состояние загрузки** таблицы.

   После завершения процесса инсталляционный пакет добавляется в список на вкладке **Загружено**. Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и перейдите к следующему шагу инструкции.

   > Если размер данных, содержащихся в выбранном дистрибутиве, превышает текущее предельное значение, отображается сообщение об ошибке. Вы можете изменить предельное значение и продолжить создание инсталляционного пакета.

6. Во время процесса загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:

   a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионное соглашение (EULA).

   b. Прочитайте появившееся на экране Лицензионное соглашение и нажмите на кнопку **Принять**.

   Загрузка продолжится после того, как вы примете Лицензионное соглашение. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

7. После завершения загрузки нажмите на кнопку **Закрыть**.

Инсталляционный пакет отображается в списке инсталляционных пакетов.

Создание инсталляционных пакетов из файла

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (такое как текстовый редактор) на клиентские устройства, например, с помощью задачи;
- создать автономный инсталляционный пакет.

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет.

Во время создания пользовательского инсталляционного пакета, вы можете указать параметры командной строки, например, для установки приложения в тихом режиме.

Чтобы создать пользовательский инсталляционный пакет:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет из файла**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

5. В открывшемся окне выберите файл архива, расположенный на доступных дисках.

Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) нельзя.

Начнется загрузка файла на Сервер администрирования.

6. Если вы указали файл приложения "Лаборатории Касперского", вам может быть предложено прочитать и принять Лицензионное соглашение для этого приложения. Чтобы продолжить, вам нужно принять условия Лицензионного соглашения. Выберите параметр **Принять условия и положения настоящего Лицензионного соглашения**, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

   Также вам будет предложено прочитать и принять условия Политики конфиденциальности. Чтобы продолжить, вам нужно принять условия Политики конфиденциальности. Выберите параметр **Я принимаю Политику конфиденциальности**, только если вы понимаете и соглашаетесь с тем, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.

7. Выберите файл (из списка файлов, которые извлечены из выбранного архивного файла) и укажите параметры командной строки исполняемого файла.

   Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   Начнется процесс создания инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

8. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя**. Название инсталляционного пакета.
  - **Источник**. Имя поставщика приложения.
  - **Приложение**. Название приложения, упакованного в пользовательский инсталляционные пакет.
  - **Версия**. Версия приложения.
  - **Язык**. Язык приложения, упакованного в пользовательский инсталляционный пакет.
  - **Размер (МБ)**. Размер инсталляционного пакета.
  - **Операционная система**. Тип операционной системы, для которой предназначен инсталляционные пакет.
  - **Создано**. Дата создания инсталляционного пакета.
  - **Изменено**. Дата изменения инсталляционного пакета.
  - **Тип**. Тип инсталляционного пакета.
- Измените параметры командной строки.

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки приложений на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл (Installer.exe), который можно разместить на Веб-сервере или в общей папке, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Open Single Management Platform. Вы можете создать автономный инсталляционный пакет для приложений "Лаборатории Касперского", так и для приложений сторонних производителей. Чтобы создать автономный инсталляционный пакет для приложений стороннего производителя, необходимо создать пользовательский инсталляционный пакет.

Убедитесь, что автономный инсталляционный пакет не доступен для третьих лиц.

Чтобы создать автономный инсталляционный пакет:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.

3. Выберите параметр **С использованием автономного инсталляционного пакета**.

   В результате запускается мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

   По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

   Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

   Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

   - **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.

- **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.

- **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** выбран по умолчанию. Если вы не хотите перемещать клиентское устройство ни в какую группу администрирования после установки Агента администрирования, не изменяйте этот параметр.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

6. После завершения процесса создания автономного инсталляционного пакета, нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создается и размещается на Веб-сервере. Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

Изменение ограничения на размер пользовательского инсталляционного пакета

Общий размер данных, распакованных при создании пользовательского инсталляционного пакета, ограничен. Ограничение по умолчанию – 1 ГБ.

Если вы попытаетесь загрузить архивный файл, содержащий данные, превышающие текущее ограничение, появится сообщение об ошибке. Возможно, вам придется увеличить это максимальное значение при создании инсталляционных пакетов из больших дистрибутивов.

Чтобы изменить максимальное значение для размера пользовательского инсталляционного пакета,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=" -fset -pv klserver -n
MaxArchivePkgSize -t d -v <количество байтов>"
```

Где <число_байтов> – количество байтов в шестнадцатеричном или десятичном формате.

Например, если требуемое максимальное значение составляет 2 ГБ, вы можете указать десятичное значение 2147483648 или шестнадцатеричное значение 0x80000000. В этом случае для локальной установки Сервера администрирования вы можете использовать следующую команду:

```
./kdt invoke ksc --action klscflag --param klscflag_param=" -fset -pv klserver -n
MaxArchivePkgSize -t d -v 2147483648"
```

Ограничение на размер пользовательских данных инсталляционного пакета изменено.

Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)

Вы можете установить Агент администрирования на устройства с операционной системой Linux с помощью файла ответов – текстового файла, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме, то есть без участия пользователя.

Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:

1. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

   Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 или выше, установите пакет libxcrypt-compat для корректной работы Агента администрирования.

2. Прочитайте Лицензионное соглашение. Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.

3. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

4. Создайте файл ответов (в формате TXT) в каталоге, который вы указали в переменной среды. Добавьте в файл ответов список переменных в формате VARIABLE_NAME = variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вам нужно включить в него минимальный набор из трех обязательных переменных:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Вы также можете добавить любые дополнительные переменные, чтобы использовать более конкретные параметры вашей удаленной установки. В следующей таблице перечислены все переменные, которые можно включать в файл ответов:

   Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

Имя переменной	Обязательная	Описание	Возможные значения
KLNAGENT_SERVER	Да	Содержит имя Сервера администрирования, представленное как полное доменное имя (FQDN) или IP-адрес.	DNS-имя устройства или IP-адрес.
KLNAGENT_AUTOINSTALL	Да	Определяет, включен ли тихий режим установки.	1 – тихий режим включен; пользователю не предлагается никаких действий во время установки. Другое – тихий режим выключен; пользователю могут быть предложены действия во время установки.
EULA_ACCEPTED	Да	Определяет, принимает ли пользователь Лицензионное соглашение Агента администрирования; если переменная не указана это может быть истолковано как отклонение Лицензионного соглашения.	1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения. Другое значение или не задано – Я не согласен с условиями Лицензионного соглашения (установка не выполняется).
KLNAGENT_PROXY_USE	Нет	Определяет, будет ли соединение с Сервером администрирования использовать параметры прокси-сервера. По умолчанию указано значение 0.	1 – используются параметры прокси-сервера. Другое – параметра прокси-сервера не используются.
KLNAGENT_PROXY_ADDR	Нет	Определяет адрес прокси-сервера, используемого для соединения с Сервером администрирования.	DNS-имя устройства или IP-адрес.
KLNAGENT_PROXY_LOGIN	Нет	Определяет имя пользователя, используемое для входа на прокси-сервер.	Любое существующее имя пользователя.
KLNAGENT_PROXY_PASSWORD	Нет	Определяет пароль пользователя, используемый для входа на прокси-сервер.	Любой набор букв и цифр, разрешенных форматом пароля в операционной системе.
KLNAGENT_VM_VDI	Нет	Определяет, установлен ли Агент администрирования на образ для создания динамических виртуальных машин.	1 – Агент администрирования установлен на образ, который затем будет использован для создания динамических виртуальных машин. Другое – во время установки образ не используется.

KLNAGENT_VM_OPTIMIZE	Нет	Определяет, являются ли параметры Агента администрирования оптимальными для гипервизора.	1 – локальные параметры Агента администрирования по умолчанию изменены таким образом, что они позволяют оптимизировать использование на гипервизоре.
KLNAGENT_TAGS	Нет	Перечисляет теги, назначенные экземпляру Агента администрирования.	Один или несколько тегов, разделенных точкой с запятой.
KLNAGENT_UDP_PORT	Нет	Определяет UDP-порт, используемый Агентом администрирования. По умолчанию указано значение 15000.	Любой существующий номер порта.
KLNAGENT_PORT	Нет	Определяет порт (не TLS), используемый Агентом администрирования. По умолчанию указано значение 14000.	Любой существующий номер порта.
KLNAGENT_SSLPORT	Нет	Определяет TLS-порт, используемый Агентом администрирования. По умолчанию указано значение 13000.	Любой существующий номер порта.
KLNAGENT_USESSL	Нет	Определяет, используется ли безопасность транспортного уровня (TLS) для подключения.	1 (по умолчанию) – используется TLS. Другое – TLS не используется.
KLNAGENT_GW_MODE	Нет	Определяет, используется ли шлюз соединения.	1 (по умолчанию) – текущие параметры не изменяются (при первом вызове шлюз соединения не указывается). 2 – шлюз соединения не используется. 3 – используется шлюз соединения. 4 – экземпляр Агента администрирования используется в качестве шлюза соединения в демилитаризованной зоне (DMZ).
KLNAGENT_GW_ADDRESS	Нет	Определяет адрес шлюза соединения. Значение применимо, только если KLNAGENT_GW_MODE = 3.	DNS-имя устройства или IP-адрес.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Нет	Позволяет запустить утилиту регистрации пользователя в качестве владельца устройства после установки Агента администрирования. Если выключено, то регистрация в качестве владельца устройства недоступна для пользователя.	1 – после установки Агента администрирования будет запущена утилита регистрации пользователя в качестве владельца устройства. Другое – выключено.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Нет	Определяет, устанавливать ли автоматически загруженные	true (по умолчанию) –

		обновления для Агента администрирования со статусом *Не определено*.	обновления устанавливаются автоматически. false – обновления приложения не устанавливаются автоматически.

5. Установка Агента администрирования:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     `# rpm -i klnagent-<номер сборки>.i386.rpm`
   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
     `# rpm -i klnagent64-<номер сборки>.x86_64.rpm`
   - Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
     `# rpm -i klnagent64-<номер сборки>.aarch64.rpm`
   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     `# apt-get install ./klnagent_<номер сборки>_i386.deb`
   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
     `# apt-get install ./klnagent64_<номер сборки>_amd64.deb`
   - Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
     `# apt-get install ./klnagent64_<номер сборки>_arm64.deb`

Установка Агента администрирования для Linux начинается в тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением Astra Linux в режиме замкнутой программной среды вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux.

Предварительные условия:

- Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux.
- Загрузите установочный файл Агента администрирования с сайта "Лаборатории Касперского".

Выполните команды, представленные в этой инструкции, под учетной записью root.

Чтобы подготовить устройство под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования:

1. Откройте файл `/etc/digsig/digsig_initramfs.conf` и укажите следующие параметры:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. В командной строке введите следующую команду, чтобы установить пакет совместимости:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Создайте директорию для ключа приложения:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Поместите ключ приложения /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg в директорию, созданную на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Если в комплект поставки Open Single Management Platform не входит ключ kaspersky_astra_pub_key.gpg, вы можете загрузить этот ключ по ссылке https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Обновите оперативную память дисков:

   ```
   update-initramfs -u -k all
   ```

   Перезагрузите систему.

6. Выполните шаги подготовки, общие для любого устройства с операционной системой Linux.

Устройство подготовлено. Теперь вы можете приступить к установке Агента администрирования.

Просмотр списка автономных инсталляционных пакетов

Вы можете просмотреть список автономных инсталляционных пакетов и свойства каждого отдельного инсталляционного пакета.

Чтобы просмотреть список автономных инсталляционных пакетов для всех инсталляционных пакетов:

Нажмите на кнопку **Просмотреть список автономных пакетов**.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии приложения, включенной в пакет.
- **Название приложения**. Имя приложения, которое включено в автономный инсталляционный пакет.
- **Версия приложения**.
- **Имя инсталляционного пакета Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Версия Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.

- **Размер**. Размер файла (МБ).
- **Группа**. Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан**. Дата и время создания автономного инсталляционного пакета.
- **Изменен**. Дата и время изменения автономного инсталляционного пакета.
- **Путь**. Полный путь к папке, в которой находится автономный инсталляционный пакет.
- **Веб-адрес**. Веб-адрес расположения автономного инсталляционного пакета.
- **Хеш файла**. Параметр используется для подтверждения того, что автономный инсталляционный пакет не был изменен третьими лицами, и у пользователя есть тот же файл, который вы создали и передали пользователю.

Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,

выберите инсталляционный пакет в списке и над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Опубликовать автономный инсталляционный пакет на Веб-сервере, с помощью кнопки **Опубликовать**. Опубликованный автономный инсталляционный пакет доступен для загрузки пользователям, которым вы отправили ссылку на автономный инсталляционный пакет.
- Отменить публикацию автономного инсталляционного пакета на Веб-сервере, нажав на кнопку **Отменить публикацию**. Неопубликованный автономный инсталляционный пакет доступен для загрузки только вам и другим администраторам.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Загрузить**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Open Single Management Platform позволяет вам создавать инсталляционные пакеты для приложений "Лаборатории Касперского" и для приложений сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать приложения из пакетов. Для оптимизации нагрузки на главном Сервере администрирования вы можете распространять инсталляционные пакеты на подчиненные Серверы администрирования. После этого подчиненные Серверы передают пакеты на клиентские устройства, после чего вы можете выполнять удаленную установку приложений на свои клиентские устройства.

Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Убедитесь что подчиненные Серверы администрирования подключены к главному Серверу администрирования.

2. в главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

4. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространить инсталляционный пакет** и укажите имя задачи.

5. На странице **Область действия задачи** выберите устройства, которым назначена задача, одним из следующих способов:

   - Если вы хотите сформировать задачу для всех подчиненных Серверов определенной группы администрирования, выберите эту группу и запустите создание групповой задачи для этой группы.

   - Если вы хотите создать задачу для определенных подчиненных Серверов администрирования, выберите эти Серверы и создайте для них задачу.

6. На странице **Распространяемые инсталляционные пакеты** выберите инсталляционные пакеты, которые необходимо скопировать на подчиненные Серверы администрирования.

7. Укажите учетную запись для запуска задачи *Распространение инсталляционного пакета* под этой учетной записью. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

8. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача, созданная для распространения инсталляционных пакетов на подчиненные Серверы администрирования, отображается в списке задач.

10. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи выбранные инсталляционные пакеты скопированы на указанные подчиненные Серверы администрирования.

Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux

Установка Агента администрирования состоит из двух шагов:

- Подготовка устройства с операционной системой Linux

- Удаленная установка Агента администрирования

Подготовка устройства с операционной системой Linux

Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:

1. Убедитесь, что на целевом устройстве с операционной системой Linux установлено следующее программное обеспечение:
   - Sudo.
   - Интерпретатор языка Perl версии 5.10 или выше.
2. Выполните проверку конфигурации устройства:
   a. Проверьте, что возможно подключение к устройству через SSH (например, приложение PuTTY).

      Если вы не можете подключиться к устройству, откройте файл `/etc/ssh/sshd_config` и убедитесь, что следующие параметры имеют значения:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Не изменяйте файл /etc/ssh/sshd_config, если вы можете без проблем подключиться к устройству; в противном случае вы можете столкнуться с ошибкой аутентификации SSH при выполнении задачи удаленной установки.

      Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

   b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

   c. Используйте команду sudo `visudo`, чтобы открыть конфигурационный файл sudoers.

      В открывшемся файле найдите строку, начинающуюся с `%sudo` (или с `%wheel` если вы используете операционную систему CentOS). Под этой строкой укажите следующее: `<имя пользователя> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<имя пользователя>` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH. Если вы используете операционную систему Astra Linux, в файл /etc/sudoers добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Сохраните и закройте файл sudoers.

   e. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.
3. Если вы хотите установить Агент администрирования на устройствах с операционной системой с системой инициализации systemd, откройте файл `/etc/systemd/logind.conf` и выполните одно из следующих действий:
   - Укажите значение `no` для параметра `KillUserProcesses`: `KillUserProcesses=no`.

- Для параметра `KillExcludeUsers` введите имя пользователя учетной записи, под которой будет выполняться удаленная установка, например, `KillExcludeUsers=root`.

Целевое устройство Astra Linux

Если целевое устройство работает под управлением Astra Linux, добавьте строку `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<имя пользователя>/.bashrc`, где `<имя пользователя>` — учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

Целевое устройство ОСнова

Если на целевом устройстве работает ОСнова, выполните следующие действия:

a. Откройте файл `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` и закомментируйте строку `#KillUserProcess=yes`.

b. Откройте файл `/usr/lib/NESS/pam-user-session` и закомментируйте строку `#loginctl terminate-session "$XDG_SESSION_ID"`.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

```
$ sudo systemctl restart systemd-logind.service
```

4. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

5. Если вы хотите установить Агент администрирования на устройства с операционной системой Astra Linux, работающей в режиме замкнутой программной среды, выполните дополнительные действия для подготовки устройств Astra Linux.

6. Если вы хотите установить Агент администрирования на устройствах под управлением Ubuntu Server или Ubuntu Desktop версии 10.04, выполните дополнительные шаги для подготовки этих устройств.

Удаленная установка Агента администрирования

Чтобы установить Агент администрирования на устройство с операционной системой Linux:

1. Загрузите и создайте инсталляционный пакет:

   a. Перед установкой пакета на устройство убедитесь, что на нем установлены зависимости (приложения, библиотеки) для данного пакета.

   Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

   b. Загрузите инсталляционный пакет Агента администрирования с помощью интерфейса приложения или с веб-сайта "Лаборатории Касперского".

   c. Для создания пакета удаленной установки используйте файлы:

   - klnagent.kpd;

- akinstall.sh;
- deb или rpm пакет Агента администрирования.

2. Создайте задачу удаленной установки приложения с параметрами:
   - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
   - На странице **Выбор учетной записи для запуска задачи** укажите параметры учетной записи, которая используется для подключения к устройству через SSH.
3. Запустите задачу удаленной установки приложения. Используйте параметр для команды `su`, чтобы сохранить среду: `-m, -p, --preserve-environment`.

Установка программ с помощью задачи удаленной установки

Open Single Management Platform позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку. Вы можете выбрать не более 1000 устройств.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке.

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными адресами или на выборку устройств.

Чтобы установить приложение на выбранные устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка приложения**.

4. Выберите один из следующих вариантов:

- **Назначить задачу группе администрирования**

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Задача Удаленная установка приложения создана для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Инсталляционные пакеты** укажите следующие параметры:

   - В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет приложения, которое требуется установить.

   - В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

     - **С помощью Агента администрирования**

       Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

       Если флажок снят, доставка инсталляционных пакетов выполняется средствами Microsoft Windows.

       Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

       По умолчанию флажок установлен.

     - **Средствами операционной системы с помощью точек распространения**

Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

  Если флажок установлен, доставка файлов на клиентские устройства будет осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию флажок установлен.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.

- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Open Single Management Platform больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу Удаленная установка приложения, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу Удаленная установка приложения.

- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другую, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

  Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно загрузить инсталляционный пакет**.

  Вы можете использовать пароль деинсталляции только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security для Windows при установке Kaspersky Endpoint Security для Windows с помощью задачи *Удаленная установка приложений*. Использование пароля деинсталляции при установке других компонентов может вызвать ошибки установки.

  Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

  - Вы используете Агент администрирования Kaspersky Security Center версии 14.2 для Windows или выше.

- Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительный параметр:

  - **Не устанавливать приложение, если оно уже установлено**

    Если флажок установлен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

    Если флажок снят, приложение будет установлено в любом случае.

    По умолчанию флажок установлен.

  - **Предварительно проверять тип операционной системы перед загрузкой**

    Перед передачей файлов на клиентские устройства Open Single Management Platform проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Open Single Management Platform не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

  - **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

    Если флажок установлен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

    Флажок доступен если выбран инсталляционный пакет Агента администрирования.

    По умолчанию флажок снят.

  - **Предлагать пользователю закрыть работающие приложения**

    Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

    Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

    Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

    По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:

  - **Устанавливать на все устройства**

Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

- **Устанавливать на устройства, управляемые только этим Сервером администрирования**

  Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними.

- Укажите, следует ли перемещать устройства в группу администрирования после установки:

  - **Не перемещать устройства**

    Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

  - **Переместить нераспределенные устройства в выбранную группу (можно выбрать только одну группу)**

    Устройства перемещаются в выбранную вами группу администрирования.

  Обратите внимание, что по умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

7. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке приложений:

   - **Не перезагружать устройство**

     Если выбран этот вариант, устройство не будет перезагружаться после установки приложения защиты.

     По умолчанию выбран этот вариант.

   - **Перезагрузить устройство**

     Если выбран этот вариант, устройство будет перезагружено после установки приложения защиты.

8. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи Удаленная установка приложения:

   - **Учетная запись не требуется (Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

  Если выбран этот вариант, можно указать учетную запись, от имени которой будет запускаться инсталлятор приложения. Учетную запись можно указать в случае если Агент администрирования не установлен на устройствах, для которых назначена задача.

  Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

  Если ни одна учетная запись не добавлена, задача запускается под той учетной записью, под которой работает служба Сервера администрирования.

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

    Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После выполнения задачи удаленной установки, выбранное приложение устанавливается на указанный набор устройств.

Установка приложений на подчиненные Серверы администрирования

Чтобы установить приложение на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи **Распространение инсталляционного пакета**.

3. Создайте задачу удаленной установки приложения на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка приложения на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранное приложение устанавливается на подчиненные Серверы администрирования.

Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете приложение на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на имя задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.
3. Перейдите в раздел **Параметры приложения** → **Параметры, специфичные для Unix**.
4. Задайте следующие параметры:

   - **Установить пароль для учетной записи root (только для развертывания через SSH)**

     Если команду `sudo` нельзя использовать на целевом устройстве без указания пароля, выберите этот параметр, а затем укажите пароль для учетной записи root. Open Single Management Platform передает пароль в зашифрованном виде на целевое устройство, расшифровывает пароль, а затем запускает процедуру установки от имени учетной записи root с указанным паролем.

     Open Single Management Platform не использует учетную запись или указанный пароль для создания SSH подключения.

   - **Укажите путь к временной папке с правами Выполнение на целевом устройстве (только для развертывания через SSH)**

     Если папка /tmp на целевом устройстве не имеет права Выполнение, выберите этот параметр, а затем укажите путь к папке с правами Выполнение. Open Single Management Platform использует указанную папку в качестве временной папки для доступа по SSH. Приложение помещает инсталляционный пакет в папку и запускает процедуру установки.
5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

Запуск и остановка приложений "Лаборатории Касперского"

Вы можете использовать задачу *Запуск или остановка приложения* для запуска и остановки приложений "Лаборатории Касперского" на управляемых устройствах.

Чтобы создать задачу запуска или остановки приложения:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите создать задачу.
4. В списке **Тип задачи** выберите задачу **Активация приложения**.
5. В поле **Название задачи** укажите имя новой задачи.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача.
7. В окне **Приложения** выполните следующее:
   - Установите флажки рядом с названиями приложений, для которых вы хотите создать задачу.
   - Выберите параметр **Запустить приложение** или **Остановить приложение**.
8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на шаге **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями и сохраните параметры.

Задача создана и настроена.

Если вы хотите запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Замещение приложений безопасности сторонних производителей

Для установки приложений безопасности "Лаборатории Касперского" средствами Open Single Management Platform может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемым приложением. Open Single Management Platform предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности в мастере развертывания защиты. Если этот параметр включен, Open Single Management Platform удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача *Удаленная деинсталляция приложения*. Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача *Удаленная деинсталляция приложения*.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Удаленная деинсталляция приложений или обновлений программного обеспечения

Вы можете удаленно деинсталлировать приложения или обновления программного обеспечения на управляемых устройствах под управлением Linux только с помощью Агента администрирования.

Чтобы удаленно деинсталлировать приложения или обновления программного обеспечения:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите Open Single Management Platform.
4. В списке **Тип задачи** выберите тип задачи **Удаленная деинсталляция приложения**.
5. В поле **Название задачи** укажите имя новой задачи.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача.

   Перейдите к следующему шагу мастера.
7. Выберите, какое приложение вы хотите деинсталлировать, а затем выберите требуемые приложения, обновления или патчи, которые вы хотите удалить:

   - **Удалить управляемое приложение**

     Отображается список приложений "Лаборатории Касперского". Выберите приложение, которое вы хотите деинсталлировать.

     Убедитесь, что параметр политики **Использовать пароль деинсталляции** выключен для управляемого приложения.

   - **Удалить несовместимое приложение**

     Отобразится список приложений, несовместимых с приложениями безопасности "Лаборатории Касперского" или с Open Single Management Platform. Установите флажки напротив приложений, которые требуется удалить.

   - **Удалить приложение из реестра приложений**

По умолчанию Агенты администрирования отправляют на Сервер администрирования информацию о приложениях, установленных на управляемых устройствах. Список установленных приложений хранится в реестре приложений.

Чтобы выбрать приложение из реестра приложений:

a. Нажмите на поле **Приложение для деинсталляции** и выберите приложение, которое вы хотите деинсталлировать.

Если вы выбрали Агент администрирования Kaspersky Security Center, при запуске задачи статус *Завершено успешно* показывает, что процесс удаления запущен. При удалении Агента администрирования Kaspersky Security Center статус не меняется. В случае сбоя задачи статус меняется на *Сбой*.

b. Укажите параметры деинсталляции:

- Способ удаления

Выберите, как вы хотите деинсталлировать приложение:

- **Автоматически определять команду удаления**

  Если у приложения есть команда деинсталляции, заданная поставщиком приложения, Open Single Management Platform использует эту команду. Рекомендуется выбрать этот вариант.

- **Задать команду удаления**

  Выберите этот вариант, если вы хотите указать свою команду для деинсталляции приложения.

  Рекомендуется сначала попробовать деинсталлировать приложение с помощью параметра **Автоматически определять команду удаления**. Если деинсталляция с помощью автоматически определенной команды не удалась, используйте свою команду.

  Введите команду установки в это поле и укажите следующий параметр:

  Используйте эту команду для удаления, только если команда по умолчанию не была обнаружена автоматически

  Open Single Management Platform проверяет, есть ли у выбранного приложения команда деинсталляции, заданная поставщиком приложения. Если команда найдена, Open Single Management Platform будет использовать ее вместо команды, указанной в поле **Команда для удаления приложения**.

  Рекомендуется включать этот параметр.

- Выполнить перезагрузку после успешного удаления приложения

Если после деинсталляции приложения требуется перезагрузка операционной системы на управляемом устройстве, операционная система перезагружается автоматически.

- **Удалить указанное обновление приложения, патч или стороннее приложение**

  Отображается список обновлений, патчей и приложений сторонних производителей. Выберите объект, который вы хотите деинсталлировать.

  Отображаемый список представляет собой общий список приложений и обновлений, и он не соответствует приложениям и обновлениям, установленным на управляемых устройствах. Перед выбором объекта рекомендуется убедиться, что приложение или обновление установлено на устройствах, определенных в области действия задачи. В окне свойств можно просмотреть список устройств, на которых установлено приложение или обновление.

  Чтобы просмотреть список устройств:

  a. Нажмите на имя приложения или обновления.

  Откроется окно свойств.

  b. Откройте раздел **Устройства**.

  Вы также можете просмотреть список установленных приложений и обновлений в окне свойств устройства.

8. Укажите, как клиентские устройства будут загружать утилиту удаления:

- **С помощью Агента администрирования**

  Файлы доставляются на клиентские устройства Агентом администрирования, установленным на этих клиентских устройствах.

  Если этот параметр выключен, файлы доставляются с помощью инструментов операционной системы Linux.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

  Параметр устарел. Используйте параметр **С помощью Агента администрирования** или **Средствами операционной системы с помощью точек распространения** вместо этого параметра.

  Файлы передаются на клиентские устройства с использованием средств операционной системы Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

- **Средствами операционной системы с помощью точек распространения**

  Файлы передаются на клиентские устройства с использованием инструментов операционной системы с помощью точек распространения. Этот параметр можно включить, если в сети есть хотя бы одна точка распространения.

  Если параметр **С помощью Агента администрирования** включен, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

- **Максимальное количество одновременных загрузок**

  Максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы. Чем больше это число, тем быстрее будет деинсталлировано приложение, но нагрузка на Сервер администрирования увеличивается.

- **Максимальное количество попыток деинсталляции**

  Если при запуске задачи *Удаленная деинсталляция приложения* не удается деинсталлировать приложение с управляемого устройства за указанное в параметрах количество запусков установок, Open Single Management Platform прекращает доставку утилиты деинсталляции на это управляемое устройство и больше не запускает установщик на устройстве.

  Параметр **Максимальное количество попыток деинсталляции** позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

  Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует деинсталляции. Администратор должен решить проблему за указанное количество попыток деинсталляции и перезапустить задачу (вручную или по расписанию).

  Если удаление не выполнено, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

  После создания задачи, количество попыток установки равно `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

  Если количество попыток деинсталляции, указанное в параметрах задачи, было превышено и устройство готово к деинсталляции приложения, вы можете увеличить значение параметра **Максимальное количество попыток деинсталляции** и запустить задачу деинсталляции приложения. Также вы можете создать другую задачу *Удаленная деинсталляция приложения*.

- **Предварительно проверять тип операционной системы перед загрузкой**

  Перед передачей файлов на клиентские устройства Open Single Management Platform проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Open Single Management Platform не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

Перейдите к следующему шагу мастера.

9. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**
  - **Принудительно перезагрузить через (мин)**

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

10. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу *Удаленная деинсталляция приложения*.

Укажите учетную запись, от имени которой будет запускаться инсталлятор приложения. Нажмите на кнопку **Добавить**, выберите **Учетная запись** и укажите данные учетной записи пользователя.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

11. Если на шаге **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи.

    Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже.

12. Нажмите на кнопку **Готово**.

    В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо.

    Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

    Задача будет создана, настроена и отобразится в списке задач, в разделе **Активы (Устройства)** → **Задачи**.

13. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

    Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

    Подробное описание параметров запуска по расписанию см. в общих параметрах задачи.

После завершения задачи, выбранное приложение будет удалено на выбранных устройствах.

Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования

Чтобы установить Агент администрирования на устройство с операционной системой SUSE Linux Enterprise Server 15:

перед установкой Агента администрирования выполните следующую команду:

```
$ sudo zypper install insserv-compat
```

Это позволит вам установить пакет insserv-compat и правильно настроить Агент администрирования.

Выполните команду `rpm -q insserv-compat`, чтобы проверить, если пакет уже установлен.

Если в вашей сети много устройств под управлением SUSE Linux Enterprise Server 15, вы можете использовать специальное программное обеспечение для настройки и управления инфраструктурой компании. Используя это программное обеспечение, вы можете автоматически установить пакет insserv-compat сразу на все необходимые устройства. Например, вы можете использовать Puppet, Ansible, Chef, или сделать свой скрипт любым удобным для вас способом.

Если на устройстве нет ключей подписи GPG для SUSE Linux Enterprise, вы можете увидеть следующее предупреждение: `Package header is not signed!` Выберите параметр `i`, чтобы игнорировать предупреждение.

После подготовки устройства с операционной системой SUSE Linux Enterprise Server 15, установите Агент администрирования.

Подготовка устройства под управлением Windows к удаленной установке. Утилита riprep

Удаленная установка приложения на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве. В этом случае ее повторное выполнение не требуется.
- Во время запуска задачи устройство было выключено. В этом случае требуется включить устройство и запустить задачу еще раз.
- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве. Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики клиентского устройства (klactgui).
- Если на устройстве не установлен Агент администрирования, при удаленной установке приложения могут возникнуть следующие проблемы:
  - на клиентском устройстве включен **Отключить простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

  Для решения проблем, возникших при установке приложения на клиентское устройство, на котором не установлен Агент администрирования, вы можете воспользоваться утилитой подготовки устройства к удаленной установке (riprep).

Используйте утилиту riprep для подготовки устройства под управлением Windows к удаленной установке. Чтобы скачать утилиту, перейдите по этой ссылке: https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe

Утилита подготовки устройства к удаленной установке не работает под управлением операционной системы Microsoft Windows XP Home Edition.

Подготовка устройства под управлением Windows к удаленной установке в интерактивном режиме

Чтобы подготовить устройство под управлением Windows к удаленной установке в интерактивном режиме:

1. На клиентском устройстве запустите файл riprep.exe.
2. В открывшемся главном окне утилиты подготовки к удаленной установке выберите следующие параметры:
   - **Отключить простой общий доступ к файлам**
   - **Запустить службу Сервера администрирования**
   - **Открыть порты**
   - **Добавить учетную запись**
   - **Отключить контроль учетных записей** (параметр доступен для операционных систем Microsoft Windows Vista, Microsoft Windows 7 и Microsoft Windows Server 2008)
3. Нажмите на кнопку **Запустить**.

   В результате в нижней части главного окна утилиты отображаются этапы подготовки устройства к удаленной установке.

Если вы выбрали параметр **Добавить учетную запись**, при создании учетной записи будет выведен запрос на ввод имени учетной записи и пароля. В результате будет создана локальная учетная запись, принадлежащая группе локальных администраторов.

Если вы выбрали параметр **Отключить контроль учетных записей**, попытка отключения контроля учетных записей будет выполняться и в том случае, когда до запуска утилиты контроль учетных записей был отключен. После отключения контроля учетных записей будет выведен запрос на перезагрузку устройства.

Подготовка устройства под управлением Windows к удаленной установке в тихом режиме

Чтобы подготовить устройство под управлением Windows к удаленной установке в тихом режиме:

на клиентском устройстве запустите файл riprep.exe из командной строки с необходимым набором ключей.

Синтаксис командной строки утилиты:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Описания ключей:

- `-silent` – запустить утилиту на выполнение в тихом режиме.

- `-cfg CONFIG_FILE` – определение конфигурации утилиты, где `CONFIG_FILE` – путь к конфигурационному файлу (файл с расширением .ini).

- `-tl traceLevel` – задание уровня трассировки, где `traceLevel` – число от 0 до 5. Если ключ не задан, то используется значение 0.

В результате запуска утилиты в тихом режиме вы можете выполнить следующие задачи:

- отключение простого общего доступа к файлам;

- запуск службы Server на клиентском устройстве;

- открытие портов;

- создание локальной учетной записи;

- отключение контроля учетных записей (UAC).

Вы можете задать параметры подготовки устройства к удаленной установке в конфигурационном файле, указанном в ключе `-cfg`. Чтобы задать эти параметры, в конфигурационный файл нужно добавить следующую информацию:

- В разделе `Common` указать, какие задачи следует выполнять:

  - `DisableSFS` – отключение простого общего доступа к файлам (0 – задача выключена; 1 – задача включена).

  - `StartServer` – запуск службы Server (0 – задача выключена; 1 – задача включена).

  - `OpenFirewallPorts` – открытие необходимых портов (0 – задача выключена; 1 – задача включена).

  - `DisableUAC` – отключение контроля учетных записей (0 – задача выключена; 1 – задача включена).

  - `RebootType` – определение поведения при необходимости перезагрузки при отключенном контроле учетных записей (UAC). Вы можете использовать следующие значения параметра:

    - 0 – никогда не перезагружать устройство;

    - 1 – перезагружать устройство, если до запуска утилиты контроль учетных записей был включен;

    - 2 – перезагружать устройство принудительно, если до запуска утилиты контроль учетных записей был включен;

    - 4 – всегда перезагружать устройство;

    - 5 – всегда принудительно перезагружать устройство.

- В разделе `UserAccount` указать имя учетной записи (`user`) и ее пароль (`Pwd`).

Пример содержимого конфигурационного файла:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1
[UserAccount]
```

```
user=Admin
Pwd=Pass123
```

По окончании работы утилиты в папке запуска создаются следующие файлы:

- riprep.txt – отчет о работе, в котором перечислены этапы работы утилиты с причинами их проведения;
- riprep.log – файл трассировки (создается, если заданный уровень трассировки больше 0).

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

Сценарий: настройка защиты сети

Создавайте и настраивайте политики и задачи, необходимые для вашей сети.

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center.
- Установили Консоль OSMP.
- Выполнили основной сценарий установки Open Single Management Platform.

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"**

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода.

2. **Настройка задач для удаленного управления приложениями "Лаборатории Касперского"**

   В группе администрирования **Управляемые устройства** создайте вручную и настройте следующие политики и задачи:

   - политика Kaspersky Endpoint Security;
   - групповая задача обновления Kaspersky Endpoint Security;
   - политика Агента администрирования;

   Инструкции: Настройка групповой задачи обновления Kaspersky Endpoint Security.

При необходимости создайте дополнительные задачи управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

3. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях в работе управляемых приложений передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции: Настройка количества событий в хранилище событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского".

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры приложений к разным устройствам, вы можете использовать один или оба типа управления в комбинации.

Управление безопасностью, ориентированное на устройства, позволяет вам применять различные параметры приложения безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования.

Управление безопасностью, ориентированное на пользователя, позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать проблемы безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры приложения. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с параметрами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center и Консоль OSMP. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователей как альтернативу или дополнительную возможность для подхода, ориентированного на устройства. Узнайте больше о двух подходах к управлению.

Этапы

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики.

2. **Создание профилей политики (если требуется)**

   Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

   Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам с определенной конфигурацией программного обеспечения или с заданными теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *CentOS*, назначить его всем устройствам под управлением операционной системы CentOS, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы CentOS установленные приложения "Лаборатории Касперского" будут управляться своим профилем политики.

   Инструкции:

   - Создание профиля политики.
   - Создание правила активации профиля политики.

3. **Распространение политик и профилей политик на управляемые устройства**

   По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Open Single Management Platform определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center и Консоль OSMP и завершили основной сценарий развертывания. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению.

Процесс

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики.

2. **Укажите пользователей в качестве владельцев устройств**

   Назначьте управляемым устройствам соответствующих пользователей.

   Инструкция: Назначение пользователя владельцем устройства.

3. **Определение пользовательских ролей, типичных для вашей организации**

   Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вам нужно разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры приложения, специфичные для этой роли.

4. **Создание пользовательских ролей**

   Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям приложения.

   Инструкция: Создание роли пользователя.

5. **Определение области для каждой роли пользователя**

   Для каждой созданной роли пользователя определите пользователей и/или группы безопасности и группы администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

   Инструкция: Изменение области для роли пользователя.

6. **Создание профилей политики**

Создайте профиль политики для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

Инструкция: Создание профиля политики.

7. **Связь профиля политики с ролями пользователей**

   Свяжите профили политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкция: Связь профилей политики с ролями.

8. **Распространение политик и профилей политик на управляемые устройства**

   По умолчанию синхронизация Open Single Management Platform с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Open Single Management Platform определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на пользователя, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики приложений и профили политик будут автоматически применяться к устройствам этого пользователя.

Политики и профили политик

В Консоли OSMP можно создавать политики для приложений "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

О политиках и профилях политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой

	группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (). В таблице ниже показаны состояния значка замка:

Статусы значка замка

Состояние	Описание
Не определено	Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются *разблокированными*.
Принудительно	Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемого приложения. Такие параметры называются *заблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

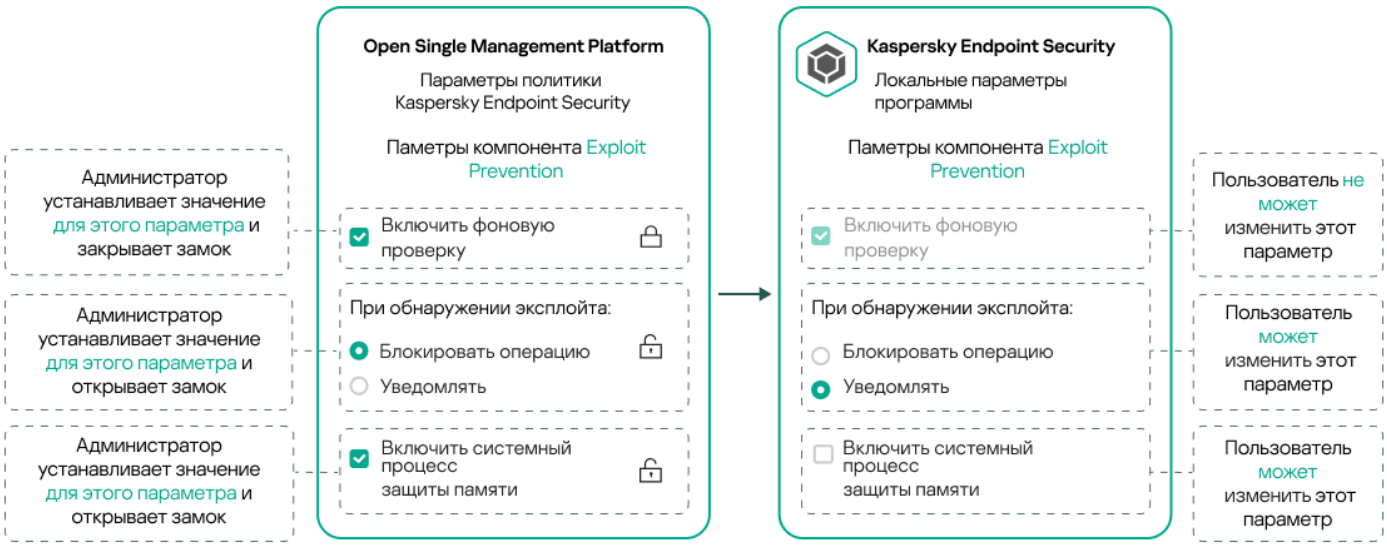
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров приложения "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемое приложение "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры приложения "Лаборатории Касперского" меняют значения на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже):



Замки и параметры приложения "Лаборатории Касперского"

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

Иерархия политик

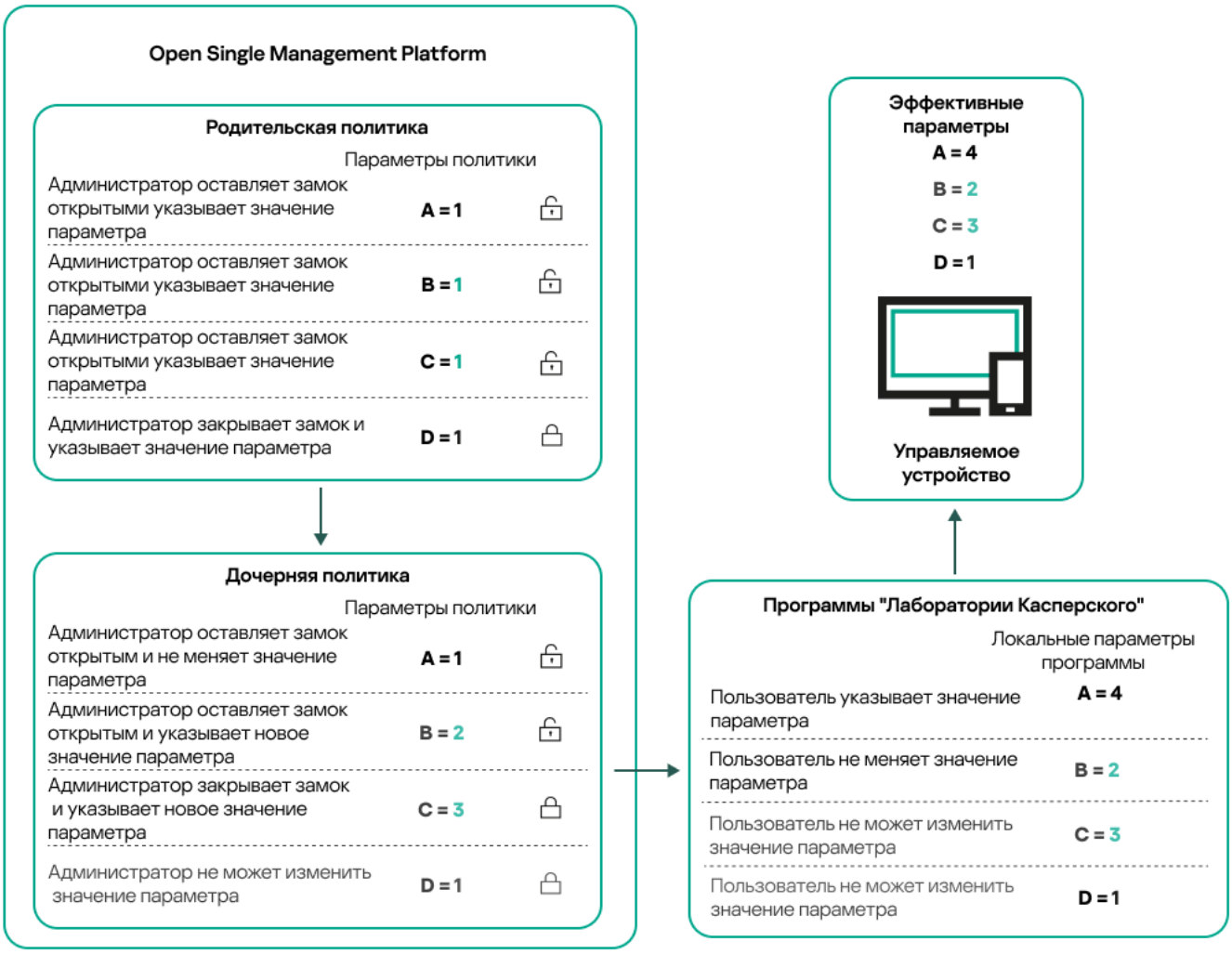
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования. Параметры политики можно *унаследовать*. Наследование – это получение значений параметров политики в подгруппах (дочерних группах) от вышестоящей политики (родительской) группы администрирования.

Политика, созданная для родительской группы, также называется *родительской политикой*. Политика, созданная для подгруппы (дочерней группы), также называется *дочерней политикой*.

По умолчанию на Сервере администрирования существует как минимум одна группа администрирования управляемых устройств. Если вы хотите создать группы администрирования, они создаются как подгруппы (дочерние группы) в группе Управляемые устройства.

Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).

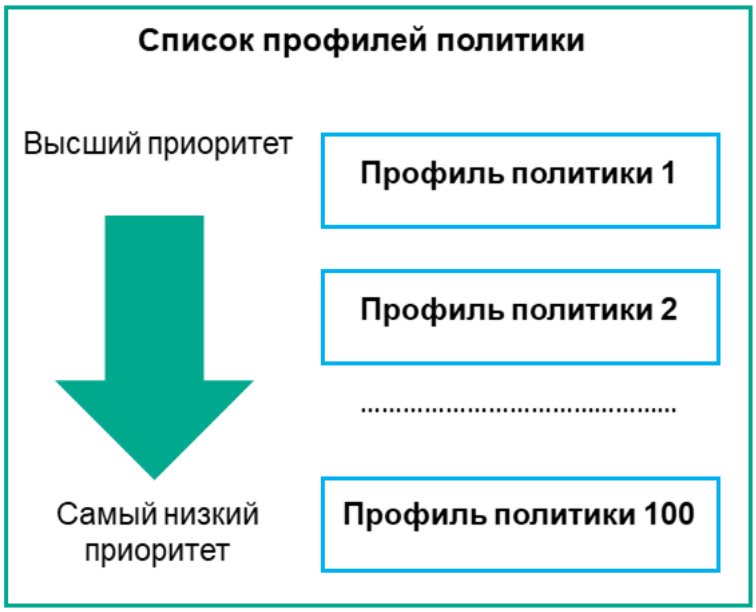


Иерархия политик

Профили политик в иерархии политик

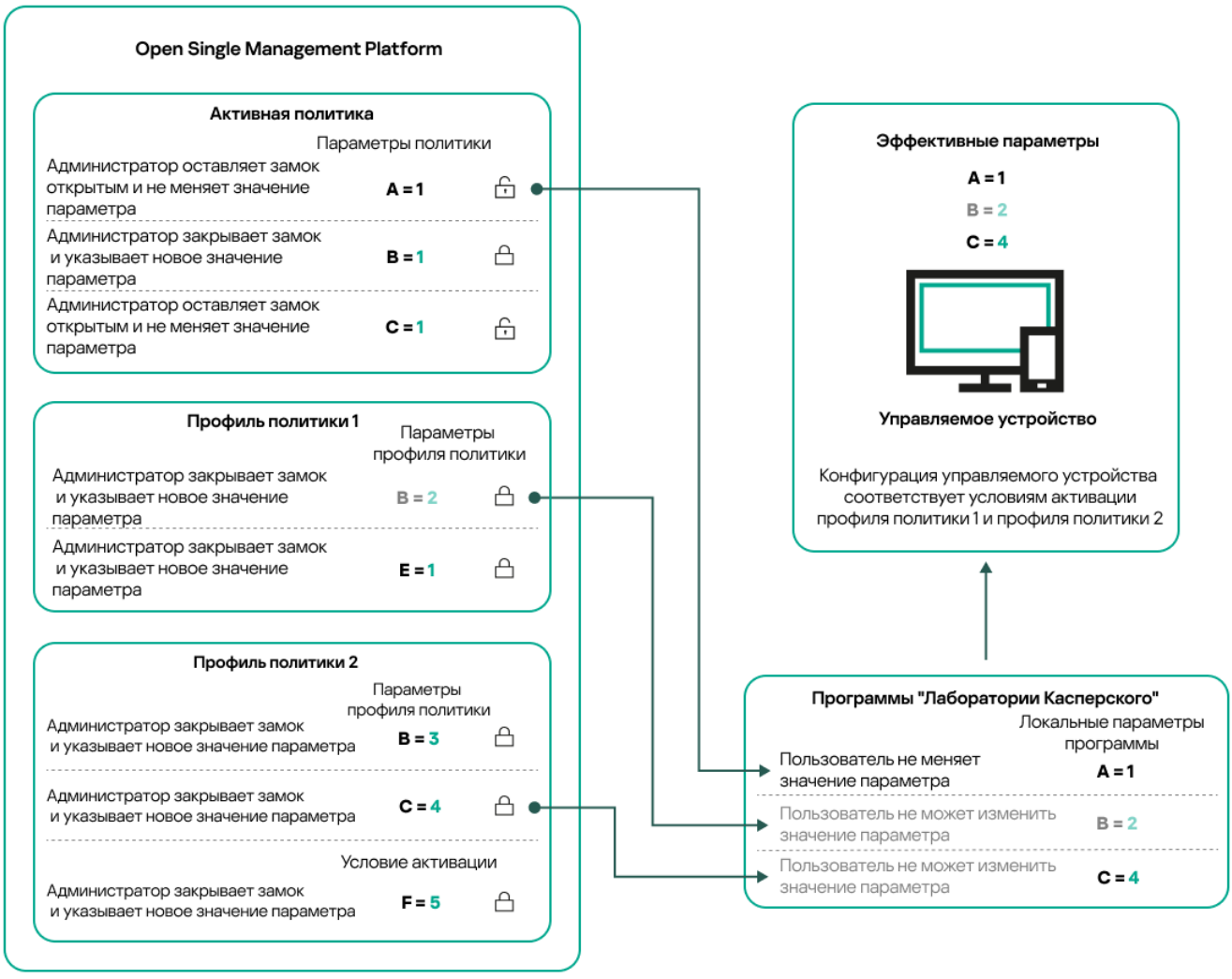
Профили политики имеют следующие условия назначения приоритета:

- Положение профиля в списке профилей политики обозначает его приоритет. Вы можете изменить приоритет профиля политики. Самая высокая позиция в списке обозначает самый высокий приоритет (см. рисунок ниже).



Определение приоритета профиля политики

- Условия активации профилей политик не зависят друг от друга. Одновременно можно активировать несколько профилей политик. Если несколько профилей политики влияют на один и тот же параметр, устройство использует значение параметра из профиля политики с наивысшим приоритетом (см. рисунок ниже).

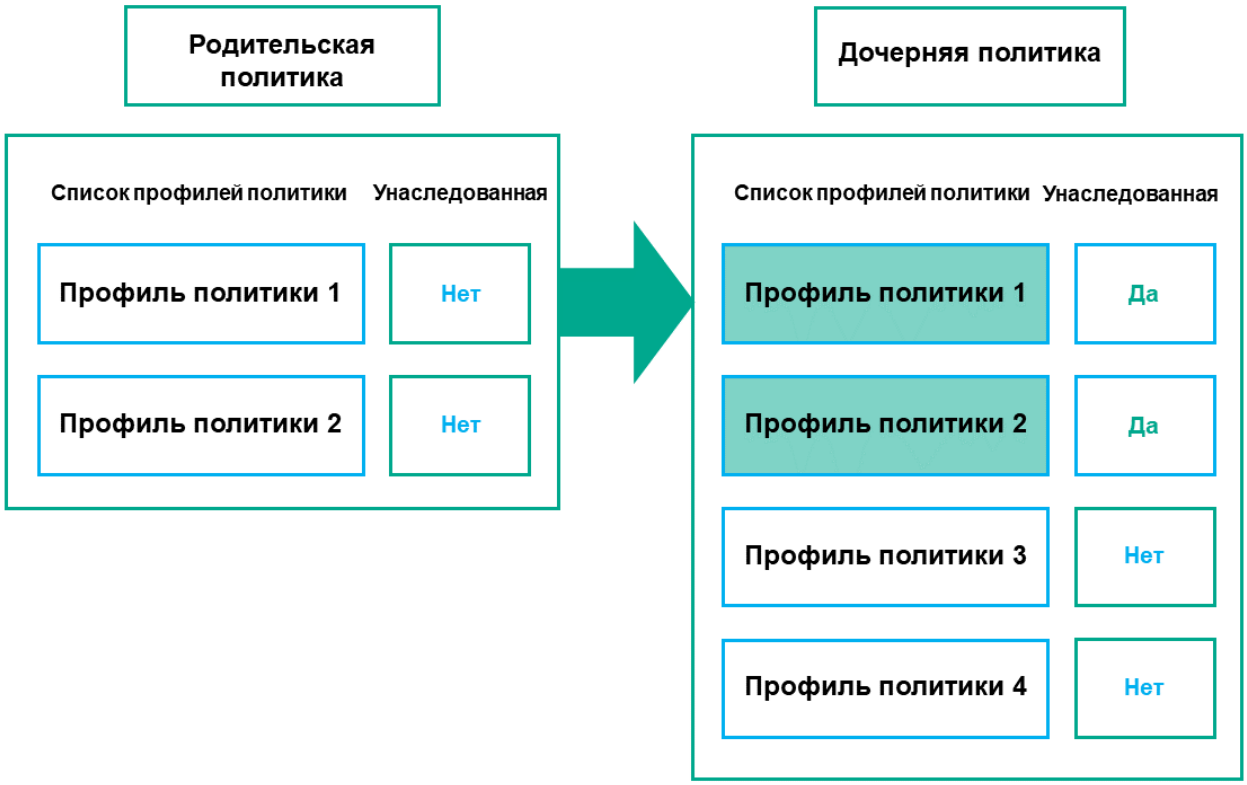


Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

Профили политик в иерархии наследования

Профили политик из политик разных уровней иерархии соответствуют следующим условиям:

- Политика нижнего уровня наследует профили политики из политики более высокого уровня. Профиль политики, унаследованный от политики более высокого уровня, получает более высокий приоритет, чем уровень исходного профиля политики.
- Вы не можете изменить приоритет унаследованного профиля политики (см. рисунок ниже).

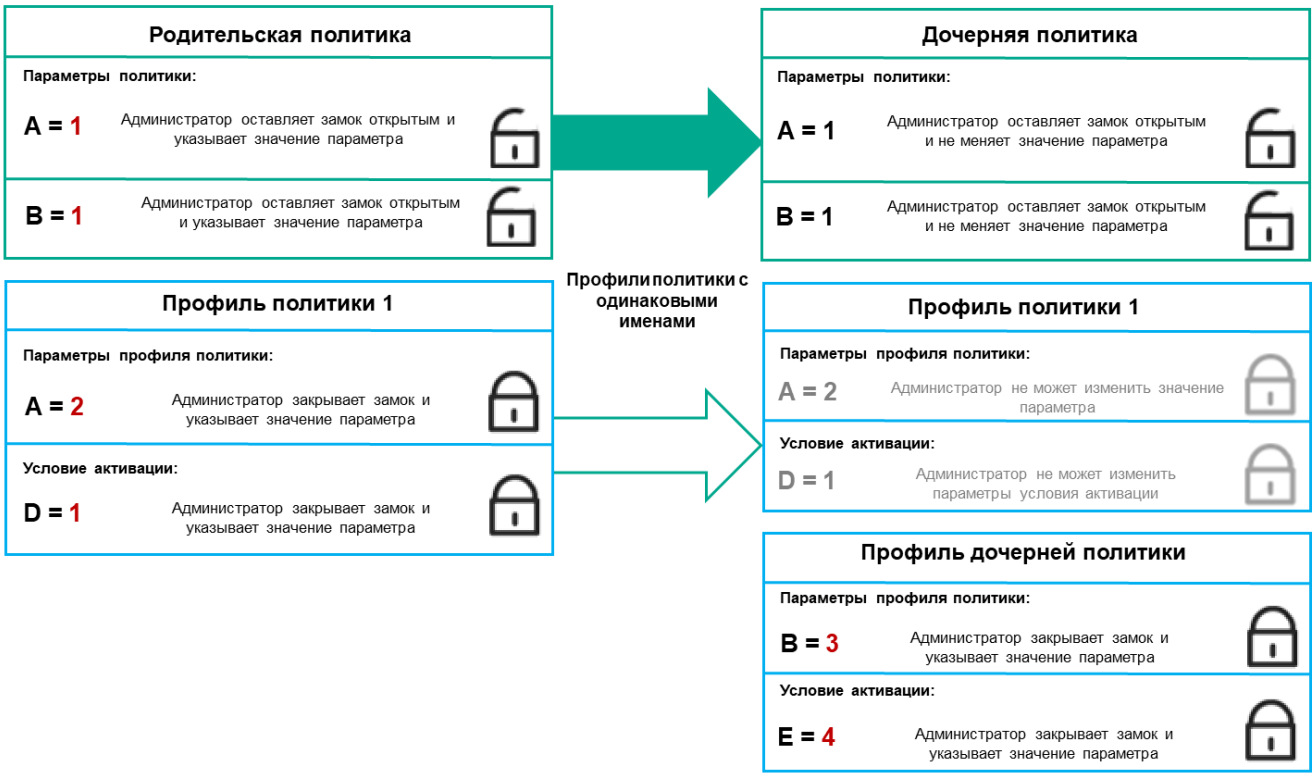


Наследование параметров профилей политики

Профили политики с одинаковыми именами

Если на разных уровнях иерархии есть две политики с одинаковыми именами, эти политики работают в соответствии со следующими правилами:

- Заблокированные параметры и условие активации профиля для профиля политики более высокого уровня изменяют параметры и условие активации профиля для профиля политики более низкого уровня (см. рисунок ниже).



Дочерний профиль наследует значения параметров из родительского профиля политики

- Разблокированные параметры и условие активации профиля для профиля политики более высокого уровня не изменяют параметры и условие активации профиля для профиля политики более низкого уровня.

Как параметры реализованы на управляемом устройстве

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемого приложения.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

Управление политиками

В этом разделе описывается управление политиками и предоставляется информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

Чтобы просмотреть список политик:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

Чтобы создать политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Выберите группу администрирования, для которой нужно создать политику:

   - Для корневой группы.

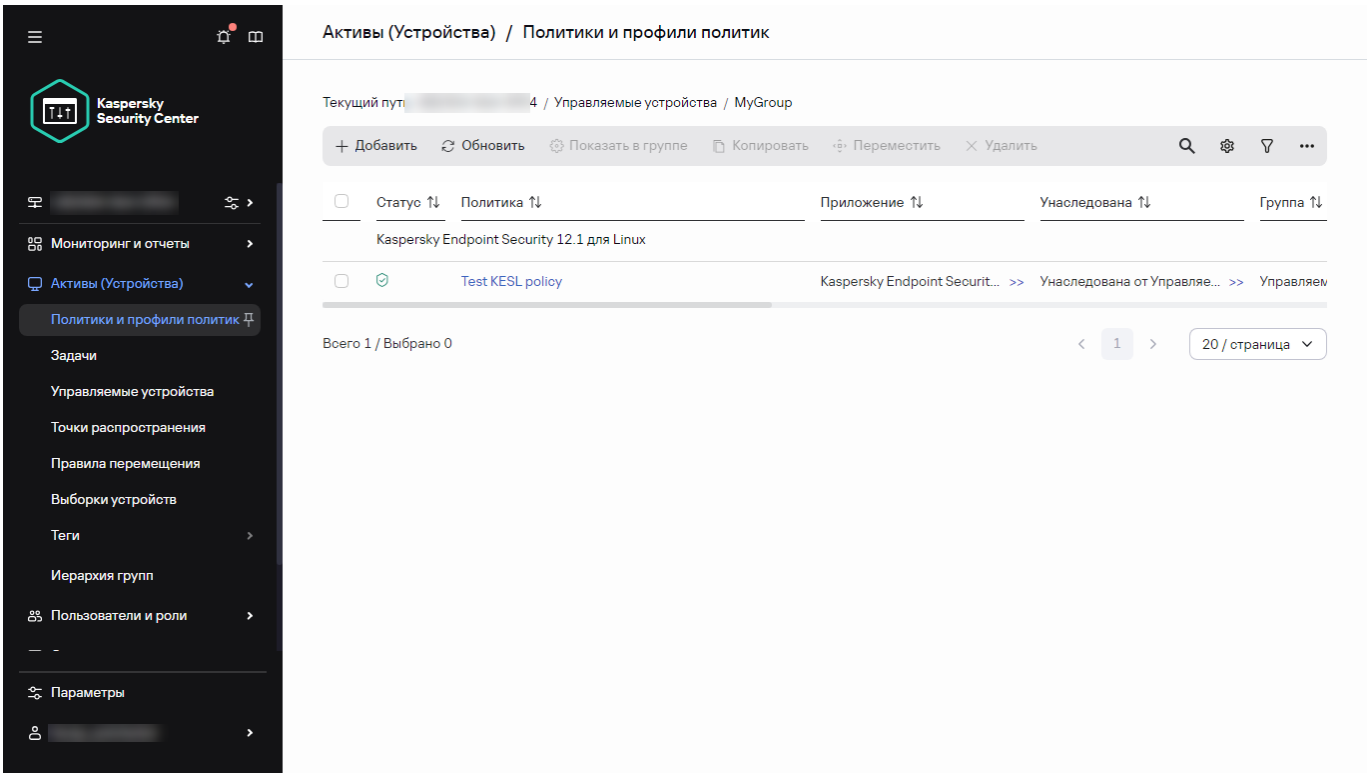
     В этом случае вы можете перейти к следующему шагу.

   - Для подгруппы:

     a. Перейдите по ссылке текущего пути в верхней части окна.

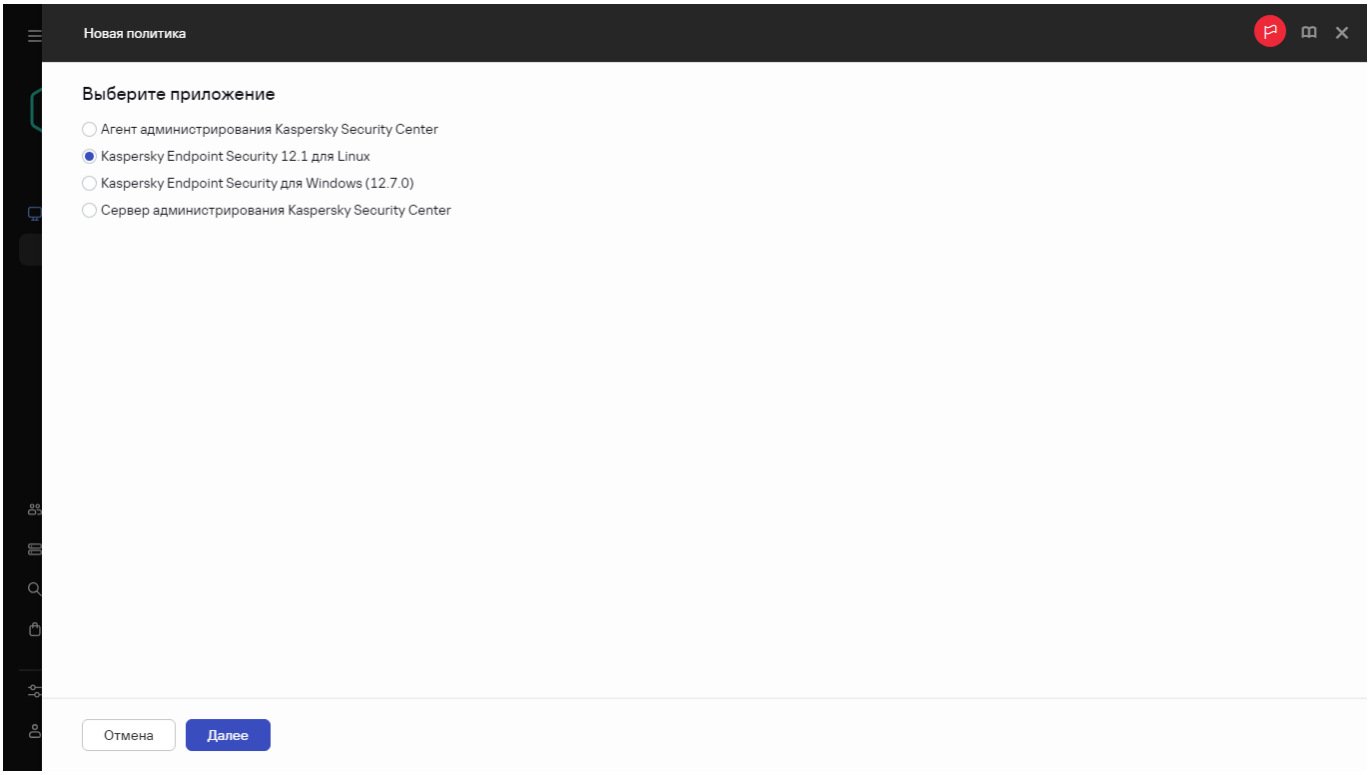
     b. В открывшейся панели перейдите по ссылке с названием нужной подгруппы.

     Текущий путь изменится, чтобы отразить выбранную подгруппу.



3. Нажмите на кнопку **Добавить**.

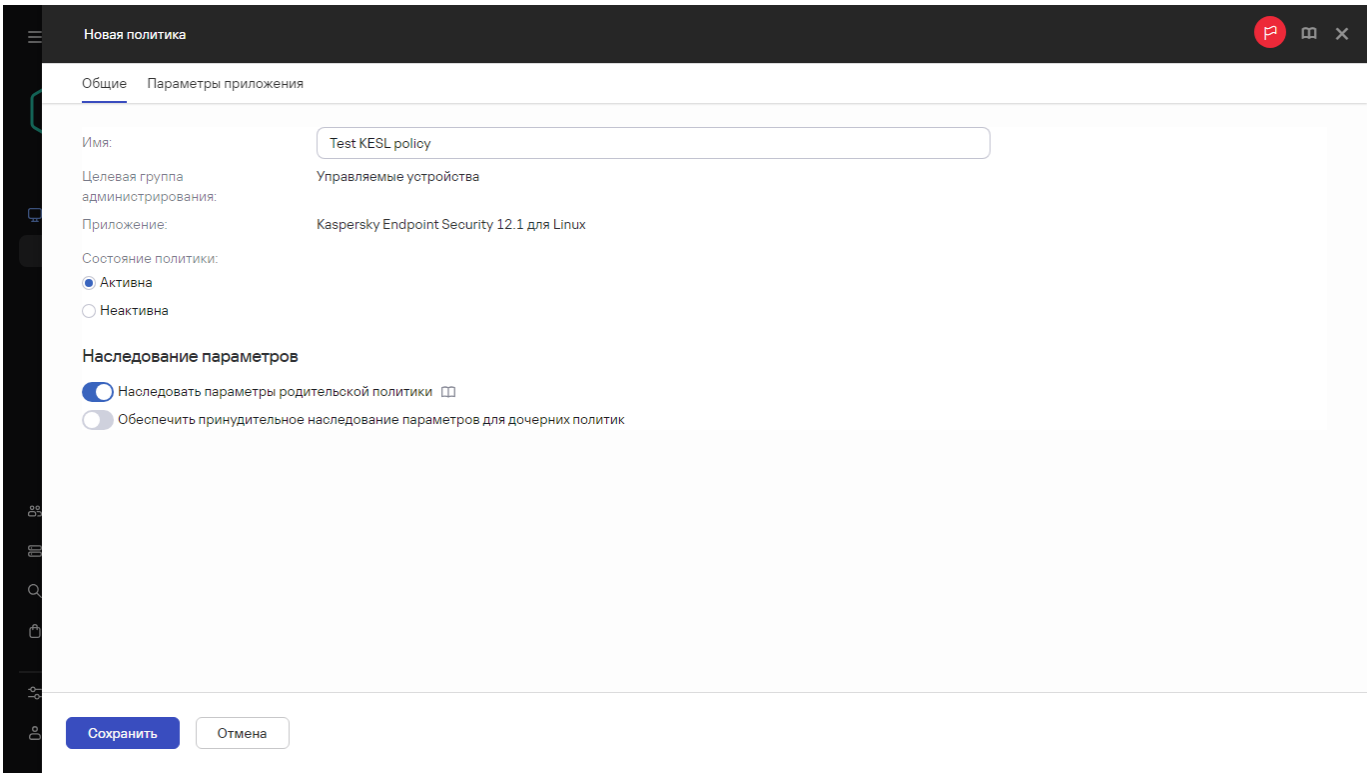
   Откроется окно **Выберите приложение**.



4. Выберите приложение, для которого требуется создать политику.

5. Нажмите на кнопку **Далее**.

   Откроется окно параметров новой политики на вкладке **Общие**. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.



6. Выберите вкладку **Параметры приложения**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.

7. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Набор параметров зависит от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Справка Kaspersky Endpoint Security для Linux
   - Справка Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к соответствующему приложению.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения политики.

В результате добавленная политика отображается в списке политик.

Общие параметры политик

Общие

На вкладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.

  - **Для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.

  - **Неактивна**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры родительской политики**

    Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию флажок установлен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

    Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию флажок снят.

Настройка событий

На вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Критическое**

  Раздел **Критическое** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). Нажав на тип события, вы можете указать следующие параметры:

- **Регистрация событий**

  Вы можете указать количество дней хранения событий и выбрать, где хранить события:

  - **Экспортировать в SIEM-систему по протоколу Syslog**
  - **Хранить в журнале событий ОС на устройстве**
  - **Хранить в журнале событий ОС на Сервере администрирования**

- **Уведомления о событиях**

  Вы можете выбрать способ уведомления о событии:

  - **Уведомлять по электронной почте**
  - **Уведомлять по SMS**
  - **Уведомлять запуском исполняемого файла или скрипта**
  - **Уведомлять по SNMP**

  По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на вкладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

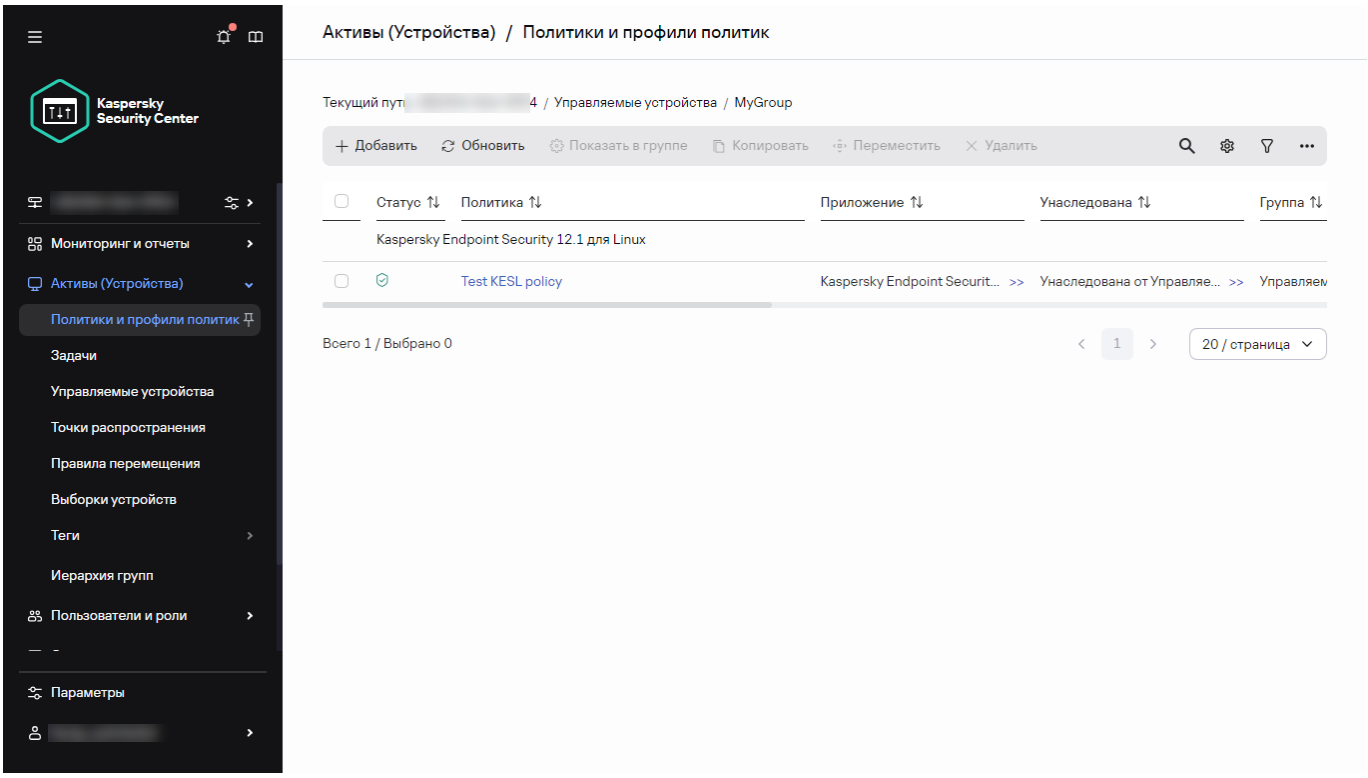
История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат.

Изменение политики

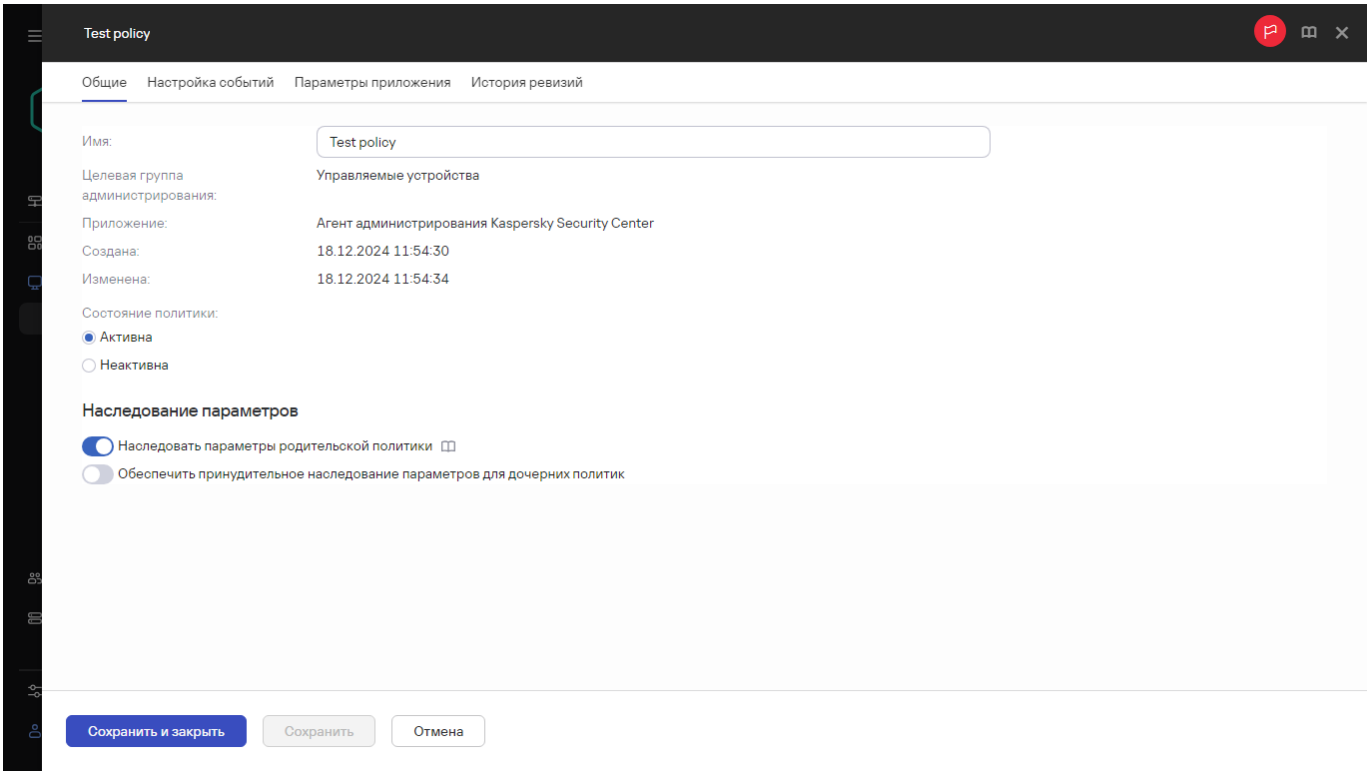
Чтобы изменить политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.



2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.



3. Укажите общие параметры и параметры приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Справка Kaspersky Endpoint Security для Linux
   - Справка Kaspersky Endpoint Security для Windows

Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.

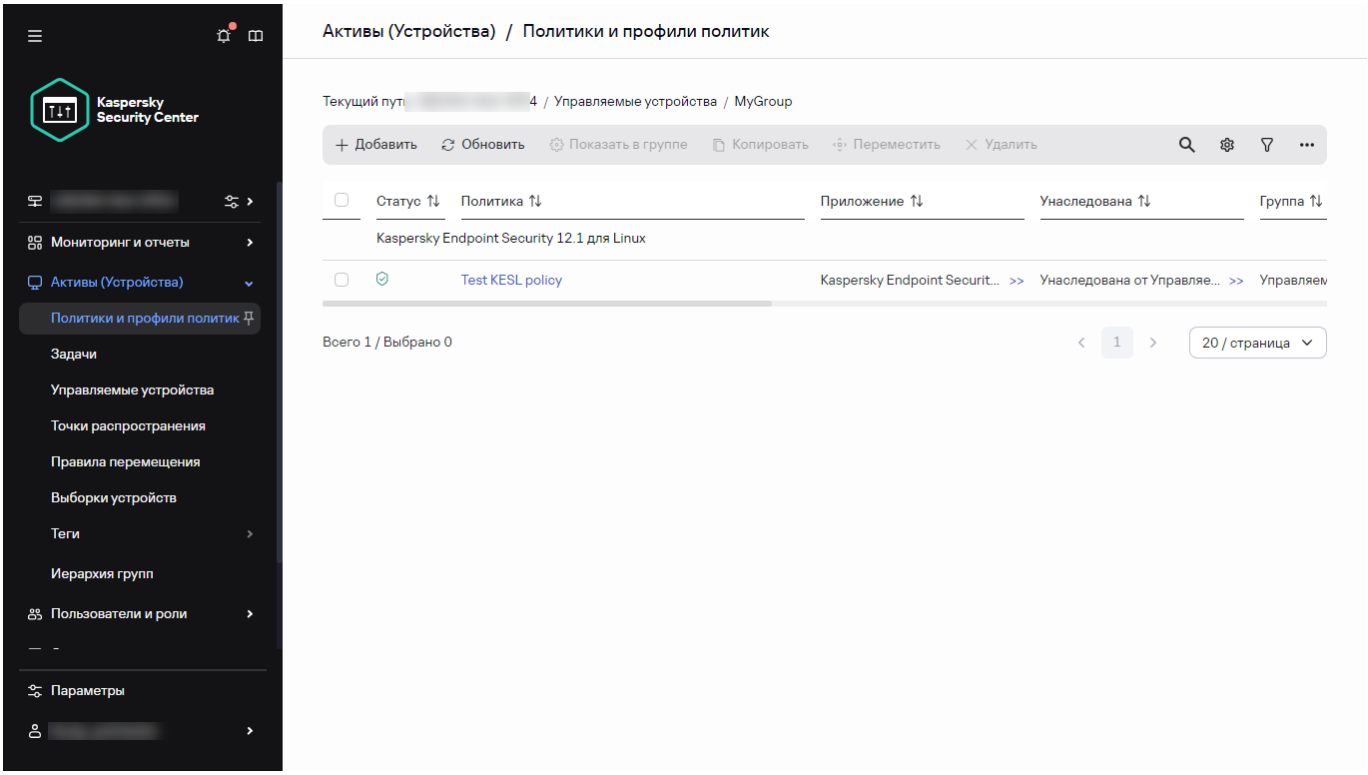
4. Нажмите на кнопку **Сохранить**.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

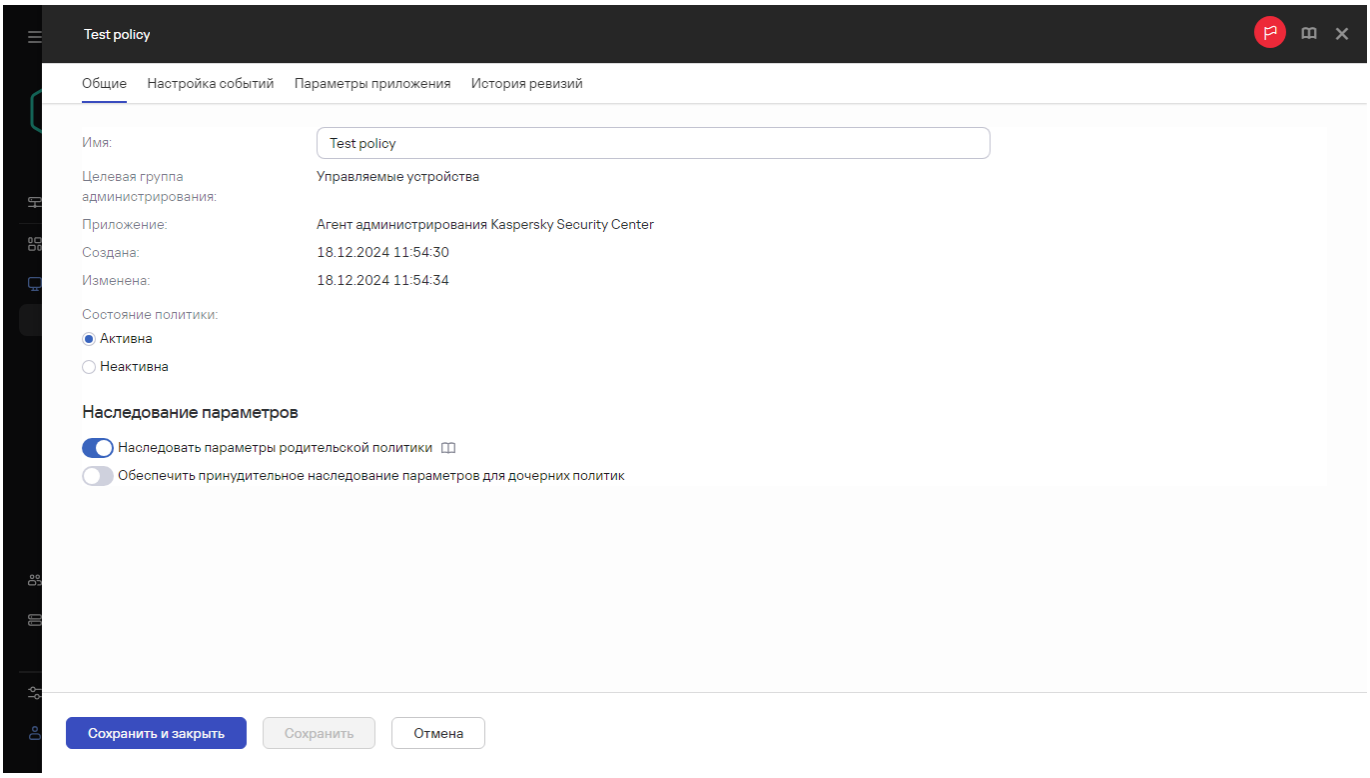
Включение и выключение параметра наследования политики

Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.



2. Откройте вкладку **Общие**.



3. Включение или выключение наследования политики:

   - Если вы включили параметр **Наследовать параметры родительской политики** для дочерней группы и администратор заблокировал некоторые параметры в родительской политике, то вы не можете изменить эти параметры политики для дочерней политики.

   - Если вы выключили параметр **Наследовать параметры родительской политики** для дочерней политики, то вы можете изменить все параметры в дочерней политике, даже если некоторые параметры "заблокированы" в родительской политике.

   - Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, или нажмите на кнопку **Отмена**, чтобы отклонить изменения.

По умолчанию, параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

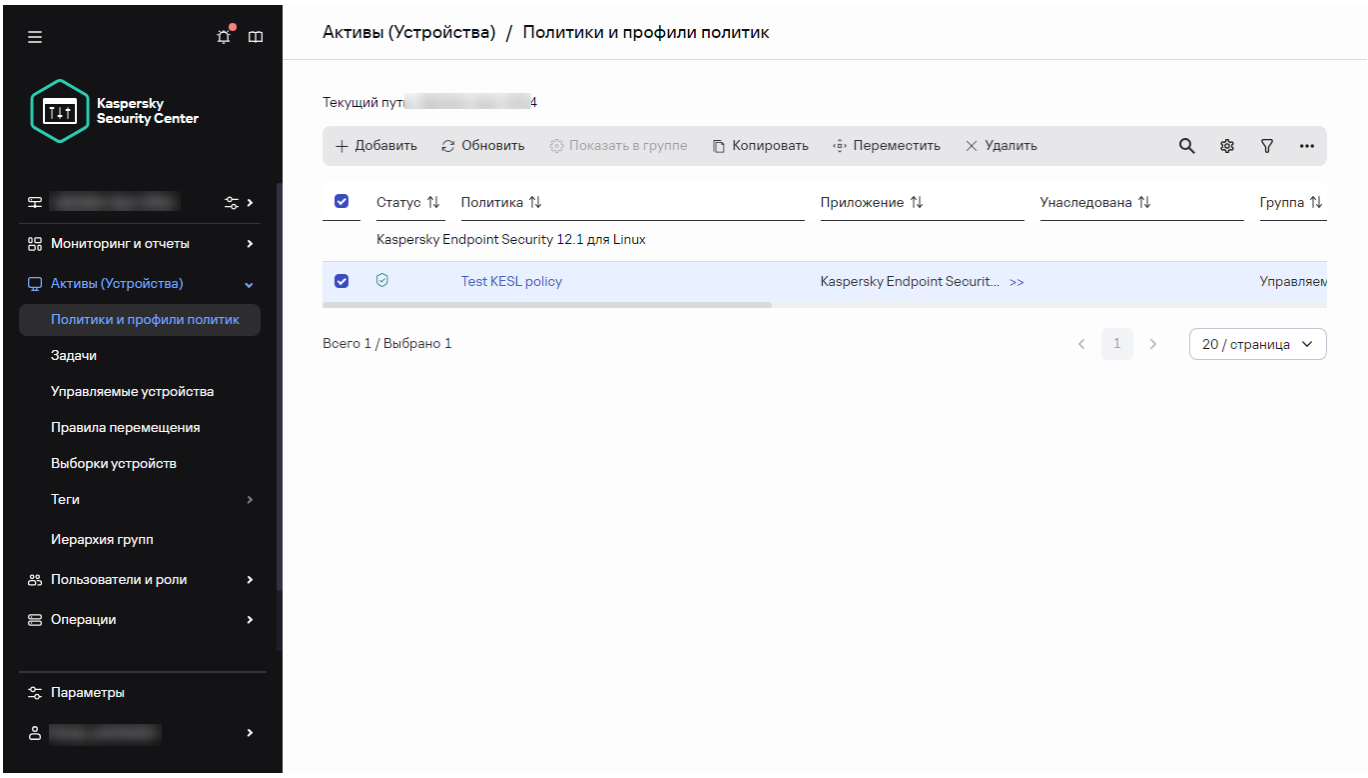
Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

Чтобы скопировать политику в другую группу администрирования:

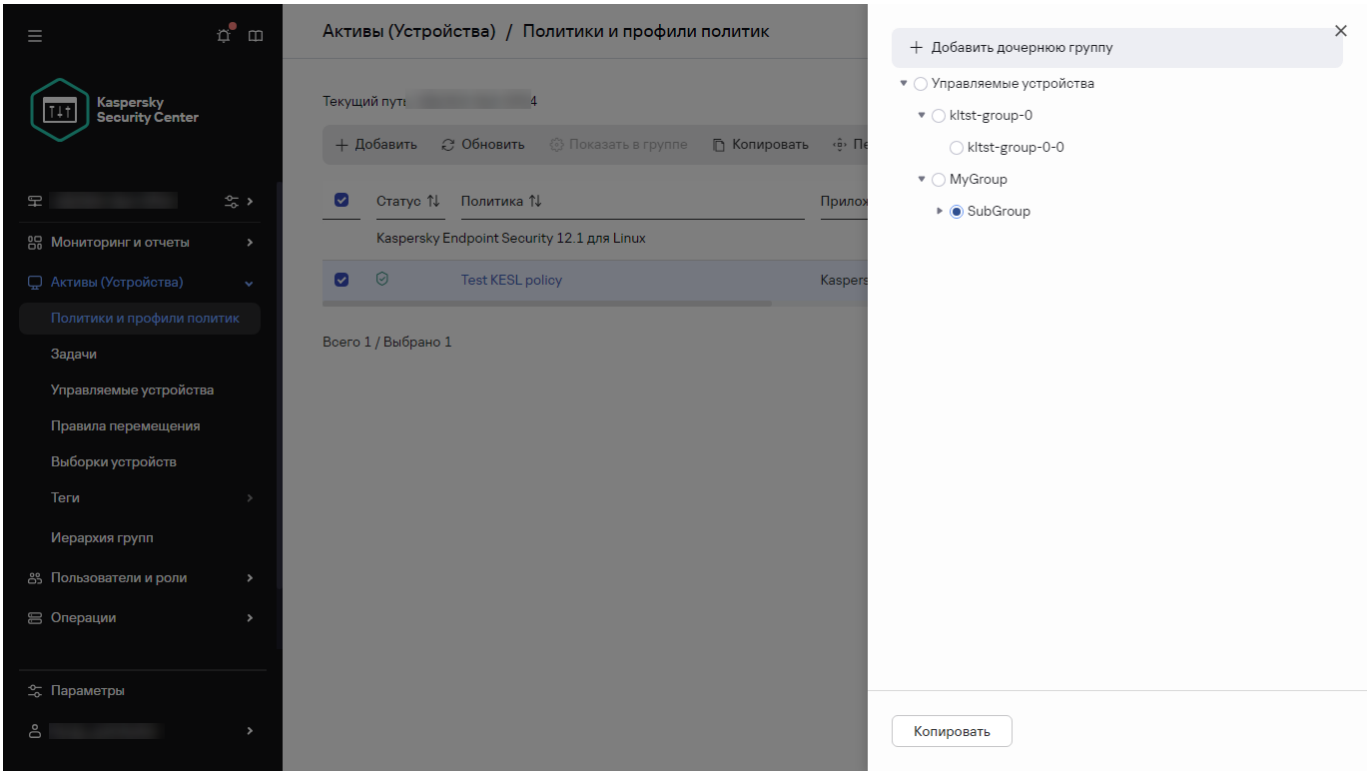
1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Установите флажок напротив политики (или политик), которую требуется скопировать.



3. Нажмите на кнопку **Копировать**.

   В правой части экрана отображается дерево групп администрирования.



4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).

5. Нажмите на кнопку **Копировать** внизу экрана.

6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

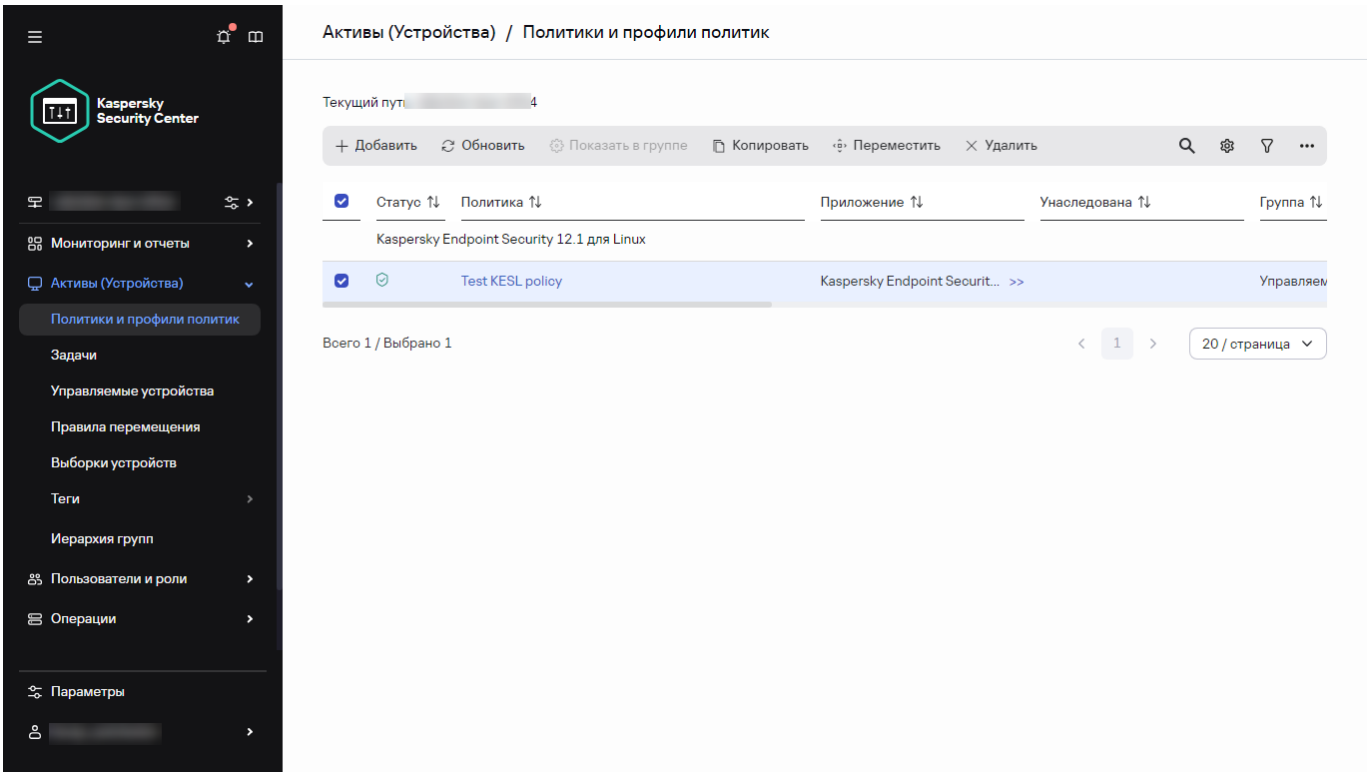
Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Перемещение политики

Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

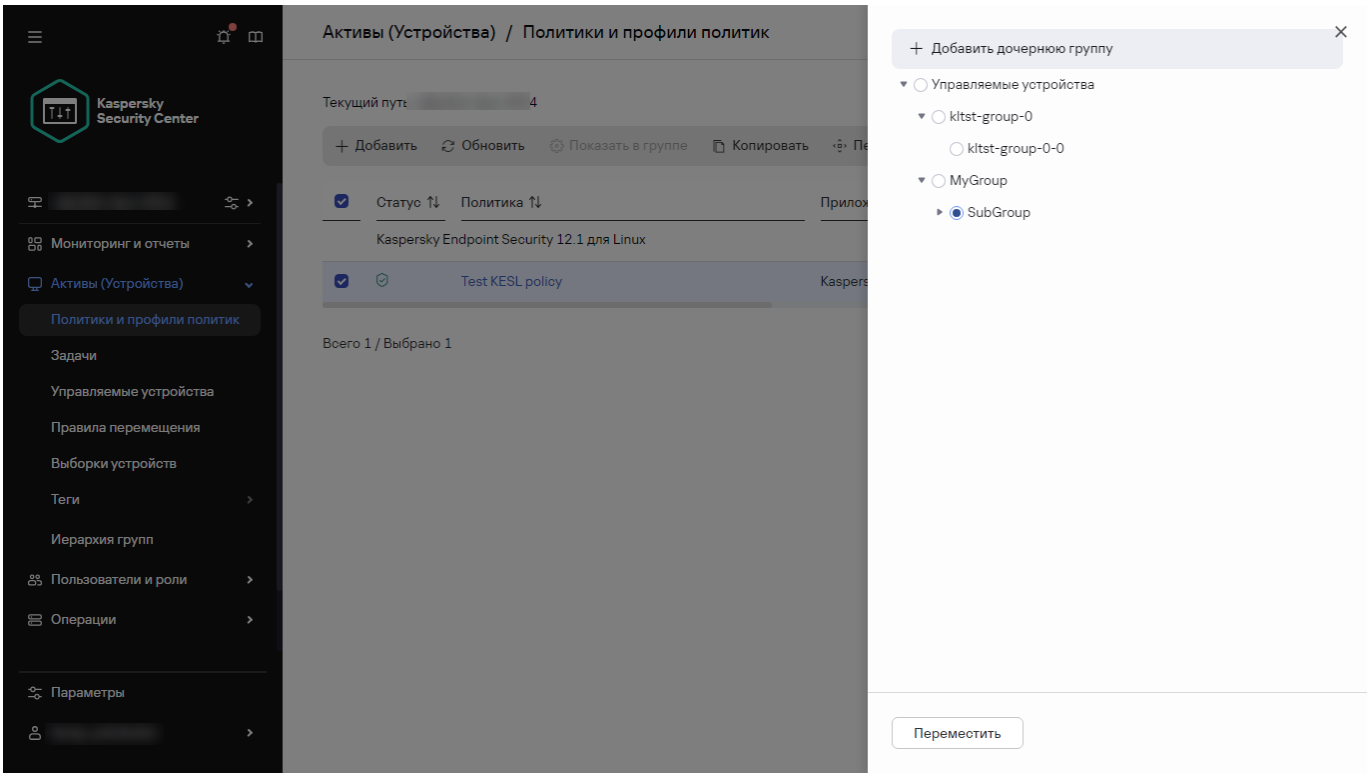
Чтобы переместить политику в другую группу администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется переместить.



3. Нажмите на кнопку **Переместить**.

   В правой части экрана отображается дерево групп администрирования.



4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).

5. Нажмите на кнопку **Переместить** внизу экрана.

6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Экспорт политики

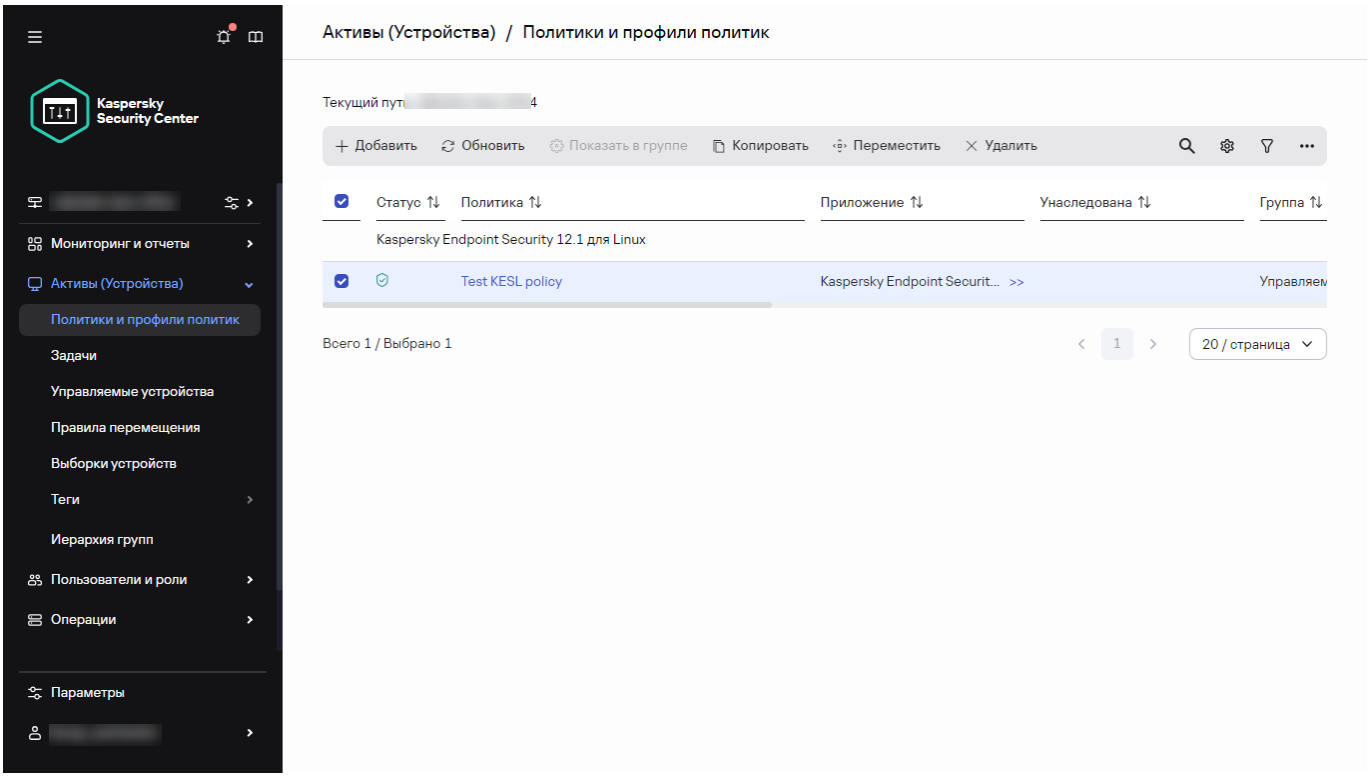
Open Single Management Platform позволяет сохранить политику, ее параметры и профили политики в файл KLP. Вы можете использовать файл KLP для импорта сохраненной политики как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Установите флажок рядом с политикой, которую вы хотите экспортировать.

   Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **Экспортировать** будет неактивна.



Выбор политики для экспорта

3. Нажмите на кнопку **Экспортировать**.

4. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл политики автоматически сохраняется в папку **Загрузки**.

Импорт политики

Open Single Management Platform позволяет импортировать политику из файла KLP. Файл KLP содержит экспортированную политику, ее параметры и профили политики.

Чтобы импортировать политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на кнопку **Импортировать**.

3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.

4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.

   Начнется обработка политики.

5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.

6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Принудительная синхронизация

Несмотря на то, что Open Single Management Platform автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору требуется точно знать, была ли выполнена синхронизация для определенного устройства в данный момент.

Синхронизация одного устройства

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать сейчас**.

Приложение выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:

1. Откройте список устройств группы администрирования или выборку устройств:
   - В главном меню перейдите в раздел **Активы (Устройства)**→ **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** над списком управляемых устройств и выберите группу администрирования, в которую входят устройства для синхронизации.
   - Запустите выборку устройств, чтобы просмотреть список устройств.
2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (...) и нажмите на кнопку **Синхронизировать сейчас**.

   Приложение выполняет синхронизацию выбранных устройств с Сервером администрирования.

4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для приложения "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

Чтобы просмотреть дату и время доставки политики приложения на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Перейдите на вкладку **Приложения**.
4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

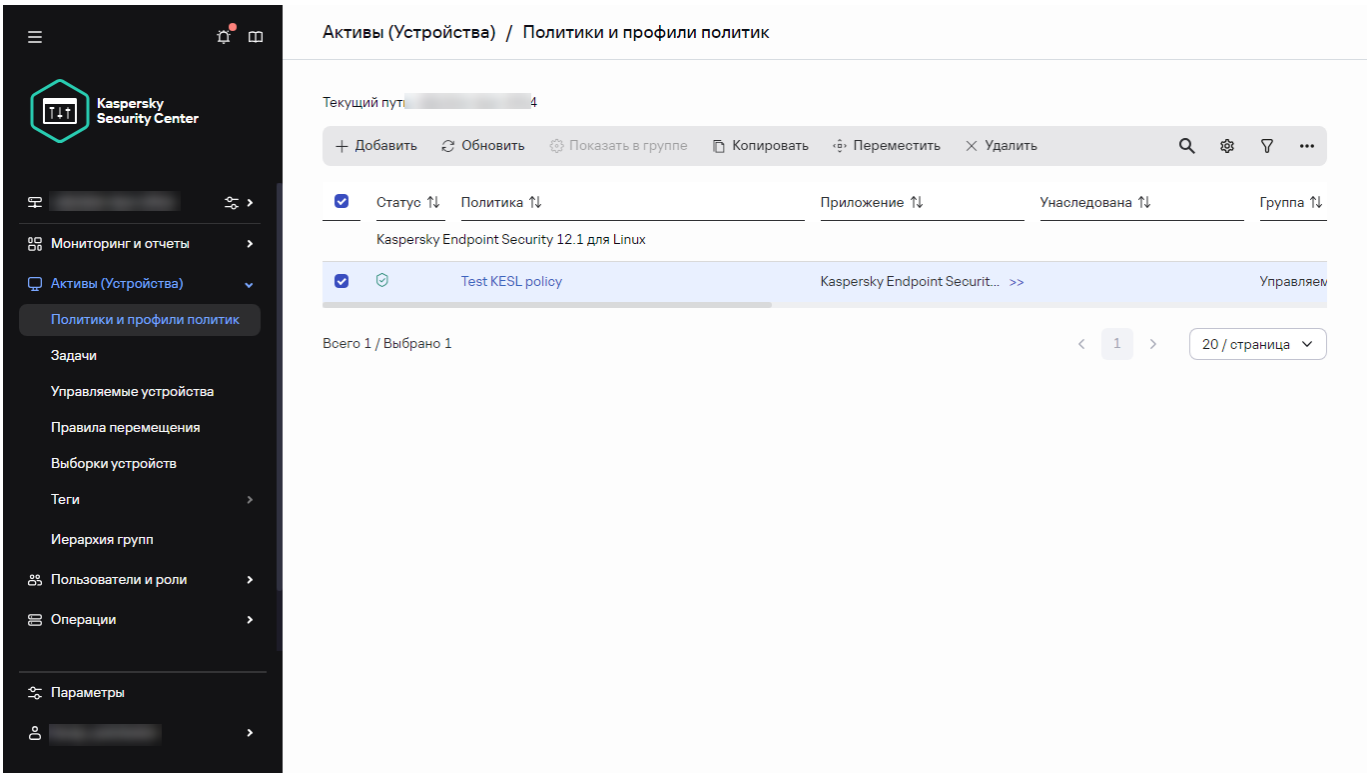
   Откроется окно политики приложения, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

Просмотр диаграммы состояния применения политики

В Open Single Management Platform вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

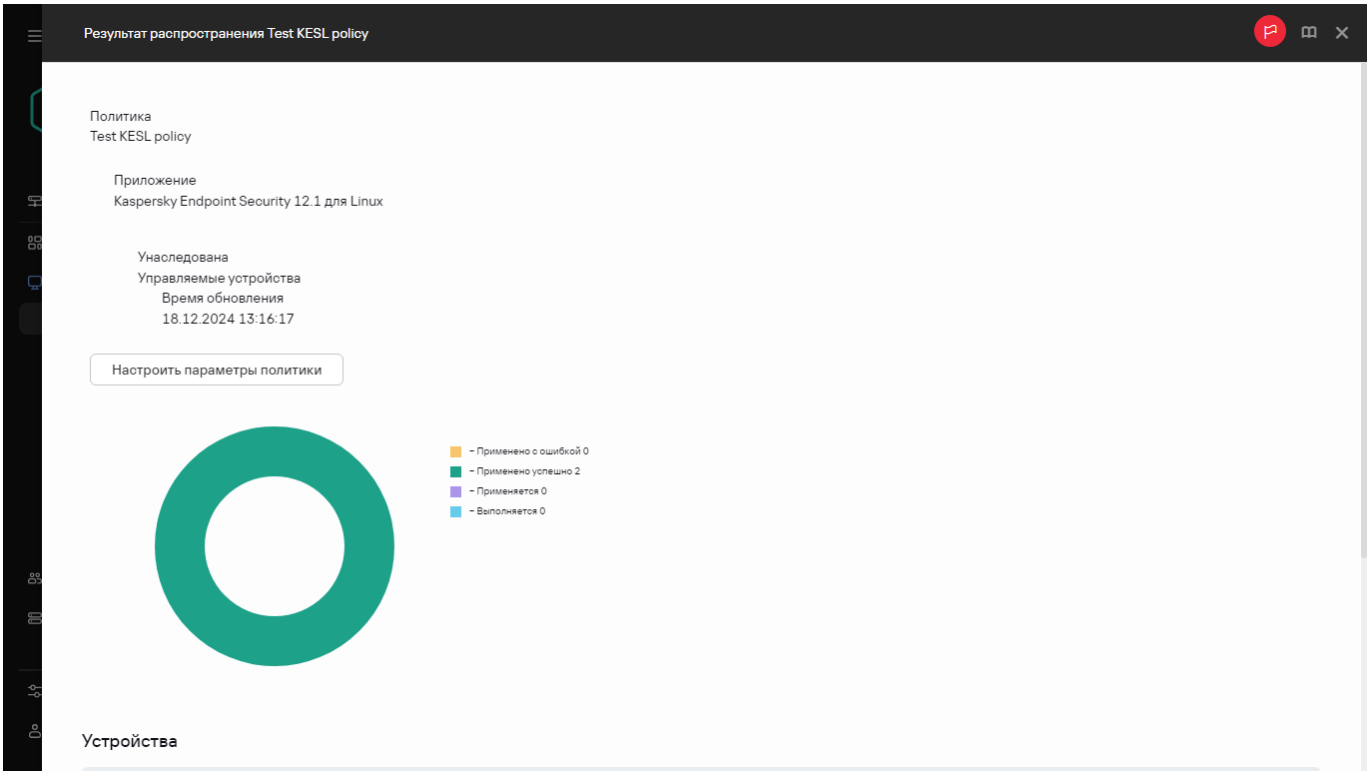
Чтобы просмотреть статус применения политики на каждом устройстве:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.



3. В появившемся меню выберите ссылку **Результаты применения**.

   Откроется окно **Результат распространения <название политики>**.



4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса.**

2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.

3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

Чтобы удалить политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Установите флажок рядом с именем политики, которую вы хотите удалить, и нажмите на кнопку **Удалить**.

   Кнопка **Удалить** становится неактивной (серой), если вы выбрали унаследованную политику.

3. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика и все ее профили политики удалены.

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

Просмотр профилей политики

Чтобы просмотреть профили политики:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на вкладке **Общие**.

3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.

Изменение приоритета профиля политики

Чтобы изменить приоритет профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.

3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

   Чем выше расположен профиль политики в списке, тем выше его приоритет.

4. Нажмите на кнопку **Сохранить**.

Приоритет выбранного профиля политики изменен и применен.

Создание профиля политики

Чтобы создать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. Нажмите на кнопку **Добавить**.

3. Если необходимо, измените заданные по умолчанию имя и параметры наследования профиля политики.

4. Выберите вкладку **Параметры приложения**.

   Можно также нажать на кнопку **Сохранить**, чтобы выйти. Созданный профиль политики отобразится в списке профилей политики, и вы сможете изменить его свойства позже.

5. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения профиля.

Профиль политики отобразится в списке профилей политики.

Копирование профиля политики

Вы можете скопировать профиль политики в текущую политику или в другую политику, например, если вы хотите иметь идентичные профили политик для разных политик. Вы также можете использовать копирование, если хотите иметь два или более профилей политики, которые отличаются небольшим количеством параметров.

Чтобы скопировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. На вкладке **Профили политики** выберите профиль, который требуется скопировать.

3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне выберите политику, в которую требуется скопировать профиль политики.

   Вы можете скопировать профиль политики в эту же политику или в политику, которую вы выбрали.

5. Нажмите на кнопку **Копировать**.

Профиль политики скопирован в политику, которую вы выбрали. Новый скопированный профиль политики имеет самый низкий приоритет. Если вы скопировали профиль политики в эту же политику, к имени такого профиля добавляется окончание вида (<порядковый номер>), например: (1), (2).

Позже вы можете изменить параметры профиля политики, включая его имя и приоритет. В этом случае исходный профиль политики не будет изменен.

Создание правила активации профиля политики

Чтобы создать правило активации профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики.

3. На вкладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.

5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   - **Общие правила активации профиля политики**

     Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

     Для этого параметра на следующем шаге укажите:

     - **Статус устройства**

Определяет условие присутствия устройства в сети:

- **В сети** – устройство находится в сети, Сервер администрирования доступен.
- **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
- **Неизвестно** – критерий не применяется.

- **Правило подключения к Серверу администрирования активно на этом устройстве**

  Выберите условие для активации профиля политики (независимо от того, выполняется ли это правило или нет) и выберите имя правила.

  Правило определяется сетевым местоположением устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

  Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

- **Правила для выбранного владельца устройства**

  Для этого параметра на следующем шаге укажите:

  - **Владелец устройства**

    Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - устройство принадлежит указанному владельцу (знак "=");
    - устройство не принадлежит указанному владельцу (знак "№").

      Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

  - **Владелец устройства включен во внутреннюю группу безопасности**

    Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - владелец устройства является членом указанной группы безопасности (знак "=");
    - владелец устройства не является членом указанной группы безопасности (знак "№").

      Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Правила для характеристик оборудования**

  Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

  Для этого параметра на следующем шаге укажите:

  - **Объем оперативной памяти (МБ)**

    Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - объем оперативной памяти устройства меньше указанного значения (знак "<");
    - объем оперативной памяти устройства больше указанного значения (знак ">").

    Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

  - **Количество логических процессоров**

    Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - количество логических процессоров устройства меньше или равно указанному значению (знак "<");
    - количество логических процессоров устройства больше или равно указанному значению (знак ">").

    Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Правила для назначения роли**

  Для этого параметра на следующем шаге укажите:

  - **Активировать профиль политики по наличию роли у владельца устройства**

    Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца. Добавить роль вручную из списка существующих ролей.

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

Для этого параметра на следующем шаге укажите:

- **Список тегов**

  В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

  Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

  В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

- **Применить к устройствам без выбранных тегов**

  Установите флажок, если необходимо инвертировать выбор тегов.

  Если флажок установлен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если флажок снят, критерий не применяется. По умолчанию флажок снят.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

6. Проверьте список настроенных параметров. Если список верен, нажмите на кнопку **Создать**.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики на вкладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Удаление профиля политики

Чтобы удалить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых приложений, установленных на устройствах групп нижнего уровня.

Параметры политики Агента администрирования

Чтобы настроить параметры политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на имя политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования. Окно свойств содержит вкладки и параметры, описанные ниже.

Обратите внимание, что для устройств под управлением Linux и Windows, доступны различные параметры.

Общие

На этой вкладке можно изменить имя политики, состояние политики и настроить наследование параметров политики:

- В поле **Имя** вы можете изменить имя политики.
- В блоке **Состояние политики** можно выбрать один из следующих режимов политики:
  - **Активна**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Неактивна**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры родительской политики**

    Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию флажок установлен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

- значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
- в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

На этой вкладке можно настроить регистрацию событий и оповещение о событиях. События распределяются по уровням важности в следующих разделах:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в разделе **Предупреждение**, вы можете настроить тип события **Произошла проблема безопасности**. Такие события могут произойти, например, когда свободное место на диске точки распространения меньше 2 ГБ (для установки приложений и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошла проблема безопасности**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаруживает проблему безопасности, вы можете управлять этой проблемой безопасности с помощью параметров управляемого устройства.

Параметры приложения

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

Если флажок установлен, клиентские устройства получают обновления только через агенты обновлений, а не напрямую с серверов обновлений.

Если флажок снят, клиентские устройства могут получать обновления из разных источников: напрямую с серверов обновлений, от главного Сервера администрирования, из локальной или сетевой папки.

По умолчанию флажок снят.

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Приложение может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для Windows). Передаваемая информация отображается в интерфейсе приложения безопасности.

  Агент администрирования передает следующую информацию:

  - время доставки политики на управляемое устройство;
  - имя активной политики и политики для автономных пользователей в момент доставки политики на управляемое устройство;
  - имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
  - список активных профилей политики.

    Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

  Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

  По умолчанию параметр выключен.

- **Использовать пароль деинсталляции**

  Если флажок установлен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

  По умолчанию флажок снят.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения. Параметры раздела Хранилища доступны только для устройств под управлением Windows:

- **Информация об установленных приложениях**

  Если флажок установлен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

  По умолчанию флажок установлен.

- **Включить информацию о патчах**

  Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

  По умолчанию параметр включен. Доступен только для Windows.

- **Информация об обновлениях Центра обновления Windows**

  Если флажок установлен, на Сервер администрирования отправляется информация об обновлениях Microsoft Windows, которые необходимо установить на клиентских устройствах.

  По умолчанию флажок установлен.

- **Информация об уязвимостях в приложениях и соответствующих обновлениях**

  Если флажок установлен, на Сервер администрирования отправляется информация об уязвимостях программного обеспечения, обнаруженных на клиентских устройствах.

  По умолчанию флажок установлен.

- **Информация о реестре оборудования**

  Если флажок установлен, на Сервер администрирования отправляется информация об оборудовании, обнаруженном в результате опроса сети.

  По умолчанию флажок установлен.

Обновления и уязвимости в приложениях

В разделе Обновления и уязвимости в приложениях вы можете включить проверку исполняемых файлов на наличие уязвимостей:

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

Если флажок установлен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

По умолчанию флажок установлен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления приложения требуется перезагрузка операционной системы управляемого устройства. Параметры раздела **Управление перезагрузкой** доступны только для устройств под управлением Windows:

- **Не перезагружать операционную систему**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **При необходимости перезагрузить операционную систему автоматически**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос периодически через (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагружать через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- Принудительно закрывать приложения в заблокированных сеансах

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

Управление патчами и обновлениями

В разделе Управление патчами и обновлениями можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

- Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"

  Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Автоматическая установка патчей со статусом *Не определено* доступна для версий Open Single Management Platform Service Pack 2 и выше.

  Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того как администратор изменит их статус на *Одобрен*.

  По умолчанию флажок установлен.

- Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)

Если флажок установлен, включена офлайн-модель получения обновлений. В этом случае, когда Сервер администрирования получает обновления, он оповещает Агенты администрирования о том, какие обновления потребуются для приложений на клиентских устройствах. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загружает все обновления, обновления становятся доступными для приложений на клиентском устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования при этом может отсутствовать, но оно и не требуется для обновления.

Если флажок снят, офлайн-модель получения обновлений выключена. Обновления распределяются по расписанию задачи обновления.

По умолчанию флажок установлен.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключиться к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:
  - **Период синхронизации (мин)**

    Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (периодический сигнал) равным 15 минут на 10 000 управляемых устройств.

    Если установлен период синхронизации меньше 15 минут, то синхронизация выполняется каждые 15 минут. Если период синхронизации установлен на 15 минут или более, синхронизация выполняется с указанным периодом.

  - **Сжимать сетевой трафик**

Если флажок установлен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

По умолчанию флажок установлен.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если флажок установлен, UDP-порт, необходимый для работы Агента администрирования, будет добавлен в список исключений сетевого экрана Microsoft Windows.

  По умолчанию флажок установлен.

- **Использовать SSL-соединение**

  Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

  По умолчанию флажок установлен.

- **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**

  Если флажок установлен, то используется шлюз соединений агента обновлений, параметры которого заданы в свойствах группы администрирования.

  По умолчанию флажок установлен.

- **Использовать UDP-порт**

  Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер **UDP-порта**. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию используется порт 15000.

  Используется десятичная форма записи.

  Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный межсетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

- **Использовать точку распространения для принудительного подключения к Серверу администрирования**

Выберите этот параметр, если вы выбрали параметр **Использовать эту точку распространения в качестве push-сервера** в окне параметров точки распространения. Иначе точка распространения не будет выполнять роль push-сервера.

В подразделе **Профили соединений** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows:

- **Параметры сетевого местоположения**

  Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

  В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

  - подключении клиентского устройства к другой локальной сети;
  - отключении устройства от локальной сети организации;
  - изменении адреса шлюза соединения или изменении адреса DNS-сервера.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если флажок установлен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если флажок снят, приложения будут использовать активные политики.

  По умолчанию флажок снят.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  Этот вариант выбран по умолчанию.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **IP-диапазоны**

  Если флажок установлен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если флажок снят, Сервер администрирования не выполняет опрос IP-диапазонов.

  Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

  По умолчанию флажок снят.

- **Zeroconf**

  Если этот параметр включен, точка распространения автоматически опрашивает сеть с устройствами IPv6, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае включенный опрос IP-диапазонов игнорируется, так как точка распространения опрашивает всю сеть.

  Чтобы можно было начать использовать Zeroconf, должны быть выполнены следующие условия:

  - Точка распространения должна работать под управлением Linux.
  - Вам нужно установить утилиту avahi-browse на точку распространения.

  Если этот параметр отключен, точка распространения не опрашивает сети с устройствами IPv6.

  По умолчанию параметр выключен.

- **Контроллеры доменов**

  Если этот параметр включен, точка распространения автоматически выполняет опрос контроллеров домена в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

  Если параметр выключен, точка распространения не выполняет опрос контроллеров домена.

  Периодичность опроса контроллеров домена для версий Агента администрирования ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

  По умолчанию параметр выключен.

Параметры сети для точек распространения

В разделе **Параметры сети для точек распространения** вы можете указать параметры доступа к интернету:

- **Использовать прокси-сервер**
- **Адрес**
- **Номер порта**
- **Не использовать прокси-сервер для локальных адресов**

Если флажок установлен, то при подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

По умолчанию флажок снят.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

Прокси-сервер KSN (точки распространения)

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки Kaspersky Security Network (KSN) запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

  Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **TCP-порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

  Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер **UDP-порта**. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Через HTTPS-порт**

  Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию параметр выключен. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

Обновления (точки распространения)

В разделе **Обновления (точки распространения)** вы можете включить функцию загрузки файлов различий, так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского".

Управление учетными записями (только для Linux)

Раздел **Управление учетными записями (только для Linux)** состоит из трех подразделов:

- **Управление пользовательскими сертификатами**
- **Добавление или изменение групп локальных администраторов**
- **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений**

В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

- **Установить корневые сертификаты**

  Если этот параметр включен, сертификаты, добавленные в таблицу, будут установлены на указанных устройствах.

  Если этот параметр выключен, сертификаты не будут установлены на указанные устройства.

  По умолчанию параметр выключен.

- **Добавить**

Нажав на эту кнопку открывается окно, в котором можно добавить сертификат.

Размер сертификата должен быть меньше 10 МБ.

Kaspersky Security Center поддерживает сертификаты с расширениями CER, CRT, CERT, PEM и KEY.

В подразделе **Добавление или изменение групп локальных администраторов** вы можете управлять группами локальных администраторов. Эти группы используются, например, при отзыве прав локального администратора. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

- **Добавить**

  Нажмите на эту кнопку, чтобы добавить локальную группу администраторов.

- **Изменить**

  Нажмите на эту кнопку, чтобы изменить локальную группу администраторов.

  Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

- **Удаление**

  Нажмите на эту кнопку, чтобы удалить выбранную группу локальных администраторов из таблицы.

  Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

В подразделе **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений** вы можете настроить управление файлом sudoers. Привилегированные группы и пользователи устройства определяются файлом sudoers на устройстве. Файл sudoers находится в папке `/etc/sudoers`. Вы можете загрузить референсный файл sudoers, чтобы защитить файл sudoers от изменений. Это предотвратит нежелательные изменения файла sudoers.

Недопустимый референсный файл sudoers может привести к неисправности устройства пользователя.

- **Контролировать файл sudoers**

  Если этот параметр включен, файл sudoers будет заменен текущим референсным файлом sudoers.

  Если этот параметр выключен, файл sudoers остается без изменений.

  По умолчанию параметр выключен.

- **Референсный файл sudoers**

  В этом поле отображается имя загруженного референсного файла sudoers.

- **Загрузить**

  Нажмите на эту кнопку, чтобы загрузить референсный файл sudoers.

- **Текущий референсный файл sudoers**

  Нажмите на эту кнопку, чтобы просмотреть текущий файл sudoers.

История ревизий

На вкладке **История ревизий** вы можете:

- Просмотреть и сохранить историю изменений политики.
- Откатить к ревизии политики.
- Добавить и изменить описание ревизии политики.

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, Linux и macOS.

Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами	✓	✓	✓
Установка приложений с помощью сторонних средств удаленной установки приложений	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Установка Агента администрирования в тихом режиме	✓	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную	✓	✓	✓
Автоматическая установка обновлений и патчей для компонентов Open Single Management Platform	✓	✓	–
Автоматическое распространение ключа	✓	✓	✓

Принудительная синхронизация	✓	✓	✓
Точка распространения			
Использование точки распространения	✓	✓	✓
Автоматическое назначение точек распространения	✓	✓ Без использования Network Location Awareness (NLA).	✓ Без использования Network Location Awareness (NLA).
Офлайн-модель получения обновлений	✓	✓	✓
Опрос сети	✓ • Опрос IP-диапазонов • Опрос контроллеров домена (Microsoft Active Directory)	✓ • Опрос IP-диапазонов • Опрос Zeroconf • Опрос контроллеров домена (Microsoft Active Directory, Samba 4 Active Directory)	—
Запуск службы прокси-сервер KSN на стороне точки распространения	✓	✓	—
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓	✓	— Если устройства с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows.
Принудительная установка приложений	✓	С ограничением: нельзя выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.	С ограничением: нельзя выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Использовать в качестве push-сервера	✓	✓	—
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства	✓	✓	✓
Настройка обновлений операционной системы в политике Агента администрирования	✓	—	—
Просмотр информации об уязвимостях в приложениях	✓	—	—
Поиск уязвимостей в приложениях	✓	—	—
Обновления программного обеспечения	✓	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			
Установка Агента администрирования на виртуальные машины	✓	✓	✓

Оптимизация параметров для VDI	✓	✓	✓
Поддержка динамических виртуальных машин	✓	✓	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—	—
Мониторинг состояния антивирусной защиты	✓	✓	✓
Управление перезагрузкой устройств	✓	—	—
Поддержка отката файловой системы	✓	✓	✓
Использование Агента администрирования в качестве шлюза соединений	✓	✓	✓
Менеджер соединений	✓	✓	✓
Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению)	✓	—	✓
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk	✓	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	—	✓ С помощью системы Virtual Network Computing (VNC).
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓	✓

Сравнение параметров Агента администрирования по операционным системам

В таблице ниже показано, какие параметры Агента администрирования доступны в зависимости от операционной системы управляемого устройства, на котором установлен Агент администрирования.

Параметры Агента администрирования: сравнение по операционным системам

Раздел Параметры	Windows	Linux	macOS
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓ Доступны следующие параметры: • **Распространять файлы только через точки распространения** • **Максимальный размер очереди событий (МБ)** • **Приложение может получать расширенные данные политики на устройстве**	✓

Хранилища	✓	✓ Доступны следующие параметры: • **Информация об установленных приложениях** • **Информация о реестре оборудования**	✓ Параметр **Информация о реестре оборудования** доступен.
Подключения → Сеть	✓	✓ Кроме параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.	✓
Подключения → Профили соединений	✓	—	✓
Подключения → Расписание соединений	✓	✓	✓
Опрос сети точками распространения	✓ Доступны следующие параметры: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры доменов**	✓ Доступны следующие параметры: • **Zeroconf** • **IP-диапазоны** • **Контроллеры доменов**	—
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	✓	—
Обновления (точки распространения)	✓	✓	—
История ревизий	✓	✓	✓

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security. Вы можете выполнить настройку в окне свойств политики. При изменении параметра, нажмите на значок замка справа от соответствующей группы параметров, чтобы применить указанные значения к рабочей станции.

Настройка Kaspersky Security Network

Kaspersky Security Network (KSN) – инфраструктура облачных служб, обладающая информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network позволяет Kaspersky Endpoint Security для Windows быстрее реагировать на различные виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Подробнее о Kaspersky Security Network см. документацию Kaspersky Endpoint Security для Windows.

Чтобы задать рекомендуемые параметры KSN:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В окне свойств политики перейдите в раздел **Параметры приложения** → **Продвинутая защита** → **Kaspersky Security Network**.
4. Убедитесь, что параметр **Использовать прокси-сервер KSN** включен. Использование этого параметра поможет перераспределить и оптимизировать трафик сети.

   Если вы используете Managed Detection and Response, необходимо включить параметр **Прокси-сервер KSN** для точки распространения и расширенный режим KSN.
5. Если служба прокси-сервера KSN недоступна, можно включить использование серверов KSN. Серверы KSN могут располагаться как на стороне "Лаборатории Касперского" (при использовании KPSN), так и у третьих сторон (при использовании KPSN).
6. Нажмите на кнопку **OK**.

Рекомендованные параметры KSN настроены.

Проверка списка сетей, которые защищает сетевой экран

Убедитесь, что сетевой экран Kaspersky Endpoint Security для Windows защищает все ваши сети. По умолчанию сетевой экран защищает сети со следующими типами подключения:

- **Общедоступная сеть**. Приложения безопасности, сетевые экраны или фильтры не защищают устройства в такой сети.
- **Локальная сеть**. Доступ к файлам и принтерам ограничен для устройств в этой сети.
- **Доверенная сеть**. Устройства в такой сети защищены от атак и несанкционированного доступа к файлам и данным.

Если вы настроили пользовательскую сеть, убедитесь, что сетевой экран защищает ее. Для этого проверьте список сетей в свойствах политики Kaspersky Endpoint Security для Windows. В списке могут отображаться не все сети.

Подробнее о сетевом экране см. документацию Kaspersky Endpoint Security для Windows.

Чтобы проверить список сетей:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры приложения** → **Базовая защита** → **Сетевой экран**.
4. В блоке **Доступные сети** перейдите по ссылке **Параметры сети**.

Отобразится окно **Сетевые подключения**. В этом окне отобразится список сетей.

5. Если в списке отсутствует сеть, добавьте ее.

Выключение проверки сетевых устройств

Проверка сетевых дисков приложением Kaspersky Endpoint Security для Windows, может оказывать на них значительную нагрузку. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

Вы можете выключить проверку сетевых дисков в свойствах политики Kaspersky Endpoint Security для Windows. Описание этих параметров политики приведено в документации Kaspersky Endpoint приведено в документации Kaspersky Endpoint Security для Windows.

Чтобы выключить проверку сетевых дисков:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры приложения** → **Базовая защита** → **Защита от файловых угроз**.
4. В блоке **Область защиты**, выключите параметр **Все сетевые диски**.
5. Нажмите на кнопку **ОК**.

Проверка сетевых дисков выключена.

Исключение сведений о программном обеспечении из памяти Сервера администрирования

Рекомендуется, настроить Сервер администрирования так, чтобы он не сохранял информацию о модулях приложений, запущенных на сетевых устройствах. В результате память Сервера администрирования не переполняется.

Вы можете выключить сохранение этой информации в свойствах политики Kaspersky Endpoint Security для Windows.

Чтобы выключить сохранение информации об установленных модулях приложений:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите **Параметры приложения** → **Общие параметры** → **Отчеты и хранилища**.

4. В блоке **Информировать Сервер администрирования**, снимите флажок **О запускаемых приложениях**, если он установлен в политике верхнего уровня.

   Когда этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Open Single Management Platform (десятки гигабайтов).

Информация об установленных модулях приложений больше не сохраняется в базе данных Сервера администрирования.

Настройка доступа к интерфейсу Kaspersky Endpoint Security для Windows на рабочих станциях

Если защитой от угроз в сети организации требуется управлять централизованно через Open Single Management Platform, укажите параметры интерфейса в свойствах политики Kaspersky Endpoint Security для Windows, как описано ниже. В результате вы предотвратите несанкционированный доступ к Kaspersky Endpoint Security для Windows на рабочих станциях и изменение параметров Kaspersky Endpoint Security для Windows.

Описание этих параметров политики приведено в документации Kaspersky Endpoint приведено в документации Kaspersky Endpoint Security для Windows.

Чтобы задать рекомендуемые параметры интерфейса:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры приложения** → **Общие параметры** → **Интерфейс**.
4. В блоке **Взаимодействие с пользователем** выберите параметр **Без интерфейса**. Отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях будет выключено, и их пользователи не могут изменять параметры Kaspersky Endpoint Security для Windows.
5. В блоке **Включить защиту паролем** включите переключатель. Это снижает риск несанкционированного или непреднамеренного изменения параметров Kaspersky Endpoint Security для Windows на рабочих станциях.

Рекомендуемые параметры интерфейса Kaspersky Endpoint Security для Windows заданы.

Сохранение важных событий политики в базе данных Сервера администрирования

Чтобы избежать переполнения базы данных Сервера администрирования, рекомендуется сохранять в базе данных только важные события.

Чтобы настроить регистрацию важных событий в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.

3. В окне свойств политики выберите вкладку **Настройка событий**.

4. В разделе **Критическое** нажмите на кнопку **Добавить событие** и установите флажок только рядом со следующим событием:

   - *Нарушено Лицензионное соглашение.*
   - *Автозапуск приложения выключен.*
   - *Ошибка активации.*
   - *Обнаружена активная угроза. Требуется запуск процедуры лечения.*
   - *Лечение невозможно.*
   - *Обнаружена ранее открытая опасная ссылка.*
   - *Процесс прерван.*
   - *Сетевая активность запрещена.*
   - *Обнаружена сетевая атака.*
   - *Запуск приложения запрещен.*
   - *Доступ запрещен (на основе локальных параметров).*
   - *Доступ запрещен (KSN).*
   - *Локальная ошибка обновления.*
   - *Невозможен запуск двух задач одновременно.*
   - *Ошибка взаимодействия с Kaspersky Security Center.*
   - *Обновлены не все компоненты.*
   - *Ошибка применения правил шифрования/расшифровки файлов.*
   - *Ошибка активации портативного режима.*
   - *Ошибка деактивации портативного режима.*
   - *Не удалось загрузить модуль шифрования.*
   - *Политика не может быть применена.*
   - *Ошибка при изменении компонентов приложения.*

5. Нажмите на кнопку **OK**.

6. В разделе **Отказ функционирования** нажмите на кнопку **Добавить событие** и установите флажок только рядом с событием *Неверные параметры задачи. Параметры задачи не применены.*

7. Нажмите на кнопку **OK**.

8. В разделе **Предупреждение** нажмите на кнопку **Добавить событие** и установите флажки только рядом со следующими событиями:

   - *Самозащита приложения выключена.*
   - *Компоненты защиты выключены.*
   - *Недопустимый резервный ключ.*
   - *Обнаружено легальное ПО, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или персональным данным (на основе локальных параметров).*
   - *Обнаружено легальное ПО, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или персональным данным (KSN).*
   - *Объект удален.*
   - *Объект вылечен.*
   - *Пользователь отказался от политики шифрования.*
   - *Файл восстановлен администратором из карантина на сервере Kaspersky Anti Targeted Attack Platform.*
   - *Файл помещен администратором на карантин на сервере Kaspersky Anti Targeted Attack Platform.*
   - *Сообщение администратору о запрете запуска приложения.*
   - *Сообщение администратору о запрете доступа к устройству.*
   - *Сообщение администратору о запрете доступа к веб-странице.*

9. Нажмите на кнопку **OK**.

10. В разделе **Информационное сообщение** нажмите на кнопку **Добавить событие** и установите флажки только рядом со следующими событиями:

    - *Создана резервная копия объекта.*
    - *Запуск приложения запрещен в тестовом режиме.*

11. Нажмите на кнопку **OK**.

Регистрация важных событий в базе данных Сервера администрирования настроена.

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на управляемых устройствах.

Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Open Single Management Platform. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN.

Open Single Management Platform поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Open Single Management Platform. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN. Специалисты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Open Single Management Platform использует это решение по умолчанию.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое предоставляет пользователям устройств с установленными приложениями "Лаборатории Касперского" доступ к базам данных Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в KSN. KPSN предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

  - Устройства пользователей не подключены к интернету.

  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

  Вы можете настроить параметры доступа Kaspersky Private Security Network в разделе **Параметры прокси-сервера KSN** окна свойств Сервера администрирования.

Вы можете начать использование KSN или отказаться от использования KSN в любой момент.

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Open Single Management Platform проверяет доступность серверов KSN. Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы. Это необходимо, чтобы убедиться, что уровень безопасности поддерживается для управляемых устройств.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Параметры прокси-сервера KSN** окна свойств Сервера администрирования.

Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

Чтобы настроить доступ Сервера администрирования к KSN:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Open Single Management Platform не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Open Single Management Platform). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Open Single Management Platform) передают в KSN.

4. Переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

KPSN поддерживают следующие приложения "Лаборатории Касперского":

- Open Single Management Platform
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Windows

Если вы включите KPSN в Open Single Management Platform, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

Open Single Management Platform не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Параметры прокси-сервера KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

6. Под блоком **Параметры подключения** настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - TCP-порт 13111 используется для подключения к прокси-серверу KSN. Для корневого Сервера администрирования этот номер порта изменить невозможно.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт**. По умолчанию параметр выключен, используется порт TCP. Если этот параметр включен, по умолчанию используется UDP-порт 15111. Для корневого Сервера администрирования этот номер порта изменить невозможно.

7. Переведите переключатель в положение **Подключать подчиненные Серверы администрирования к KSN через главный Сервер Включено**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Параметры прокси-сервера KSN** также переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

8. Нажмите на кнопку **Сохранить**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):

1. Убедитесь, что точка распространения была назначена вручную.
2. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Общие** выберите раздел **Точки распространения**.
4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.
5. В окне свойств точки распространения в разделе **Прокси-сервер KSN**, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
6. Нажмите на кнопку **OK**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Обратите внимание, что точка распространения не поддерживает проверку подлинности управляемого устройства по протоколу NTLM.

Включение и выключение использования KSN

Чтобы включить использование KSN:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

Прокси-сервер KSN включен и отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и приложений "Лаборатории Касперского".

1. В зависимости от используемого решения инфраструктуры KSN, включите соответствующие переключатели.

   - Если вы используете Глобальный KSN, переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

     Теперь доступна отправка данных в KSN. При включении этого параметра, вам нужно прочитать и принять условия Положения о KSN.

- Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

  При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

2. Нажмите на кнопку **Сохранить**.

Чтобы выключить использование KSN:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Переключите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Выключено**, чтобы выключить службу прокси-сервера KSN.

4. Нажмите на кнопку **Сохранить**.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

Чтобы просмотреть принятое Положение о KSN:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования с предыдущей версии, обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. Нажмите на значок **Просмотреть уведомления о событиях** в правом верхнем углу главного окна приложения.

   Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

   Откроется окно **Обновление Положения о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

   - **Я принимаю условия обновленного Положения о KSN**
   - **Использовать KSN со старым Положением о KSN**

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN в свойствах Сервера администрирования.

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер Kaspersky Security Network (KSN). Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:

1. На устройстве точки распространения выполните команду `ps aux`, чтобы отобразить список запущенных процессов.

2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/klnagent64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/klnagent64/sbin/ksnproxy` запущен, Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все приложения** → **Администрирование** → **Службы**).

2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

Управление задачами

В этом разделе описаны задачи, которые используются в Open Single Management Platform.

О задачах

Open Single Management Platform управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения в Консоли OSMP, только если для этого приложения установлен плагин управления на Сервере Консоли OSMP.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования, включают:

- автоматическая рассылка отчетов;
- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором с помощью Консоли OSMP, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область задачи

Область задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал) или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

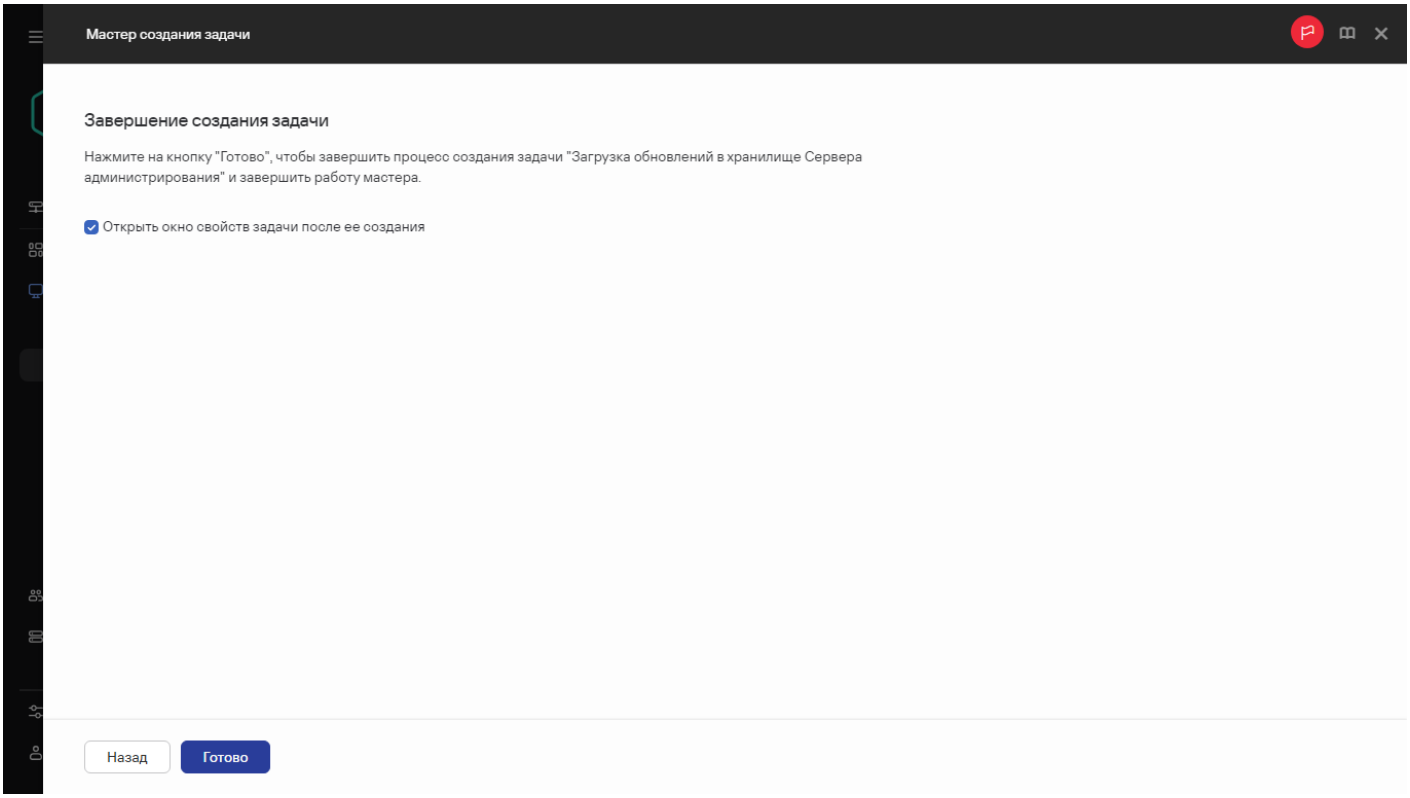
Создание задачи

Чтобы создать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.
3. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.



Завершение создания задачи

Чтобы создать задачу, назначенную выбранным устройствам:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.
2. В списке управляемых устройств установите флажки рядом с устройствами, для которых нужно запустить задачу. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.
3. Нажмите на кнопку **Запустить задачу** и выберите **Создание задачи**.

   Запустится мастер создания задачи.

На первом шаге мастера вы можете удалить устройства, выбранные для включения в область действия задачи. Следуйте инструкциям мастера.

4. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

Запуск задачи вручную

Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Управляемые устройства** и запустить для них существующую задачу.

Чтобы запустить задачу вручную:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в столбце **Статус** или нажав на кнопку **Результат выполнения**.

Запуск задачи для выбранных устройств.

Вы можете выбрать одно или несколько клиентских устройств в списке устройств, а затем запустить для них ранее созданную задачу. Это позволяет запускать задачи, созданные ранее для заданного набора устройств.

Это действие изменит в задаче список устройств, к которым применяется эта задача.

Чтобы запустить задачу для выбранных устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**. Отобразится список управляемых устройств.
2. В списке управляемых устройств используйте флажки, чтобы выбрать устройства, для которых будет выполняться задача. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.
3. Нажмите на кнопку **Запустить задачу** и выберите **Применить существующую задачу**.

   Отобразится список существующих задач.
4. Выбранные устройства отображаются над списком задач. При необходимости вы можете удалить устройство из этого списка. Вы можете удалить все устройства, кроме одного.
5. Выберите необходимую задачу в списке. Вы можете использовать поле поиска над списком для поиска задачи по ее названию. Можно выбрать только одну задачу.

6. Нажмите на кнопку **Сохранить и запустить задачу**.

Выбранная задача сразу запускается для выбранных устройств. Параметры запуска по расписанию в задаче не меняются.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Open Single Management Platform.

Чтобы просмотреть список задач,

в главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача *Удаленная установка приложения* относится к Серверу администрирования, а задача *Обновление* относится к Kaspersky Endpoint Security.

Чтобы просмотреть свойства задачи,

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными вкладками. Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **Расписание**.

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  - **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- Принудительно закрывать приложения в заблокированных сеансах

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Параметры расписания задачи:

  Типы расписаний могут изменяться в зависимости от задачи.

  - **Параметры Запуск задачи:**

    - Каждый N час

      Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

      Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

      По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

    - Каждые N дней

      Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

    - Каждые N минут

      Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

    - По дням недели

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- Ежемесячно

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

  Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

  По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- Вручную

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Open Single Management Platform при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- Ежемесячно, в указанные дни выбранных недель

  Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

  Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

  По умолчанию все флажки сняты.

- При загрузке обновлений в хранилище

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки обновлений в хранилище.

- По завершении другой задачи

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **После завершения другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

  - **Имя задачи**. В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
  - **Результат выполнения**. В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- Запускать пропущенные задачи

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

  Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию флажок установлен.

  Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

  По умолчанию флажок снят.

  Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

- Окно Выбор устройств, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи:

  - **Учетная запись по умолчанию.**

    Задача будет запускаться под той же учетной записью, под которой была установлена и запущена приложение, выполняющая эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль.**

    Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
  - **Распространить на подгруппы**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:

    - группу администрирования, которую вы выбрали при создании задачи;
    - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

    Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

    По умолчанию параметр включен.

  - **Распространить на подчиненные и виртуальные Серверы администрирования**

    При включении этого параметра задача, действующая на главном Сервере администрирования, применяется и на подчиненных Серверах администрирования (в том числе виртуальных). Если на подчиненном Сервере администрирования уже существует задача такого же типа, то на подчиненном Сервере администрирования применяются обе задачи — существующая и унаследованная от главного Сервера администрирования.

    Этот параметр доступен, только если параметр **Распространить на подгруппы** включен.

    По умолчанию параметр выключен.

- Дополнительные параметры расписания:
  - **Включать устройства перед запуском задачи функцией Wake-on-LAN за**

    Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

    Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

    Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

    По умолчанию параметр выключен.

  - **Выключать устройства после выполнения задачи**

    Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

    По умолчанию параметр выключен.

  - **Остановить, если задача выполняется дольше**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
  - Блок **Сохранять информацию о результатах**:
    - Хранить в базе данных Сервера администрирования в течение (сут)

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

      По умолчанию параметр включен.

    - Хранить в журнале событий ОС на устройстве

      События приложения, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

      По умолчанию параметр выключен.

    - Хранить в журнале событий ОС на Сервере администрирования

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

      По умолчанию параметр выключен.

    - Сохранять все события

      Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

    - Сохранять события, связанные с ходом выполнения задачи

      Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

    - Сохранять только результат выполнения задачи

      Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

  - Уведомлять администратора о результатах

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

  Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

  Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

  По умолчанию параметр включен.

- Параметры безопасности.
- Параметры области действия задачи.

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

    Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

    Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **выборкам устройств.**

    Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

    Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**.

Экспорт задачи

Open Single Management Platform позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Установите флажок рядом с задачей, которую вы хотите экспортировать.

   Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспортировать** будет неактивна. Задачи Сервера администрирования также недоступны для экспорта.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла задачи и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл задачи автоматически сохраняется в папку **Загрузки**.

Импорт задачи

Open Single Management Platform позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу и ее параметры.

Чтобы импортировать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл задачи, которую вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу KLT задачи и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл задачи.

   Начнется обработка задачи.
5. После того как задача будет успешно обработана, выберите устройства, которым вы хотите назначить задачу. Для этого выберите один из следующих параметров:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

6. Укажите область действия задачи.

7. Нажмите на кнопку **Завершить**, чтобы завершить задачу импорта.

Появится уведомление с результатами импорта. Если задача успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств задачи.

После успешного импорта задача отображается в списке задач. Параметры задачи и расписание также импортируются. Задача будет запущена в соответствии с расписанием.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Запуск мастера изменения паролей задач

Для не-локальной задачи можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете изменить пароль вручную в свойствах каждой задачи.

Чтобы запустить мастер изменения паролей задач

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

Следуйте далее указаниям мастера.

Шаг 1. Выбор учетных данных

Укажите новые учетные данные, которые в настоящее время действительны в вашей системе. При переходе на следующий шаг мастера, Open Single Management Platform проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

Чтобы указать новую учетную запись, выберите один из вариантов:

- **Использовать текущую учетную запись**

  Мастер использует имя учетной записи, под которой вы в настоящее время вошли в Консоль OSMP. Вручную укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

- **Указать другую учетную запись**

  Укажите имя учетной записи, под которой должны запускаться задачи. Укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

При заполнении поля **Предыдущий пароль (необязательно; если вы хотите заменить его на текущий)** Open Single Management Platform заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали предыдущий пароль или если указанный старый пароль не соответствует паролям, которые указаны в свойствах задач, необходимо выбрать действие, выполняемое с этими задачами.

Чтобы выбрать действие с задачей:

1. Установите флажок около задачи, с которой вы хотите выполнить действие.
2. Выполните одно из следующих действий:
   - Чтобы удалить пароль в свойствах задачи, нажмите **Удалить учетные данные**.

     Задача переключена на запуск под учетной записью по умолчанию.
   - Чтобы заменить пароль на новый, нажмите **Принудительно изменить пароль, даже если старый пароль неверен или не указан**.
   - Чтобы отменить изменение пароля, нажмите **Действие не выбрано**.

Выбранные действия применяются после перехода к следующему шагу мастера.

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Open Single Management Platform позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования.

Чтобы посмотреть результаты выполнения задачи, выполните следующие действия:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

Чтобы просмотреть результаты задачи для подчиненного Сервера администрирования:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.
3. Нажмите на **Статистика подчиненного Сервера**.
4. Выберите подчиненный Сервер, для которого вы хотите отобразить окно **Результаты выполнения задачи**.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства Если автоматически заданное расписание задачи групповой проверки не подходит для вашей организации, вам нужно вручную настроить наиболее удобное расписание для этой задачи на основе правил рабочего процесса, принятых в организации.

Например, для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**. Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. В этом случае вам необходимо настроить задачу групповой проверки вручную.

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Параметры расписания задачи:

  Типы расписаний могут изменяться в зависимости от задачи.

  - **Параметры Запуск задачи:**

    - **Каждый N час**

      Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

      Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

      По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

    - **Каждые N дней**

      Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

    - **Каждые N минут**

      Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

    - **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

  Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

  По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Open Single Management Platform при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

  Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

  Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

  По умолчанию все флажки сняты.

- **При загрузке обновлений в хранилище**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки обновлений в хранилище.

- **По завершении другой задачи**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **После завершения другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

  - **Имя задачи**. В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
  - **Результат выполнения**. В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

  Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию флажок установлен.

  Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

  По умолчанию флажок снят.

  Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

- Окно Выбор устройств, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи:

  - **Учетная запись по умолчанию.**

    Задача будет запускаться под той же учетной записью, под которой была установлена и запущена приложение, выполняющая эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль.**

    Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
  - **Распространить на подгруппы**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:

    - группу администрирования, которую вы выбрали при создании задачи;
    - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

    Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

    По умолчанию параметр включен.

  - **Распространить на подчиненные и виртуальные Серверы администрирования**

    При включении этого параметра задача, действующая на главном Сервере администрирования, применяется и на подчиненных Серверах администрирования (в том числе виртуальных). Если на подчиненном Сервере администрирования уже существует задача такого же типа, то на подчиненном Сервере администрирования применяются обе задачи — существующая и унаследованная от главного Сервера администрирования.

    Этот параметр доступен, только если параметр **Распространить на подгруппы** включен.

    По умолчанию параметр выключен.

- Дополнительные параметры расписания:
  - **Включать устройства перед запуском задачи функцией Wake-on-LAN за**

    Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

    Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

    Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

    По умолчанию параметр выключен.

  - **Выключать устройства после выполнения задачи**

    Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

    По умолчанию параметр выключен.

  - **Остановить, если задача выполняется дольше**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
  - Блок **Сохранять информацию о результатах**:
    - Хранить в базе данных Сервера администрирования в течение (сут)

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

      По умолчанию параметр включен.

    - Хранить в журнале событий ОС на устройстве

      События приложения, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

      По умолчанию параметр выключен.

    - Хранить в журнале событий ОС на Сервере администрирования

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

      По умолчанию параметр выключен.

    - Сохранять все события

      Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

    - Сохранять события, связанные с ходом выполнения задачи

      Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

    - Сохранять только результат выполнения задачи

      Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

  - Уведомлять администратора о результатах

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

  Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

  Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

  По умолчанию параметр включен.

- Параметры безопасности.
- Параметры области действия задачи.

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

    Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

    Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **выборкам устройств.**

    Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

    Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**.

Теги приложений

Open Single Management Platform позволяет назначать теги приложениям из реестра приложений. Тег представляет собой метку приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению тег можно использовать в условиях для выборок устройств.

Например, можно создать тег `[Браузеры]` и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Создание тегов приложений

Чтобы создать тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. Укажите тег.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов приложения.

Изменение тегов приложений

Чтобы переименовать тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените имя тега.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов приложений.

Назначение тегов приложениям

Чтобы назначить приложению теги:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Выберите приложение, для которого требуется назначить теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.
4. Установите флажки в столбце **Назначенный тег** для тегов, которые требуется назначить.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены приложению.

Снятие назначенных тегов с приложений

Чтобы снять теги с приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Выберите приложение, с которого требуется снять теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.
4. Снимите флажки в столбце **Назначенный тег** для тегов, которые требуется снять.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с приложения.

Снятые с приложений теги не удаляются. При необходимости их можно удалить вручную.

Удаление тегов приложений

Чтобы удалить тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. В списке выберите теги приложения, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств

В компоненте Контроль устройств политики Kaspersky Endpoint Security вы можете управлять доступом пользователей к внешним устройствам, которые установлены или подключены к клиентскому устройству (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

Если вам необходимо предоставить временный доступ к внешнему устройству, заблокированному компонентом Контроль устройств, но невозможно добавить устройство в список доверенных устройств, вы можете предоставить временный автономный доступ к внешнему устройству. Автономный доступ означает, что клиентское устройство не имеет доступа к сети.

Вы можете предоставить автономный доступ к внешнему устройству, заблокированному Контролем устройств, только если в параметрах политики Kaspersky Endpoint Security включен параметр **Разрешать запрашивать временный доступ** в разделе **Параметры приложения → Контроль безопасности → Контроль устройств**.

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств, включает в себя следующие этапы:

1. В диалоговом окне Kaspersky Endpoint Security пользователь устройства, который хочет получить доступ к заблокированному внешнему устройству, формирует файл запроса доступа и отправляет его администратору Open Single Management Platform.

2. Получив этот запрос, администратор Open Single Management Platform создает файл ключа доступа и отправляет его пользователю устройства.

3. В диалоговом окне Kaspersky Endpoint Security пользователь устройства активирует файл ключа доступа и получает временный доступ к внешнему устройству.

Чтобы предоставить временный доступ к внешнему устройству, заблокированному компонентом Контроль устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В этом списке выберите пользовательское устройство, которое запрашивает доступ к внешнему устройству, заблокированному компонентом Контроль устройств.

   Можно выбрать только одно устройство.

3. Над списком управляемых устройств нажмите на кнопку с многоточием (...) и нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

4. В открывшемся окне **Параметры приложения** в разделе **Контроль устройств** нажмите на кнопку **Обзор**.

5. Выберите файл запроса доступа, который вы получили от пользователя, а затем нажмите на кнопку **Открыть**. Файл должен иметь формат AKEY.

   Отображается информация о заблокированном устройстве, к которому пользователь запросил доступ.

6. Укажите значение параметра **Длительность доступа к устройству**.

   Этот параметр определяет продолжительность времени, в течение которого вы предоставляете пользователю доступ к заблокированному устройству. Значением по умолчанию является значение, указанное пользователем при создании файла запроса доступа.

7. Укажите значение параметра **Период активации**.

Этот параметр определяет период, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.

8. Нажмите на кнопку **Сохранить**.

9. Выберите папку назначения, в которой вы хотите сохранить файл, содержащий ключ доступа для заблокированного устройства.

10. Нажмите на кнопку **Сохранить**.

В результате, когда вы отправляете пользователю файл ключа доступа и он активирует его в диалоговом окне Kaspersky Endpoint Security, пользователь получает временный доступ к заблокированному устройству на определенный период.

Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Консоли OSMP

Чтобы начать работу с приложением Kaspersky Industrial CyberSecurity for Networks через консоль OSMP, необходимо предварительно зарегистрировать ее в Консоли OSMP.

Чтобы зарегистрировать приложение Kaspersky Industrial CyberSecurity for Networks:

1. Убедитесь, что сделано следующее:

   - Вы скачали и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks.

     Можно сделать это позже, ожидая синхронизацию Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования. После загрузки и установки плагина в главном меню Консоли OSMP отображается раздел **KICS for Networks**.

   - В веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks настраивается и включается взаимодействие с Open Single Management Platform. Подробную информацию см. в справке Kaspersky Industrial CyberSecurity for Networks.

2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:

   a. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Нераспределенные устройства**.

   b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.

   c. Нажмите на кнопку **Переместить в группу**.

   d. В иерархии групп администрирования установите флажок рядом с группой **Управляемые устройства**.

   e. Нажмите на кнопку **Переместить**.

3. Откройте окно свойств устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.

4. На странице свойств устройства в разделе **Общие**, выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.

5. В окне свойств устройства выберите раздел **Приложения**.

6. В разделе **Приложения** выберите Агент администрирования Kaspersky Security Center Network.

7. Если текущий статус приложения *Остановлено*, подождите, пока он не изменится на *Выполняется*.

   Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас.

8. Если вы хотите просматривать статистику работы Kaspersky Industrial CyberSecurity for Networks, вы можете добавить веб-виджеты на панель управления. Чтобы добавить веб-виджеты, выполните следующее:

   a. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

   b. В панели управления нажмите на кнопку **Добавить или восстановить веб-виджет**.

   c. В появившемся веб-виджете нажмите на кнопку **Другое**.

   d. Выберите веб-виджет, который вы хотите добавить.

      - Карта размещения KICS for Networks
      - Информация о Серверах KICS for Networks
      - Актуальные события KICS for Networks
      - Устройства, требующие внимания в KICS for Networks
      - Критические события KICS for Networks
      - Статусы KICS for Networks

9. Чтобы перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

   a. В главном окне приложения перейдите в раздел **KICS for Networks** → **Поиск**.

   b. Нажмите на кнопку **Найти события или устройства**.

   c. В открывшемся окне **Параметры запроса** нажмите на поле **Сервер**.

   d. В раскрывающемся списке серверов, интегрированных с Open Single Management Platform, выберите Сервер Kaspersky Industrial CyberSecurity for Networks и нажмите на кнопку **Найти**.

   e. Перейдите по ссылке **Перейти на Сервер** рядом с названием Сервера Kaspersky Industrial CyberSecurity for Networks.

      Откроется страница входа в Kaspersky Industrial CyberSecurity for Networks.

      Для входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks вам необходимо ввести учетные данные пользователя приложения.

Управление пользователями и ролями пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

Об учетных записях пользователей

Open Single Management Platform позволяет управлять учетными записями пользователей и группами безопасности. Приложение поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих локальных пользователей при опросе сети организации.
- Учетные записи внутренних пользователей Open Single Management Platform. Вы можете создавать учетные записи внутренних пользователей на портале. Эти учетные записи используются только в Open Single Management Platform.

Группа kladmins не может быть использована для доступа к Консоли OSMP в Open Single Management Platform. Группа kladmins может содержать только учетные записи, которые используются для запуска служб Open Single Management Platform.

Чтобы просмотреть таблицы учетных записей пользователей и групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. Выберите вкладку **Пользователи** или **Группы**.

Откроется таблица пользователей или групп безопасности. Если вы хотите просмотреть таблицу только с учетными записями внутренних пользователей или групп, установите в фильтре **Подтип** критерий **Внутренний** или **Локальный**.

О ролях пользователей

Роль пользователя (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами приложениями "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп безопасности на любом уровне иерархии групп администрирования, Серверов администрирования либо на уровне конкретных объектов.

Если вы управляете устройствами с помощью иерархии Серверов администрирования, в которую входят виртуальные Серверы администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только на физическом Сервере администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы.

Вы можете связывать роли с профилями политик. Если пользователю назначена роль, этот пользователь получает параметры безопасности, требуемые для выполнения служебных обязанностей.

Роль пользователя может быть связана с устройствами пользователей заданной группы администрирования

Область роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Преимущество использования ролей

Преимущество использования ролей заключается в том, что вам не нужно указывать параметры безопасности для каждого управляемого устройства или для каждого из пользователей отдельно. Количество пользователей и устройств в компании может быть большим, но количество различных функций работы, требующих разных настроек безопасности, значительно меньше.

Отличия от использования профилей политики

Профили политики – это свойства политики, созданной для каждого приложения "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных приложений. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

Настройка прав доступа к функциям приложения Управление доступом на основе ролей

Open Single Management Platform предоставляет доступ на основе ролей к функциям Open Single Management Platform и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения для пользователей Open Single Management Platform одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложение можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права.

Права доступа к функциям приложения

В таблице ниже приведены функции Open Single Management Platform с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Функциональная область **Общие функции**: **Доступ к объектам независимо от их списков ACL** предназначена для аудита. Когда пользователям предоставляется право **Чтение** в этой функциональной области, они получают полный доступ на **Чтение** ко всем объектам и могут выполнять любые созданные задачи на выбранных устройствах, подключенных к Серверу администрирования через Агент администрирования с правами локального администратора (root для Linux). Рекомендуется предоставлять эти права ограниченному кругу пользователей, которым они нужны для выполнения своих служебных обязанностей.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общие функции: Базовая функциональность**.

Права доступа к функциям приложения

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Управление группами администрирования**	**Запись.**	• Добавление устройства в группу администрирования: **Запись**. • Удаление устройства из состава группы администрирования: **Запись**. • Добавление группы администрирования в другую группу администрирования: **Запись**. • Удаление группы администрирования из другой группы администрирования: **Запись**.	Отсутствует.	Отсутствует.	От
Общие функции: **Доступ к объектам независимо от их списков ACL**	**Чтение.**	Получение доступа на чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.	До пр не др ес за на оп об
Общие функции: **Базовая функциональность**.	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее заражаемых устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках.	От

		• Получение мобильного протокола пользовательского сертификата (LWNGT): **Чтение**. • Установка мобильного протокола пользовательского сертификата (LWNGT): **Запись**. • Получить список сетей, определенных NLA: **Чтение**. • Добавить, изменить или удалить список сетей, определенных NLA: **Запись**. • Просмотр списка контроля доступа групп: **Чтение**. • Просмотр журнала операционной системы: **Чтение**.	Серверы администрирования.	• Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет об инцидентах. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет о запрещенных приложениях. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет о правах доступа к зашифрованным дискам. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа к зашифрованным файлам. • Отчет об эффективных правах пользователя. • Отчет о правах.	
Общие функции: **Удаленные объекты**	• **Чтение.**	• Просмотр удаленных объектов в корзине:	Отсутствует.	Отсутствует.	От

	• **Запись.**	**Чтение**. • Удаление объектов из корзины: **Запись**.			
Общие функции: **Обработка событий**	• **Удаление событий.** • **Изменение параметров уведомления о событиях.** • **Изменение параметров записи событий в журнал событий.** • **Запись.**	• Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий**. • Изменение параметров уведомления о событиях: **Изменение параметров уведомления о событиях**. • Удаление событий: **Удаление событий**.	Отсутствует.	Отсутствует.	Па • •
Общие функции: **Операции с Сервером администрирования**	• **Чтение.** • **Запись.** • **Выполнение.** • **Изменение списков ACL объекта.** • **Выполнение действий над выборками устройств.**	• Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись**. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись**. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись**. • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись**. • Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись**. • Изменение SSL-портов Сервера администрирования для подключения с помощью Консоли OSMP: **Запись**. • Изменение портов Сервера администрирования для подключения	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	От

		мобильных устройств: **Запись**. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Запись**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Запись**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись**.			
Общие функции: **Развертывание приложений "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях приложений "Лаборатории Касперского". • Отчет о несовместимых приложениях. • Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	Ин па "Ла Ка
Общие функции: **Управление лицензионными ключами**	• **Экспорт файл ключа.** • **Запись.**	• Экспорт файл ключа: **Экспорт файл ключа.** • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	От
Общие функции: **Управление отчетами**	• **Чтение.** • **Запись.**	• Создание отчетов для объектов независимо от их списков ACL: **Запись**. • Выполнять отчеты независимо от их	Отсутствует.	Отсутствует.	От

		списков ACLs: **Чтение**.			
Общие функции: **Иерархия Серверов администрирования**	**Настройка иерархии Серверов администрирования**	• Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования**.	Отсутствует.	Отсутствует.	От
Общие функции: **Права пользователя**	**Изменение списков ACL объекта.**	• Изменение свойств Безопасности любого объекта: **Изменение списков ACL объекта**. • Управление ролями пользователей: **Изменение списков ACL объекта**. • Управление внутренними пользователями: **Изменение списков ACL объекта**. • Управление группами безопасности: **Изменение списков ACL объекта**. • Управление псевдонимами: **Изменение списков ACL объекта**.	Отсутствует.	Отсутствует.	От
Общие функции: **Виртуальные Серверы администрирования**	• **Управление виртуальными Серверами администрирования.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение списка виртуальных Серверов администрирования: **Чтение**. • Получение информации о виртуальном Сервере администрирования: **Чтение**. • Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования**. • Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными**	Отсутствует.	Отсутствует.	От

		Серверами администрирования. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования**.			
Общие функции: **Управление ключами шифрования**	**Запись.**	Подтверждение запуска плейбука в обучающем режиме: **Запись**.	Отсутствует.	Отсутствует.	От

Предопределенные роли пользователей

Роли пользователей (далее также *роли*), назначенные пользователям Open Single Management Platform, предоставляют им набор прав доступа к функциям приложения.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных ролей, доступных в Open Single Management Platform, можно связать с определенными должностями, например **Аудитор**, **Специалист по безопасности**, **Контролер**. Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано, как роли могут быть связаны с определенными должностями.

Примеры ролей для определенных должностей

Роль	Описание
Аудитор	Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права **Чтение** и **Запись** для области **Удаленные объекты**). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Контролер	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за ИТ-безопасность в вашей организации.
Специалист по безопасности	Разрешены все операции просмотра, разрешено управление отчетами. Предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за ИТ-безопасность в вашей организации.

В таблице ниже приведены права для каждой предопределенной роли пользователя.

Возможности функциональной области **Управление мобильными устройствами**: **Общие** и **Управление системой** недоступны в Open Single Management Platform. Пользователь с ролями **Администратор Системного администрирования/Оператор** и **Администратор управления мобильными устройствами/Оператор** имеют права доступа только в функциональной области **Общие функции**: **Базовая функциональность**.

Права предопределенных ролей пользователей

Роль	Описание
Основные роли	
Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях: • **Общие функции**: • **Базовая функциональность**.

	• **Обработка событий**. • **Иерархия Серверов администрирования**. • **Виртуальные Серверы администрирования**. Предоставляет права на **Чтение** и **Запись** в области **Общие функции**: **Управление ключами шифрования**.
Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** в следующих функциональных областях: • **Общие функции**: • **Базовая функциональность**. • **Виртуальные Серверы администрирования**.
Аудитор	Разрешает все операции в следующих функциональных областях: • **Общие функции**: • **Доступ к объектам независимо от их списков ACL**. • **Удаленные объекты**. • **Управление отчетами**. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Администратор установки приложений	Разрешает все операции в следующих функциональных областях: • **Общие функции**: • **Базовая функциональность**. • **Развертывание приложений "Лаборатории Касперского"**. • **Управление лицензионными ключами**. Предоставляет права на **Чтение** и **Выполнение** в области **Общие функции**: **Виртуальные Серверы администрирования**.
Оператор установки приложений	Предоставляет права на **Чтение** и **Выполнение** в следующих функциональных областях: • **Общие функции**: • **Базовая функциональность**. • **Развертывание приложений "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области). • **Виртуальные Серверы администрирования**.
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общие функции**: **Базовая функциональность**. • Область Kaspersky Endpoint Security, включая все функции. Предоставляет права на **Чтение** и **Запись** в области **Общие функции**: **Управление ключами шифрования**.
Оператор Kaspersky Endpoint Security	Предоставляет права на **Чтение** и **Выполнение** в следующих функциональных областях: • **Общие функции**: **Базовая функциональность**. • Область Kaspersky Endpoint Security, включая все функции.
Главный администратор	Разрешает все операции во всех функциональных областях, кроме следующих областей: • **Общие функции:** • **Доступ к объектам независимо от их списков ACL**. • **Управление отчетами**. Предоставляет права на **Чтение** и **Запись** в области **Общие функции**: **Управление ключами шифрования**.
Главный оператор	Предоставляет права на **Чтение** и **Выполнение** (если применимо) в следующих функциональных областях: • **Общие функции**: • **Базовая функциональность**.

	• **Удаленные объекты**. • **Операции с Сервером администрирования**. • **Развертывание приложений "Лаборатории Касперского"**. • **Виртуальные Серверы администрирования**. • Область Kaspersky Endpoint Security, включая все функции.
Администратор управления мобильными устройствами	Разрешает все операции в области **Общие функции**: **Базовая функциональность**.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: • **Общие функции**: • **Доступ к объектам независимо от их списков ACL**. • **Управление отчетами**. Предоставляет права на **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств** в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за ИТ-безопасность в вашей организации.
Пользователь Self Service Portal	Разрешает все операции в области **Управление мобильными устройствами**: **Self Service Portal**. Эта функция не поддерживается в версиях приложения Kaspersky Security Center 11 и выше.
Контролер	Предоставляет права на **Чтение** в областях **Общие функции**: **Доступ к объектам независимо от их списков ACL** и **Общие функции**: **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за ИТ-безопасность в вашей организации.
XDR-роли	
Главный администратор	Разрешает все операции в функциональных областях XDR: • **Алерты и инциденты**. • **НКЦКИ-инциденты**. • **Плейбуки и действия по реагированию**. • **Управление активами**. • **IAM**. • **Тенанты**. • **Интеграции**. • **Лицензии**.
Администратор тенанта	Разрешает все операции в функциональных областях XDR: • **Алерты и инциденты**. • **НКЦКИ-инциденты**. • **Плейбуки и действия по реагированию**. • **Управление активами**. • **IAM**. • **Тенанты**. • **Интеграции**. • **Лицензии**. Эта роль соответствует роли Главного администратора, но имеет ограничение. В KUMA администратор тенанта имеет ограниченный доступ к предустановленным объектам.

Администратор SOC	Предоставляет следующие права в функциональных областях XDR: • **Плейбуки и действия по реагированию**: **Чтение**, **Запись** и **Удаление**. • **IAM**: **Чтение пользователей и ролей**, **Назначение ролей** и **Списки пользователей**. • **Тенанты**: **Чтение** и **Запись**. • **Интеграции**: **Чтение**, **Запись** и **Удаление**. • **Лицензии**: **Чтение**.
Младший аналитик	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Плейбуки и действия по реагированию**: **Чтение** и **Выполнение**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**.
Аналитик 2-го уровня	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Плейбуки и действия по реагированию**: **Чтение**, **Запись**, **Удаление** и **Выполнение**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**.
Аналитик 1-го уровня	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Плейбуки и действия по реагированию**: **Чтение**, **Запись**, **Удаление** и **Выполнение**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**. Эта роль соответствует роли Аналитик 2-го уровня, но она имеет ограничение. В KUMA аналитик 1-го уровня может изменять только свои объекты.
Менеджер SOC	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**.

	• **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**.
Подтверждающий	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение**, **Запись**, **Закрытие**. • **Плейбуки и действия по реагированию**: **Чтение** и **Подтверждение действий по реагированию**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**.
Наблюдатель	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**.
Работа с НКЦКИ	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **НКЦКИ-инциденты**: **Чтение** и **Запись**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**. Вы можете работать с XDR-инцидентами, создавать НКЦКИ-инциденты на их основе и экспортировать НКЦКИ-инциденты (без доступа к критически важной информационной инфраструктуре).
Доступ к объектам КИИ	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение**, **Запись**, просмотр наличия затронутых объектов КИИ. • **Управление активами**: **Чтение**. • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграции**: **Чтение**. • **Лицензии**: **Чтение**. Вы можете посмотреть список алертов и инцидентов, которые включают хотя бы один актив, являющийся объектом критической информационной инфраструктуры (КИИ).

Автоматическое реагирование на угрозы	Предоставляет учетным записям служб право реагировать на угрозы. Права доступа настраиваются автоматически в соответствии с правами доступа на основе ролей политик Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского". Вы можете назначать эту роль только учетным записям служб. Эту роль невозможно изменить.

Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера, вы можете настроить доступ к конкретным объектам, например, к требуемой задаче. Приложение позволяет указать права доступа к следующим типам объектов:

- Группы администрирования
- Задачи
- Отчеты
- Выборки устройств
- Выборки событий

Чтобы назначить права доступа к конкретному объекту:

1. В зависимости от типа объекта в главном меню перейдите в соответствующий раздел:
   - **Активы (Устройства) → Иерархия групп**.
   - **Активы (Устройства) → Задачи**.
   - **Мониторинг и отчеты → Отчеты**.
   - **Активы (Устройства) → Выборки устройств**.
   - **Мониторинг и отчеты → Выборки событий**.
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.

   Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.
3. В окне свойств откройте раздел **Права доступа**.

   Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.
4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.
5. Настройте права доступа:
   - Используйте кнопки **Добавить** и **Удалить** для изменения списка.

- Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:

  - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.

  - Если вы хотите назначить пользовательскую роль пользователю или группе безопасности, выберите пользователя или группу безопасности, нажмите на кнопку **Роли** и выберите роль для назначения.

6. Нажмите на кнопку **Сохранить**.

Права доступа к объекту настроены.

Назначение прав пользователям или группам пользователей

Вы можете назначить права пользователям или группам безопасности, чтобы использовать различные возможности Сервера администрирования и приложений "Лаборатории Касперского", для которых у вас есть плагины управления, например Kaspersky Endpoint Security для Windows.

Чтобы назначить права пользователю или группе безопасности:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

   a. Разверните узел с функциями Сервера администрирования или другого приложения "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**Чтение**, **Запись** и **Выполнение**).

      Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **OK**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:

    - Управление группами администрирования.
    - Доступ к объектам независимо от их списков ACL.
    - Базовая функциональность.
    - Удаленные объекты.
    - Управление ключами шифрования
    - Обработка событий.
    - Операции с Сервером администрирования.
    - Теги устройств.
    - Развертывание приложений "Лаборатории Касперского"
    - Управление лицензионными ключами.
    - Управление отчетами.
    - Иерархия Серверов.
    - Права пользователей.
    - Виртуальные Серверы администрирования.
- Управление мобильными устройствами:
    - Общие.
- Управление системой:
    - Подключения.
    - Инвентаризация оборудования.
    - Управление доступом в сеть.
    - Развертывание операционной системы.
    - Управление уязвимостями и патчами.
    - Удаленная установка.
    - Инвентаризация приложений

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;

- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Также вы можете добавить пользователей и группы безопасности в область пользовательской роли, чтобы использовать различные возможности Сервера администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Добавление учетной записи внутреннего пользователя

Чтобы добавить учетную запись пользователя Open Single Management Platform:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Добавить пользователя** укажите параметры нового пользователя:
   - **Имя**.
   - **Пароль** для подключения пользователя к Open Single Management Platform.

     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 256 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A-Z);
       - нижний регистр (a-z);
       - числа (0-9);
       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

     Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

     Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля".

Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Учетная запись пользователей добавлена в список пользователей.

Создание группы безопасности

Чтобы создать группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Создать группу безопасности** укажите следующие параметры новой группы безопасности:
   - **Имя группы**
   - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Группа безопасности добавлена в список групп.

Изменение учетной записи внутреннего пользователя

Чтобы изменить учетную запись внутреннего пользователя Open Single Management Platform:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне на вкладке **Общие** измените параметры учетной записи пользователя:
   - **Описание**
   - **Полное имя**
   - **Адрес электронной почты**
   - **Основной телефон**
   - **Задать новый пароль** для подключения пользователя к Open Single Management Platform.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
  - верхний регистр (A-Z);
  - нижний регистр (a-z);
  - числа (0-9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

> Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить разрешенное количество попыток; однако из соображений безопасности не рекомендуется уменьшать это число. Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости переведите переключатель в положение **Выключено**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.

4. На вкладке **Дополнительные настройки безопасности** вы можете указать параметры безопасности для этой учетной записи.
5. На вкладке **Группы** можно добавить пользователя или группу безопасности.
6. На вкладке **Устройства** можно назначить устройства пользователю.
7. На вкладке **Роли** можно назначить роль пользователю.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная учетная запись пользователя отобразится в списке пользователей.

Изменение группы безопасности

Чтобы изменить группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Выберите группу безопасности, которую требуется изменить.

3. В открывшемся окне измените параметры группы безопасности:

   - На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.
   - На вкладке **Пользователи** можно добавить пользователей в группу безопасности. Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
   - На вкладке **Роли** можно назначить роль группе безопасности.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

Назначение роли пользователю или группе безопасности

Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел U **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Выберите имя пользователя или группы безопасности, которой нужно назначить роль.

   Можно выбрать несколько имен.
3. В меню нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли.
4. Следуйте инструкциям мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, и выберите область действия роли.

   Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

В результате роль с набором прав для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности отображается флажок в столбце **Имеет назначенные роли**.

Добавление учетных записей пользователей во внутреннюю группу безопасности

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу безопасности.

Чтобы добавить учетные записи пользователей в группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу безопасности.

3. Нажмите на кнопку **Назначить группу**.

4. В открывшемся окне **Назначить группу** выберите группу безопасности, в которую требуется добавить учетные записи пользователей.

5. Нажмите на кнопку **Сохранить**.

Учетные записи пользователей добавлены в группу безопасности. Также можно добавить внутренних пользователей в группу безопасности, используя параметры группы.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Security для мобильных устройств.

Чтобы назначить пользователя владельцем устройства:

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:

   a. В главном меню нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

2. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

   Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.

3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.

4. В открывшемся окне свойств пользователя выберите вкладку **Устройства**.

5. Нажмите на кнопку **Добавить**.

6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.

7. Нажмите на кнопку **ОК**.

   Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Активы (Устройства)** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

Двухэтапная проверка

В этом разделе описывается использование двухэтапной проверки для снижения риска несанкционированного доступа к Консоли OSMP.

Сценарий: настройка двухэтапной проверки для всех пользователей

В этом сценарии описывается, как включить двухэтапную проверку для всех пользователей и как исключить учетные записи пользователей из двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, приложение сначала откроет окно включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

Предварительные требования

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение для аутентификации.

Этапы

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

1. **Установка приложения для аутентификации на устройство**

   Вы можете установить любое приложение для аутентификации, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

   - Google Authenticator.
   - Microsoft Authenticator.
   - Bitrix24 OTP.
   - Яндекс ключ.
   - Avanpost Authenticator.
   - Aladdin 2FA.

Чтобы проверить, поддерживает ли Open Single Management Platform приложение для аутентификации, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Open Single Management Platform поддерживает выбранное приложение для аутентификации.

> Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования.

2. **Синхронизация времени приложения для аутентификации и время устройства, на котором установлен Сервер администрирования**

   Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени. Иначе возможны сбои при аутентификации и активации двухэтапной проверки.

3. **Включение двухэтапной проверки и получение секретного ключа для своей учетной записи**

   После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

4. **Включение двухэтапной проверки для всех пользователей**

   Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

5. **Запретить новым пользователям настраивать для себя двухэтапную проверку**

   Чтобы еще больше повысить безопасность доступа к Консоли OSMP, вы можете запретить новым пользователям настраивать для себя двухэтапную проверку.

6. **Изменение имени издателя кода безопасности**

   Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

7. **Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку**

   При необходимости исключите учетные записи пользователей из двухэтапной проверки. Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

8. **Настройка двухэтапной проверки для вашей учетной записи**

   Если пользователи не исключены из двухэтапной проверки и двухэтапная проверка еще не настроена для их учетных записей, им необходимо настроить ее в окне, открывающемся при входе в Консоли OSMP. Иначе они не смогут получить доступ к Серверу администрирования в соответствии со своими правами.

Результаты

После выполнения этого сценария:

- Двухэтапная проверка для вашей учетной записи включена.
- Двухэтапная проверка включена для всех учетных записей пользователей Сервера администрирования, кроме исключенных учетных записей пользователей.

О двухэтапной проверке

Если для учетной записи включена двухэтапная проверка, для входа в Консоль администрирования или Консоль OSMP требуется одноразовый код безопасности, помимо имени пользователя и пароля. При включенной доменной аутентификации пользователю достаточно ввести одноразовый код безопасности.

Чтобы использовать двухэтапную проверку, установите на мобильное устройство или компьютер приложение для аутентификации, которое генерирует одноразовые коды безопасности. Вы можете использовать любое приложение для аутентификации, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

- Google Authenticator.
- Microsoft Authenticator.
- Bitrix24 OTP.
- Яндекс ключ.
- Avanpost Authenticator.
- Aladdin 2FA.

Чтобы проверить, поддерживает ли Open Single Management Platform приложение для аутентификации, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Open Single Management Platform поддерживает выбранное приложение для аутентификации.

> Настоятельно рекомендуется сохранить секретный ключ или QR-код и хранить его в надежном месте. Это поможет вам восстановить доступ к Консоли OSMP в случае потери доступа к мобильному устройству.

Чтобы обезопасить использование Open Single Management Platform, вы можете включить двухэтапную проверку для своей учетной записи и включить двухэтапную проверку для всех пользователей.

> Вы можете исключить учетные записи из двухэтапной проверки. Это может быть необходимо для служебных учетных записей, которые не могут получить защитный код для аутентификации.

Правила и ограничения

Чтобы иметь возможность активировать двухэтапную проверку для всех пользователей и деактивировать двухэтапную проверку для отдельных пользователей:

- Убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом к объектам в функциональной области **Общие функции: Права пользователя**.
- Двухэтапная проверка для учетной записи включена.

Чтобы выключить двухэтапную проверку для всех пользователей:

- Убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом к объектам в функциональной области **Общие функции: Права пользователя**.
- Войдите в Консоль OSMP с помощью двухэтапной проверки.

Если для учетной записи на Сервере администрирования OSMP версии 13 или выше включена двухэтапная проверка, то пользователь не сможет войти в Консоль OSMP версий 12, 12.1 или 12.2.

Перевыпуск секретного ключа

Любой пользователь может повторно выпустить секретный ключ, используемый для двухэтапной проверки. Когда пользователь входит на Сервер администрирования с перевыпущенным секретным ключом, новый секретный ключ сохраняется для учетной записи пользователя. Если пользователь неправильно вводит новый секретный ключ, новый секретный ключ не сохраняется, а текущий секретный ключ остается действительным.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении для аутентификации. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. Вы можете изменить имя издателя кода безопасности. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению для аутентификации.

Включение двухэтапной проверки для вашей учетной записи

Вы можете включить двухэтапную проверку только для своей учетной записи.

Перед тем как включить двухэтапную проверку для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время, установленное в приложении для аутентификации, синхронизировано со временем устройства, на котором установлен Сервер администрирования.

Чтобы включить двухэтапную проверку для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на имя вашей учетной записи.
3. В открывшемся окне свойств пользователя выберите вкладку **Дополнительные настройки безопасности**.
4. На вкладке **Дополнительные настройки безопасности**:
   a. Выберите параметр **Запрашивать только имя пользователя, пароль и код безопасности (двухэтапная проверка)**. Нажмите на кнопку **Сохранить**.
   b. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.

Введите секретный ключ в приложении для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи включена.

Включение обязательной двухэтапной проверки для всех пользователей

Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

Чтобы включить двухэтапную проверку для всех пользователей:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Дополнительные настройки безопасности** окна свойств включите **двухэтапную проверку для всех пользователей**.

3. Если вы не включили двухэтапную проверку для своей учетной записи, приложение откроет окно включения двухэтапной проверки для вашей учетной записи.

   a. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.

   b. Введите секретный ключ вручную в приложении для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

   c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

Двухэтапная проверка для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения двухэтапной проверки для всех пользователей, необходимо настроить двухэтапную проверку для своих учетных записей, за исключением пользователей, учетные записи которых исключены из двухэтапной проверки.

Выключение двухэтапной проверки для учетной записи пользователя

Вы можете выключить двухэтапную проверку для своей учетной записи, а также для учетной записи любого другого пользователя.

Вы можете выключить двухэтапную проверку для другой учетной записи пользователя, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

Чтобы выключить двухэтапную проверку для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите выключить двухэтапную проверку. Это может быть ваша собственная учетная запись или учетная запись любого другого пользователя.
3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.
4. На вкладке **Защита учетной записи** выберите параметр **Запрашивать только имя пользователя и пароль**, если вы хотите выключить двухэтапную проверку для учетной записи пользователя.
5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи выключена.

Если вы хотите восстановить доступ пользователя, который не может войти в OSMP с помощью двухэтапной проверки, выключите двухэтапную проверку для этой учетной записи пользователя и выберите параметр **Запрашивать только имя пользователя и пароль** как описано выше. После этого войдите в Консоль OSMP под учетной записью пользователя, для которого вы выключили двухэтапную проверку, и снова включите проверку.

Выключение обязательной двухэтапной проверки для всех пользователей

Вы можете выключить обязательную двухэтапную проверку для всех пользователей, если двухэтапная проверка включена для вашей учетной записи и у вашей учетной записи есть право Изменение списков ACL объекта в разделе **Общие функции: Права пользователей**. Если двухэтапная проверка не включена для вашей учетной записи, вам нужно включить двухэтапную проверку для своей учетной записи, прежде чем выключить ее для всех пользователей.

Чтобы выключить двухэтапную проверку для всех пользователей:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Дополнительные настройки безопасности** окна свойств выключите переключатель **двухэтапной проверки для всех пользователей**.
3. Введите учетные данные своей учетной записи в окне аутентификации.

Двухэтапная проверка для всех пользователей выключена. Выключение двухэтапной проверки для всех пользователей не применяется к конкретным учетным записям, для которых двухэтапная проверка ранее была включена отдельно.

Исключение учетных записей из двухэтапной проверки.

Вы можете исключить учетные записи пользователей из двухэтапной проверки, если у вас есть право Изменение списков ACL объекта в функциональной области **Общие функции: Права пользователя**.

Если учетная запись пользователя исключена из списка двухэтапной проверки для всех пользователей, этому пользователю не нужно использовать двухэтапную проверку.

Исключение учетных записей из двухэтапной проверки может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

Если вы хотите исключить некоторые учетные записи пользователей из двухэтапной проверки:

1. Вам нужно выполнить опрос контроллера домена Microsoft Active Directory, чтобы обновить список пользователей Сервера администрирования, если вы хотите исключить учетные записи Active Directory.
2. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Дополнительные настройки безопасности** окна свойств в таблице исключений для двухэтапной проверки нажмите на кнопку **Добавить**.
4. В открывшемся окне:

   a. Выберите учетную запись пользователя, которую вы хотите исключить.

   b. Нажмите на кнопку **OK**.

Выбранные учетные записи пользователей исключены из двухэтапной проверки.

Настройка двухэтапной проверки для вашей учетной записи

При первом входе в Open Single Management Platform после включения двухэтапной проверки откроется окно настройки двухэтапной проверки для вашей учетной записи.

Перед тем как настроить двухэтапную проверку для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени.

Чтобы настроить двухэтапную проверку для учетной записи:

1. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве. Для этого выполните одно из следующих действий:

   - Введите секретный ключ в приложение для аутентификации вручную.

- Нажмите на кнопку **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации.

Код безопасности отобразится на мобильном устройстве.

2. В окне настройки двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

Двухэтапная проверка для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Запретить новым пользователям настраивать для себя двухэтапную проверку

Чтобы еще больше повысить безопасность доступа к Консоли OSMP, вы можете запретить новым пользователям настраивать для себя двухэтапную проверку.

Если этот параметр включен, пользователь с выключенной двухэтапной проверкой, например новый администратор домена, не сможет настроить двухэтапную проверку для себя. Следовательно, такой пользователь не может быть аутентифицирован на Сервере администрирования и не может войти в Консоль OSMP без одобрения другого администратора Open Single Management Platform, у которого уже включена двухэтапная проверка.

Этот параметр доступен, если для всех пользователей включена двухэтапная проверка.

Чтобы запретить новым пользователям настраивать для себя двухэтапную проверку:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Дополнительные настройки безопасности** в окне свойств включите переключатель **Запретить новым пользователям настраивать для себя двухэтапную проверку**.

Этот параметр не влияет на учетные записи пользователей, добавленных в исключения двухэтапной проверки.

Чтобы предоставить доступ к Консоли OSMP пользователю с выключенной двухэтапной проверкой, временно выключите параметр **Запретить новым пользователям настраивать для себя двухэтапную проверку**, попросите пользователя включить двухэтапную проверку, а затем включите параметр снова.

Генерация нового секретного ключа

Вы можете сгенерировать новый секретный ключ для двухэтапной проверки своей учетной записи, только если вы авторизованы с помощью двухэтапной проверки.

Чтобы сгенерировать новый секретный ключ для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи**.

2. Нажмите на учетную запись пользователя, для которой вы хотите сгенерировать новый секретный ключ для двухэтапной проверки.

3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.

4. На вкладке **Защита учетной записи** перейдите по ссылке **Сгенерировать секретный ключ**.

5. В открывшемся окне двухэтапной проверки укажите новый ключ безопасности, сгенерированный приложением для аутентификации.

6. Нажмите на кнопку **Проверить и применить**.

Новый секретный ключ для пользователя создан.

Если вы потеряете мобильное устройство, можно установить приложение для аутентификации на другое мобильное устройство и сгенерировать новый секретный ключ для восстановления доступа к Консоли OSMP.

Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, если Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению для аутентификации.

Чтобы указать новое имя издателя кода безопасности:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.

3. На вкладке **Защита учетной записи**, перейдите по ссылке **Редактировать**.

   Откроется раздел **Изменить издателя кода безопасности**.

4. Укажите новое имя издателя кода безопасности.

5. Нажмите на кнопку **OK**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

Изменение количества попыток ввода пароля

Пользователь Open Single Management Platform может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля, следуя инструкции ниже.

Чтобы изменить количество попыток ввода пароля, выполните следующие действия:

1. На устройстве, на котором установлен Сервер администрирования, запустите командную строку Linux.
2. Для утилиты klscflag выполните следующую команду:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   где N – количество попыток ввода пароля.
3. Чтобы изменения вступили в силу, перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

Удаление пользователей или групп безопасности:

1. В главном окне приложения перейдите в раздел U **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Пользователь или группа безопасности удалены.

Создание роли пользователя

Чтобы создать роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. В открывшемся окне измените параметры роли:

   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена типовых ролей.

   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.

- На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

Изменение роли пользователя

Чтобы изменить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.
3. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена типовых ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

Изменение области для роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Чтобы добавить пользователей, группы безопасности и группы администрирования в область роли пользователя, воспользуйтесь одним из следующих способов:

Способ 1:

1. В главном окне приложения перейдите в раздел U **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Установите флажки напротив имен пользователей или групп безопасности, которые требуется добавить в область роли.
3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На шаге **Выбор роли** выберите роль, которую требуется назначить.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 2:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, для которой требуется задать область.

3. В открывшемся окне свойств роли выберите вкладку **Параметры**.

4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. На шаге **Выбор пользователей** выберите пользователей и группы безопасности, которые требуется добавить в область роли.

7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

8. Нажмите на кнопку **Закрыть** (✕), чтобы закрыть окно свойств.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 3:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым вы хотите добавить область пользовательской роли, и нажмите на кнопку **Роли**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.

3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, примените и сохраните изменения.

   Выбранные пользователи или группы безопасности добавлены в область роли.

Удаление роли пользователя

Чтобы удалить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Установите флажок напротив роли, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Роль пользователя будет удалена.

Связь профилей политики с ролями

Вы можете связывать роли с профилями политик. В этом случае правило активации для профиля политики определяется в зависимости от роли: профиль политики становится активным для пользователя с определенной ролью.

Например, политика запрещает запуск приложений городской навигации для всех устройств группы администрирования. Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль "Курьер" владельцу этого устройства и создать профиль политики, разрешающий использовать приложения городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать приложения городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать приложения городской навигации на устройстве, принадлежащем вашей организации. Однако использование приложений городской навигации будет запрещено на других устройствах этой группы администрирования.

Чтобы связать роль с профилем политики:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на вкладке **Общие**.
3. Выберите вкладку **Параметры** и прокрутите вниз до раздела **Политики и профили политик**.
4. Нажмите на кнопку **Изменить**.
5. Чтобы связать роль с:

   - **Существующим профилем политики** – нажмите на значок (>) рядом с именем требуемой политики, а затем установите флажок рядом с профилем политики, с которым вы хотите связать роль.
   - **Новым профилем политики**:

     a. Установите флажок около политики, для которой вы хотите создать профиль политики.

     b. Нажмите на кнопку **Новый профиль политики**.

     c. Укажите имя нового профиля политики и настройте параметры профиля политики.

     d. Нажмите на кнопку **Сохранить**.

e. Установите флажок рядом с новым профилем политики.

6. Нажмите на кнопку **Назначить роли**.

Выбранный профиль политики связывается с ролью и появляется в свойствах роли. Профиль автоматически применяется ко всем устройствам, владельцам которых назначена эта роль.

Обновление баз и приложений "Лаборатории Касперского"

В этом разделе описаны шаги, которые вам нужно выполнить для регулярных обновлений:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации, вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Консоли OSMP.

2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.

3. Назначено соответствующее количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор схемы обновления**

   Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Open Single Management Platform и приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

2. **Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

   Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования* вручную.

   Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Open Single Management Platform. После загрузки обновлений их можно распространять на управляемые устройства.

   Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

   Инструкции: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

3. **Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)**

   По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Open Single Management Platform так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

   Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

   Инструкция: Создание задачи загрузки обновлений в хранилища точек распространения

4. **Настройка точек распространения**

   Если в вашей сети назначены точки распространения, убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

5. **Оптимизация процесса обновления с помощью файлов различий (если требуется)**

Вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами с помощью файлов различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкция: Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

6. **Настройка автоматической установки обновлений для приложений безопасности**

   Создайте задачу *Обновление* для управляемых приложений, чтобы обеспечить своевременное обновление модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Чтобы обеспечить своевременное обновление, рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище**.

   Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять приложения безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования версии 13.2 и Агент администрирования версии 13.2.

   Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

7. **Одобрение и отклонение обновлений управляемых приложений "Лаборатории Касперского"**

   По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление управляемых приложений "Лаборатории Касперского" требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для управляемого приложения было установлено, Open Single Management Platform попытается удалить обновления со всех устройств.

   Одобрение и отклонение обновлений доступно только для управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Консоли OSMP и веб-плагинов управления не поддерживается.

   Инструкция: Одобрение и отклонение обновлений программного обеспечения.

Результаты

После завершения сценария, Open Single Management Platform настроен на обновление баз "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования. Теперь вы можете приступить к мониторингу состояния сети.

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

Open Single Management Platform проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

  Open Single Management Platform позволяет автоматически обновлять Агент администрирования и приложения "Лаборатории Касперского", установленные на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Консоли OSMP и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
  - задачи *Загрузка обновлений в хранилище Сервера администрирования*.
  - задачи *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи Загрузка обновлений в хранилище Сервера администрирования

В этой схеме Open Single Management Platform загружает обновления с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).

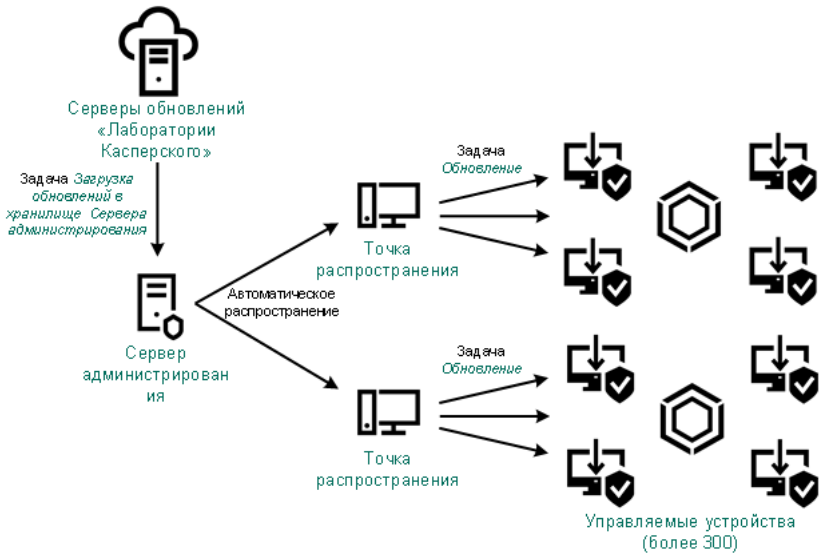
Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* и без точек распространения

В качестве источника обновлений можно использовать не только серверы обновлений "Лаборатории Касперского", но и сетевую папку.

По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* с точками распространения

После выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования*, обновления баз "Лаборатории Касперского" и модули приложений для Kaspersky Endpoint Security загружены в хранилище Сервера администрирования. Эти обновления устанавливаются с помощью задачи *Обновление* Kaspersky Endpoint Security.

Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

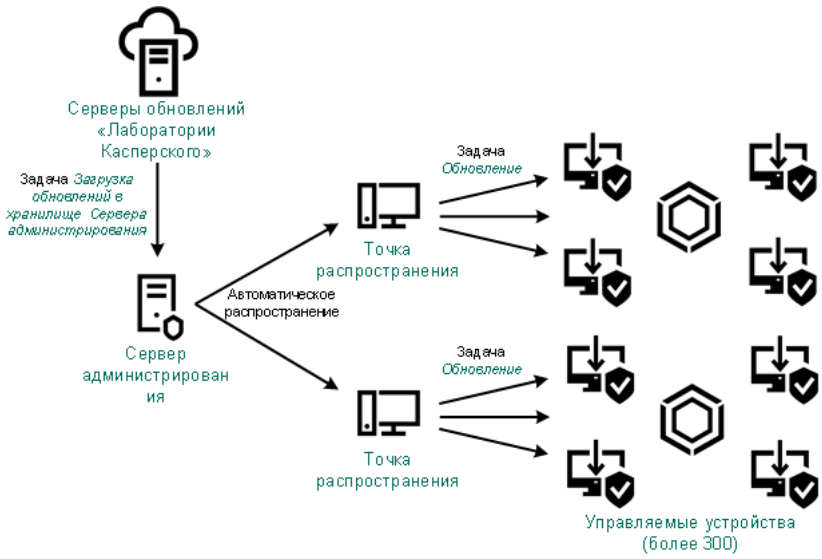
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" protects information in accordance with requirements established by law.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* и задачи *Загрузка обновлений в хранилища точек распространения*

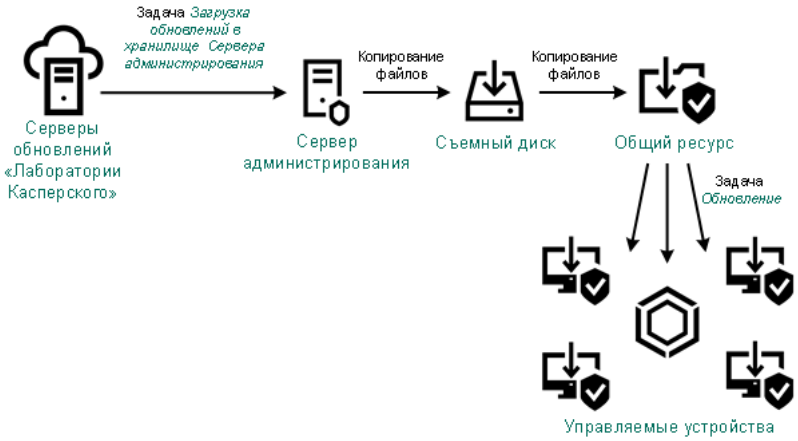
По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и модулей приложений "Лаборатории Касперского" для Open Single Management Platform.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security (см. рисунок ниже).



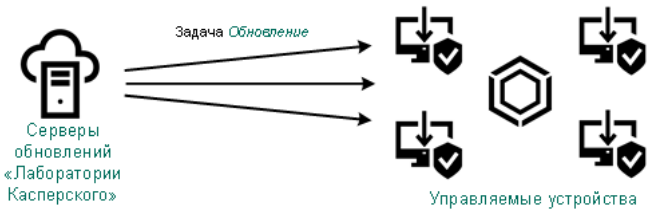
Обновление через общую папку или FTP-сервер

Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Windows

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложения безопасности не используют хранилища, предоставленные Open Single Management Platform. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в приложении безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Windows

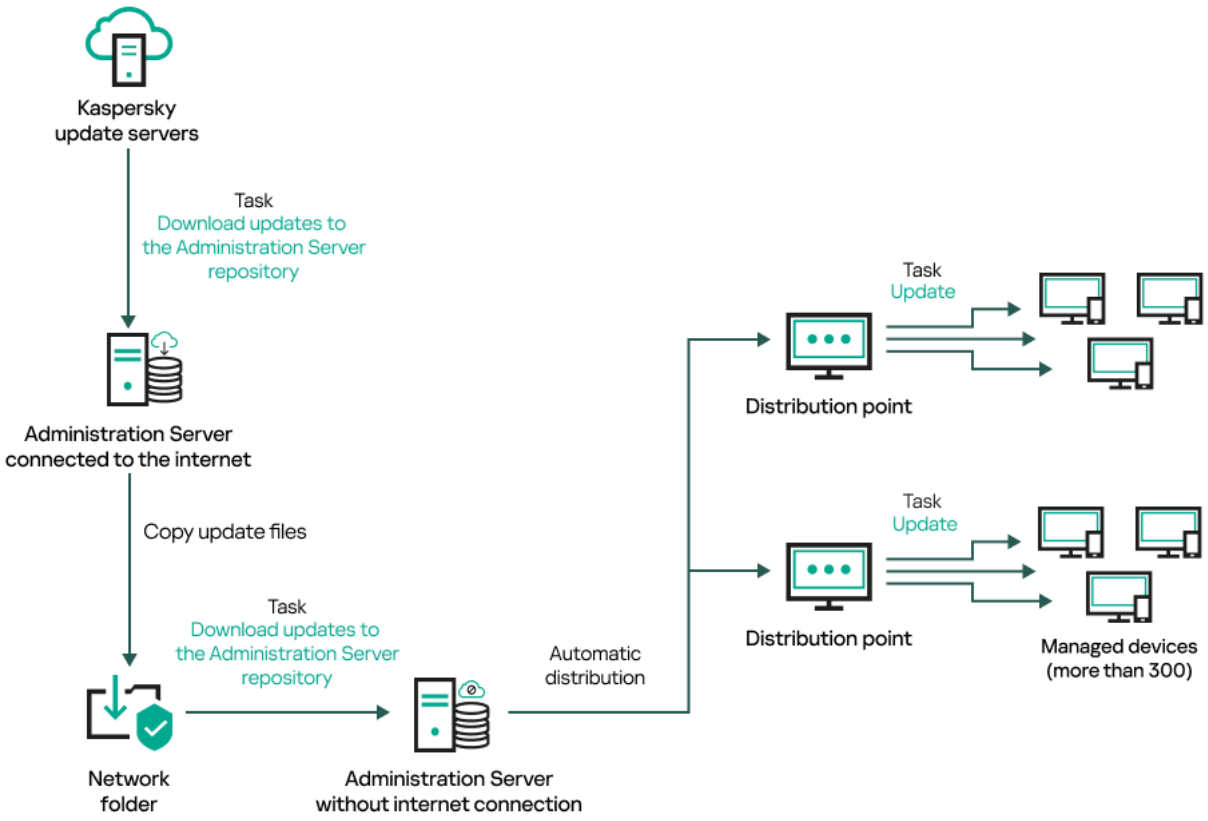
Через сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

  Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Загружать обновления, используя старую схему**.



Обновление через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

- Kaspersky Update Utility

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр *Загружать обновления, используя старую схему*.

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* позволяет загружать обновления баз и модулей приложения безопасности "Лаборатории Касперского" с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. В списке задач может быть только одна задача *Загрузка обновлений в хранилище Сервера администрирования*.

После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* и загрузки обновлений их можно распространять на управляемые устройства.

Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений*. Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить обновления перед распространением, настройте параметр **Выполнить проверку обновлений** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы создать задачу Загрузка обновлений в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Open Single Management Platform выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.
6. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
7. Чтобы открыть окно свойств задачи, нажмите на имя созданной задачи.
8. В окне свойств задачи на вкладке **Параметры приложения** укажите следующие параметры:

   - **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"

  HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

  Выбрано по умолчанию.

- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

  > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

Если общая папка с обновлениями защищена паролем, включите параметр **Задать учетную запись для доступа к общей папке источника обновлений (если используется)** и введите учетные данные, необходимые для доступа.

- **Папка для хранения обновлений**

  Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Принудительно обновить подчиненные Серверы**

  Если параметр включен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

  По умолчанию параметр выключен.

- **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

  Начиная с версии 14, Open Single Management Platform загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих приложений:

  - Kaspersky Update Utility

    Эта утилита загружает обновления по старой схеме.

  - Open Single Management Platform

    Например, один Сервер администрирования не имеет подключения к интернету. В этом случае можно загружать обновления с помощью второго Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную или сетевую папку, чтобы использовать ее в качестве источника обновлений для первого Сервера. Если второй Сервер администрирования имеет номер версии 13.2 или ниже, включите параметр **Загружать обновления, используя старую схему** в задаче для первого Сервера администрирования.

  По умолчанию параметр выключен.

- **Выполнить проверку обновлений**

Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу Проверка обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

По умолчанию параметр выключен.

9. В окне свойств задачи на вкладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск задачи**:

     - Вручную (выбрано по умолчанию)

       Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Open Single Management Platform при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

     - Каждые N минут

       Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

     - Каждый N час

       Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

       Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

       По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

     - Каждые N дней

       Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

     - Каждую N неделю

       Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

     - Ежедневно (не поддерживается переход на летнее время)

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

  Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

  Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

  Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

  По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Ежемесячно, в указанные дни выбранных недель**

  Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

  Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

  По умолчанию все флажки сняты.

- **По завершении другой задачи**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **После завершения другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

- **Имя задачи**. В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения**. В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- Дополнительные параметры задачи:
  - Запускать пропущенные задачи

    Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

    Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

  - Использовать автоматическое определение случайного интервала между запусками задачи

    Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

    Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

    Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

    По умолчанию флажок установлен.

    Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

  - Использовать автоматическую случайную задержку запуска задачи в интервале

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

10. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модулей приложений копируются с источника обновлений и размещаются на Сервере администрирования. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Просмотр полученных обновлений

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модулей приложений копируются с источника обновлений и размещаются на Сервере администрирования. Просмотреть загруженные обновления можно в разделе **Обновления баз и модулей приложений "Лаборатории Касперского"**.

Чтобы просмотреть список полученных обновлений,

В главном окне приложения перейдите в раздел **Операции** → **Приложения "Лаборатории Касперского"** → **Обновления баз и модулей приложений "Лаборатории Касперского"**.

Отобразится список доступных обновлений.

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в хранилище Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Update verification* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в хранилище Сервера администрирования не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты приложения безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи обновления и поиска вредоносного ПО для какого-нибудь приложения, которое поддерживает Open Single Management Platform, например, Kaspersky Endpoint Security для Linux. При создании задач обновления и поиска вредоносного ПО укажите группу администрирования с тестовыми устройствами.

   Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вредоносного ПО на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вредоносного ПО.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы Open Single Management Platform проверял полученные обновления перед распространением их на клиентские устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на имя задачи **Загрузка обновлений в хранилище Сервера администрирования**.

3. В открывшемся окне свойств задачи выберите вкладку **Параметры приложения** и включите параметр **Выполнить проверку обновлений**.

4. Если задача *Проверка обновлений* существует, нажмите на кнопку **Выберите задачу**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.

5. Если вы не создавали задачу *Проверка обновлений* ранее, выполните следующие действия:

   a. Нажмите на кнопку **Новая задача**.

   b. В открывшемся мастере создания задачи укажите имя задачи, если вы хотите изменить предустановленное имя.

   c. Выберите созданную ранее группу администрирования с тестовыми устройствами.

   d. Выберите задачу обновления нужного приложения, поддерживаемой Open Single Management Platform, а затем выберите задачу поиска вредоносного ПО.

   После этого появляются следующие параметры. Рекомендуется оставить их включенными:

   - **Перезагружать устройство после обновления баз**

     После обновления антивирусных баз на устройстве рекомендуется перезагрузить устройство.

     По умолчанию параметр включен.

   - **Проверять статус постоянной защиты после обновления баз и перезапуска устройства**

     Если этот параметр включен, задача *Проверка обновлений* проверяет, актуальны ли обновления, загруженные в хранилище Сервера администрирования, и не снизился ли уровень защиты после обновления антивирусных баз и перезагрузки устройства.

     По умолчанию параметр включен.

   e. Укажите учетную запись, под которой будет запущена задача *Проверка обновлений*. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

6. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **Сохранить**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

Создание задачи загрузки обновлений в хранилища точек распространения

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Open Single Management Platform;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

*Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Open Single Management Platform выберите в поле **Тип задачи** выберите **Загрузка обновлений в хранилища точек распространения**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Нажмите на кнопку выбора, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.
6. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. На вкладке **Параметры приложения** окна свойств задачи укажите следующие параметры:

   - Источники обновлений

В качестве источника обновлений для точек распространения могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"

  HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

  По умолчанию этот вариант выбран.

- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

  FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Папка для хранения обновлений**

  Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

Начиная с версии 14, Open Single Management Platform загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих приложений:

- Kaspersky Update Utility

  Эта утилита загружает обновления по старой схеме.

- Open Single Management Platform

  Например, точка распространения настроена на получение обновлений из локальной или сетевой папки. В этом случае вы можете загружать обновления с помощью Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную папку на точке распространения. Если Сервер администрирования имеет номер версии 13.2 или ниже, включите параметр **Загружать обновления, используя старую схему** в задаче *Загружать обновления в хранилища точек распространения*.

По умолчанию параметр выключен.

10. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**:

  - **Вручную** (выбрано по умолчанию)

    Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Open Single Management Platform при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

  - **Каждые N минут**

    Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

  - **Каждый N час**

    Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

    Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

    По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

  - **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

  Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Ежедневно (не поддерживается переход на летнее время)**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

  Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

  Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

  Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

  По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Ежемесячно, в указанные дни выбранных недель**

  Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

  Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

  По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

  - Антивирусами для рабочих станций и файловых серверов;
  - Антивирусами защиты периметра;
  - Антивирусами для почтовых систем.

    По умолчанию установлены все флажки.

- **По завершении другой задачи**

  Если в раскрывающемся списке **Запуск по расписанию** выбран режим **После завершения другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

  - **Имя задачи**. В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
  - **Результат выполнения**. В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

  Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

  Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Закрытие уязвимостей).

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и модулей приложений копируются с источника обновлений и размещаются в хранилищах точек распространения. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования

При создании или использовании задачи загрузки обновлений в хранилище Сервера администрирования, вы можете выбрать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского"
- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Сетевая папка

В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала смонтируйте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Open Single Management Platform не потребует от вас ввода учетных данных.

Серверы обновлений "Лаборатории Касперского" используются по умолчанию, но также можно загружать обновления из локальной или сетевой папки. Можно использовать эту папку, если ваша сеть не имеет доступа к интернету. В этом случае можно вручную загрузить обновления с серверов обновлений "Лаборатории Касперского" и поместить загруженные файлы в нужную папку.

Можно указать только один путь к локальной или сетевой папке. В качестве локальной папки необходимо указать папку на устройстве, где установлен Сервер администрирования В качестве сетевой папки можно использовать FTP-сервер или HTTP-сервер или общий ресурс SMB. Если общий ресурс SMB требует аутентификации, его нужно заранее подключить к системе с необходимыми учетными данными. Не рекомендуется использовать протокол SMB1, так как он небезопасен.

Если вы добавите и серверы обновлений "Лаборатории Касперского", и локальную или сетевую папку, то сначала будут загружаться обновления из папки. В случае ошибки при загрузке будут использоваться серверы обновлений "Лаборатории Касперского".

Если общая папка с обновлениями защищена паролем, включите параметр **Задать учетную запись для доступа к общей папке источника обновлений (если используется)** и введите учетные данные, необходимые для доступа.

Чтобы добавить источники обновлений:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Загрузка обновлений в хранилище Сервера администрирования**.
3. Выберите вкладку **Параметры приложения**.
4. Около **Источники обновлений** нажмите на кнопку **Настроить**.
5. В появившемся окне нажмите на кнопку **Добавить**.

6. В списке источников обновлений добавьте необходимые источники. Если вы установите флажок **Сетевая папка** или **Локальная или сетевая папка**, укажите путь к папке.

7. Нажмите на кнопку **ОК**, а затем закройте окно свойств источника обновлений.

8. В окне источника обновлений нажмите на кнопку **ОК**.

9. Нажмите на кнопку **Сохранить** в окне задач.

Теперь обновления загружаются в хранилище Сервера администрирования из указанных источников.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений, установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Консоли OSMP и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения "Лаборатории Касперского"** → **Обновления**.

   Отобразится список доступных обновлений.

   Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. При необходимости примите Лицензионное соглашение, нажав на кнопку **Просмотреть и принять Лицензионные соглашения**.

3. Выберите обновления, которые требуется подтвердить или отклонить.

4. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Open Single Management Platform не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.

Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security для Windows на клиентских устройствах.

Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите область действия задачи.
6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.
7. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:

    - **Локальный режим**: между устройством и Сервером администрирования установлена связь.

- **Мобильный режим**: между устройством и Open Single Management Platform не установлена связь (например, если устройство не подключено к интернету).

11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.

12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.

    Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Open Single Management Platform.

    Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.

    Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.

14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.

15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

Когда Open Single Management Platform загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

О функции загрузки файлов различий

Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и модулей приложений.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Включение функции загрузки файлов различий

Этапы

1. **Включение функции на Сервере администрирования**

   Включите функцию в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

2. **Включение функции для точки распространения**

   Включить функцию для точки распространения, которая получает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения*.

   Включите функцию в параметрах политики Агента администрирования для точки распространения, которая получает обновления с Сервера администрирования.

   Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

   Эта функция включается в свойствах политики Агента администрирования и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения**.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

Загрузка обновлений точками распространения

Open Single Management Platform позволяет точкам распространения получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

Чтобы настроить получение обновлений для точки распространения, выполните следующие действия:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, через которую будут доставляться обновления на клиентские устройства в группе.

4. В окне свойств точки распространения выберите раздел **Источник обновлений**.

5. Выберите источник обновлений для точки распространения:

   - **Источник обновлений**

     Выберите источник обновлений для точки распространения:

     - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.
     - Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*.
       - Если такая задача уже существует для устройства, выберите задачу в списке.
       - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   - **Загрузить файлы различий**

     Этот параметр включает функцию загрузки файлов различий.

     По умолчанию параметр включен.

В результате точка распространения будет получать обновления из указанного источника.

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление с помощью хранилища Сервера администрирования.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

Чтобы хранилище Сервера администрирования содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должно быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища Сервера администрирования с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*.

- Любого устройства, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища Сервера администрирования.

Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.
2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления расположены: \\<server name>\KLSHARE\Updates.

   Также вы можете настроить в Open Single Management Platform регулярное копирование обновлений в выбранную вами папку. Для этого используйте параметр **Копировать полученные обновления в дополнительные папки** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*. Если вы укажете папку, расположенную на запоминающем устройстве или внешнем жестком диске, в качестве папки назначения для этого параметра, это запоминающее устройство всегда будет содержать последнюю версию обновлений.
3. На автономных устройствах настройте Kaspersky Endpoint Security на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.

   Инструкции:

   - Справка Kaspersky Endpoint Security для Linux
   - Справка Kaspersky Endpoint Security для Windows
4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.
5. На автономном устройстве, требующем установки обновлений, запустите задачу Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows *Обновление*, в зависимости от операционной системы автономного устройства.

После завершения задачи обновления базы данных и модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;

- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

Чтобы открыть окно удаленной диагностики:

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:
   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.
4. В появившемся окне нажмите на кнопку **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh.

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.
4. Если вы хотите включить трассировку:

   a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

   - **Уровень трассировки**

     Уровень трассировки определяет состав информации, которую содержит файл трассировки.

   - **Трассировка на основе ротации**

     Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

     Этот параметр доступен только для Kaspersky Endpoint Security.

   c. Нажмите на кнопку **Сохранить**.

   Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

   На клиентских устройствах под управлением Linux трассировка компонента Обновление Агента администрирования регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.
5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите Kaspersky Endpoint Security для Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.

4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса специалиста Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

   - **Детальный уровень**

     Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

   b. Выберите один из уровней трассировки Xperf:

   - **Базовый тип**

     Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

     По умолчанию выбран этот вариант.

   - **Тип перезагрузки**

     Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

c. Определите размер файла ротации.

d. Нажмите на кнопку **Сохранить**.

Трассировка Xperf включена и настроена.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

Трассировка Xperf выключена.

Загрузка файла трассировки приложения

Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.

4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

Откроется окно **Журналы событий трассировки устройства**, где отображается список файлов трассировки.

5. В списке файлов трассировки выберите файл, который вы хотите загрузить.

6. Выполните одно из следующих действий:

- Загрузите выбранный файл, нажав на кнопку **Загрузить**. Вы можете выбрать один или несколько файлов для загрузки.

- Загрузите часть выбранного файла:

a. Нажмите на кнопку **Загрузить часть**.

Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Загрузить часть** будет неактивна.

b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

Для устройств под управлением Linux изменение имени части файла недоступно.

c. Нажмите на кнопку **Загрузить**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.
3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   > Ссылка **Журналы службы Центра обновления Windows** доступна только для клиентских устройств под управлением Windows.

   Откроется окно **Журналы событий трассировки устройства**, где отображается список файлов трассировки.
4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Чтобы загрузить с клиентского устройства параметры приложений:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Загрузить** для загрузки информации о параметрах приложений, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка системной информации с клиентского устройства

Чтобы загрузить системную информацию с клиентского устройства выполните следующие действия:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Информация о системе**.
3. Нажмите на кнопку **Загрузить** для загрузки системной информации о клиентском устройстве.

Если вы получаете системную информацию об устройстве под управлением Linux, в получившийся файл добавляется файл дампа для аварийно завершенных приложений.

Файл с информацией загрузится в указанное расположение.

Загрузка журналов событий

Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Журнал событий всех устройств**.
3. В окне **Журнал событий всех устройств** выберите один или несколько журналов событий.
4. Выполните одно из следующих действий:
   - Загрузите выбранный журнал событий, нажав на кнопку **Загрузить весь файл**.
   - Загрузите часть выбранного журнала событий:
     a. Нажмите на кнопку **Загрузить часть**.
     Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Загрузить часть** будет неактивна.
     b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.
     Для устройств под управлением Linux изменение имени части журнала событий недоступно.
     c. Нажмите на кнопку **Загрузить**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:
   - **Остановить приложение**
     Эта кнопка доступна, только если приложение в данный момент запущено.

- **Перезапустить приложение**

  Эта кнопка доступна, только если приложение в данный момент запущено.

- **Запустить приложение**

  Эта кнопка доступна, только если приложение в данный момент не запущено.

В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов

Чтобы запустить диагностику Агента администрирования Kaspersky Security Center на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите **Агент администрирования Kaspersky Security Center**.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. После завершения процесса диагностики кнопка **Загрузить отчет диагностики** становится доступной.
5. Нажмите на кнопку **Загрузить отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

Чтобы запустить приложение на клиентском устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Файлы приложения** нажмите на кнопку **Обзор** для выбора ZIP-архива с приложением, которое вы хотите запустить на клиентском устройстве.

ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

При необходимости можно указать имя исполняемого файла и аргументы командной строки. Для этого заполните поля **Исполняемый файл в архиве для запуска на удаленном устройстве** и **Аргументы командной строки**.

4. Нажмите на кнопку **Загрузить и запустить** для запуска указанного приложения на клиентском устройстве.

5. Следуйте указаниям сотрудника службы поддержки "Лаборатории Касперского".

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

Получение файлов дампа с клиентских устройств с операционной системой Linux не поддерживается.

Чтобы получить файлы дампа с помощью удаленной диагностики, используется утилита kldumper. Эта утилита предназначена для получения файлов дампа процессов приложений "Лаборатории Касперского" по запросу специалистов Службы технической поддержки. Подробную информацию о требованиях к использованию утилиты kldumper приведена в Базе знаний Open Single Management Platform.

Чтобы создать файл дампа для приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В разделе **Формирование дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.

4. Нажмите на кнопку **Загрузить дамп файла**.

   Архив с файлом дампа для указанного приложения загружен.

   Если указанное приложение не запущено на клиентском устройстве, папка "result" в загруженном архиве будет пустой.

   Если указанное приложение запущено, но загрузка завершается с ошибкой или папка "result" в загруженном архиве пуста, см. Базу знаний Open Single Management Platform.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Open Single Management Platform позволяет загружать основную диагностическую информацию с клиентского устройства. Кроме того, вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Open Single Management Platform, вам нужно будет пройти все разделы интерфейса удаленной диагностики. Кроме того, диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:

1. Загрузите скрипт collect.sh, который запакован в архив collect.tar.gz.
2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.
3. Выполните следующую команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните следующую команду, чтобы указать права на выполнение скрипта:

   ```
   # chmod +x collect.sh
   ```

5. Запустите сценарий collect.sh под учетной записью с правами администратора:

   ```
   # ./collect.sh
   ```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/$HOST_NAME-collect.tar.gz.

Управление приложениями и исполняемыми файлами на клиентских устройствах

В этом разделе описаны возможности Open Single Management Platform связанные с управлением приложений и исполняемых файлов на клиентских устройствах.

Использование компонента Контроль приложений для управления исполняемыми файлами

Вы можете использовать компонент Контроль приложений, чтобы разрешить или запретить запуск исполняемых файлов на пользовательских устройствах. Компонент Контроль приложений поддерживает операционные системы Windows и Linux.

Для операционных систем Linux компонент Контроль приложений доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Open Single Management Platform развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows создана и активна. Компонент Контроль приложений включен в политике.

Этапы

Сценарий использования компонента Контроль приложений состоит из следующих этапов:

1. **Формирование и просмотр списка исполняемых файлов на клиентских устройствах**

   Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации.

   Инструкции: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

2. **Создание категорий для исполняемых файлов, используемых в вашей организации**

   Проанализируйте списки приложений и исполняемых файлов, хранящихся на управляемых устройствах. На основе анализа сформируйте категории для исполняемых файлов. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор исполняемых файлов, используемых в вашей организации. Если разные группы безопасности используют свои наборы исполняемых файлов в своей работе, для каждой группы безопасности можно создать отдельную категорию.

   Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

   - *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
   - *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

   Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Open Single Management Platform существует три типа категорий исполняемых файлов:

   - Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, путь к файлу, чтобы включить исполняемые файлы в категорию.
   - Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
   - Категория, в которую входят исполняемые файлы из выбранных папок. Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security для Linux с использованием категорий, которые вы создали на предыдущем этапе.

   Инструкция: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows.

4. **Включение компонента Контроль приложений в тестовом режиме**

   Чтобы правила Контроля приложений не блокировали исполняемые файлы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

   При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

   - Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
   - Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

   Инструкции для Консоли OSMP: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

5. **Изменение параметров компонента Контроль приложений**

   Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию пополняемую вручную.

   Инструкции для Консоли OSMP: Добавление исполняемых файлов, связанных с событием, в категорию приложения.

6. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции для Консоли OSMP: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

7. **Проверка конфигурации Контроля приложений**

   Убедитесь, что вы выполнили следующее:

   - Создали категории для исполняемых файлов.
   - Настроили Контроль приложений с использованием категорий.
   - Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Режимы и категории компонента Контроль приложений

Компонент Контроль приложений контролирует попытки пользователей запуска приложений. Вы можете использовать правила компонента Контроль приложений для контроля запуска приложений.

Компонент Контроль приложений доступен для версии приложения Kaspersky Endpoint Security 11.2 для Linux и выше.

Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Open Single Management Platform существует три типа категорий:

- Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
- Категория, в которую входят исполняемые файлы из выбранных папок. Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Получение и просмотр списка приложений, установленных на клиентских устройствах

Open Single Management Platform выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.

   На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

2. Вы можете группировать и фильтровать данные таблицы с установленными приложениями следующим образом:

   - Нажмите на значок параметров ( ) в правом верхнем углу таблицы.

     В открывшемся меню **Параметры столбцов** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлено приложение, выберите столбец **Тип операционной системы**.

   - Нажмите на значок фильтрации ( ) в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица установленных приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Устройства** → **Управляемые устройства** → **<имя устройства>** → **Дополнительно** → **Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Каждый раз, когда пользователь пытается запустить исполняемый файл, этот файл автоматически добавляется в список компонента Контроль приложений. Вы можете создать задачу инвентаризации и получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вам нужно создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для приложения Kaspersky Endpoint Security для Linux версии 11.2 и выше.

Вы можете снизить нагрузку на базу данных при получении списка исполняемых файлов. Для этого рекомендуется запускать задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений.

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows в зависимости от типа операционной системы клиентских устройств.

4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.

5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

   После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

При выполнении инвентаризации приложение обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML-файлы.

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

Чтобы создать пополняемую вручную категорию приложений:

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Категории приложений**.

   Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории приложений и выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.

5. На шаге **Критерии условия** выберите тип правила для создания категории из списка:

- **Из KL-категории**

  Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

- **Выберите сертификат из хранилища сертификатов**

  Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Задайте путь к приложению (поддерживаются маски)**

  Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.

- **Съемный диск**

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

  - **Выберите из списка исполняемых файлов**

    Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

  - **Выберите из реестра приложений**

    Если выбран этот параметр, отображается реестр приложений. Вы можете выбрать приложения из реестра и указать следующие метаданные файла:

    - Имя файла.
    - Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Название приложения.
    - Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Производитель.

  - **Задайте вручную**

Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

Хеш файла

В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Open Single Management Platform для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

Выберите один из вариантов вычисления хеш-функции приложением Open Single Management Platform для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.
- Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

Метаданные

Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Метаданные будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в категорию приложений.

Сертификат

Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- Из архивной папки

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

Выбранный критерий добавлен в список условий.

Вы можете добавить столько критериев для создания категории приложений, сколько вам нужно.

6. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.

7. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Убедитесь, что выполнены следующие предварительные требования:

- Компонент Контроль приложений включен в политике Kaspersky Endpoint Security.
- Получен список исполняемых файлов, хранящихся на управляемых устройствах.

Чтобы создать категорию приложений, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Категории приложений**.

   Откроется страница со списком категорий исполняемых файлов.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.

4. Нажмите на кнопку **Добавить**.

5. В открывшемся окне выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории приложений.

6. Задайте следующие параметры:

   - **Алгоритм вычисления хеш-функции**

В зависимости от версии приложения защиты, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии приложения защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

- Если в вашей сети установлены версии приложений защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.

- Если на разных устройствах в вашей сети используются новые и ранние версии приложения защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Синхронизировать данные с хранилищем Сервера администрирования**

Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

По умолчанию параметр выключен.

Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

- **Тип файла**

В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

  В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

  Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

  Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

После завершения работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете создать категорию при настройке компонента Контроль приложений.

Создание категории приложений, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию, в которую входят исполняемые файлы из выбранных папок:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

   Откроется страница со списком категорий.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.

4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории.

5. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Open Single Management Platform.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Open Single Management Platform.

По умолчанию флажок снят.

- Алгоритм вычисления хеш-функции: **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

  В зависимости от версии приложения защиты, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

  SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

  Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

  - Если в вашей сети установлены версии приложения защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

  - Если в вашей сети установлены версии приложений защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.

  - Если на разных устройствах в вашей сети используются новые и ранние версии приложения защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

  По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

  По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- Принудительно проверять папку на наличие изменений

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

После завершения работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете использовать категорию для настройки компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий исполняемых файлов и параметры каждой категории.

Чтобы просмотреть список категорий приложений,

В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

Откроется страница со списком категорий.

Чтобы просмотреть свойства категории приложений,

нажмите на имя категории.

Откроется окно свойств выбранной категории. Параметры сгруппированы на нескольких вкладках.

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security для Windows.

Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

   Отобразится страница со списком политик.

2. Нажмите на политику **Kaspersky Endpoint Security для Windows**.

   Откроется окно свойств политики.

3. Перейдите в раздел **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

   Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.

4. Параметр **Контроль приложений** включен по умолчанию. Выключите переключатель Контроль **приложений [Выключен**], чтобы выключить параметр.

5. В блоке **Параметры Контроля приложений** включите режим работы с применением правил Контроля приложений и разрешите Kaspersky Endpoint Security для Windows блокировку запуска приложений.

Если вы хотите протестировать правила Контроля приложений, в разделе **Параметры Контроля приложений**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security для Windows не блокирует запуск приложений, но фиксирует информацию о сработавших правилах в отчете. Перейдите по ссылке **Просмотреть отчет** для просмотра этой информации.

6. Включите параметр **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security для Windows контролировало загрузку модулей DLL при запуске приложений пользователями.

   Информация о модуле и приложении, которое загрузило модуль, будет сохранена в отчете.

   Kaspersky Endpoint Security для Windows контролирует только DLL модули и драйверы, которые были загружены после того, как параметр **Управление загрузкой модулей DLL** был включен. Перезагрузите устройство после выбора параметра **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security для Windows контролировало все модули и драйверы DLL, включая те, которые были загружены до запуска Kaspersky Endpoint Security для Windows.

7. (Если требуется.) В блоке **Шаблоны сообщений** измените шаблон сообщения, которое отображается, когда приложение заблокировано для запуска, и шаблон сообщения электронной почты, которое отправляется вам.

8. В блоке параметров **Режим Контроля приложений** выберите режим **Список запрещенных** или **Список разрешенных**.

   По умолчанию выбран режим **Список запрещенных**.

9. Перейдите по ссылке **Параметры списков правил**.

   Откроется окно **Списки запрещенных и разрешенных**, в котором можно добавить категорию приложений. По умолчанию отображается вкладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается вкладка **Список разрешенных**, если выбран режим **Список разрешенных**.

10. В окне **Списки запрещенных и разрешенных** нажмите на кнопку **Добавить**.

    Откроется окно **Правило Контроля приложений**.

11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

    Откроется окно **Категории приложений**.

12. Добавьте категорию приложений (или категории), которые вы создали ранее.

    Вы можете изменить параметры категории, нажав на кнопку **Изменить**.

    Вы можете создать категорию, нажав на кнопку **Добавить**.

    Вы можете удалить категорию, нажав на кнопку **Удалить**.

13. После того как формирование списка категорий приложений завершено, нажмите кнопку **ОК**.

    Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Добавление исполняемых файлов, связанных с событием, в категорию приложения

После настройки компонента Компонента Контроль приложений в политиках Kaspersky Endpoint Security в списке событий могут отображаться следующие события:

- **Запуск приложения запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил.
- **Запуск приложения запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска приложения** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль приложений для применения правил, а пользователь запросил доступ к приложению, которое заблокировано для запуска.

Рекомендуется создавать выборки событий для просмотра событий, связанных с компонентом Контроль приложений.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля приложений, в существующую категорию приложений или в новую категорию приложений. Вы можете добавлять исполняемые файлы только в категорию приложений пополняемую вручную.

Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий.

   Если вы не создали выборку событий, связанную с Контролем приложений, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.

   Отобразится список событий.

3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию приложений, и нажмите на кнопку **Назначить категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На странице мастера укажите необходимые параметры:

   - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:

     - **Добавить в новую категорию приложений**

Выберите этот параметр, если вы хотите создать категорию приложений на основе исполняемых файлов, связанных с событиями.

По умолчанию выбран этот вариант.

Если вы выбрали этот параметр, укажите имя новой категории.

- **Добавить в существующую категорию**

  Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию приложений.

  По умолчанию вариант не выбран.

  Если вы выбрали этот параметр, выберите категорию приложений, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

- В разделе **Тип правила** выберите следующие параметры:
  - **Правила для добавления в область действия**
  - **Правила для добавления в исключения**
- В разделе **Параметр, используемый в качестве условия** выберите один из следующих вариантов:
  - **Данные сертификата (или SHA256 для файлов без сертификата)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

    По умолчанию этот вариант выбран.

  - **Данные сертификата (файлы без сертификата пропускаются)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

  - **Только SHA256 (файлы без хеша пропускаются)**

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

- **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**

  Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

  Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

5. Нажмите на кнопку **OK**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля приложений, добавляются в существующую категорию приложений или в новую категорию приложений. Вы можете просмотреть параметры категории приложений, которую вы изменили или создали.

Подробное описание компонента Контроль приложений см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

О лицензии

Лицензия – это ограниченное по времени право на использование Open Single Management Platform, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Open Single Management Platform прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая* – платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Open Single Management Platform вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

Справочное руководство API

Справочное руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную. Например, как администратор вы можете использовать Kaspersky Security Center OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.

- Пользовательская разработка. Используя OpenAPI, вы можете разработать клиентское приложение.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

Справочное руководство OpenAPI

Примеры сценариев

Справочное руководство по OpenAPI содержит примеры сценариев Python, перечисленные в таблице ниже. Примеры показывают, как вы можете вызывать методы OpenAPI и автоматически выполнять различные задачи по защите вашей сети, например, создавать иерархию "главный/подчиненный", запускать задачи в Open Single Management Platform или назначать точки распространения. Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

Чтобы вызвать методы OpenAPI и запустить сценарии:

1. Загрузите архив KlAkOAPI.tar.gz. Этот архив включает в себя пакет KlAkOAPI и примеры (их можно скопировать из архива или справочного руководства по OpenAPI). Также архив KlAkOAPI.tar.gz находится в папке установки Open Single Management Platform.

2. Установите пакет KlAkOAPI из архива KlAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования.

   Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI.

Сопоставление пользовательских сценариев и примеров методов Kaspersky Security Center OpenAPI

Пример	Назначение примера	Сценарий
Журнал событий KlAkParams	Вы можете извлекать и обрабатывать данные, используя `KlAkParams` структуру данных. В примере показано, как работать с этой структурой данных. Пример вывода может быть представлен по-разному. Вы можете получить данные для отправки HTTP-метода или использовать их в своем коде.	Мониторинг и отчеты
Создание и удаление иерархии "главный/подчиненный"	Вы можете добавить подчиненный Сервер администрирования и установить таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Или вы можете исключить подчиненный Сервер администрирования из иерархии.	Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования и удаление иерархии Серверов администрирования
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений

Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования	Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию.	Лицензирование управляемых приложений
Создайте отчет об эффективных правах пользователей	Вы можете создать разные отчеты. Например, вы можете сгенерировать отчет об эффективных правах пользователя, используя этот пример. В этом отчете представлена информация о правах, которыми обладает пользователь в зависимости от его группы и роли. Вы можете загрузить отчет в формате HTML, PDF или Excel.	Генерация и просмотр отчета
Запустите задачу на устройстве	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем запустить необходимую задачу.	Запуск задачи вручную
Регистрация точек распространения для устройств в группе	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и приложений "Лаборатории Касперского"
Перечисление всех групп	Вы можете выполнять различные действия с группами администрирования. В примере показано, как выполнить следующее: • Получить идентификатор корневой группы "Управляемые устройства". • Переместить по иерархии групп. • Получить полную развернутую иерархию групп с их именами и вложенностью.	Настройка Сервера администрирования
Перечисление задач, запрос статистики задач и запуск задач	Вы можете ознакомиться со следующей информацией: • Историей выполнения задачи. • Текущим статусом задачи. • Количеством задач в разных статусах. Вы также можете запустить задачу. По умолчанию пример запускает задачу после вывода статистики.	Запуск задачи вручную
Создание и запуск задачи	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Имя. • Группа устройств, для которой будет использоваться задача. По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи.	Создание задачи
Перечисление лицензионных ключей	Вы можете получить список всех активных лицензионных ключей для приложений "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения о каждом лицензионном ключе, такие как имя, тип или срок действия.	Лицензирование
Создание пользовательской категории	Вы можете создать категорию приложений с требуемыми параметрами.	Создание пополняемой вручную категории приложений
Перечисление пользователей с помощью SrvView	Вы можете использовать класс SrvView для запроса подробной информации с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление пользователями и ролями пользователей

Взаимодействие приложений с Open Single Management Platform через OpenAPI

Некоторые приложения взаимодействуют с Open Single Management Platform через OpenAPI. К таким приложениям относятся, например, Kaspersky Anti Targeted Attack Platform. Это также может быть пользовательское клиентское приложение, разработанное вами на основе OpenAPI.

Приложения, взаимодействующие с Open Single Management Platform через OpenAPI, подключаются к Серверу администрирования. Чтобы узнать, работает ли используемое вами приложение с OpenAPI, обратитесь к справке этого приложения.

Мониторинг, отчеты и аудит

В этом разделе описаны функции мониторинга и работа с отчетами в Open Single Management Platform. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Open Single Management Platform можно настраивать функции мониторинга и параметры отчетов.

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Open Single Management Platform.

Предварительные требования

После развертывания Open Single Management Platform в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Open Single Management Platform и к формированию отчетов.

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

1. **Настройка переключения статусов устройств**

   Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры, вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*. При настройке переключения состояний устройства убедитесь, что:

   - новые параметры не противоречат политикам информационной безопасности вашей организации;
   - вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

2. **Настройка параметров уведомлений о событиях на клиентских устройствах**

   Инструкции:

   Настройка уведомлений (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах.

3. **Выполнение рекомендуемых действий для критических и предупреждающих уведомлений**

   Инструкции:

   Выполните рекомендуемые действия для сети вашей организации.

4. **Просмотр состояния безопасности сети вашей организации**

   Инструкции:

   - Просмотр веб-виджета Состояние защиты.
   - Генерация и просмотр отчета Отчет о состоянии защиты.
   - Генерация и просмотр отчета Отчет об ошибках.

5. **Нахождение незащищенных клиентских устройств**

   Инструкции:

- Просмотр веб-виджета Новые устройства.
- Генерация и просмотр отчета Отчет о развертывании защиты.

6. **Проверка защиты клиентских устройств**

   Инструкции:

   - Генерация и просмотр отчета из категорий Состояние защиты и Статистика угроз.
   - Запуск и просмотр выборки событий Критическое.

7. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции:

   - Ограничение максимального количества событий.

8. **Просмотр информации о лицензии**

   Инструкции:

   - Добавление веб-виджета Используемые лицензионные ключи на панель мониторинга и его просмотр.
   - Генерация и просмотр отчета Отчет об использовании лицензионных ключей.

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. Консоль OSMP предоставляет следующие виды мониторинга и отчетов в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления

Панель мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Отчеты

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Выборки событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Консоли OSMP.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования. Эта информация хранится в виде списка в папке **Правила срабатываний в статусе Интеллектуальное обучение**, вложенной в папку **Хранилища**. Вы можете подтвердить обнаружение как корректное или добавить его в исключения, после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security для Windows.

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В дереве Консоли выберите требуемый узел Сервера администрирования.

2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Статус**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Пусто – если администратор не обработал обнаружение.

   - **Количество срабатываний для всех правил**

     Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

   - **Имя пользователя**

     Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

   - **Путь исходного процесса**

     Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

   - **Хеш исходного процесса**

     Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

  Дата обнаружения аномалии.

Чтобы просмотреть свойства каждого элемента:

1. В дереве Консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области папки **Правила срабатываний в статусе Интеллектуальное обучение** выберите нужный объект.
4. Выполните одно из следующих действий:
   - Перейдите по ссылке **Свойства** в рабочей области в правой части экрана.
   - В контекстном меню объекта выберите пункт **Свойства**.

В открывшемся окне свойства объекта отображается информация объекта.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

Чтобы подтвердить объект,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждение**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в справке Kaspersky Endpoint Security 11 для Windows).

Чтобы добавить объект в исключения,

В контекстном меню объекта (или нескольких объектов) списка обнаружений выберите пункт **Добавить в исключения**.

В результате запустится мастер добавления исключений. Следуйте инструкциям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Вы можете запустить мастер с помощью одного из способов ниже.

Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:

1. В дереве Консоли выберите узел с именем нужного вам Сервера администрирования.
2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области в списке обнаружений в контекстном меню объекта (или нескольких объектов) выберите пункт **Добавить в исключения**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

   В результате запустится мастер добавления исключений. Для продолжения работы мастера нажмите на кнопку **Далее**.

Чтобы запустить мастер добавления исключений из других узлов в дереве консоли:

- Откройте вкладку **События** главного окна Сервера администрирования, затем выберите **Запросы пользователей** или **Последние события**.
- В окне **Отчет о состоянии правил Адаптивного контроля аномалий** выберите столбец **Количество обнаружений**.

Чтобы добавить исключения из правил Адаптивного контроля аномалий с помощью мастера добавления исключений:

1. На первом шаге мастера выберите приложение из списка приложение "Лаборатории Касперского", чьи плагины управления позволяют добавлять исключения в политики для этих приложений.

   Этот шаг можно пропустить, если у вас есть только приложения Kaspersky Endpoint Security для Windows и нет других приложений, поддерживающих правила Адаптивного контроля аномалий.

2. Выберите политики и профили политик, в которые вы хотите добавить исключения.

   Следующий шаг отображает ход обработки политики. Вы можете прервать обработку политики, нажав на кнопку **Отмена**.

   Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика также не будет обновлена.

   Когда все политики обработаны (или обработка политик прервана), создается отчет. Отчет отображает, какие политики были успешно обновлены (зеленый значок), а какие политики не были обновлены (красный значок).

3. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Исключение из правил Адаптивного контроля аномалий настроено и применено.

Панель мониторинга и веб-виджеты

В этом разделе содержится информация о панели мониторинга и веб-виджетах, представленных на панели мониторинга. Раздел содержит инструкции по управлению веб-виджетами и настройке веб-виджетов.

Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в Консоли OSMP: в разделе **Мониторинг и отчеты** → **Панель мониторинга**.

На панели мониторинга представлены настраиваемые веб-виджеты. Вы можете выбрать большое количество различных веб-виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в веб-виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа веб-виджета. Вы можете обновить данные веб-виджета вручную с помощью меню в любое время.

Панель управления включает в себя вкладки **Администрирование и защита** и **Обнаружение и реагирование**, на которые вы можете добавлять веб-виджеты.

Вкладка Администрирование и защита

Вкладка **Администрирование и защита** может содержать веб-виджеты, которые отображают информацию о всех событиях, хранящихся в базе данных Сервера администрирования.

На вкладке **Администрирование и защита** доступны веб-виджеты следующих категорий:

- **Состояние защиты**

- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вкладка Обнаружение и реагирование

Вкладка **Обнаружение и реагирование** может содержать веб-виджеты, которые отображают информацию о зарегистрированных алертах и инцидентах, а также действиях по реагированию на них. Вы можете просматривать данные только для тех тенантов, к которым у вас есть доступ.

На вкладке **Обнаружение и реагирование** доступны веб-виджеты следующих категорий:

- **События**
- **Активные листы**
- **Алерты**
- **Активы**
- **Инциденты**
- **Источники событий**
- **Пользователи**
- **Плейбуки**

Веб-виджеты администрирования и защиты

При настройке вкладки **Администрирование и защита** в панели мониторинга можно добавлять веб-виджеты, скрывать веб-виджеты, а также менять внешний вид или размер веб-виджетов, перемещать веб-виджеты и изменять параметры веб-виджетов.

Некоторые веб-виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

На вкладке **Администрирование и защита** в панели мониторинга доступны следующие категории веб-виджетов и веб-виджеты:

- **Состояние защиты**

  В группу входят следующие веб-виджеты:

  - **История уязвимостей программного обеспечения**
  - **Количество уязвимых устройств**
  - **Распределение устройств по уровню критичности уязвимостей**

- **Статус выбранного устройства**
- **Состояние защиты**

- **Развертывание**

  Эта группа включает в себя веб-виджет **Новые устройства**.

- **Обновления**

  Эта группа включает следующие веб-виджеты:

  - **Статистика обновлений Центра обновления Windows.**
  - **Распространение антивирусных баз.**
  - **Активные алерты.**
  - **Статистика результатов установки обновлений по категории обновления.**
  - **Статистика состояния установки обновлений по категории обновления.**
  - **Статистика состояния установки обновлений.**

- **Статистика угроз**

  Эта группа включает следующие веб-виджеты:

  - **Обнаружение угроз с помощью указанного компонента приложения, отсортированных по результатам их лечения**
  - **Обнаружение угроз компонентами приложения**
  - **Запрещенные приложения**
  - **Типы сетевых атак**
  - **Типы обнаруженных вирусов и результаты лечения**
  - **История помещения файлов на карантин**
  - **История обнаружения возможно зараженных объектов**
  - **История сетевых атак**
  - **История активности угроз по типам приложений**
  - **Активность угроз**
  - **Пользователи 10 наиболее зараженных устройств**
  - **Наиболее зараженные устройства**
  - **Самые заражаемые виртуальные Серверы**
  - **Наиболее распространенные угрозы**
  - **Наиболее заражаемые Windows-домены**

- **Наиболее заражаемые группы**
- **Алерты**

- **Другое**

  Эта группа включает следующие веб-виджеты:

  - **Использование лицензионных ключей**
  - **Уведомления, выбранные по уровню важности**
  - **Десять наиболее частых событий базы данных**
  - **Текущее состояние выбранной задачи Сервера администрирования**
  - **История задачи**

Добавление веб-виджета на информационную панель

Чтобы добавить веб-виджет на информационную панель:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет, который требуется добавить на информационную панель.

   Веб-виджеты сгруппированы по категориям. Чтобы посмотреть, какие веб-виджеты входят в категорию, нажмите на значок шеврона (>) рядом с именем категории.
4. Нажмите на кнопку **Добавить**.

Выбранные веб-виджеты будут добавлены в конец информационной панели.

Можно изменить внешний вид и параметры добавленных веб-виджетов.

Удаление веб-виджета с информационной панели

Чтобы удалить веб-виджет с информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется удалить.
3. Выберите **Скрыть веб-виджет**.
4. В появившемся окне **Предупреждение** нажмите на кнопку **ОК**.

Выбранный веб-виджет будет удален с информационной панели. В дальнейшем можно опять добавить веб-виджет на информационную панель.

Перемещение веб-виджета на информационной панели

Чтобы переместить веб-виджет на информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется переместить.
3. Выберите **Переместить**.
4. Укажите место, куда требуется переместить веб-виджет. Можно выбрать только другой веб-виджет.

Выбранные веб-виджеты поменяются местами.

Изменение размера или внешнего вида веб-виджета

Можно изменить внешний вид веб-виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых веб-виджетов можно изменить размер: маленький, средний или крупный.

Чтобы изменить внешний вид веб-виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется изменить.
3. Выполните одно из следующих действий:
   - Чтобы веб-виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
   - Чтобы веб-виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
   - Чтобы поменять размер области, занимаемой веб-виджетом, выберите одно из значений:
     - **Минимальный**
     - **Минимальный (только линейчатая диаграмма)**
     - **Средний (кольцевой график)**
     - **Средний (линейчатая диаграмма)**
     - **Максимальный**

Внешний вид выбранного веб-виджета будет изменен.

Изменение параметров веб-виджета

Чтобы изменить параметры веб-виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется изменить.
3. Выберите **Показать параметры**.
4. В открывшемся окне параметров веб-виджета измените требуемые параметры веб-виджета.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Параметры выбранного веб-виджета будут изменены.

Набор параметров зависит от конкретного веб-виджета. Ниже приведены некоторые общие параметры:

- **Область веб-виджета** – набор объектов, для которых веб-виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выберите задачу** – задача, для которой веб-виджет отображает информацию.
- **Период** – период, за который отображается информация в веб-виджете; например, между двумя заданными датами, от заданной даты до настоящего времени или за указанное количество дней до настоящего времени.
- **Установить статус "Критический", если** и **Установить статус "Предупреждение", если** – правила, в соответствии с которыми назначаются цвета на графике статусов.

После изменения параметров веб-виджета вы можете обновить данные веб-виджета вручную.

Чтобы обновить данные веб-виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется переместить.
3. Нажмите на кнопку **Обновить**.

Данные веб-виджета обновлены.

Веб-виджеты обнаружения и реагирования

На вкладке **Обнаружение и реагирование** вы можете добавлять, настраивать и удалять веб-виджеты.

Набор веб-виджетов, используемых на вкладке **Обнаружение и реагирование**, называется *макетом*. Все веб-виджеты должны быть размещены на макетах. Open Single Management Platform позволяет создавать, изменять и удалять макеты. Также доступны преднастроенные макеты панели мониторинга. При необходимости вы можете изменять параметры веб-виджета в предварительно настроенных макетах. По умолчанию на вкладке **Обнаружение и реагирование** выбран макет **Обзор алертов**.

Веб-виджет отображает данные за период, выбранный в параметрах веб-виджета или макета, только для тенантов, указанных в параметрах веб-виджета или макета.

Перейдя по ссылке с названием веб-виджета о событиях, алертах, инцидентах или активных листах, вы можете перейти в соответствующий раздел интерфейса Open Single Management Platform. Обратите внимание, что этот параметр недоступен для некоторых веб-виджетов.

На вкладке **Обнаружение и реагирование** в панели мониторинга доступны следующие категории веб-виджетов и веб-виджеты:

- **События**. Веб-виджет для создания аналитики на основе событий.
- **Активные листы**. Веб-виджет для создания аналитики на основе активных листов корреляторов.
- Alerts. Группа для аналитиков, которые работают с алертами. Включает информацию об алертах и инцидентах, предоставляемую Open Single Management Platform.

  В группу входят следующие веб-виджеты:

  - **Активные алерты**. Количество незакрытых алертов.
  - **Активные алерты по тенантам**. Количество незакрытых алертов, сгруппированных по тенантам.
  - **Алерты по тенантам**. Количество алертов всех статусов, сгруппированных по тенантам.
  - **Неназначенные алерты**. Количество алертов, у которых нет исполнителя.
  - **Алерты по статусу**. Количество алертов со статусами Новый, Открыт, Назначен или Эскалирован. Сгруппированы по статусу.
  - **Последние алерты**. Таблица с информацией о последних 10 незакрытых алертах, принадлежащих выбранным в макете тенантам.
  - **Распределение алертов**. Количество алертов, созданных в течение указанного для веб-виджета периода.
  - **Алерты по исполнителю**. Количество алертов со статусом Назначен. Сгруппированы по имени учетной записи.
  - **Алертов по уровню критичности**. Количество незавершенных алертов, сгруппированных по уровню критичности.
  - **Алертов по правилу**. Количество незакрытых алертов, сгруппированных по правилу корреляции.
- **Активы**. Группа для аналитики об активах из обработанных событий. Эта группа включает следующие веб-виджеты:

  - **Затронутые активы в алертах**. Таблица с информацией об активах и количестве незакрытых алертов, которые связаны с этими активами. Переход от веб-виджета к разделу со списком активов недоступен.
  - **Категории затронутых активов**. Категории активов, привязанных к незакрытым алертам.
  - **Количество активов**. Количество активов, добавленных в Open Single Management Platform.
  - **Активы в инцидентах по тенантам**. Количество активов в незакрытых инцидентах. Сгруппированы по тенантам.
  - **Активы в алертах по тенантам**. Количество активов в незакрытых алертах, сгруппированных по тенантам.

- **Инциденты**. Группа для аналитиков, которые работают с инцидентами.

  В группу входят следующие веб-виджеты:

  - **Активные инциденты**. Количество незакрытых инцидентов.
  - **Неназначенные инциденты**. Количество инцидентов со статусом Открыт.
  - **Распределение инцидентов**. Количество инцидентов, созданных в течение указанного для веб-виджета периода.
  - **Инциденты по статусам**. Количество инцидентов, сгруппированных по статусам.
  - **Инцидентов по типу**. Количество инцидентов в любом статусе, сгруппированных по типу.
  - **Активные инциденты по тенантам**. Количество незакрытых инцидентов, сгруппированных по тенантам, доступным пользователю.
  - **Все инциденты**. Количество инцидентов всех статусов.
  - **Все инциденты по тенантам**. Количество инцидентов всех статусов, сгруппированных по тенантам.
  - **Категории активов в инцидентах**. Категории активов, которые затронуты незакрытыми инцидентами.
  - **Последние инциденты**. Таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в макете тенантам.
  - **Инциденты по исполнителю**. Количество инцидентов со статусом Назначен. Сгруппированы по имени учетной записи пользователя.
  - **Инцидентов по уровню критичности**. Количество незавершенных инцидентов, сгруппированных по уровню критичности.
  - **Затронутые активы в инцидентах**. Количество активов в незакрытых инцидентах. Переход от веб-виджета к разделу со списком активов недоступен.
  - **Затронутые в инцидентах пользователи**. Количество пользователей, связанных с инцидентами. Переход от веб-виджета к разделу со списком пользователей недоступен.

- **Источники событий**. Группа для аналитиков, которые работают с событиями. В группу входят следующие веб-виджеты:

  - **Топ источников событий по количеству алертов**. Количество незакрытых алертов, сгруппированных по источникам событий.
  - **Топ источников событий по условному рейтингу**. Количество событий, для которых существует незакрытый алерт, сгруппированных по источникам событий. Группировка осуществляется по источнику событий.

    В некоторых случаях количество алертов, созданных источниками, может быть искажено. Для получения точной статистики рекомендуется в правиле корреляции указать поле события Device Product в качестве уникального, а также включить хранение всех базовых событий в корреляционном событии. Правила корреляции с такими параметрами являются более ресурсоемкими.

- **Пользователи**. Группа для аналитики о пользователях из обработанных событий. В группу входят следующие веб-виджеты:

  - **Затронутые пользователи в алертах**. Количество учетных записей, связанных с незакрытыми алертами. Переход от веб-виджета к разделу со списком пользователей недоступен.

  - **Количество пользователей AD**. Количество учетных записей в Active Directory, полученных по LDAP в течение указанного в веб-виджете периода.

    > В таблице событий, в области сведений о событиях, в окне алертов и в веб-виджетах имена активов, учетных записей и служб отображаются вместо идентификаторов в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID. При экспорте событий в файл идентификаторы сохраняются, но в файл добавляются столбцы с именами. Идентификаторы также отображаются при наведении курсора мыши на названия активов, учетных записей или служб.
    > Поиск полей с идентификаторами возможен только по идентификаторам.

- **Плейбуки**. Группа для аналитиков, которые работают с плейбуками.

  > Для просмотра веб-виджетов в этой группе у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Младший аналитик, Аналитик первого уровня, Аналитик второго уровня, Подтверждающий, Наблюдатель.

  В группу входят следующие веб-виджеты:

  - **Статистика MTTR**. Изменение времени первого действия по реагированию на алерты и инциденты за указанный период времени (по умолчанию 30 дней). Веб-виджет отображает столбчатую диаграмму.

    Доступны следующие параметры конфигурации веб-виджета **Статистика MTTR**:

    - **Тип MTTR:**

      - **Значение**. Изменяет среднее время до первого действия по реагированию на алерт и инциденты.

      - **Минимальный**. Изменяет минимальное время до первого действия по реагированию на алерты и инциденты.

      - **Максимальный**. Изменяет максимальное время до первого действия по реагированию на алерты и инциденты.

    - **Режим реагирования:**

      - **Вручную**. Изменяет время только для первых действий по реагированию вручную.

      - **Автоматически**. Изменяет время только для автоматических первых действий по реагированию.

      - **Все**. Изменяет время на все первые действия по реагированию.

    - **Область действия:**

      - **Алерты**. Изменяет время до первого действия по реагированию только на алерты.

      - **Инциденты**. Изменяет время до первого действия по реагированию только на инциденты.

- **Все**. Изменяет время до первого действия по реагированию на алерты и инциденты.

- **Автоматический и ручной запуск плейбуков**. Общее количество автоматических и ручных запусков плейбуков за определенный период. Веб-виджет отображает столбчатую диаграмму.

  Параметр **Тип запуска** для веб-виджета указывает, следует ли отображать только количество автоматических запусков, только запусков вручную или общее количество запусков плейбуков за определенный период.

  Для веб-виджетов **Статистика MTTR** и **Автоматический и ручной запуск плейбуков** вы также можете установить параметр **Длина сегментов периода**. Этот параметр указывает период, в течение которого будут сгруппированы данные. Вы можете группировать данные за каждый час, каждые 4 часа или каждые 24 часа. На столбчатой диаграмме параметр **Длина сегментов периода** указывает ширину столбца.

- **Покрытие алертов и инцидентов с помощью плейбука**. Количество активных алертов и инцидентов. Вы можете выбрать, какие компоненты отображать: инциденты, алерты или все.

  На кольцевой диаграмме отображаются алерты/инциденты в следующих секторах:

  - Алерты/инциденты, для которых был запущен плейбук в режиме **Автоматический**.
  - Алерты/инциденты, для которых был запущен плейбук в режиме **Обучение**.
  - Все остальные алерты/инциденты.

- **Экономия времени с помощью плейбуков**. Экономия времени за счет запуска всех плейбуков со **статусом Успешно** или Предупреждение.

  По умолчанию веб-виджет не отображается.

Вы можете просмотреть полный список плейбуков, нажав на имя любого веб-виджета плейбука.

Создание веб-виджета

Вы можете создать веб-виджет в макете панели мониторинга во время создания или изменения макета.

Чтобы создать веб-виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Создайте макет или переключитесь в режим редактирования для выбранного макета.
3. Нажмите на кнопку **Добавить веб-виджет**.
4. В раскрывшемся списке выберите тип веб-виджета.

   Откроется окно с параметрами веб-виджета.
5. Измените параметры веб-виджета.
6. Если вы хотите увидеть, как данные будут отображаться в веб-виджете, нажмите на кнопку **Предварительный просмотр**.
7. Нажмите на кнопку **Добавить**.

Веб-виджет появится на макете в панели мониторинга.

Изменение веб-виджета

Чтобы изменить веб-виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на кнопку Изменить ( ).

   Откроется окно **Настройка макета**.
5. В веб-виджете, который вы хотите изменить, нажмите на значок параметров ( ).
6. Выберите **Изменить**.

   Откроется окно с параметрами веб-виджета.
7. Измените параметры веб-виджета.
8. Нажмите на кнопку **Сохранить** в окне свойств веб-виджета.
9. Нажмите на кнопку **Сохранить** в окне **Настройка макета**.

Веб-виджет изменен.

Удаление веб-виджета

Чтобы удалить веб-виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на кнопку Изменить ( ).

   Откроется окно **Настройка макета**.
5. В веб-виджете, который вы хотите удалить, нажмите на значок параметров ( ).
6. Выберите пункт **Удалить**.
7. В открывшемся окне подтверждения нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**.

Веб-виджет удален.

Создание макета панели мониторинга

Чтобы создать макет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Откройте раскрывающийся список в правом верхнем углу окна и выберите **Создать макет**.

   Откроется окно **Новый макет**.

3. В раскрывающемся списке **Тенанты** выберите тенанты, которым будет принадлежать созданный макет и данные которых будут использоваться для заполнения веб-виджетов макета.

   Выбор тенантов в этом раскрывающемся списке не имеет значения, если вы хотите создать универсальный макет (см. ниже).

4. В раскрывающемся списке **Период** выберите период, за который требуется аналитика:

   - **1 час**
   - **1 день** (это значение выбрано по умолчанию)
   - **7 дней**
   - **30 дней**
   - **За период** – получать аналитику за выбранный период. Период устанавливается с помощью календаря, который отображается при выборе этого параметра.

     Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

5. В раскрывающемся списке **Обновлять каждые** выберите частоту обновления данных в веб-виджетах макета:

   - **1 минута**
   - **5 минут**
   - **15 минут**
   - **1 час** (это значение выбрано по умолчанию)
   - **24 часа**

6. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет и настройте его параметры.

   В макет можно добавить несколько веб-виджетов.

   Вы также можете перетаскивать веб-виджеты по окну и изменять их размер с помощью кнопки ⤡, которая появляется при наведении курсора мыши на веб-виджет.

Вы можете изменять или удалять веб-виджеты, добавленные на макет. Для этого нажмите на значок параметров ( ) и выберите пункт **Изменить**, чтобы изменить их конфигурацию, или пункт **Удалить**, чтобы удалить их из макета.

Чтобы добавить веб-виджет:

1. В раскрывающемся списке Добавить веб-виджет выберите нужный веб-виджет.

   Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку Предварительный просмотр.

2. Настройте параметры веб-виджета и нажмите на кнопку Добавить.

Чтобы добавить веб-виджет:

1. В раскрывающемся списке **Добавить веб-виджет** выберите нужный веб-виджет.

   Откроется окно с параметрами веб-виджета. Вы можете увидеть, как будет выглядеть веб-виджет, нажав на кнопку **Предварительный просмотр**.

2. Настройте параметры веб-виджета и нажмите на кнопку **Добавить**.

7. В поле **Имя макета** введите уникальное имя для этого макета. Имя должно содержать от 1 до 128 символов Юникода.

8. При необходимости нажмите на значок параметров ( ) справа от поля названия макета и установите флажки рядом с дополнительными параметрами макета:

   - **Универсальный** – если вы установите этот флажок, веб-виджеты макета будут отображать данные тенантов, которые вы выбрали в разделе **Выбранные тенанты** в меню слева. Это означает, что данные в веб-виджетах макета будут изменяться в зависимости от выбранных вами тенантов без необходимости изменять параметры макета. Для универсальных макетов **тенанты**, выбранные в раскрывающемся списке, не учитываются.

     Если этот флажок снят, веб-виджеты макета отображают данные от тенантов, выбранных в раскрывающемся списке **Тенанты** в параметрах макета. Если какой-либо из выбранных в макете тенантов недоступен для вас, их данные не будут отображаться в веб-виджетах макета.

     Вы не можете использовать веб-виджет Активные листы в универсальных макетах.

     Универсальные макеты может создавать и изменять только пользователь, которому назначена роль Главного администратора. Такие макеты могут просматривать все пользователи.

   - **Показать данные, связанные с CII** – если вы установите этот флажок, веб-виджеты макета также будут отображать данные об активах, алертах и инцидентах, связанных с критической информационной инфраструктурой (КИИ). В этом случае эти макеты будут доступны для просмотра только пользователям, в параметрах которых установлен флажок **Доступ к средствам CII**.

     Если этот флажок снят, веб-виджеты макета не будут отображать данные об активах, алертах и инцидентах, связанных с CII, даже если у пользователя есть доступ к объектам CII.

9. Нажмите на кнопку **Сохранить**.

Макет будет создан и отобразится на вкладке **Обнаружение и реагирования** в панели мониторинга.

Выбор макета панели мониторинга

Чтобы выбрать макет панели мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Выберите соответствующий макет.

Выбранный макет отображается на вкладке **Обнаружение и реагирование** в панели мониторинга.

Выбор макета панели мониторинга по умолчанию

Чтобы установить макет в панели мониторинга по умолчанию:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок звездочка (☆).

Выбранный макет по умолчанию отображается на вкладке **Обнаружение и реагирование** в панели мониторинга.

Изменение макета панели мониторинга

Чтобы изменить макет панели мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок редактирования ( ).

   Откроется окно **Настройка макета**.
5. Измените макет панели мониторинга. Параметры, доступные для изменения, такие же, как и параметры, доступные при создании макета.
6. Нажмите на кнопку **Сохранить**.

Макет панели мониторинга изменен и отображается на вкладке **Обнаружение и реагирование**.

Если макет был удален или назначен другому тенанту во время его изменения, при нажатии на кнопку **Сохранить** отображается ошибка. Макет не сохранен. Обновите страницу интерфейса Open Single Management Platform, чтобы увидеть список доступных макетов в раскрывающемся списке.

Удаление макета панели мониторинга

Чтобы удалить макет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок удаления ( ) и подтвердите это действие.

Макет удален.

Включение и отключение режима ТВ

Для удобного отображения информации на вкладке **Обнаружение и реагирование** вы можете включить режим ТВ. Этот режим позволяет просматривать вкладку **Обнаружение и реагирование** в панели мониторинга в полноэкранном режиме с разрешением FullHD. В режиме ТВ вы также можете настроить отображение слайд-шоу для выбранных макетов.

Рекомендуется для отображения аналитики в режиме ТВ создать отдельного пользователя с минимально необходимым набором прав.

Чтобы включить режим ТВ:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. В правом верхнем углу нажмите на кнопку .

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Включено**.
4. Чтобы настроить показ веб-виджетов в режиме слайд-шоу, выполните следующие действия:
   a. Переведите переключатель **Слайд-шоу** в положение **Включено**.
   b. В поле **Время ожидания** укажите, через сколько секунд должно происходить переключение веб-виджетов.
   c. В раскрывающемся списке **Очередь** выберите веб-виджеты для просмотра. Если макет не выбран, в режиме слайд-шоу по очереди отображаются все доступные пользователю макеты.
   d. Если требуется, измените порядок показа веб-виджетов, перетаскивая их с помощью кнопки .

5. Нажмите на кнопку **Сохранить**.

Режим ТВ включен. Чтобы вернуться к работе с веб-интерфейсом Open Single Management Platform, нужно отключить режим ТВ.

Чтобы отключить режим ТВ:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. В правом верхнем углу нажмите на кнопку .

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Выключено**.
4. Нажмите на кнопку **Сохранить**.

Режим ТВ выключен. В левой части экрана отобразится панель с разделами веб-интерфейса Open Single Management Platform.

Когда вы вносите изменения в макеты, выбранные для слайд-шоу, эти изменения будут автоматически применены к активным сеансам слайд-шоу.

Преднастроенные макеты панели мониторинга

Open Single Management Platform поставляется с набором преднастроенных макетов, которые содержат следующие веб-виджеты:

- Макет **Alerts Overview** (Обзор алертов):
  - Active alerts (Активные алерты) – количество незакрытых алертов.
  - Неназначенные алерты – количество алертов, у которых нет исполнителя.
  - Latest alerts (Последние алерты) – таблица с информацией о последних 10 незакрытых алертах, принадлежащих выбранным в макете тенантам.
  - Alerts distribution (Распределение алертов) – количество алертов, созданных в течение указанного для веб-виджета периода.
  - Alerts by priority (Алерты по приоритету) – количество незакрытых алертов, сгруппированных по приоритету.
  - Alerts by assignee (Алерты по исполнителю) – количество алертов со статусом **Назначен**. Сгруппированы по имени учетной записи.
  - Alerts by status (Алерты по статусу) – количество алертов со статусами **Новый**, **Открыт**, **Назначен** или **Эскалирован**. Сгруппированы по статусу.
  - Affected users in alerts (Затронутые пользователи) – количество пользователей, связанных с алертами со статусами **Новый**, **Назначен** или **Эскалирован**. Сгруппированы по имени учетной записи.

- Affected assets (Затронутые активы) – таблица с информацией об уровне важности активов и количестве незакрытых алертов, с которыми они связаны.
- Affected assets categories (Затронутые категории активов) – категории активов, привязанных к незакрытым алертам.
- Top event source by alerts number (Топ источников событий по количеству алертов) – количество алертов со статусом **Новый**, **Назначен** или **Эскалирован**, сгруппированных по источнику алерты (поле события **DeviceProduct**).

  На веб-виджете отображается не более 10 источников событий.

- Alerts by rule (Количество алертов по правилу) – количество алертов со статусом **Новый**, **Назначен** или **Эскалирован**, сгруппированных по правилам корреляции.

- Макет **Incidents Overview** (Обзор инцидентов):
  - Active incidents (Активные инциденты) – количество незакрытых инцидентов.
  - Unassigned Incidents (Неназначенные инциденты) – количество инцидентов со статусом **Открыт**.
  - Latest Incidents (Последние инциденты) – таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в макете тенантам.
  - Incidents distribution (Распределение инцидентов) – количество инцидентов, созданных в течение указанного для веб-виджета периода.
  - Incidents by priority (Инциденты по уровню важности) – количество незакрытых инцидентов, сгруппированных по уровню важности.
  - Incidents by assignee (Инциденты по исполнителю) – количество инцидентов со статусом **Назначен**. Сгруппированы по имени учетной записи пользователя.
  - Incidents by status (Инциденты по статусам) – количество инцидентов, сгруппированных по статусу.
  - Affected assets in incidents (Активы в инцидентах) – количество активов, связанных с незакрытыми инцидентами.
  - Affected users in incidents (Пользователи в инцидентах) – пользователи, связанные с инцидентами.
  - Affected asset categories in incidents (Категории активов в инцидентах) – категории активов, связанных с незакрытыми инцидентами.
  - Active incidents by tenant (Инциденты по тенантам) – количество инцидентов всех статусов, сгруппированных по тенантам.

- Макет **Network Overview** (Обзор сетевой активности):
  - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внутренним IP-адресам активов.

    На веб-виджете отображается не более 10 IP-адресов.

  - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внешним IP-

адресам активов.

- Netflow top hosts for remote control (Топ активов, на которые были обращения на порты для удаленного управления) – количество событий, связанных с обращением на один из следующих портов: 3389, 22, 135. Данные сгруппированы по именам активов.

- Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика) – количество байт, переданное на внутренние порты активов. Данные сгруппированы по номерам портов.

- Top Log Sources by Events count (Топ источников событий) – 10 источников, от которых было получено наибольшее количество событий.

По умолчанию для преднастроенных макетов указан период обновления **Никогда**. Вы можете изменять эти макеты при необходимости.

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Open Single Management Platform (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором веб-виджетов. Таким образом, пользователь может просматривать указанную в веб-виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.

- Пользователь не может выполнять действия с веб-виджетами, например, добавлять или скрывать их. Поэтому нужно разместить на панели мониторинга все необходимые пользователю веб-виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**.

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Modify object ACLs** в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.

- Пользователь с правом **Чтение** в области **Общие функции: Базовая функциональность**.

Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна на вкладке **Пользователи** в разделе **Пользователи и роли → Пользователи и группы**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга нельзя.

Чтобы настроить режим Просмотра только панели мониторинга:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы** и выберите вкладку **Пользователи**.

2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с веб-виджетами.

3. В открывшемся окне свойств учетной записи выберите вкладку **Панель мониторинга**.

   На открывшейся вкладке отображается та же панель мониторинга, что и для пользователя.

4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также нельзя изменить панель мониторинга. После выключения параметра можно управлять веб-виджетами.

5. Настройте внешний вид панели мониторинга. Набор веб-виджетов, подготовленный на вкладке **Панель мониторинга**, доступен для пользователя с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер веб-виджетов, добавлять или удалять веб-виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. С этой целью на вкладке **Панель мониторинга** можно выполнять те же действия с веб-виджетами, что и в разделе **Мониторинг и отчеты → Панель мониторинга**:

   - Добавлять веб-виджеты на панель мониторинга.
   - Скрывать веб-виджеты, которые не нужны пользователю.
   - Перемещать веб-виджеты в определенном порядке.
   - Изменять размер или внешний вид веб-виджетов.
   - Изменять параметры веб-виджетов.

6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

   После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

   Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Open Single Management Platform, в том числе изменять параметры безопасности и веб-виджеты.

7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.

8. Если пользователь хочет просмотреть статистику поддерживаемых приложений "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права для этого пользователя. После этого

данные приложений "Лаборатории Касперского" отображаются у пользователя в веб-виджетах этих приложений.

Теперь пользователь может входить в Open Single Management Platform под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в Консоли OSMP в разделе **Мониторинг и отчеты** → **Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Open Single Management Platform имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вы можете создавать пользовательские шаблоны отчетов, редактировать шаблоны отчетов и удалять их.

Можно создавать отчеты на основе существующих шаблонов, экспортировать отчеты в файл и создавать задачи рассылки отчетов.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Введите название отчета и выберите тип отчета.

4. На шаге мастера **Область действия** выберите набор клиентских устройств (групп администрирования, выборок устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.

5. На шаге мастера **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:

   - между двумя указанными датами;
   - от указанной даты до даты создания отчета;
   - от даты создания отчета минус указанное количество дней до даты создания отчета.

   В некоторых отчетах эта страница может не отображаться.

6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.

7. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

Чтобы просмотреть и изменить свойства шаблона отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.

2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.

   В качестве альтернативы можно сначала сформировать отчет, а затем нажать на кнопку **Изменить**.

3. Нажмите на кнопку **Открыть свойства шаблона отчета**.

   Откроется окно **Изменение отчета <имя отчета>** на вкладке **Общие**.

4. Измените свойства шаблона отчета:

   - Вкладка **Общие**:
     - Название шаблона отчета
     - Максимальное число отображаемых записей

Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Столбцы → Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

По умолчанию параметр включен. По умолчанию указано значение 1000.

- **Группа**

  Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

- **Период**

  Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

  - между двумя указанными датами;
  - от указанной даты до даты создания отчета;
  - от даты создания отчета минус указанное количество дней до даты создания отчета.

- **Включать данные подчиненных и виртуальных Серверов администрирования**

  Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

  Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

  По умолчанию параметр включен.

- **До уровня вложенности**

  Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

  По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования через заданные интервалы времени (указанные в часах) передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

  По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию параметр выключен.

- Вкладка **Столбцы**

  Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Экспорт отчета в файл

Вы можете сохранить один или несколько отчетов в форматах XML, HTML или PDF. Open Single Management Platform позволяет экспортировать до 10 отчетов в файлы указанного формата одновременно.

Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

Чтобы экспортировать отчет в файл:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Отчеты**.

2. Выберите отчеты, которые вы хотите экспортировать.

   Если вы выберете более десяти отчетов, кнопка **Экспортировать отчет** будет неактивна.

3. Нажмите на кнопку **Экспортировать отчет**.

4. В открывшемся окне настройте следующие параметры экспорта:

   - **Имя файла**.

     Если вы выбрали один отчет для экспорта, укажите имя файла отчета.

     Если вы выбрали несколько отчетов, имена файлов отчетов будут совпадать с именами выбранных шаблонов отчетов.

   - **Максимальное количество записей**.

     Укажите максимальное количество записей, которые будут включены в файл отчета. По умолчанию указано значение 10 000.

     Вы можете экспортировать отчет с неограниченным количеством записей. Обратите внимание, что если ваш отчет содержит большое количество записей, время, необходимое для создания и экспорта отчета, увеличивается.

   - **Формат файла**.

Выберите формат файла отчета: XML, HTML или PDF. При экспорте нескольких отчетов все выбранные отчеты сохраняются в указанном формате в виде отдельных файлов.

Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF подчиненный Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на Сервер администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.

5. Нажмите на кнопку **Экспортировать отчет**.

Отчет будет сохранен в файл в указанном формате.

Генерация и просмотр отчета.

Чтобы сформировать и просмотреть отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

   Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В сформированных отчетах некоторые шрифты могут некорректно отображаться на диаграммах. Чтобы избежать этого, установите библиотеку fontconfig. Также убедитесь, что в операционной системе установлены шрифты, соответствующие языковому стандарту вашей операционной системы.

В отчете отображаются следующие данные:

- На вкладке **Сводная информация**:
  - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
  - графическая диаграмма с наиболее характерными данными отчета;
  - сводная таблица с вычисляемыми показателями отчета.
- На вкладке **Подробнее** отобразится таблица с подробными данными отчета.

Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

Чтобы создать задачу рассылки отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. [Не обязательно] Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Создать задачу рассылки отчетов**.
4. Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. На первой странице мастера укажите имя задачи. По умолчанию используется название **Рассылка отчетов (<N>)**, где <N> – это порядковый номер задачи.
6. На странице параметров задачи в мастере укажите следующие параметры:
   a. Шаблоны отчетов, рассылаемых задачей. Если вы их выбрали на шаге 2, пропустите этот шаг.
   b. Формат отчета: HTML, XLS или PDF.

      > Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

      Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF подчиненный Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на Сервер администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.
   c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.
   d. Будут ли отчеты сохраняться в папку, будут ли перезаписываться сохраненные ранее отчеты в этой папке и будет ли использоваться отдельная учетная запись для доступа к папке (для папки общего доступа).
7. Если требуется изменить другие параметры задачи после ее создания, на странице **Завершение создания задачи** в мастере включите параметр **Открыть окно свойств задачи после ее создания**.
8. Нажмите на кнопку **Создать**, чтобы создать задачу и закрыть мастер.

   Будет создана задача отправки отчета. Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи.

Удаление шаблонов отчетов

Чтобы удалить шаблоны отчетов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Open Single Management Platform, и об управлении блокировкой частых событий.

О событиях в Open Single Management Platform

Open Single Management Platform позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

События по типу

В Open Single Management Platform существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

События по источнику

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими приложениями:

- Компоненты Open Single Management Platform:
  - Сервер администрирования
  - Агент администрирования
- Управляемые приложения "Лаборатории Касперского"

Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

События по уровню важности

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Open Single Management Platform. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

События компонентов Open Single Management Platform

Каждый компонент Open Single Management Platform имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования, Агенте администрирования, Сервере iOS MDM и Сервере мобильных устройств Exchange ActiveSync. Типы событий, которые возникают в приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события**. Этот текст отображается в Open Single Management Platform, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.

- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Open Single Management Platform и при экспорте событий в SIEM-системы.

- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.

- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

  Можно изменить время хранения событий: Настройка срока хранения события.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Критические события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Open Single Management Platform проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются.	180 дней

			• Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Open Single Management Platform определяет правила генерации событий при превышении лицензионного ограничения.	
Устройство стало неуправляемым	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней
Статус устройства "Критический"	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Критический*.	180 дней
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в запрещенный список. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней
Срок действия лицензии скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии. Один раз в день Open Single Management Platform проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Это количество дней невозможно изменить. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Open Single Management Platform работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если	180 дней

			предоплата поставщику услуг была своевременно внесена.	
Срок действия сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истекает срок действия сертификата Сервера администрирования для Управления мобильными устройствами. Вам необходимо обновить сертификат, срок действия которого истекает.	180 дней
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	180 дней
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Open Single Management Platform начинает работать в режиме базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: • Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Open Single Management Platform (добавьте действительный код активации или файл ключа на Сервер администрирования). • Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	180 дней
Обновления модулей приложений "Лаборатории Касперского" отозваны	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	События этого типа возникают, если обновления были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус *Отозвано*. Событие не относится к патчам Open Single Management Platform и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней
Вирусная атака	• 26 (для компонента Защита от файловых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.	

	• 27 (для компонента Защита от почтовых угроз) • 28 (для сетевого экрана)		Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при возникновении этого события.	

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События отказа функционирования Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверьте, не были ли изменены имя пользователя и/или пароль к папке (к папкам). • Проверьте подключение к интернету, так как это может	180 дней

			быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен.	180 дней
Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security,	180 дней

			касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	
Не удалось выполнить опрос облачного сегмента	4143	KLSRV_KLCLOUD_SCAN_ERROR	События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом.	Не хранится

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обнаружено получение частого события		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Open Single Management Platform проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество	90 дней

			устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Open Single Management Platform определяет правила генерации событий при превышении лицензионного ограничения.	
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Консоли OSMP. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли OSMP.	90 дней
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	90 дней
Статус устройства "Предупреждение"	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Предупреждение*.	90 дней

Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно** выключен. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. • Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	90 дней
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится

Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes").	90 дней
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK). Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes"). • Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	90 дней
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Google Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом.	90 дней

			Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	
Мало свободного места на жестком диске	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней
Мало свободного места в базе Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	90 дней
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение.	90 дней

			Одобрите или отклоните обновления с помощью Kaspersky Security Center Web Console.	
Превышено ограничение числа событий, началось удаление событий из базы данных	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится
Превышено ограничение числа событий, удалены события из базы данных	4146	KLSRV_EVP_DB_TRUNCATED	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится
Аудит: Не удалось выполнить проверку подключения к SIEM-серверу	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают при сбое автоматической проверки подключения к SIEM-серверу.	90 дней

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Сервера администрирования

Отображаемое имя	Идентификатор	Тип события	Описание	Срок

типа события	типа события			хранения по умолчанию
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 90% от общего количества лицензионных единиц, охватываемых лицензией. Даже при превышении лицензионных ограничений клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Open Single Management Platform определяет правила генерации событий при превышении лицензионного ограничения.	30 дней
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	События этого типа возникают при обнаружении новых сетевых устройств.	30 дней
Устройство автоматически добавлено в группу	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	События этого типа возникают, если устройства были отнесены к группе в соответствии с правилами перемещения устройств.	30 дней
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	События этого типа возникают, если устройства были перемещены в группы администрирования в соответствии с правилами перемещения устройств.	30 дней
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	События этого типа возникают, когда устройства были автоматически удалены из группы из-за неактивности.	30 дней
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	События этого типа возникают при изменении токена Firebase Cloud Messaging на устройстве. Информацию о ротации токенов FCM см. в документации сервиса Firebase.	30 дней

Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	События этого типа возникают, когда задача Загрузка обновлений в хранилище Сервера администрирования завершает копирование файлов в указанную папку.	30 дней
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Подробнее см. в статье Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования.	30 дней
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 дней
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED		30 дней
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	События этого типа возникают, когда задача Загрузка обновлений в хранилище Сервера администрирования завершает обновление базы данных.	30 дней
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT		30 дней
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.	30 дней
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	Например, это событие возникает, если задача завершилась ошибкой.	30 дней
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	События этого типа возникают при изменении группы безопасности.	30 дней
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT		30 дней
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер;	30 дней

			• виртуальный Сервер.	
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED		30 дней
Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования	5100	KLAUD_EV_DPEKEYSEXPORT	Например, это событие происходит во время переноса данных.	30 дней
Аудит: Проверка подключения к SIEM-серверу выполнена успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS	События этого типа возникают при успешном подключении к SIEM-серверу.	30 дней

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURED	События этого типа возникают при обнаружении инцидента на устройстве. Например, это событие возникает, когда на устройстве мало места на диске.	30 дней
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	События этого типа возникают при сбое тестового соединения для настроенного подключения прокси-сервера KSN.	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Например, события этого типа возникают, когда отклоняется Лицензионное соглашение для установки обновлений приложений сторонних производителей.	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней
Возвращено предупреждение во время установки	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте	30 дней

обновления модулей приложений			значение поля KLRI_PATCH_RES_DESC.	
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WRN	Общее событие предупреждения.	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	События этого типа возникают, если есть несовпадение между файлом sudoers и референсным файлом.	30 дней

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней
Обновление для приложений стороннего производителя установлено успешно	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней
Запущена установка обновления модулей приложений	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: предоставлен	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней

Совместный доступ к рабочему столу Windows: завершен	7716	KLUSRLOG_EV_WDS_END	30 дней
Файл sudoers успешно восстановлен до референсного значения	7725	KLNAG_EV_SUDOER_RESTORED	30 дней
Корневой сертификат установлен	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 дней
Корневые сертификаты удалены	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 дней
Веб-Сервер запущен на устройстве	—	WEB_SERVER_STARTED	30 дней
Веб-Сервер остановлен на устройстве	—	WEB_SERVER_STOPPED	30 дней

Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Консоли OSMP.

Выборки событий доступны в Консоли OSMP в разделе **Мониторинг и отчеты** → **Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Open Single Management Platform имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**
  - **Предупреждения.**
  - **Информационные сообщения.**
- **Запросы пользователей** (события управляемых приложений).
- **Последние события** (за последнюю неделю).
- [События аудита](#).

В Open Single Management Platform отображаются события аудита, связанные с операциями службы в Консоли OSMP. Эти события обусловлены действиями специалистов "Лаборатории Касперского". Такие события, например, включают: вход на Сервер администрирования; изменение портов Сервера администрирования; резервное копирование данных Сервера администрирования; создание, изменение и удаление учетных записей пользователей.

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий. В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию приложения и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Open Single Management Platform отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

Вы можете выполнить следующее:

- Изменить параметры выборки событий.
- Сгенерировать выборки событий.
- Просмотреть сведения о выбранных выборках событий.
- Удалить выборки событий.
- Удалить события из базы данных Сервера администрирования.

Создание выборки событий

Чтобы создать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры новой выборки событий. Параметры можно указать в нескольких разделах этого окна.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.
5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к результатам выборки**.
6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

Если был установлен флажок **Перейти к результатам выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

Изменение выборки событий

Чтобы изменить выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.
3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.
4. Отредактируйте свойства выборки событий.

   > Для стандартной выборки событий можно редактировать свойства только на следующих вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

   Для пользовательских выборок можно редактировать все свойства.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

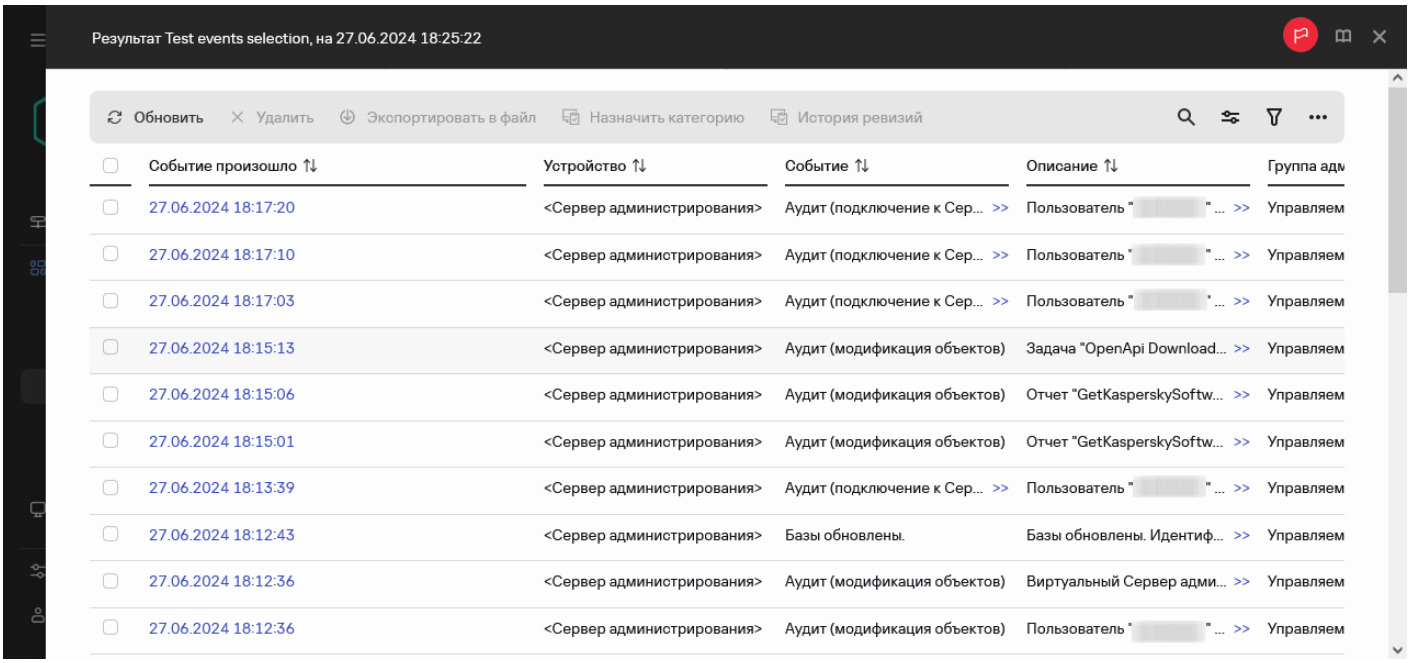
Измененная выборка событий отображается в списке.

Просмотр списка выборки событий

Просмотр выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:
   - Чтобы настроить сортировку для результатов выборки событий:
     a. Нажмите на кнопку **Изменить сортировку и запустить**.
     b. В отобразившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.
     c. Нажмите на имя выборки.
   - В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.



Результат выборки событий

Экспорт выборки событий

Open Single Management Platform позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Open Single Management Platform (предопределенные выборки), не может быть сохранен в файл.

Чтобы экспортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется экспортировать.

   Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя и путь к файлу выборки событий, а затем нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл выборки событий автоматически сохраняется в папку **Загрузки**.

Импорт выборки событий

Open Single Management Platform позволяет импортировать выборку событий из файла KLO. Файл KLO содержит экспортированную выборку событий и ее параметры.

Чтобы импортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.
3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

   Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр информации о событии

Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий.
2. Нажмите на требуемое событие.

   Откроется окно **Свойства события**.
3. В открывшемся окне можно выполнить следующие действия:
   - Просмотреть информацию выбранного события.
   - Перейти к следующему или к предыдущему событию в списке – результате выборки событий.
   - Перейти к устройству, на котором возникло событие.
   - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
   - Для события, связанного с задачей, перейдите в свойства задачи.

Экспорт событий в файл

Чтобы экспортировать события в файл:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **Экспортировать в файл**.

   Выбранные события экспортированы в файл.

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями, вы можете перейти к истории ревизий объекта.

Чтобы просмотреть историю объекта из события:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

   Откроется история ревизий объекта.

Удаление событий

Чтобы удалить одно или несколько событий:

1. Запустите выборку событий.
2. Установите флажки рядом с требуемыми событиями.
3. Нажмите на кнопку **Удалить**.

   Выбранные события удалены и не могут быть восстановлены.

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

Чтобы удалить выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**.

Выборка событий будет удалена.

Настройка срока хранения события

Open Single Management Platform позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике приложения "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного периода.

Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Выполните одно из следующих действий:

   - Чтобы настроить срок хранения событий Агента администрирования или управляемого приложения "Лаборатории Касперского" нажмите на имя соответствующей политики.

     Откроется страница свойств политики.

   - Чтобы настроить события Сервера администрирования, в главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

     Если у вас есть политика для Сервера администрирования, вы можете нажать на название этой политики.

     Откроется страница свойств Сервера администрирования (или страница свойств политики Сервера администрирования).

3. Выберите вкладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий.

4. Выберите раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.

5. В списке типов событий на правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.

   В открывшемся окне в разделе **Регистрация событий** включите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

6. В поле редактирования под переключателем укажите количество дней для сохранения события.

7. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

   Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования Kaspersky Security Center, вы не сможете изменить значение срока хранения события.

8. Нажмите на кнопку **ОК**.

   Окно свойств политики закроется.

Теперь, когда Сервер администрирования получает и сохраняет события выбранного типа, они будут иметь измененный срок хранения. Сервер администрирования не изменяет срок хранения ранее полученных событий.

Блокировка частых событий

В этом разделе представлена информация об управлении блокировкой частых событий и об отмене блокировки частых событий.

О блокировке частых событий

Управляемое приложение, например Kaspersky Endpoint Security для Windows, установленное на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных.

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Чтобы узнать, заблокировано ли событие, вы можете просмотреть список уведомлений или просмотреть, присутствует ли это событие в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку частых событий.

Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете разблокировать и продолжать получать частые события. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

Чтобы управлять блокировкой частых событий:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Заблокированные частые события**.

3. В разделе **Заблокированные частые события**:

   - Если вы хотите разблокировать прием частых событий:

     a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.

     b. Нажмите на кнопку **Сохранить**.

   - Если вы хотите заблокировать прием частых событий:

     a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировано**.

     b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

Чтобы отменить блокировку частых событий:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Заблокированные частые события**.

3. В разделе **Заблокированные частые события** нажмите строку частого события, для которого вы хотите отменить блокировку.

4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

Обработка и хранение событий на Сервере администрирования

Информация о событиях в работе приложения и управляемых устройств сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

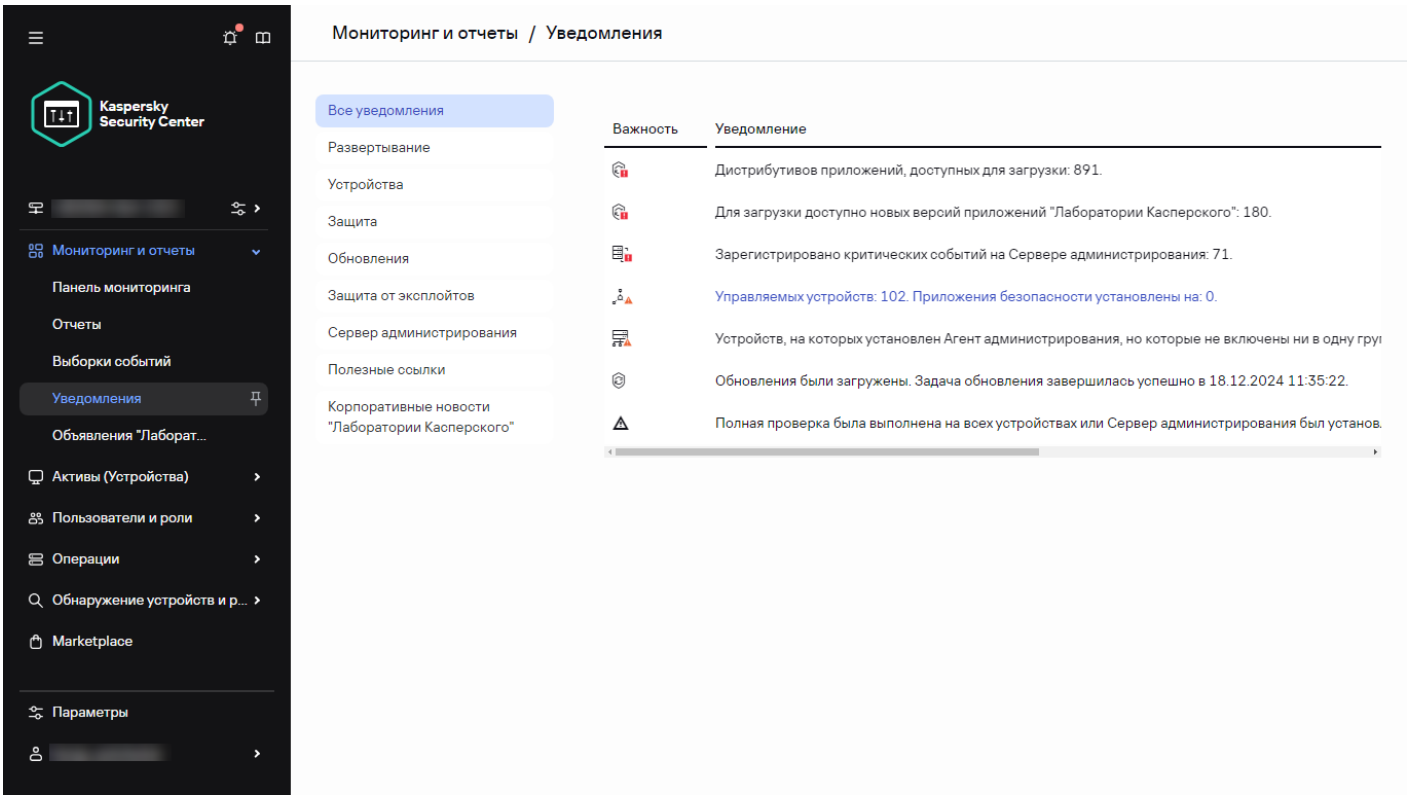
Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

Уведомления и статусы устройств

В этом разделе содержится информация о том, как просматривать уведомления, настраивать доставку уведомлений, использовать статусы устройств и включать изменение статусов устройств.

Использование уведомлений

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.



Список уведомлений

В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- экранные уведомления;
- уведомление по SMS;
- уведомление по электронной почте;
- уведомление запуском исполняемого файла или скрипта.

Экранные уведомления

Экранные уведомления предупреждают вас о событиях, сгруппированных по уровням важности (*Критическое уведомление*, *Предупреждающие уведомление*, и *Информационное уведомление*).

Экранные уведомления могут иметь один из двух статусов:

- *Просмотрено*. Это означает, что вы выполнили рекомендованное действие для уведомления или вы назначили этот статус для уведомления вручную.
- *Не просмотрено*. Это означает, что вы не выполнили рекомендуемое действие для уведомления или не назначили этот статус для уведомления вручную.

По умолчанию в список уведомлений входят уведомления со статусом *Не просмотрено*.

Вы можете контролировать сеть вашей организации, просматривая уведомления на экране и отвечая на них в режиме реального времени.

Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта

Open Single Management Platform позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомления по электронной почте, SMS или запустив исполняемый файл или скрипт.

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

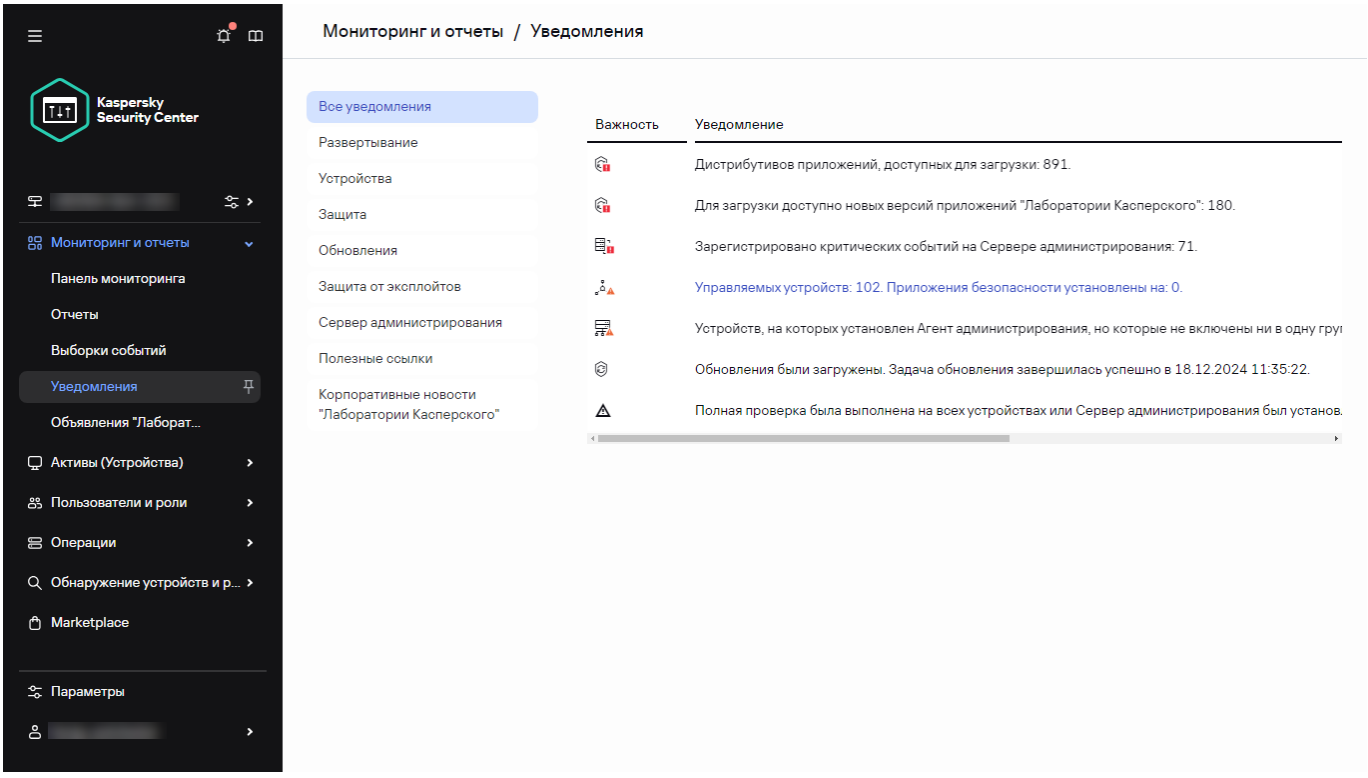
- В разделе **Мониторинг и отчеты → Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.
- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.
- В веб-виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг и отчеты → Панель мониторинга**. В этом веб-виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

Чтобы просмотреть уведомления предопределенной категории:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Уведомления**.

   На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.



Список уведомлений

2. На левой панели выберите одну из следующих категорий:

- **Развертывание**
- **Устройства**
- **Защита**
- **Обновления** (сюда входят уведомления о доступных для загрузки приложениях "Лаборатории Касперского" и уведомления о загруженных обновлениях антивирусных баз)
- **Защита от эксплойтов**
- **Сервер администрирования** (это уведомление включает в себя события, относящиеся только к Серверу администрирования)
- **Полезные ссылки** (сюда входят ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию)
- **Корпоративные новости "Лаборатории Касперского"** (сюда входит информация о выпусках приложений "Лаборатории Касперского")

В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления** (), **Предупреждающие уведомления** (), **Информационные уведомления**. Уведомления в списке сгруппированы по уровню важности.
- **Уведомление**. Здесь содержится описание уведомления.
- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу и установить приложение безопасности на устройства, просмотреть список устройств или список событий. После того, как вы выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено*.
- **Зарегистрированный статус**. Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:

1. Нажмите на значок флага () в правом верхнем углу Консоли OSMP.

   Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

   Откроется окно со списком уведомлений. По умолчанию выбрана вкладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите вкладку **Система**.

   Отображается список уведомлений с уровнями важности *Критические уведомления* () и *Предупреждающие уведомления* (). Список уведомление включает следующее:

- Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.
- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления(), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Описание уведомления.
- Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.
- Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите вкладку **Больше**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на вкладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

Чтобы просмотреть экранные уведомления на веб-виджете:

1. В разделе **Панель мониторинга** выберите **Добавить или восстановить веб-виджет**.
2. В открывшемся окне нажмите на категорию **Другие**, выберите веб-виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку Добавить.

   Веб-виджет отображается на вкладке **Панель мониторинга**. По умолчанию на веб-виджете отображаются уведомления с уровнем важности *Критическое*.

   Вы можете нажать на кнопку **Параметры** на веб-виджете и изменить параметры веб-виджета, чтобы просмотреть уведомления с уровнем важности *Предупреждающие уведомления*. Или вы можете добавить другой веб-виджет: **Уведомления, выбранные по уровню важности** с уровнем важности *Предупреждающие уведомления*.

   Список уведомлений на веб-виджете ограничен размером и включает только два уведомления. Эти два уведомления относятся к последним событиям.

Список уведомлений веб-виджета включает следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Описание уведомления со ссылкой на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.
- Ссылка на другие уведомления. Перейдите по ссылке к просмотру уведомлений в разделе **Уведомления** в разделе **Мониторинг и отчеты**.

О статусах устройства

Open Single Management Platform присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Open Single Management Platform учитывает видимость устройства в сети (см. таблицу ниже). Если Open Single Management Platform не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический/Видим в сети*.
- *Предупреждение* или *Предупреждение/Видим в сети*.
- *OK* или *OK/Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.

Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача *Синхронизация обновлений Windows Update* больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.

Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлено*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Переключатель выключен. • Переключатель включен.

Open Single Management Platform позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Open Single Management Platform с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Open Single Management Platform присваивает устройству статус, для некоторых условий (см. столбец "Описание условий" в таблице выше) учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

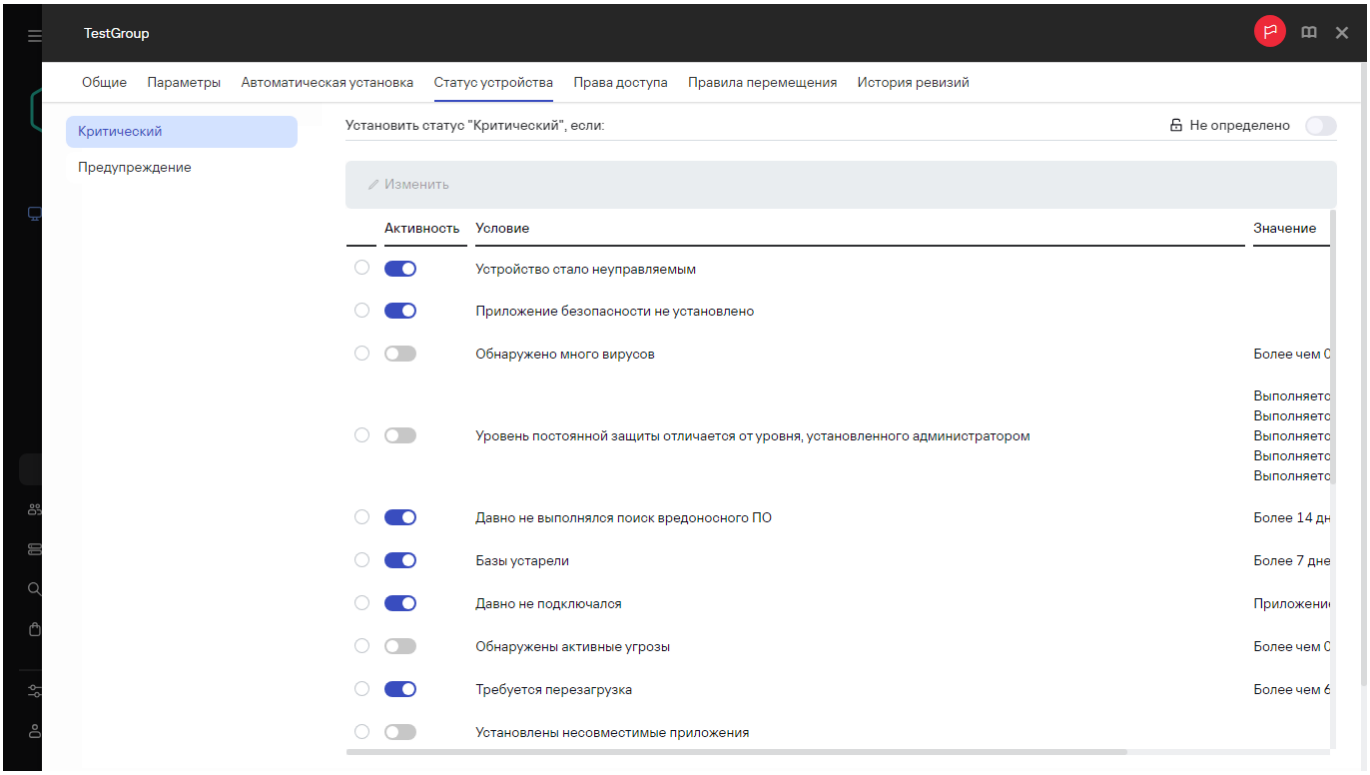
1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.

3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Критический**.

5. В блоке **Установить статус "Критический", если** включите условие, чтобы переключить устройство в состояние *Критическое*.



> Однако вы можете изменить параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

При невыполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.

3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Предупреждение**.

5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Однако вы можете изменить параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

При невыполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Настройка параметров доставки уведомлений

Вы можете настроить уведомления о событиях, возникающих в Open Single Management Platform. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события приложение Open Single Management Platform посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события приложение Open Single Management Platform посылает уведомления на указанные номера телефонов.
- Исполняемый файл – при возникновении события исполняемый файл запускается на Сервере администрирования.

Чтобы настроить параметры доставки уведомлений о событиях, возникших в Open Single Management Platform:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Уведомление** и на правой панели выберите вкладку с требуемым способом уведомления:

   - Электронная почта

На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Open Single Management Platform проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Open Single Management Platform не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер с сертификатом в формате PKCS#12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

По нажатию на кнопку **Отправить тестовое сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **Тема** укажите тему электронной почты. Вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, автоматически отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Внимание: не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры с подробными данными события.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

- SMS

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать файл сертификата SMTP-сервера, перейдя по ссылке **Задать сертификаты**:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Open Single Management Platform проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Open Single Management Platform не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **Тема** укажите тему электронной почты.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Внимание: не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый приложением при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

Если выбран этот способ уведомления, в поле ввода можно указать, какое приложение будет запущено при возникновении события.

В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится. Перед указанием файла подготовьте файл и укажите подстановочные параметры, которые определяют сведения о событии, которые будут отправлены в сообщении. Указанные папка и файл должны находиться на Сервере администрирования.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

3. На вкладке настройте параметры уведомлений.

4. Нажмите на кнопку **OK**, чтобы закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Open Single Management Platform.

Можно изменить значения параметров доставки уведомлений для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

Чтобы проверить распространение уведомлений о событиях:

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Затем снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с тестовым "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

Чтобы открыть запись об обнаружении тестового "вируса":

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.

2. Нажмите на название выборки **Последние события**.

   В открывшемся окне отображается уведомление о тестовом "вирусе".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR.

Уведомление о событиях с помощью исполняемого файла

Open Single Management Platform позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору (см. таблицу ниже).

Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Возникшая ошибка** • **Критическое**
%COMPUTER%	Имя устройства, на котором произошло событие. Максимальная длина имени устройства – 256 символов.
%DOMAIN%	Доменное имя устройства, на котором произошло событие.
%EVENT%	Название типа события. Максимальная длина названия типа события – 50 символов.
%DESCR%	Описание события. Максимальная длина описания – 1000 символов.
%RISE_TIME%	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Имя задачи. Максимальная длина имени задачи – 100 символов.
%KL_PRODUCT%	Название приложения.

%KL_VERSION%	Номер версии приложения.
%KLCSAK_EVENT_SEVERITY_NUM%	Номер уровня важности события. Возможные значения: • 1 – **Информационное сообщение** • 2 – **Предупреждение** • 3 – **Error** • 4 – **Критическое**
%HOST_IP%	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	IP-адрес подключения устройства, на котором произошло событие.

Пример:
Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

Об объявлениях "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Open Single Management Platform и управляемых приложениях, установленных на управляемых устройствах. Open Single Management Platform периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Open Single Management Platform показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

  Объявления, связанные с безопасностью, предназначены для того, чтобы приложения "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для приложений "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в приложениях "Лаборатории Касперского". По умолчанию объявления, связанные с безопасностью, включены. Если вы не хотите получать объявления, вы можете отключить эту функцию.

Чтобы показать вам информацию, которая соответствует вашей конфигурации защиты сети, Open Single Management Platform отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при установке Сервера администрирования Kaspersky Security Center.

- Рекламные объявления.

  Рекламные объявления включают информацию о специальных предложениях для ваших приложений "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

  Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Open Single Management Platform отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN.

Информация разделена на следующие категории по важности:

1. Критическая информация.
2. Важная новость.
3. Предупреждение.
4. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" Консоли OSMP отображает метку уведомления, соответствующую уровню важности объявлений. Вы можете нажать на метку, чтобы просмотреть это объявление в разделе Объявления "Лаборатории Касперского".

Вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и место отображения метки уведомления. Если вы не хотите получать объявления, вы можете отключить эту функцию.

Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и где отображать метку уведомления.

Чтобы настроить объявления "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Объявления "Лаборатории Касперского"**.
2. Перейдите по ссылке **Параметры**.

   Откроется окно объявлений "Лаборатории Касперского".
3. Задайте следующие параметры:

   - Выберите уровень важности объявлений, которые вы хотите просматривать. Объявления других категорий отображаться не будут.

- Выберите расположение, где вы хотите видеть метку уведомления. Метка может отображаться во всех разделах консоли или в разделе **Мониторинг и отчеты** и его подразделах.

4. Нажмите на кнопку **ОК**.

   Параметры объявлений "Лаборатории Касперского" настроены.

Выключение объявлений "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Open Single Management Platform и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

Чтобы выключить объявления, связанные с безопасностью:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.

3. Переведите переключатель в положение **Объявления, связанные с безопасностью**, выключено.

4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Чтобы отключить объявления:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Выключите параметр **Использовать Kaspersky Security Network Включено**.

4. Нажмите на кнопку **Сохранить**.

   Объявления выключены.

Cloud Discovery

Open Single Management Platform позволяет контролировать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к облачным сервисам, которые вы считаете нежелательными. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Блокировать доступ можно только, если вы активировали Open Single Management Platform по лицензии Open Single Management Platform EDR Optimum или XDR Expert.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.
- Вы приобрели лицензию на Kaspersky Next, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробнее см. справку Kaspersky Next.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в веб-виджете Cloud Discovery и в отчетах Cloud Discovery. Веб-виджет также показывает уровень риска каждого облачного сервиса. Open Single Management Platform получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности или профилями, в которых они включены.

Включение функции Cloud Discovery с помощью веб-виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security для Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью веб-виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security для Windows.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security для Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы включить функцию Cloud Discovery с помощью веб-виджета Cloud Discovery:

1. Перейдите в Консоль Open Single Management Platform.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
3. В веб-виджете **Cloud Discovery** нажмите на кнопку **Включить**.

   Если у вас установлен Kaspersky Endpoint Security для Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows. Подробнее см. раздел Cloud Discovery справки Kaspersky Endpoint Security для Windows.

   Если у вас версия Kaspersky Endpoint Security для Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security для Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

   Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, веб-виджет добавлен в панель мониторинга.

Добавление веб-виджета Cloud Discovery в панель мониторинга

Вы можете добавить веб-виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить веб-виджет Cloud Discovery в панель инструментов, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы добавить веб-виджет Cloud Discovery в панель мониторинга:

1. Перейдите в Консоль Open Single Management Platform.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
4. В списке доступных веб-виджетов нажмите на значок шеврона (›) рядом с категорией **Другое**.
5. Выберите веб-виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью веб-виджета.

Выбранный веб-виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Веб-виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Веб-виджет также показывает уровень риска каждого облачного сервиса. Open Single Management Platform получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Перед просмотром убедитесь, что:

- Веб-виджет Cloud Discovery добавлен в панель мониторинга.
- Функция Cloud Discovery включена.
- У вас есть право **Чтение** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы посмотреть веб-виджет Cloud Discovery:

1. Откройте Консоль Open Single Management Platform.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

   Веб-виджет **Cloud Discovery** отображается в панели мониторинга.
3. В левой части веб-виджета **Cloud Discovery** выберите категорию облачных сервисов.

   В таблице в правой части веб-виджета отображается до пяти сервисов из выбранной категории, к которым пользователи чаще всего пытаются получить доступ. Учитываются как успешные, так и заблокированные попытки доступа.
4. В правой части веб-виджета выберите требуемый сервис.

   В таблице ниже отображается до десяти устройств, наиболее часто обращающихся к этому сервису. В этой таблице вы можете сформировать два типа отчетов: отчет об успешных попытках доступа и отчет о заблокированных попытках доступа.

   Также в этой таблице вы можете заблокировать доступ к облачной службе для определенного устройства.

В веб-виджете отображаются запрашиваемые данные.

В отображаемом веб-виджете можно выполнить следующие действия:

- Перейдите в раздел **Мониторинг и отчеты** → **Отчеты**, чтобы просмотреть отчеты Cloud Discovery.
- Заблокируйте или разрешите доступ к выбранному облачному сервису.

Блокировать доступ можно только, если вы активировали Open Single Management Platform по лицензии Open Single Management Platform EDR Optimum или XDR Expert.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Уровень риска облачного сервиса

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить службы, не соответствующие требованиям безопасности вашей организации. Например, вы можете принять во внимание уровень риска при принятии решения о блокировке доступа к определенной службе.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных служб отображаются в веб-виджете Cloud Discovery и в списке всех контролируемых облачных служб.

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью веб-виджета Cloud Discovery.

  В этом случае вы можете заблокировать доступ к сервисам по очереди.

- В свойствах политики Kaspersky Endpoint Security для Windows.

  В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows.

Чтобы заблокировать или разрешить доступ к облачному сервису с помощью веб-виджета:

1. Откройте веб-виджет Cloud Discovery и выберите требуемый облачный сервис.
2. В панели **Топ-10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.
3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:

- Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.
- Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.

4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Сценарий: настройка экспорта событий в SIEM-системы

Open Single Management Platform позволяет настроить экспорт событий в SIEM-системы одним из следующих способов: экспорт в любую SIEM-систему, использующую формат Syslog, или экспорт событий в SIEM-системы непосредственно из базы данных Kaspersky Security Center. После завершения этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

Предварительные требования

Перед началом настройки экспорта событий в Open Single Management Platform:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что у вас есть значения системных параметров.

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- **Настройка SIEM-системы для получения событий из Open Single Management Platform**

  Инструкции: Настройка экспорта событий в SIEM-системе.

- **Выбор событий, которые вы хотите экспортировать в SIEM-систему**

  Отметьте события, которые вы хотите экспортировать в SIEM-систему. Отметьте общие события, которые возникают во всех управляемых приложениях "Лаборатории Касперского". Затем можно отметить события для экспорта для определенных управляемых приложений.

- **Настройка экспорта событий в SIEM-систему**

  Экспортировать события можно следующими способами:

  - Укажите протоколы TCP/IP, UDP или TLS over TCP.
  - Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта, если вы выбрали события, которые хотите экспортировать.

Предварительные условия

При настройке автоматического экспорта событий в Open Single Management Platform необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Open Single Management Platform.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

Об экспорте событий

Open Single Management Platform позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться на панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Open Single Management Platform во внешние SIEM-системы участвуют две стороны: отправитель событий – Open Single Management Platform и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Open Single Management Platform. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Open Single Management Platform, а затем получение событий в SIEM-системе, либо наоборот.

Экспорт событий в формате Syslog

Вы можете отправлять события в формате Syslog в любую SIEM-систему. Используя формат Syslog, вы можете передавать любые события, произошедшие на Сервере администрирования и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий в формате Syslog можно выбирать, какие именно события будут переданы в SIEM-систему.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Open Single Management Platform. Для этого необходимо выполнить настройку SIEM-системы. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Open Single Management Platform во внешние SIEM-системы участвуют две стороны: отправитель событий – Open Single Management Platform и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Open Single Management Platform.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Open Single Management Platform. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта**

  Протокол передачи сообщений UDP, TCP или TLS, over TCP. Необходимо указать тот же протокол, который был выбран в Open Single Management Platform для передачи событий.

- **Порт**

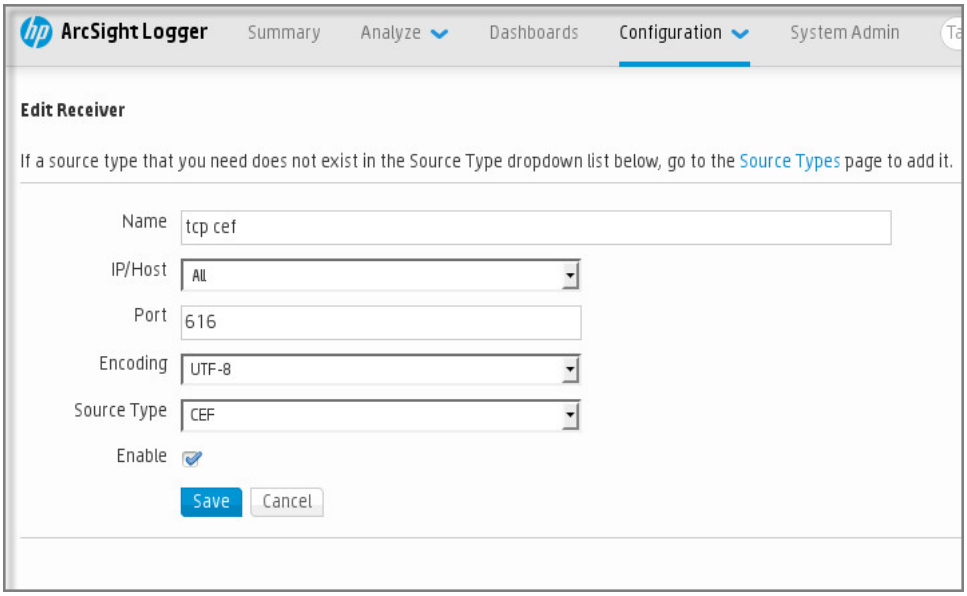
  Укажите номер порта для подключения к Open Single Management Platform. Этот порт должен совпадать с портом, который вы указываете в Open Single Management Platform при настройке экспорта событий в SIEM-систему.

- **Формат даты**

  Укажите формат Syslog.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.



Настройка приемника в ArcSight

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание, параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Open Single Management Platform, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

Выбор событий для экспорта в SIEM-системы в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемой этой политикой.

- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

О выборе событий для экспорта в SIEM-систему в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемой этой политикой.

- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенном управляемом приложении, установленном на управляемых устройствах, выберите события для экспорта политике приложения. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

Чтобы отметить события для экспорта для определенного управляемого приложения:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Выберите политику приложения, для которого нужно отметить события.

   Откроется окно свойств политики.

3. Перейти в раздел **Настройка событий**.

4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемого приложения готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике приложения, вам не удастся переопределить выбранные события для управляемого устройства.

Чтобы выбрать события для управляемого устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.

   Откроется окно свойств выбранного устройства.

3. Перейти в раздел **Приложения**.

4. Перейдите по ссылке с названием требуемого приложения в списке приложений.

5. Перейдите в раздел **Настройка событий**.

6. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

7. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

8. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

Выбор общих событий для экспорта в формате Syslog

Вы можете отметить общие события, которые Сервер администрирования будет экспортировать в SIEM-системы, используя формат Syslog.

Чтобы выбрать общие события для экспорта в SIEM-систему:

1. Выполните одно из следующих действий:

   - В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.
   - В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**, а затем перейдите по ссылке политики.

2. В открывшемся окне выберите вкладку **Настройка событий**.

3. Нажмите **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

4. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других приложениях "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 используется для экспорта событий из Open Single Management Platform во внешние системы.

В Open Single Management Platform можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Open Single Management Platform таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Open Single Management Platform начинается сразу после включения автоматического экспорта.

2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

Настройка Open Single Management Platform для экспорта событий в SIEM-систему

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Open Single Management Platform.

Чтобы настроить экспорт в SIEM-системы из Консоли OSMP:

1. В главном меню нажмите на значок параметров (⚙) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **SIEM**.

3. Перейдите по ссылке **Параметры**.

   Откроется раздел **Параметры экспорта**.

4. Укажите параметры в разделе **Параметры экспорта**:

   - **Адрес сервера SIEM-системы**

     Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

   - **Порт SIEM-системы**

     Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

   - **Протокол**

     Выберите протокол передачи сообщений в SIEM-систему. Можно выбрать протокол TCP/IP или UDP. Протокол TCP/IP является более надежным и поддерживает уведомление о получении сообщений. Протокол UDP является более простым, он применяется в случаях, когда проверка и исправление ошибок передачи сообщений не обязательны или выполняются внутри приложения.

5. Вы можете экспортировать заархивированные события из базы данных Сервера администрирования и установить дату начала, с которой вы хотите начать экспорт заархивированных событий:

   a. Перейдите по ссылке **Установите дату начала экспорта**.

   b. В открывшемся разделе, укажите дату начала экспорта в поле **Дата начала экспорта**.

   c. Нажмите на кнопку **OK**.

6. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы Включено**.

7. Чтобы убедиться, что соединение с SIEM-системой успешно настроено, нажмите на кнопку **Проверить подключение**.

   Отобразится статус подключения.

8. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует выбранные события в SIEM-систему. Если вы установите дату начала экспорта, Сервер администрирования также экспортирует выбранные события, хранящиеся в базе данных Сервера администрирования, с указанной даты.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Open Single Management Platform, не используя интерфейс Open Single Management Platform. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Open Single Management Platform предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Open Single Management Platform, например, устройствам, приложениям, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по созданию SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Open Single Management Platform, например, имя инстанса и имя базы данных, приведена в соответствующем разделе.

Создание SQL-запроса с помощью утилиты klsql2

В этой статье приведены инструкции по использованию утилиты klsql2, а также по созданию SQL-запроса с использованием этой утилиты. Используйте версию утилиты klsql2, которая входит в вашу установленную версию Open Single Management Platform.

Чтобы использовать утилиту klsql2:

1. Перейдите в папку установки Сервера администрирования Open Single Management Platform Administration. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
2. В этой папке создайте пустой файл src.sql.
3. Откройте файл src.sql с помощью любого текстового редактора.
4. В файле src.sql введите требуемый SQL-запрос и сохраните файл.
5. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:

   ```
   sudo ./klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```

   где `<имя пользователя>` и `<пароль>` являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.
6. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.
7. Откройте созданный файл result.xml и посмотрите результаты выполнения запроса.

Вы можете редактировать файл src.sql и создавать в нем любые запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить запрос и сохранить результаты в файл.

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

Пример:

```
SELECT
e.nId,                                                  /* идентификатор события */
e.tmRiseTime,                                           /* время возникновения события */
e.strEventType,                                         /* внутреннее имя типа события */
e.wstrEventTypeDisplayName,                             /* отображаемое имя события */
e.wstrDescription,                                      /* отображаемое описание события */
e.wstrGroupName,                                        /* имя группы устройств */
h.wstrDisplayName,                                      /* отображаемое имя устройства, на котором произошло
событие */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp            /* IP-адрес устройства, на котором произошло событие */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Просмотр имени базы данных Open Single Management Platform

Для доступа к базе данных Open Single Management Platform с помощью MySQL или MariaDB необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

Чтобы просмотреть имя базы данных Open Single Management Platform:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Информация об используемой базе данных**.

Имя базы данных указано в поле **Имя базы данных**. Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

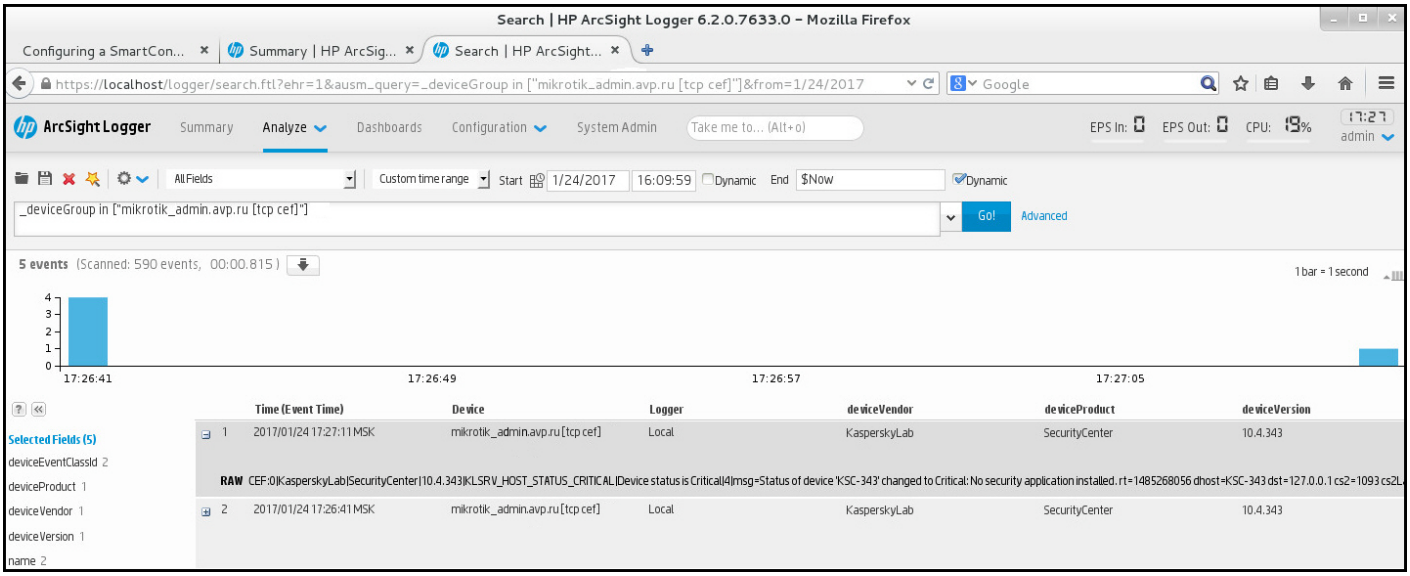
Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Open Single Management Platform события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Open Single Management Platform и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.



Пример событий

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Open Single Management Platform позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия*. Каждая ревизия имеет номер.

Объекты приложения, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (доступно только для политик);
- откатывать изменения объекта к выбранной ревизии;

- сохранять ревизии в виде файла JSON (доступно только для политик).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес Консоли OSMP, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Просмотр и сохранение ревизии политики

Open Single Management Platform позволяет просмотреть, какие изменения были внесены в политику за определенный период, и сохранить информацию об этих изменениях в файле.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью Консоли OSMP невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта выберите вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

   Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

Удаление объектов

В этом разделе описано, как удалять объекты и просматривать информацию объектов после того, как они были удалены.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации удаленных объектов такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии права на **Изменение** для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Open Single Management Platform обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.

- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств.

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

  > При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить выбранные устройства** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

  Чтобы расшифровать диск требуется выполнение следующих условий:

  - Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.

  - Пользователь устройства помнит пароль для расшифровки.

  - Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено на устройстве.

  Если диск был зашифрован с помощью технологии Kaspersky Disk Encryption, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Open Single Management Platform обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

Загрузка и удаление файлов из Карантина и Резервного хранилища

В этом разделе представлена информация о том, как загрузить и удалить файлы из Карантина и Резервного хранилища в Консоли OSMP.

Загрузка файлов из Карантина и Резервного хранилища

Вы можете загрузить файлы из Карантина и Резервного хранилища, только если выполняется одно из двух условий: либо включен параметр **Не разрывать соединение с Сервером администрирования** в свойствах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск:

1. Выполните одно из следующих действий:

   - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Карантин**.

   - Если вы хотите сохранить копию файла из Резервного хранилища, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Резервное хранилище**.

2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Загрузить**.

   Начнется загрузка. Копия файла, помещенного в Карантин на клиентском устройстве, сохраняется в указанную папку.

Об удалении объектов из Карантина, Резервного хранилища или Активных угроз

Когда приложения безопасности "Лаборатории Касперского", установленные на клиентских устройствах, помещают объекты на Карантин, в Резервное хранилище или Активные угрозы, они передают информацию о добавленных объектах в разделы **Карантин**, **Резервное хранилище** или **Активные угрозы** в Open Single Management Platform. При открытии одного из этих разделов выберите объект из списка и нажмите на кнопку **Удалить**, Open Single Management Platform выполняет одно из следующих действий или оба действия:

- Удаляет выбранный объект из списка.

- Удаляет выбранный объект из хранилища.

Действие, которое необходимо выполнить, определяется приложением "Лаборатории Касперского", поместившим выбранный объект в хранилище. Приложение "Лаборатории Касперского" указано в **поле** Запись добавлена. Подробную информацию о том, какое действие необходимо выполнить, см. в документации к приложению "Лаборатории Касперского".

Операции по диагностике компонентов Open Single Management Platform

В этом разделе описано, как получить диагностическую информацию о компонентах Open Single Management Platform.

Получение диагностической информации о компонентах Open Single Management Platform

KDT позволяет получать диагностическую информацию о компонентах Open Single Management Platform и кластере Kubernetes, устранять проблемы самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Чтобы получить диагностическую информацию о компонентах Open Single Management Platform и веб-плагинах управления,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt logs get <flags>
```

Где `<flags>` – параметры команды, которая позволяет настроить результат сохранения событий.

Вы можете указать следующие параметры ведения журнала событий:

- `--app <список_компонентов>` – получить диагностическую информацию для перечисленных компонентов Open Single Management Platform.
- `--auto-dest-dir` – получить журналы событий и сохранить их в директории kdt-default-logs-<current_date_and_time>, которая автоматически создается в текущей директории. Если период хранения событий не указан, вы будете получать диагностическую информацию за последний час.

  Например, если вы хотите получить журналы событий за последний час для Сервера администрирования и KUMA и сохранить эти журналы событий в автоматически созданной директории, выполните следующую команду:

  ```
  ./kdt logs get --app ksc,kuma --auto-dest-dir
  ```

- `-d, --destination <путь_к_файлу>` – получить журналы событий и сохранить их в указанном файле.
- `-D, --destination-dir <путь_к_директории>` – получить журналы событий и сохранить их в указанной директории, которая должна быть создана заранее. Если параметр `<directory_path>` пуст, журналы событий сохраняются в стандартном потоке вывода (stdout). Если период хранения событий не указан, вы будете получать диагностическую информацию за последний час.
- `--to-archive` – получить журналы событий и сохранить их в kdt-default-logs-<current_date_and_time>.tar.gz. Созданный архив сохраняется в текущей директории. Если период хранения событий не указан, вы будете получать диагностическую информацию за последний час.
- `--last=<часы>h` – получить журналы событий за указанное количество часов в актуальном состоянии.

  Например, если вы хотите получить архив с журналами за последние три часа, выполните следующую команду:

  ```
  ./kdt logs get --to-archive --last=3h
  ```

- `--start=<дата_и время>` – получить журналы событий, начиная с указанной даты и времени (в формате Unix timestamp) до настоящего времени или до даты и времени, указанных в параметре `--end`.

  Например, если вы хотите получить журналы с 26.03.2024 10:00:00 по настоящее время и сохранить их в директории kdt-default-logs-<current_date_and_time>, созданной в текущей директории, выполните следующую команду:

```
./kdt logs get --auto-dest-dir --start=1711447200
```

- `--end=< дата_и_время >` – получить журналы событий, начиная с даты и времени, указанных в параметре `--start`, до даты и времени, указанных в параметре `--end` (в формате Unix timestamp). Если параметр `--start` не указан, журналы событий будут получены за последний час до даты и времени, заданных параметром `--end`.

  Например, если вы хотите сохранить журналы событий за 10 минут (с 26.03.2024 10:00:00 до 26.03.2024 10:10:00) в директории журналов событий, выполните следующую команду:

  ```
  ./kdt logs get -D ./logs/ start=1711447200 --end=1711447800
  ```

Чтобы просмотреть доступные флаги, вы можете выполнить одну из следующих команд:

- `./kdt logs get -h`
- `./kdt logs get --help`

Просмотр метрик OSMP

OSMP позволяет контролировать метрики для дальнейшего анализа работоспособности и производительности его компонентов.

Вы можете просмотреть метрики OSMP одним из следующих способов:

- Используя веб-адрес `<monitoring_host>.<smp_domain>`.

  В этом случае вам необходимо просматривать метрики с помощью Grafana, инструмента для визуализации данных, который устанавливается вместе с Open Single Management Platform. Чтобы получить доступ к метрикам с помощью Grafana, вам нужно указать учетные данные Grafana в конфигурационном файле (параметры `grafana_admin_user` и `grafana_admin_password`).

- Используя свои инструменты.

  В этом случае вам необходимо настроить инструменты для получения метрик с адреса API – <api_host>.<smp_domain>/metrics.

Параметры `<api_host>` и `<monitoring_host>` являются именами устройств, `<smp_domain>` является доменным именем. Эти параметры представляют собой FQDN служб Open Single Management Platform и устанавливаются в конфигурационном файле при развертывании Open Single Management Platform.

Open Single Management Platform предоставляет свои метрики в формате OpenMetrics.

> Если вы хотите просмотреть информацию о производительности Ядра KUMA, хранилища, коллекторов и коррелляторов, вам необходимо просмотреть метрики KUMA.

Хранение диагностической информации о компонентах Open Single Management Platform

Диагностическая информация о компонентах Open Single Management Platform хранится на рабочем узле кластера Kubernetes. Объем дискового пространства, необходимый для хранения этой информации, указывается в конфигурационном файле перед развертыванием Open Single Management Platform (параметр `loki_size`).

Чтобы проверить объем дискового пространства, на котором хранится диагностическая информация о компонентах Open Single Management Platform,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду:

```
./kdt invoke observability --action getPvSize
```

Отображается объем выделенного свободного места на диске в гигабайтах.

Вы также можете увеличить дисковое пространство, используемое для хранения диагностической информации о компонентах Open Single Management Platform после установки Open Single Management Platform. Вы не можете установить объем дискового пространства меньше указанного ранее.

Чтобы увеличить дисковое пространство, используемое для хранения диагностической информации о компонентах Open Single Management Platform,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите необходимое свободное место на диске в гигабайтах (например, "50Gi"):

```
./kdt invoke observability --action setPvSize --param loki_size="
<новый_объем_дискового_пространства>Gi"
```

Объем свободного дискового пространства, выделяемого для хранения диагностической информации о компонентах Open Single Management Platform, изменен.

Получение файлов трассировки

KDT позволяет получать файлы трассировки для компонентов OSMP, чтобы устранять проблемы инфраструктуры самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Файлы трассировки загружаются в формате OpenTelemetry.

Чтобы получить файл трассировки для OSMP:

1. На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите путь к файлу, в который вы хотите сохранить список файлов трассировки:

   ```
   ./kdt traces find -o <output_file_path>
   ```

   Список файлов трассировки с их идентификаторами выводится в указанный файл.

2. Чтобы вывести конкретный файл трассировки, выполните следующую команду и укажите путь к выходному файлу и идентификатор файла трассировки:

   ```
   ./kdt traces get -o <output_file_path> --trace-id=<trace_ID>
   ```

   Указанный файл трассировки сохранен.

Запись событий запусков пользовательских действий

KDT позволяет получить историю запуска пользовательского действия для конкретного компонента Open Single Management Platform, а также журналы событий запуска определенного пользовательского действия. Полученные журналы событий могут помочь вам исследовать проблемы с работой компонентов Open Single Management Platform самостоятельно или с помощью Службы технической поддержки "Лаборатории Касперского".

Чтобы получить историю запусков пользовательских действий для конкретного компонента Open Single Management Platform, выполните следующие действия:

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя компонента:

```
./kdt state -H <component_name>
```

Отображается список выполненных пользовательских действий с их идентификаторами.

Чтобы получить журналы событий запуска настраиваемого действия,

На устройстве администратора, на котором расположена утилита KDT, выполните следующую команду и укажите имя компонента и идентификатор запуска пользовательского действия:

```
./kdt state -l <component_name> -m <custom_action_launch_ID>
```

Отобразятся журналы событий запуска указанного пользовательского действия.

Мультитенантность

Open Single Management Platform поддерживает мультитенантный режим. Этот режим позволяет главному администратору предоставлять функциональность Open Single Management Platform нескольким клиентам независимо или разделять активы, параметры приложения и объекты для разных офисов. Каждый клиент или офис изолирован от других и называется тенантом.

Обычно режим мультитенантности используется в следующих случаях:

- Поставщик услуг имеет несколько клиентских организаций и хочет предоставить функциональность Open Single Management Platform каждой клиентской организации в отдельности. Для этого администратор поставщика услуг может создать тенант для каждой клиентской организации.
- Администратор крупного предприятия может захотеть изолировать параметры активов и приложений и объекты для офисов или подразделений организации и управлять офисами или подразделениями организации независимо. Для этого администратор может создать тенант для каждого офиса или подразделения.

Мультитенантный режим имеет следующие особенности:

- Изоляция тенантов.
- Межтенантные сценарии.

Изоляция тенантов

Тенант изолирован и управляется независимо от других тенантов. Только пользователи, которым назначены права доступа к тенанту, могут работать с этим тенантом и управлять им. Администратор другого тенанта не может получить доступ к данным, ресурсам и активам тенанта, если только главный администратор не предоставит соответствующие права доступа администратору в явном виде.

Для каждого тенанта вы определяете ряд объектов, в том числе следующие:

- Активы

  Список активов уникален для каждого тенанта. Каждый актив может принадлежать только одному тенанту.
- Пользователи и их права доступа.
- События, алерты и инциденты.
- Плейбуки.
- Интеграция с другими приложениями и службами "Лаборатории Касперского", а также с решениями сторонних производителей.

Межтенантные сценарии

Все тенанты организованы в иерархию тенантов. По умолчанию иерархия тенантов содержит предварительно созданный корневой тенант вверху иерархии. Никакие другие тенанты не могут быть созданы на том же уровне, что и корневой тенант. Вы создаете тенант в качестве дочернего по отношению к любому существующему тенанту, включая корневой тенант. Иерархия тенантов может иметь любое количество уровней вложенности.

Иерархия тенантов используется для предоставления кросс-тенантных сценариев, включая следующие:

- Наследование и копирование

  Дочерний тенант получает от родительского тенанта следующие объекты:

  - Пользователи и их права доступа.

    Права доступа наследуются по иерархии и не могут быть отозваны на более низком уровне иерархии.

  - Параметры тенанта, включая параметры интеграции и плейбуки.

    Параметры тенанта и плейбука копируются из родительского тенанта в его дочерний тенант. После создания дочернего тенанта вы можете настроить скопированные параметры в соответствии с требованиями нового тенанта.

- Лицензирование

  Лицензионный ключ для Open Single Management Platform применяется на уровне главного Сервера администрирования, который привязан к корневому тенанту. Далее лицензионный ключ автоматически применяется ко всем тенантам в иерархии.

Роли пользователей

Open Single Management Platform предоставляет вам заранее определенный набор ролей пользователей. Вы предоставляете пользователям права на управление тенантами, назначая пользователям роли.

Роли пользователей	Права пользователей		
	Чтение	Запись	Удаление
Главный администратор	✓	✓	✓
Администратор тенанта	✓	✓	✓
Администратор SOC	✓	✓	—
Аналитик 1-го уровня	✓	—	—
Аналитик 2-го уровня	✓	—	—
Младший аналитик	✓	—	—
Менеджер SOC	✓	—	—
Подтверждающий	✓	—	—
Наблюдатель	✓	—	—
Работа с НКЦКИ	✓	—	—

Тенанты и Серверы администрирования Kaspersky Security Center

Вы можете привязать тенанты к Серверам администрирования Kaspersky Security Center, физическим или виртуальным. Связь между тенантом и Сервером администрирования позволяет объединить возможности обоих решений – Kaspersky Symphony XDR и Open Single Management Platform.

Фильтр тенантов в интерфейсе приложения

В интерфейсе Open Single Management Platform вы можете настроить списки объектов для отображения только тех объектов, которые относятся к выбранным тенантам. Фильтр тенантов применяется к следующим объектам:

- Алерты в разделе **Алерты**.

- Инциденты в разделе **Инциденты**.
- События в разделе **Поиск угроз**.
- Плейбуки в разделе **Плейбуки**.

Когда вы применяете фильтр тенантов, новые параметры применяются ко всем типам объектов в интерфейсе и на обеих консолях – в Консоли OSMP и в Консоли KUMA.

О привязке тенантов к Серверам администрирования

Вы можете привязать тенанты к Серверам администрирования Kaspersky Security Center. Связь между тенантом и Сервером администрирования позволяет связать активы, которыми управляет Сервер администрирования, с тенантом.

Вы не можете привязывать тенанты к виртуальным Серверам администрирования, только к физическим.

У тенантов могут быть субтенанты, поэтому они организованы в иерархию тенантов. Серверы администрирования могут иметь подчиненные Серверы администрирования, поэтому они организованы в иерархию Серверов. Вы не можете привязать произвольный тенант к произвольному Серверу, поскольку это может привести к недопустимой привязке. Например, пользователь может не иметь прав доступа к тенанту в иерархии тенантов, но тот же пользователь может иметь права доступа к устройствам этого тенанта. Это может произойти, если у этого пользователя есть права доступа к Серверу администрирования 2, который является главным для Сервера администрирования 1, привязанного к тенанту. Следовательно, по умолчанию этот пользователь унаследовал права доступа к Серверу администрирования 1 и его управляемым устройствам. Чтобы исключить такую ситуацию, привязывать тенанты и Серверы администрирования друг к другу можно только в соответствии с правилами привязки.

Есть два типа привязок:

- Явная привязка.

  Этот тип привязки устанавливается при выборе Сервера администрирования, к которому вы хотите привязать тенант.

- Унаследованная привязка.

  Когда вы устанавливаете явную привязку к Серверу администрирования, у которого есть подчиненные Серверы администрирования, подчиненные Серверы администрирования привязываются к тенанту через унаследованный тип привязки. Таким образом, тенант может быть привязан к нескольким Серверам администрирования.

Правила привязки:

- Корневой тенант всегда привязан к корневому Серверу администрирования. Вы не можете удалить эту привязку.
- Тенант может быть не привязан к Серверу администрирования. У такого тенанта могут быть субтенанты, и эти субтенанты могут быть привязаны к Серверам администрирования.
- Вы можете привязать два Сервера администрирования, которые организованы в иерархию, только к двум тенантам, которые также организованы в иерархию, и только если иерархия Серверов администрирования совпадает с иерархией тенантов.

- Сервер администрирования может быть привязан только к одному тенанту явно или через унаследованный тип привязки.
- При явной привязке тенанта к Серверу администрирования:
  - Если Сервер администрирования был привязан к другому тенанту явно, эта привязка автоматически удаляется.
  - Если у Сервера администрирования есть подчиненные Серверы администрирования, подчиненные Серверы администрирования привязываются к новому тенанту через унаследованный тип привязки, за исключением тех Серверов администрирования, которые были привязаны к своим тенантам явно. Перед этой операцией Open Single Management Platform проверяет, все ли новые привязки законны. В противном случае привязка не может быть установлена.
- При удалении явной привязки между тенантом и Сервером администрирования (отмена привязки Сервера администрирования) Сервер администрирования и все его подчиненные Серверы администрирования (если есть) автоматически привязываются через унаследованный тип привязки к тенанту, к которому привязан главный Сервер администрирования выбранного Сервера администрирования. Если некоторые из подчиненных Серверов администрирования привязаны к своим тенантам явно, эти Серверы администрирования сохраняют свои привязки.
- При добавлении нового Сервера администрирования в иерархию этот Сервер администрирования автоматически привязывается через унаследованный тип привязки к тенанту, к которому привязан его главный Сервер администрирования.
- Когда вы удаляете Сервер администрирования из иерархии и Сервер администрирования имеет явную привязку к тенанту, эта привязка удаляется.

Настройка интеграции с Open Single Management Platform

Вы можете привязать тенанты к Серверам администрирования Kaspersky Security Center. Связь между тенантом и Сервером администрирования позволяет связать активы, которыми управляет Сервер администрирования, с тенантом.

Вы не можете привязывать тенанты к виртуальным Серверам администрирования, только к физическим.

Предварительные условия:

- Убедитесь, что вы знакомы с правилами привязки.
- Вы создали тенант, который хотите привязать к Серверу администрирования.
- При необходимости вы добавили подчиненный Сервер администрирования, который хотите привязать к тенанту.

Чтобы привязать тенант к Серверу администрирования или удалить его привязку от Сервера, у вас должна быть роль, которая предоставляет право на **Запись** в функциональных областях Тенанты и Интеграции.

Привязка тенанта к Серверу администрирования

Чтобы привязать тенант к Серверу администрирования:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** установите флажок рядом с тенантом, который вы хотите привязать к Серверу администрирования, а затем нажмите на кнопку **Привязать Сервер администрирования**.

4. В открывшемся окне выберите Сервер администрирования, который вы хотите привязать к тенанту.

   Если вы хотите добавить новый Сервер в иерархию или удалить существующий, вы можете сделать это в свойствах Сервера администрирования.

5. Нажмите на кнопку **Привязать**.

Процесс привязки может занять некоторое время. Вы можете отслеживать этот процесс в столбце **Статус привязки** списка Серверов администрирования в окне свойств тенанта.

Удаление привязки тенанта к Серверу администрирования

Чтобы удалить привязку тенанта к Серверу администрирования:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** установите флажок рядом с тенантом, для которого вы хотите удалить привязку к Серверу администрирования, а затем нажмите на кнопку **Удалить привязку**.

Просмотр и изменение тенантов

Вы можете использовать тенанты, чтобы предоставлять функциональность Open Single Management Platform клиентской организации независимо или разделять активы и параметры приложения и объекты для разных офисов.

Чтобы просмотреть или изменить свойства тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

Откроется окно свойств тенанта. Если у вас есть права доступа только для **Чтения** к этому тенанту, свойства будут открыты в режиме только для чтения. Если у вас есть право на **Запись**, вы сможете изменять свойства тенанта.

3. Измените свойства тенанта и нажмите на кнопку **Сохранить**.

Свойства тенанта изменены и сохранены.

Общие

Вкладка **Общие** содержит общую информацию о тенанте. Вы можете изменить имя и описание тенанта.

Параметры

Вкладка **Параметры** содержит следующие разделы:

- **Интеграции с приложениями "Лаборатории Касперского"**

  В этом разделе вы можете настроить параметры интеграции приложений "Лаборатории Касперского", которые вы хотите интегрировать в Open Single Management Platform для текущего тенанта.

- **Интеграция со сторонними приложениями**

  В этом разделе вы можете настроить параметры интеграции для сторонних приложений, которые вы хотите интегрировать в Open Single Management Platform для текущего тенанта.

- **Обнаружения и реагирование**

  В этом разделе можно настроить параметры и объекты, связанные с обнаружением угроз и реагированием на них:

  - Срок хранения

    Сроки хранения алертов и инцидентов зависят от лицензии Open Single Management Platform, которую вы используете.

  - Плейбуки
  - Шаблоны электронных писем
  - Правила сегментации
  - Подключение к почтовому серверу

Вам не нужно настраивать параметры общего тенанта.

Роли

На вкладке **Роли** перечислены пользователи, имеющие права доступа к тенанту. Вы можете изменить этот список и назначить пользователям роли.

Добавление тенантов

Прежде чем начать, ознакомьтесь с общей информацией о тенантах.

Чтобы добавлять дочерние тенанты, у вас должны быть права на **Чтение** и **Запись** в функциональной области **Тенанты** в родительском тенанте или в тенанте более высокого уровня в иерархии тенантов.

Чтобы добавить тенант:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Установите флажок рядом с родительским тенантом. Новый тенант будет создан как дочерний по отношению к выбранному тенанту.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Добавить тенант** введите имя нового тенанта.
5. При необходимости добавьте описание тенанту.
6. Нажмите на кнопку **Добавить**.

Новый тенант появится в списке тенантов.

Дочерний тенант наследует от родительского тенанта следующие объекты:

- пользователей и их права доступа;
- параметры интеграции.

После создания тенанта вы можете перенастроить унаследованные объекты в соответствии с требованиями нового тенанта.

Назначение ролей пользователям тенанта

Вы можете назначать XDR-роли пользователям Open Single Management Platform, чтобы предоставить им наборы прав доступа в тенанте.

Для этого у вас должна быть одна из следующих XDR-ролей в тенанте, в котором вы хотите назначить роли пользователям: Главный администратор, Администратор SOC или Администратор тенанта.

Так как тенанты изолированы и управляются независимо от других тенантов, только пользователи, которым назначены права доступа к тенанту, могут работать с этим тенантом и управлять им.

Права доступа наследуются по иерархии и не могут быть отозваны на более низком уровне иерархии.

Чтобы назначить роли пользователю в тенанте:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Роли пользователей** и нажмите на кнопку **Добавить пользователя**.

4. В открывшемся окне выполните следующие действия:

   a. В поле **Пользователь** введите имя пользователя или адрес электронной почты.

   b. Установите флажки рядом с ролями, которые вы хотите назначить пользователю.

      При необходимости вы можете выбрать несколько ролей.

   c. Нажмите на кнопку **Добавить**.

   Окно закрывается, и пользователь отображается в списке пользователей.

5. Нажмите на кнопку **Сохранить**.

Пользователь добавлен в тенант, и ему назначены роли. При необходимости вы можете изменить роли пользователей, нажав на имя пользователя и выполнив действия, описанные в шагах 4–5.

Удаление тенантов

За один раз можно удалить только один тенант. Если у выбранного тенанта есть дочерние тенанты, они также будут удалены. Обратите внимание, что плейбуки, связанные с тенантами, будут удалены, а информация об алертах и инцидентах, связанных с тенантом, станет недоступной.

Чтобы удалить тенант, у вас должны быть права на **Чтение** и **Запись** в функциональной области **Тенанты** в выбранном тенанте.

Невозможно удалить следующие тенанты:

- Корневой тенант.
- Тенанты, которые были перенесены из интегрированных приложений (например, Kaspersky Unified Monitoring and Analysis Platform) и отмечены в этих приложениях как не подлежащие удалению.

Чтобы удалить тенант:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Установите флажок напротив тенанта, который требуется удалить. Если у выбранного тенанта есть дочерние тенанты, они будут выбраны автоматически, и отменить их выбор невозможно.

3. Нажмите на кнопку **Удалить**.

4. Чтобы подтвердить операцию, введите имя тенанта, который вы хотите удалить. Если у тенанта есть дочерние тенанты, они также будут перечислены как тенанты, подлежащие удалению.

Выбранный тенант и его дочерние тенанты (если есть) удалены.

Настройка подключения к SMTP

Вы можете настроить уведомления по электронной почте о событиях, происходящих в Open Single Management Platform, через Сервер администрирования Kaspersky Security Center и внешний SMTP-сервер. Для этого необходимо настроить параметры подключения к SMTP-серверу.

Чтобы настроить подключение к SMTP-серверу:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Список тенантов отображается на экране.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры** и в разделе **Обнаружение и реагирование** нажмите на **Подключение к почтовому серверу**.

4. В правой панели нажмите на кнопку **Просмотреть свойства**.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

   В окне отображаются свойства главного Сервера администрирования и параметры SMTP для главного Сервера администрирования независимо от того, к какому Серверу администрирования привязан тенант.

5. Настройте параметры, как описано в шаге 2 Настройка параметров доставки уведомлений.

После настройки подключения к SMTP-серверу пользователи начнут получать электронные письма от Open Single Management Platform.

Настройка шаблонов уведомлений

После того как вы настроите подключение к SMTP-серверу, вы можете настроить шаблоны для отправки уведомлений по электронной почте о событиях, возникающих в Open Single Management Platform.

Чтобы изменить шаблоны уведомлений, вам нужно иметь одну из следующих XDR-ролей: Главный администратор, Администратор тенанта или Администратор SOC.

Когда вы разворачиваете Open Single Management Platform, у вас есть шаблоны для уведомлений по электронной почте в корневом тенанте. Если вы создаете дочерний тенант, он автоматически копирует параметры родительского тенанта. Так как параметры дочернего тенанта и родительского не связаны, изменения, которые вы вносите в параметры дочернего тенанта, не влияют на параметры родительского тенанта и наоборот.

Чтобы настроить шаблоны уведомлений для отправки по электронной почте:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Отобразится список тенантов.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Выберите вкладку **Параметры** и в разделе **Обнаружение и реагирование** нажмите на **Шаблоны электронных писем**.

4. В правой панели в поле **Введите имя сервера** укажите адрес, который будет использоваться в ссылках на алерты и инциденты в электронных письмах.

   Также отображается таблица типов событий, для которых вы можете настроить шаблоны уведомлений. В таблице содержатся следующие типы событий:

   - **Создание алерта**
   - **Назначение алерта оператору**
   - **Автоматическое создание нового инцидента**
   - **Назначение инцидента оператору**

5. В таблице в столбце **Тип события** нажмите на название шаблона уведомления, который вы хотите изменить.

6. В открывшемся окне **Изменить шаблон электронной почты** выполните следующие действия:

   - Если вы хотите включить уведомления по электронной почте для выбранного типа события, переведите переключатель в положение **Включено** в поле **Статус**.

     По умолчанию уведомления по электронной почте выключены. Вы также можете включить уведомления по электронной почте из таблицы типов событий. Для этого переведите переключатель в положение **Включено**.

   - В поле **Тема** укажите тему электронного письма.

     Вы можете получить доступ к полям алертов, полям инцидентов, нормализованным полям событий KUMA, например, `New incident in OSMP: {{ .InternalID }}, {{ .Name }}`.

   - В поле **Шаблон** напишите текст уведомления по электронной почте.

     Пример уведомления по электронной почте

```
Hello,<br>
<br>
Alert {{ .InternalID }}{{ with escapeHTML .Rules.Names }} "{{ . }}"{{ else }}{{ end }} was registered
at {{ .CreatedAt }}.<br>
<br>
Details on alert:<br>
<br>
Tenant: {{ .TenantID }}<br>
Alert severity: {{ .Severity }}<br>
Alert first seen: {{ .FirstEventTime }}<br>
Alert last seen: {{ .LastEventTime }}<br>
Full information about the alert is available in OSMP web-interface: {{ link_alert . }}<br>
<br>
Open Single Management Platform
```

Вы можете получить доступ к полям алертов, полям инцидентов, нормализованным полям событий KUMA и использовать HTML-теги.

При написании шаблона вы можете использовать следующие функции:

- `date` – определяет формат даты и времени. Функция принимает время в миллисекундах (UNIX-время) в качестве первого параметра. Второй параметр может быть использован для передачи времени в формате стандарта RFC. Часовой пояс невозможно изменить.

- `range` – обращается к вложенным объектам. Некоторые поля алертов содержат массивы данных с полями алертов, содержащими связанные события, активы и учетные записи пользователей. Функция range последовательно обращается к полям первых 50 вложенных объектов. Если вы используете функцию range для запроса поля, которое не содержит массив данных, возвращается ошибка. **Пример использования функции range**

  ```
  {{range .Events }}
  Service name: {{.Event.ServiceName}}
  Device host name: {{.Event.DeviceHostName}}
  Message: {{.Event.Message}}
  {{end}}
  ```

  Вложенные объекты могут иметь свои собственные вложенные объекты. Вы можете получить доступ к ним с помощью вложенных функций range.

- `limit` – ограничивает количество объектов, возвращаемых функцией range.

- `link_alert` – генерирует ссылку на алерт с указанным URL в поле **Введите имя сервера**.

- `link_incident` – генерирует ссылку на инцидент с указанным URL в поле **Введите имя сервера**.

- `link` – принимает форму ссылки, которую пользователь может открыть, когда он получает уведомление по электронной почте.

- В поле **Получатели** укажите один или несколько адресов электронной почты для отправки уведомлений.

- При необходимости в поле **Описание** напишите описание шаблона уведомления.

7. Нажмите на кнопку **Подтвердить**.

   Окно **Изменить шаблон электронной почты** закроется.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Шаблон для уведомлений по электронной почте изменен и настроен. При возникновении событий выбранных типов в Open Single Management Platform шаблоны уведомлений будут отправлены на указанные адреса электронной почты.

Обращение в Службу технической поддержки

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

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Open Single Management Platform, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Open Single Management Platform.

Kaspersky предоставляет поддержку Open Single Management Platform в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;

- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Список ограничений

Open Single Management Platform имеет ряд ограничений, не критичных для работы приложения:

- После удаления некорневого тенанта, который был привязан к Серверу администрирования, попытка открыть раздел **KSC** в окне свойств тенанта возвращает ошибку. Обратитесь в Службу технической поддержки для решения проблемы. Чтобы предотвратить возникновение этой проблемы, удалите привязку тенанта от Сервера администрирования перед удалением тенанта.

- После добавления или удаления тенантов в разделе **Тенанты** (**Параметры** → **Тенанты**) изменения в списке тенантов не синхронизируются с фильтром тенантов в разделе **Поиск угроз**. Фильтр тенантов по-прежнему содержит удаленные тенанты и не содержит добавленных.

- После выключения серверов инфраструктуры кластера Kubernetes и повторного их запуска попытка входа в Консоль OSMP возвращает ошибку.

- Когда вы пишете выражение jq при создании правила сегментации, может появиться ошибка о недопустимом выражении, хотя выражение является корректным. Эта ошибка не блокирует создание правила сегментации.

- Если вы включите параметр **Использовать права пользователей** на вкладке **Права доступа** в свойствах группы администрирования Управляемые устройства, клиентские устройства невозможно будет экспортировать из Open Single Management Platform в KUMA.

- Плейбуки, содержащие действия по реагированию с помощью Kaspersky Endpoint Security для Windows, отображаются как доступные в списке плейбуков, даже если веб-плагин Kaspersky Endpoint Security для Windows не установлен в Open Single Management Platform.

- При импорте задачи *Загрузить обновления в хранилища точек распространения* или задачи *Проверка обновлений* параметр **Выбор устройств, которым будет назначена задача** включен. Эти задачи невозможно назначить выборкам устройств или заданным устройствам. Если вы назначите задачу *Загрузить обновления в хранилища точек распространения* или задачу *Проверка обновлений* на определенные устройства, задача будет импортирована некорректно.

- В графе расследования перестановка узлов выполняется неправильно.

- При переносе данных с подчиненного Сервера администрирования Kaspersky Security Center Windows на главный Сервер администрирования Open Single Management Platform мастер переноса данных не завершает шаг **Импорт данных**. Эта проблема возникает, если вы создаете глобальную задачу на подчиненном Сервере администрирования (например, задачу *Удаленная установка приложения*) и выбираете только значение **Сервера администрирования Kaspersky Security Center** для параметра **Управляемые приложения для экспорта** в мастере переноса данных.

- Получение объявлений " Лаборатории Касперского" недоступно.

- В окне свойств Сервера администрирования содержатся параметры для мобильных устройств, однако Open Single Management Platform не поддерживает управление мобильными устройствами.

- Уведомления о новых версиях доступных для загрузки веб-плагинов отключены. Вы можете обновить плагины с помощью Kaspersky Deployment Toolkit.

- После создания нового тенанта алерты, связанные с ним, отправляются на сервер, но не отображаются в таблице алертов. Вам может потребоваться обновить веб-страницу, чтобы обновить данные таблицы.

Список известных проблем Open Single Management Platform см. в документации Kaspersky Security Center.

Приложения

В этом разделе представлены приложения к основному тексту документа.

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла KUMA /opt/kaspersky/kuma/kuma, с помощью которого можно вручную запустить или установить компоненты KUMA. Это может пригодиться в случае, если вам нужно увидеть выходные данные в консоли операционной системы сервера.

Параметры команд

Команды	Описание
`tools`	Запуск инструментов управления KUMA.
`collector`	Установка, запуск или удаление сервиса коллектора.
`core`	Установка, запуск или удаление сервиса Ядра.
`correlator`	Установка, запуск или удаление сервиса коррелятора.
`agent`	Установка, запуск или удаление сервиса агента.
`help`	Получение информации о доступных командах и параметрах.
`license`	Получение информации о лицензии.
`storage`	Запуск или установка Хранилища.
`version`	Получение информации о версии приложения.

Флаги:

`-h`, `--h` используются для получения справочной информации о командах файла kuma. Например: `kuma <компонент> --help`.

Примеры:

- `kuma version` – получение информации о версии установщика KUMA.
- `kuma core -h` – получение справки по команде core установщика KUMA.
- `kuma collector --core <адрес сервера, где должен получить свои параметры коллектор> --id <идентификатор устанавливаемого сервиса> --api.port <порт>` используется для запуска установки сервиса коллектора.

Проверка целостности файлов KUMA

Целостность компонентов KUMA проверяется с помощью набора скриптов, основанных на инструменте integrity_checker, расположенных в директории /opt/kaspersky/kuma/integrity/bin. При проверке целостности используются xml-файлы манифестов из директории /opt/kaspersky/kuma/integrity/manifest/*, подписанные криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с правами не ниже прав учетной записи kuma.

Проверка целостности выполняется раздельно для компонентов KUMA и должна выполняться раздельно на серверах с соответствующими компонентами. При проверке целостности также проверяется целостность использованного xml-файла.

Чтобы проверить целостность файлов компонентов:

1. Перейдите в директорию, содержащую набор скриптов с помощью следующей команды:

   ```
   cd /opt/kaspersky/kuma/integrity/bin
   ```

2. Выполните команду из таблицы ниже, в зависимости от того, целостность какого компонента KUMA вы хотите проверить:

   - `./check_all.sh` – компоненты Ядра KUMA и хранилища;
   - `./check_core.sh` – компоненты Ядра KUMA;
   - `./check_collector.sh` – компоненты коллектора KUMA;
   - `./check_correlator.sh` – компоненты коррелятора KUMA;
   - `./check_storage.sh` – компоненты хранилища;
   - `./check_kuma_exe.sh <полный путь к файлу kuma.exe без указания имени файла>` – агент KUMA для Windows. Стандартное расположение исполняемого файла агента на устройстве Window: C:\Program Files\Kaspersky Lab\KUMA\.

   Целостность файлов компонентов будет проверена.

Результат проверки каждого компонента отображается в следующем формате:

- Блок Summary описывает количество проверенных объектов со статусом проверки: целостность не подтверждена/объект пропущен/целостность подтверждена:
  - Manifests – количество обработанных файлов манифеста.
  - Files – при проверке целостности KUMA не используется.
  - Directories – при проверке целостности KUMA не используется.
  - Registries – при проверке целостности KUMA не используется.
  - Registry values – при проверке целостности KUMA не используется.
- Результат проверки целостности компонента:
  - SUCCEEDED – целостность подтверждена.
  - FAILED – целостность нарушена.

Модель данных нормализованного события

В этом разделе вы можете найти модель данных нормализованного события KUMA. Все события, которые обрабатываются корреляторами KUMA с целью обнаружения алертов, должны соответствовать этой модели.

События, несовместимые с этой моделью данных, необходимо импортировать в этот формат (нормализовать) с помощью коллекторов.

Модель данных нормализованного события

Название поля	Тип данных	Размер поля	Опи
Назначение данных полей определено в названии поля. Поля доступны для изменени			
ApplicationProtocol	Строка	31 символов	Название протокола прикладного уровня. Например, HTTI
BytesIn	Число	От -9223372036854775808 до 9223372036854775807	Количество полученных байт.
BytesOut	Число	От -9223372036854775808 до 9223372036854775807	Количество отправленных байт.
DestinationAddress	Строка	45 символов	IPv4 или IPv6-адрес актива, с которым будет выполнено д xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DestinationCity	Строка	1023 символов	Город, соответствующий IP-адресу из поля DestinationAd
DestinationCountry	Строка	1023 символов	Страна, соответствующая IP-адресу из поля DestinationA
DestinationDnsDomain	Строка	255 символов	DNS-часть полного доменного имени точки назначения.
DestinationHostName	Строка	1023 символов	Название устройства точки назначения. FQDN точки назн
DestinationLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля Destination/
DestinationLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля DestinationA
DestinationMacAddress	Строка	17 символов	MAC-адрес точки назначения. Например, aa:bb:cc:dd:ee:0
DestinationNtDomain	Строка	255 символов	Windows Domain Name точки назначения.
DestinationPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта точки назначения.
DestinationProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса, зарегистрированн
DestinationProcessName	Строка	1023 символов	Название системного процесса, зарегистрированного на
DestinationRegion	Строка	1023 символов	Регион, соответствующий IP-адресу из поля DestinationA
DestinationServiceName	Строка	1023 символов	Название сервиса или службы на стороне точки назначен
DestinationTranslatedAddress	Строка	45 символов	IPv4 или IPv6-адрес точки назначения после трансляции.
DestinationTranslatedPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта на точке назначения после трансляции.
DestinationUserID	Строка	1023 символов	Идентификатор пользователя точки назначения.
DestinationUserName	Строка	1023 символов	Имя пользователя точки назначения.
DestinationUserPrivileges	Строка	1023 символов	Названия ролей, которые идентифицируют пользовательс Administrator и т.п.

DeviceAction	Строка	63 символов	Действие, которое было предпринято источником событи
DeviceAddress	Строка	45 символов	IPv4 или IPv6-адрес устройства, с которого было получен xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceCity	Строка	1023 символов	Город, соответствующий IP-адресу из поля DeviceAddress
DeviceCountry	Строка	1023 символов	Страна, соответствующая IP-адресу из поля DeviceAddre
DeviceDnsDomain	Строка	255 символов	DNS-часть полного доменного имени устройства, с котор
DeviceEventClassID	Строка	1023 символов	Идентификатор типа события, присвоенный источником с
DeviceExternalID	Строка	255 символов	Идентификатор устройства или приложения, присвоенны
DeviceFacility	Строка	1023 символов	Значение параметра facility, установленное источником с
DeviceHostName	Строка	100 символов	Имя устройства, с которого было получено событие. FQD
DeviceInboundinterface	Строка	128 символов	Название интерфейса входящего соединения.
DeviceLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля DeviceAddre
DeviceLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля DeviceAddre
DeviceMacAddress	Строка	17 символов	MAC-адрес актива, с которого было получено событие. H
DeviceNtDomain	Строка	255 символов	Windows Domain Name устройства.
DeviceOutboundinterface	Строка	128 символов	Название интерфейса исходящего соединения.
DevicePayloadID	Строка	128 символов	Уникальный идентификатор полезной нагрузки (Payload),
DeviceProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса на устройстве, кото
DeviceProcessName;	Строка	1023 символов	Название процесса.
DeviceProduct	Строка	63 символов	Название приложения, сформировавшего событие. Devic идентифицируют источник журнала.
DeviceReceiptTime	Число	От -9223372036854775808 до 9223372036854775807	Время получения события устройством.
DeviceRegion	Строка	1023 символов	Регион, соответствующий IP-адресу из поля DeviceAddre
DeviceTimeZone	Строка	255 символов	Временная зона устройства, на котором было создано со
DeviceTranslatedAddress	Строка	45 символов	Ретранслированный IPv4 или IPv6-адрес устройства, с ко xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceVendor	Строка	63 символов	Название производителя источника события. DeviceVend идентифицируют источник журнала.
DeviceVersion	Строка	31 символов	Версия приложения источника события. DeviceVendor, De источник журнала.
EndTime	Число	От -9223372036854775808 до 9223372036854775807	Дата и время (timestamp) завершения события.
EventOutcome	Строка	63 символов	Результат выполнения операции. Например, success, failu
ExternalID	Строка	40 символов	Поле в которое может быть сохранен идентификатор.
FileCreateTime	Число	От -9223372036854775808 до 9223372036854775807	Время создания файла.
FileHash	Строка	255 символов	Хеш-сумма файла. Пример: CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C
FileID	Строка	1023 символов	Значение идентификатора файла.

FileModificationTime	Число	От -9223372036854775808 до 9223372036854775807	Время последнего изменения файла.
FileName	Строка	1023 символов	Имя файла, без указания пути к файлу.
FilePath	Строка	1023 символов	Путь к файлу, включая имя файла.
FilePermission	Строка	1023 символов	Список разрешений файла.
FileSize	Число	От -9223372036854775808 до 9223372036854775807	Размер файла.
FileType	Строка	1023 символов	Тип файла.
Message	Строка	1023 символов	Краткое описание события.
Name	Строка	512 символов	Название события.
OldFileCreateTime	Число	От -9223372036854775808 до 9223372036854775807	Время создания OLD-файла из события. Время указывае часовому поясу браузера пользователя.
OldFileHash	Строка	255 символов	Хеш-сумма OLD-файла. Пример: CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C
OldFileID	Строка	1023 символов	Идентификатор OLD-файла.
OldFileModificationTime	Число	От -9223372036854775808 до 9223372036854775807	Время последнего изменения OLD-файла.
OldFileName	Строка	1023 символов	Имя OLD-файла (без пути).
OldFilePath	Строка	1023 символов	Путь к OLD-файлу, включая имя файла.
OldFilePermission	Строка	1023 символов	Список разрешений OLD-файла.
OldFileSize	Число	От -9223372036854775808 до 9223372036854775807	Размер OLD-файла.
OldFileType	Строка	1023 символов	Тип OLD-файла.
Reason	Строка	1023 символов	Информация о причине возникновения события.
RequestClientApplication	Строка	1023 символов	Значение параметра "user-agent" http-запроса.
RequestContext	Строка	2048 символов	Описание контекста http-запроса.
RequestCookies	Строка	1023 символов	Cookies, связанные с http-запросом.
RequestMethod	Строка	1023 символов	Метод, который использовался при выполнении http-запр
RequestUrl	Строка	1023 символов	Запрошенный URL.
Severity	Строка	1023 символов	Приоритет. Это может быть поле Severity или поле Level и
SourceAddress	Строка	45 символов	IPv4 или IPv6-адрес источника. Пример формата: 0.0.0.0 и
SourceCity	Строка	1023 символов	Город, соответствующий IP-адресу из поля SourceAddres
SourceCountry	Строка	1023 символов	Страна, соответствующая IP-адресу из поля SourceAddre
SourceDnsDomain	Строка	255 символов	DNS-часть полного доменного имени источника.
SourceHostName	Строка	1023 символов	Доменное имя Windows-устройства источника события.
SourceLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля SourceAddr
SourceLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля SourceAddr

SourceMacAddress	Строка	17 символов	MAC-адрес источника. Пример формата: aa:bb:cc:dd:ee:0
SourceNtDomain	Строка	255 символов	Windows Domain Name источника.
SourcePort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта источника.
SourceProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса.
SourceProcessName	Строка	1023 символов	Название системного процесса на источнике. Например,
SourceRegion	Строка	1023 символов	Регион, соответствующий IP-адресу из поля SourceAddre
SourceServiceName	Строка	1023 символов	Название сервиса или службы на стороне источника. Нап
SourceTranslatedAddress	Строка	15 символов	IPv4 или IPv6-адрес источника после трансляции. Пример
SourceTranslatedPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта на источнике после трансляции.
SourceUserID	Строка	1023 символов	Идентификатор пользователя источника.
SourceUserName	Строка	1023 символов	Имя пользователя источника.
SourceUserPrivileges	Строка	1023 символов	Названия ролей, которые идентифицируют пользовательс Administrator и т.п.
StartTime	Число	От -9223372036854775808 до 9223372036854775807	Дата и время (timestamp) в которые, началась активность
Tactic	Строка	128 символов	Название тактики из матрицы MITRE ATT&CK.
Technique	Строка	128 символов	Название техники из матрицы MITRE ATT&CK.
TransportProtocol	Строка	31 символов	Название протокола Транспортного уровня сетевой моде
Тип	Число	От -9223372036854775808 до 9223372036854775807	Тип события: 1 – базовое, 2 - агрегированное, 3 - корреля
Поля, назначение которых может быть определено пользователем. Поля доступны для изм			
DeviceCustomDate1	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). отображается по часовому поясу браузера пользователя
DeviceCustomDate1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomDate1.
DeviceCustomDate2	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). отображается по часовому поясу браузера пользователя
DeviceCustomDate2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomDate2.
DeviceCustomFloatingPoint1	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatin
DeviceCustomFloatingPoint2	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatin
DeviceCustomFloatingPoint3	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.

DeviceCustomFloatingPoint3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatin
DeviceCustomFloatingPoint4	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint4Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatin
DeviceCustomIPv6Address1	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример форма
DeviceCustomIPv6Address1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Ad
DeviceCustomIPv6Address2	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример форма
DeviceCustomIPv6Address2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Ad
DeviceCustomIPv6Address3	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример форма
DeviceCustomIPv6Address3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Ad
DeviceCustomIPv6Address4	Строка	45 символов	Поле для маппинга значения IPv6 address. Например, y:y:y
DeviceCustomIPv6Address4Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Ad
DeviceCustomNumber1	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomNumbe
DeviceCustomNumber2	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomNumbe
DeviceCustomNumber3	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomNumbe
DeviceCustomString1	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString1
DeviceCustomString2	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString2
DeviceCustomString3	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString3
DeviceCustomString4	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString4Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString4
DeviceCustomString5	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString5Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString5
DeviceCustomString6	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString6Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString6
DeviceDirection	Число	От -9223372036854775808 до 9223372036854775807	Поле для описания направления соединения события. "0"
DeviceEventCategory	Строка	1023 символов	Категория события, присвоенная устройством, направивш
FlexDate1	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). отображается по часовому поясу браузера пользователя
FlexDate1Label	Строка	128 символов	Поле для описания назначения поля FlexDate1Label.

FlexNumber1	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
FlexNumber1Label	Строка	128 символов	Поле для описания назначения поля FlexNumber1Label.
FlexNumber2	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
FlexNumber2Label	Строка	128 символов	Поле для описания назначения поля FlexNumber2Label.
FlexString1	Строка	1023 символов	Поле для маппинга строкового значения.
FlexString1Label	Строка	128 символов	Поле для описания назначения поля FlexString1Label.
FlexString2	Строка	1023 символов	Поле для маппинга строкового значения.
FlexString2Label	Строка	128 символов	Поле для описания назначения поля FlexString2Label.
		Служебные поля. Недоступны для редактирования.	
AffectedAssets	Вложенная структура [Affected]	-	Вложенная структура, из которой можно обратиться к св узнать, сколько раз они фигурируют в событиях алерта.
AggregationRuleID	Строка	-	Идентификатор агрегационного правила.
AggregationRuleName	Строка	-	Название агрегационного правила, которое обработало с
BaseEventCount	Число	-	Для агрегированного базового события — количество баз правилом. Для корреляционного события — это количест корреляционным правилом, которое создало корреляцио
BaseEvents	Вложенный список [Event]	-	Вложенная структура со списком базовых событий. Поле
Code	Строка	-	В базовом событии это код возврата процесса, функции и
CorrelationRuleID	Строка	-	ID корреляционного правила.
CorrelationRuleName	Строка	-	Название корреляционного правила, в результате срабат Заполняется только для корреляционных событий.
DestinationAccountID	Строка	-	Поле хранит идентификатор пользователя.
DestinationAssetID	Строка	-	Поле хранит идентификатор актива точки назначения.
DeviceAssetID	Строка	-	Поле хранит идентификатор актива, направившего событ
Extra	Вложенный словарь [строка:строка]	-	Поле, в которое во время нормализации "сырого" события сопоставление с полями события KUMA. Это поле может размер поля — 4 МБ.
GroupedBy	Строка	-	Список названия полей, по которым была группировка в к корреляционного события.
ID	Строка	-	Уникальный идентификатор события типа UUID. Для базов генерирует коллектор. Идентификатор корреляционного меняет своего значения.
Raw	Строка	-	Не нормализованный текст исходного "сырого" события. М
ReplayID	Строка	-	Идентификатор ретроспективной проверки, в процессе к
ServiceID	Строка	-	Идентификатор экземпляра сервиса: коррелятора, коллек
ServiceName	Строка	-	Название экземпляра микросервиса, которое присваивае
SourceAccountID	Строка	-	Поле хранит идентификатор пользователя.
SourceAssetID	Строка	-	Поле хранит идентификатор актива источника событий.
SpaceID	Строка	-	Идентификатор пространства.
TenantID	Строка	-	Поле хранит идентификатор тенанта.
TI	Вложенный словарь [строка:строка]	-	Поле, в котором в формате словаря содержатся категори индикаторам из события.

TICategories	map[String]	-	Поле, содержит категории, полученные от внешнего TI-по
Timestamp	Число	-	Время создания базового события на коллекторе. Время указывается в UTC0. В Консоли KUMA значение отобража

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Активы`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Значение`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

Поля, формируемые KUMA

KUMA формирует следующие поля, не подлежащие изменениям: BranchID, BranchName, DestinationAccountName, DestinationAssetName, DeviceAssetName, SourceAccountName, SourceAssetName, TenantName.

Настройка модели данных нормализованного события из KATA EDR

Для расследования данных необходимо, чтобы идентификаторы события и процесса KATA/EDR попадали в определенные поля нормализованного события. Для построения дерева процессов для событий, поступающих из KATA/EDR, необходимо настроить копирование данных из полей исходных событий в поля нормализованного события в нормализаторах в KUMA следующим образом:

1. Для любых событий KATA/EDR должна быть настроена нормализация с копированием следующих полей:

   - поле события KATA/EDR `EventType` должно копироваться в поле нормализованного события KUMA `DeviceEventCategory`;
   - поле события KATA/EDR `HostName` должно копироваться в поле нормализованного события KUMA `DeviceHostName`.

2. Для любого события, где поле DeviceProduct = 'KATA' должна быть настроена нормализация в соответствии таблице ниже.

Нормализация полей событий из KATA/EDR

Поле в событии KATA/EDR	Поле нормализованного события
IOATag	DeviceCustomIPv6Address2
	IOATag
IOAImportance	DeviceCustomIPv6Address1
	IOAImportance

FilePath	FilePath
FileName	FileName
MD5	FileHash
FileSize	FileSize

3. Для событий, перечисленными в таблице ниже, должна быть настроена дополнительная нормализация с копированием полей в соответствии с таблицей.

Дополнительная нормализация с копированием полей событий из KATA/EDR

Событие	Поле исходного события	Поле нормализованного события
Process	UniqueParentPid	FlexString1
	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
AppLock	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
BlockedDocument	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Module	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
FileChange	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Driver	HostName	DeviceHostName
	FileName	FileName
	ProductName	DeviceCustomString5,
		ProductName
	ProductVendor	DeviceCustomString6
		ProductVendor
Connection	UniquePid	FlexString2
	HostName	DeviceHostName
	URI	RequestURL
	RemoteIP	DestinationAddress
	RemotePort	DestinationPort
PortListen	UniquePid	FlexString2
	HostName	DeviceHostName
	LocalIP	SourceAddress
	LocalPort	SourcePort
Registry	UniquePid	FlexString2
	HostName	DeviceHostName
	ValueName	DeviceCustomString5

		New Value Name
	KeyName	DeviceCustomString4
		New Key Name
	PreviousKeyName	FlexString2
		Old Key Name
	ValueData	DeviceCustomString6
		New Value Data
	PreviousValueData	FlexString1
		Old Value Data
	ValueType	FlexNumber1
		Value Type
	PreviousValueType	FlexNumber2
		Previous Value Type
SystemEventLog	UniquePid	FlexString2
	HostName	DeviceHostName
	OperationResult	EventOutcome
	EventId	DeviceCustomNumber3
		EventId
	EventRecordId	DeviceCustomNumber2
		EventRecordId
	Channel	DeviceCustomString6
		Channel
	ProviderName	SourceUserID
ThreatDetect	UniquePid	FlexString2
	HostName	DeviceHostName
	VerdictName	EventOutcome
	DetectedObjectType	OldFileType
	isSilent	FlexString1
		Is Silent
	RecordId	DeviceCustomString5
		Record ID
	DatabaseTimestamp	DeviceCustomDate2
		Database Timestamp
ThreatDetectProcessingResult	UniquePid	FlexString2
	HostName	DeviceHostName
	ThreatStatus	DeviceCustomString5
		Threat Status
PROCESS_INTERPRET_FILE_RUN	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
	InterpretedFilePath	OldFilePath
	InterpretedFileSize	OldFileSize

	InterpretedFileHash	OldFileHash
PROCESS_CONSOLE_INTERACTIVE_INPUT	UniquePid	FlexString2
	HostName	DeviceHostName
	InteractiveInputText	DeviceCustomString4
		Command Line
AMSI SCAN	UniquePid	FlexString2
	HostName	DeviceHostName
	ObjectContent	DeviceCustomString5
		Object Content

Модель данных актива

Структура актива представлена полями, в которых содержатся значения. Поля также могут содержать вложенные структуры.

Поле актива	Тип значения	Описание
`ID`	Строка	Идентификатор актива.
`TenantName`	Строка	Название тенанта.
`DeletedAt`	Число	Дата удаления актива.
`CreatedAt`	Число	Дата создания актива.
`TenantID`	Строка	Идентификатор тенанта.
`DirectCategories`	Вложенный список строк	Категории актива.
`CategoryModels`	Вложенная структура `[Category]`	Изменение категорий актива.
`AffectedByIncidents`	Вложенный словарь: [строка:строка `TRUE/FALSE`]	Идентификаторы инцидентов.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.
`Owner`	Вложенная структура [OwnerInfo]	Сведения о владельце актива.
`OS`	Вложенная структура [OS]	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`APISoft`	Вложенная структура [Software]	ПО, установленное на активе.
`APIVulns`	Вложенная структура [Vulnerability]	Уязвимости актива.
`KICSServerIp`	Строка	IP-адрес сервера KICS for Networks.
`KICSConnectorID`	Число	Идентификатор коннектора KICS for Networks.

KICSDeviceID	Число	Идентификатор актива в KICS for Networks.
KICSStatus	Строка	Статус актива в KICS for Networks.
KICSHardware	Вложенная структура [KICSSystemInfo]	Аппаратные сведения об активе, полученные из KICS for Networks.
KICSSoft	Вложенная структура [KICSSystemInfo]	Сведения о ПО актива, полученные из KICS for Networks.
KICSRisks	Вложенная структура [KICSRisk]	Сведения об уязвимостях актива, полученные из KICS for Networks.
Sources	Вложенная структура [Sources]	Основные сведения об активе, поступавшие из разных источников.
FromKSC	Строка со значениями TRUE/FALSE	Индикатор, указывающий, что сведения об активе импортированы из Kaspersky Security Center.
NAgentID	Строка	Идентификатор Агента администрирования Kaspersky Security Center, от которого получены сведения об активе.
KSCServerFQDN	Строка	FQDN Сервера Kaspersky Security Center.
KSCInstanceID	Строка	Идентификатор экземпляра Kaspersky Security Center.
KSCMasterHostname	Строка	Имя устройства Сервера администрирования Kaspersky Security Center.
KSCGroupID	Число	Идентификатор группы Kaspersky Security Center.
KSCGroupName	Строка	Название группы администрирования Kaspersky Security Center.
LastVisible	Число	Дата, когда от Kaspersky Security Center в последний раз были получены сведения об активе.
Products	Вложенный словарь: [строка:вложенная структура [ProductInfo]]	Сведения об установленных на активе приложениях Kaspersky, полученные из Kaspersky Security Center.
Hardware	Вложенная структура [Hardware]	Аппаратные сведения об активе, полученные из Kaspersky Security Center.
KSCSoft	Вложенная структура [Software]	Сведения о ПО актива, полученные из Kaspersky Security Center.
KSCVulns	Вложенная структура [Vulnerability]	Сведения об уязвимостях актива, полученные из Kaspersky Security Center.

Вложенная структура Category

Поле	Тип значения	Описание
ID	Строка	Идентификатор категории.
TenantID	Строка	Идентификатор тенанта.
TenantName	Строка	Название тенанта.
Parent	Строка	Родительская категория.
Path	Вложенный список строк	Структура категорий.
Name	Строка	Название категории.
UpdatedAt	Число	Последнее обновление категории.
CreatedAt	Число	Дата создания категории.
Описание	Строка	Описание категории.
Weight	Число	Уровень важности категории.
CategorizationKind	Строка	Тип присвоения категории активам.
CategorizationAt	Число	Дата категоризации.
CategorizationInterval	Строка	Интервал присвоения категорий.

Вложенная структура OwnerInfo

Поле	Тип значения	Описание
`DisplayName`	Строка	Имя владельца актива.

Вложенная структура OS

Поле	Тип значения	Описание
`Name`	Строка	Название операционной системы.
`BuildNumber`	Число	Версия операционной системы.

Вложенная структура Software

Поле	Тип значения	Описание
`DisplayName`	Строка	Название ПО.
`DisplayVersion`	Строка	Версия ПО.
`Publisher`	Строка	Издатель ПО.
`InstallDate`	Строка	Дата установки.
`HasMSIInstaller`	Строка `TRUE/FALSE`	Признак, имеет ли ПО MSI-установщик.

Вложенная структура Vulnerability

Поле	Тип значения	Описание
`KasperskyID`	Строка	Идентификатор уязвимости, присвоенный Kaspersky.
`ProductName`	Строка	Название ПО.
`DescriptionURL`	Строка	URL с описанием уязвимости.
`RecommendedMajorPatch`	Строка	Рекомендуемое обновление.
`RecommendedMinorPatch`	Строка	Рекомендуемое обновление.
`SeverityStr`	Строка	Уровень важности уязвимости.
`Severity`	Число	Уровень важности уязвимости.
`CVE`	Вложенный список строк	Идентификатор уязвимости CVE.
`ExploitExists`	Строка `TRUE/FALSE`	Существует ли эксплойт.
`MalwareExists`	Строка `TRUE/FALSE`	Существует ли вредоносное приложение.

Вложенная структура KICSSystemInfo

Поле	Тип значения	Описание
`Model`	Строка	Модель устройства.
`Version.`	Строка	Версия устройства.
`Производитель;`	Строка	Производитель.

Вложенная структура KICSRisk

Поле	Тип значения	Описание
`ID`	Число	Идентификатор риска KICS for Networks.
`Name`	Строка	Название риска.
`Category`	Строка	Тип риска.
`Описание`	Строка	Описание риска.
`DescriptionUrl`	Строка	Ссылка на описание риска.
`Severity`	Число	Уровень важности риска.
`Cvss`	Число	Оценка CVSS.

Вложенная структура Sources

Поле	Тип значения	Описание
`KSC`	Вложенная структура [SourceInfo]	Сведения об активе, полученные из Kaspersky Security Center.
`API`	Вложенная структура [SourceInfo]	Сведения об активе, поступившие через REST API.
`Manual`	Вложенная структура [SourceInfo]	Сведения об активе, введенные вручную.
`KICS`	Вложенная структура [SourceInfo]	Сведения об активе, поступившие из KICS for Networks.

Вложенная структура Sources

Поле	Тип значения	Описание
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.
`Owner`	Вложенная структура [OwnerInfo]	Сведения о владельце актива.
`OS`	Вложенная структура [OS]	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.

Вложенная структура ProductInfo

Поле	Тип значения	Описание
`ProductVersion`	Строка	Версия ПО.
`ProductName`	Строка	Название ПО.

Вложенная структура Hardware

Поле	Тип значения	Описание
NetCards	Вложенная структура [NetCard]	Перечень сетевых карт актива.
Процессор	Вложенная структура [CPU]	Перечень процессоров актива.
ОЗУ	Вложенная структура [RAM]	Перечень ОЗУ актива.
Disk	Вложенная структура [Disk]	Перечень дисков актива.

Вложенная структура NetCard

Поле	Тип значения	Описание
ID	Строка	Идентификатор сетевой карты.
MACAddresses	Вложенный список строк	MAC-адреса сетевой карты.
Name	Строка	Название сетевой карты.
Manufacture	Строка	Производитель сетевой карты.
DriverVersion	Строка	Версия драйвера.

Вложенная структура RAM

Поле	Тип значения	Описание
Frequency	Строка	Частота ОЗУ.
TotalBytes	Число	Объем ОЗУ в байтах.

Вложенная структура CPU

Поле	Тип значения	Описание
ID	Строка	Идентификатор процессора.
Name	Строка	Название процессора.
CoreCount	Строка	Количество ядер.
CoreSpeed	Строка	Частота.

Вложенная структура Disk

Поле	Тип значения	Описание
FreeBytes	Число	Свободное пространство на диске.
TotalBytes	Число	Общее пространство на диске.

Модель данных учетной записи

К полям учетной записи можно обращаться из шаблонов электронной почты, а также при корреляции событий.

Поле	Тип значения	Описание

ID	Строка	Идентификатор учетной записи.
ObjectGUID	Строка	Атрибут Active Directory. Идентификатор учетной записи в Active Directory.
TenantID	Строка	Идентификатор тенанта.
TenantName	Строка	Название тенанта.
UpdatedAt	Число	Последнее обновление учетной записи.
Домен.	Строка	Домен.
CN	Строка	Атрибут Active Directory. Имя пользователя.
DisplayName	Строка	Атрибут Active Directory. Отображаемое имя пользователя.
DistinguishedName	Строка	Атрибут Active Directory. Название объекта LDAP.
EmployeeID	Строка	Атрибут Active Directory. Идентификатор сотрудника.
Mail	Строка	Атрибут Active Directory. Электронная почта пользователя.
MailNickname	Строка	Атрибут Active Directory. Альтернативный адрес электронной почты.
Mobile	Строка	Атрибут Active Directory. Номер мобильного телефона.
ObjectSID	Строка	Атрибут Active Directory. Идентификатор безопасности.
SAMAccountName	Строка	Атрибут Active Directory. Учетная запись.
TelephoneNumber	Строка	Атрибут Active Directory. Номер телефона.
UserPrincipalName	Строка	Атрибут Active Directory. Имя участника-пользователя.
Archived	Строка TRUE/FALSE	Признак, определяющий, является ли учетная запись устаревшей.
MemberOf	Список строк	Атрибут Active Directory. Группы Active Directory, в которые внесен пользователь. По этому атрибуту события можно искать при корреляции.
PreliminarilyArchived	Строка TRUE/FALSE	Признак, определяющий, требуется ли обозначить учетную запись как устаревшую.
CreatedAt	Число	Дата создания учетной записи.
SN	Строка	Атрибут Active Directory. Фамилия пользователя.
SAMAccountType	Строка	Атрибут Active Directory. Тип учетной записи.
Title	Строка	Атрибут Active Directory. Должность пользователя.
деление;	Строка	Атрибут Active Directory. Подразделение пользователя.
Department	Строка	Атрибут Active Directory. Отдел пользователя.
Manager	Строка	Атрибут Active Directory. Руководитель пользователя.
Расположение	Строка	Атрибут Active Directory. Местоположение пользователя.
Company	Строка	Атрибут Active Directory. Компания пользователя.
StreetAddress	Строка	Атрибут Active Directory. Адрес компании.
PhysicalDeliveryOfficeName	Строка	Атрибут Active Directory. Адрес для доставки.
ManagedObjects	Список строк	Атрибут Active Directory. Объекты, находящиеся под управлением пользователя.
UserAccountControl	Число	Атрибут Active Directory. Тип учетной записи Active Directory.
WhenCreated	Число	Атрибут Active Directory. Дата создания учетной записи.
WhenChanged	Число	Атрибут Active Directory. Дата изменения учетной записи.
AccountExpires	Число	Атрибут Active Directory. Дата истечения срока учетной записи.
BadPasswordTime	Число	Атрибут Active Directory. Дата последней неудачной попытки входа в систему.

События аудита KUMA

События аудита создаются при выполнении в KUMA определенных действий, связанных с безопасностью. Эти события используются для обеспечения целостности системы. Этот раздел содержит информацию о событиях аудита KUMA.

Поля событий с общей информацией

Каждое событие аудита имеет поля событий, описанные ниже.

Название поля события	Значение поля
ID	Уникальный идентификатор события в виде UUID.
Timestamp	Время события.
DeviceHostName	Устройство источника события. Для событий аудита это имя устройства, на котором установлена служба kuma-core, потому что она является источником событий.
DeviceTimeZone	Часовой пояс системного времени сервера, на котором установлено Ядро KUMA в формате +-чч:мм.
Тип	Тип события аудита. Событию аудита соответствует значение 4.
TenantID	Идентификатор главного тенанта.
DeviceVendor	`"Лаборатория Касперского".`
DeviceProduct	`KUMA`
EndTime	Время создания события.

Пользователь успешно вошел в систему или не смог войти

Название поля события	Значение поля
DeviceAction	`user login`
EventOutcome	`succeeded` или `failed` – статус зависит от результата операции.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя.
SourceUserID	Идентификатор пользователя.
Message	Описание ошибки; появляется только в том случае, если при входе в систему произошла ошибка. В противном случае поле будет пустым.

Пользователь успешно вышел из системы

Это событие создается только тогда, когда пользователь нажимает кнопку выхода.

Это событие не создается, если пользователь покидает систему из-за окончания сеанса или если пользователь снова входит в систему из другого браузера.

Название поля события	Значение поля
DeviceAction	`user logout`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя.
SourceUserID	Идентификатор пользователя.

Сервис успешно создан

Название поля события	Значение поля
DeviceAction	`service created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно удален

Название поля события	Значение поля
DeviceAction	`service deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления сервиса.
SourceUserID	Идентификатор пользователя, который использовался для удаления сервиса.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DestinationHostName	Полное доменное имя компьютера, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно запущен

Название поля события	Значение поля
DeviceAction	`service started`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, который сообщил информацию о запуске сервиса. Это может быть адрес прокси-сервера, если информация передается через прокси.
SourcePort	Порт, передавший информацию о запуске сервиса. Это может быть порт прокси-сервера, если информация передается через прокси.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, на котором был запущен сервис.
DestinationHostName	Полное доменное имя устройства, на котором был запущен сервис.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно сопряжен

Название поля события	Значение поля
DeviceAction	`service paired`

EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого был отправлен запрос на сопряжение сервисов. Это может быть адрес прокси-сервера, если запрос передается через прокси.
SourcePort	Порт, отправивший запрос на сопряжение сервисов. Это может быть порт прокси-сервера, если запрос передается через прокси.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно перезагружен

Название поля события	Значение поля
DeviceAction	`service reloaded`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для перезагрузки сервиса.
SourceUserID	Идентификатор пользователя, который использовался для перезапуска сервиса.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно перезапущен

Название поля события	Значение поля
DeviceAction	`service restarted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для перезапуска сервиса.
SourceUserID	Идентификатор пользователя, который использовался для перезапуска сервиса.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Раздел хранилища автоматически удален в связи с истечением срока действия

Название поля события	Значение поля
DeviceAction	`partition deleted`
EventOutcome	`succeeded`
Name	Имя индекса
SourceServiceName	`scheduler`
Message	`deleted by retention period settings`

Раздел хранилища удален пользователем

Название поля события	Значение поля
DeviceAction	`partition deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления.
SourceUserID	Идентификатор пользователя, который использовался для удаления.
Name	Имя индекса.
Message	`deleted by user`

Активный лист успешно очищен или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на очистку активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что активный лист может быть очищен успешно, но событие все равно будет иметь статус `failed`, так как EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус `succeeded` или `failed` активного листа.

Название поля события	Значение поля
DeviceAction	`active list cleared`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для очистки активного листа.
SourceUserID	Идентификатор пользователя, который использовался для очистки активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если `EventOutcome = failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент активного листа успешно изменен или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на изменение элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до изменения или после изменения.

Это означает, что элемент активного листа может быть изменен успешно, но событие все равно будет иметь статус `failed`, так как EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус элемента `succeeded` или `failed` активного листа.

Название поля события	Значение поля
DeviceAction	`active list item changed`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для изменения элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был изменен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	`key`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Элемент активного листа успешно удален или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на удаление элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что элемент активного листа может быть удален успешно, но событие все равно будет иметь статус `failed`, так как EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус удаленного элемента `succeeded` или `failed` активного листа.

Название поля события	Значение поля
DeviceAction	`active list item deleted`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет

	указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для удаления элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	`key`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Активный лист успешно импортирован или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов.

Импорт элементов активного листа выполняется по частям через удаленное подключение.

Поскольку импорт осуществляется через удаленное соединение, ошибка передачи данных может произойти в любой момент: когда данные частично или полностью импортированы. EventOutcome возвращает статус подключения, а не статус проверки импорта.

Название поля события	Значение поля
DeviceAction	`active list imported`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для выполнения импорта.
SourceUserID	Идентификатор пользователя, который использовался для импорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Активный лист успешно экспортирован

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов.

Название поля события	Значение поля
DeviceAction	`active list exported`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Ресурс успешно добавлен.

Название поля события	Значение поля
DeviceAction	`resource added`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для добавления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName;	Имя ресурса.
DeviceFacility	Тип ресурса:

	• activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Ресурс успешно удален.

Название поля события	Значение поля
DeviceAction	`resource deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для удаления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName;	Имя ресурса.
DeviceFacility	Тип ресурса: • activeList • agent

	• aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс успешно обновлен.

Название поля события	Значение поля
DeviceAction	resource updated
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для обновления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для обновления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName;	Имя ресурса.
DeviceFacility	Тип ресурса: • activeList • agent • aggregationRule • collector

	• connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Актив успешно создан

Название поля события	Значение поля
DeviceAction	asset created
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceExternalID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	addresses
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Актив успешно удален

Название поля события	Значение поля
DeviceAction	`asset deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceExternalID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	`addresses`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Категория актива успешно добавлена

Название поля события	Значение поля
DeviceAction	`category created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления категории.
SourceUserID	Идентификатор пользователя, который использовался для добавления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Категория актива успешно удалена

Название поля события	Значение поля
DeviceAction	`category deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления категории.
SourceUserID	Идентификатор пользователя, который использовался для удаления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Параметры успешно обновлены

Название поля события	Значение поля
DeviceAction	`settings updated`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для обновления параметров.
SourceUserID	Идентификатор пользователя, который использовался для обновления параметров.
DeviceFacility	Тип параметров.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Словарь успешно обновлен на сервисе или операция завершилась ошибкой

Название поля события	Значение поля
DeviceAction	`service created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	Идентификатор сервиса.
ExternalID	Идентификатор словаря.
DeviceProcessName;	Имя службы.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.

Действие по реагированию в Active Directory

Название поля события	Значение поля
DeviceAction	`ad response`
DeviceFacility	`manual response` или `automatic response`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных тенанта.
SourceUserID	Идентификатор пользователя, который использовался для изменения данных тенанта.
DeviceCustomString3	Наименование правила реагирования: CHANGE_PASSWORD, ADD_TO_GROUP, REMOVE_FROM_GROUP, BLOCK_USER.
DeviceCustomString3Label	`response rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DestinationUserName	Учетная запись пользователя Active Directory, на которую вызван ответ (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую вызван ответ.

DestinatinUserID	UUID учетной записи в KUMA.
FlexString1	Информация о группе, куда был добавлен или удален пользователь.
FlexString1Label	`group DN`

Реагирование через KICS for Networks

Название поля события	Значение поля
DeviceAction	`KICS responce`
DeviceFacility	`manual response` или `automatic response`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString3	Наименование правила реагирования: `Authorized`, `Not Authorized`.
DeviceCustomString3Label	`response rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DeviceExternalID	Идентификатор актива.
SourceHostName	FQDN актива.
Name	Название актива.
DeviceCustomString1	Перечень ip-адресов актива.
DeviceCustomString1Label	`addresses`

Реагирование через Kaspersky Automated Security Awareness Platform

Название поля события	Значение поля
DeviceAction	`KASAP response`
DeviceFacility	`manual response`
EventOutcome	`succeeded` или `failed`
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.

SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString1	Менеджер пользователя, на которого назначен курс.
DeviceCustomString1Label	`manager`
DeviceCustomString3	Информация о группе, где был пользователь. Отсутствует в случае `failed`.
DeviceCustomString3Label	`manager`
DeviceCustomString4	Информация о группе, куда добавили пользователя.
DeviceCustomString4Label	`new kasap group`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DestinationUserID	Идентификатор учетной записи пользователя Active Directory, на которую происходит реагирование.
DestinationUserName	Имя учетной записи (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую происходит реагирование.

KEDR response

Название поля события	Значение поля
DeviceAction	`KEDR response`
DeviceFacility	`manual response` или `automatic response`
EventOutcome	`succeeded` или `failed`
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
SourceAssetID	Идентификатор актива в KUMA, для которого производится реагирование. Значение не указывается, если реагирование производится по хешу или для всех активов.
DeviceExternalID	Параметр external ID, присвоенный KUMA в KEDR. Если external id один, при запуске по пользовательским устройствам не заполняется.
DeviceCustomString1	Перечисление IP/FQDN-адресов актива для правила запрета для устройства по выбранному хешу из карточки события.
DeviceCustomString1Label	`user defined list of ips or hostnames`
DeviceCustomString2	Параметр sensor ID в KEDR (UUIDv4 | 'all' | 'custom').
DeviceCustomString2Label	`sensor id of asset in KATA/EDR`
ServiceID	Идентификатор сервиса, который вызвал реагирование. Заполняется только при автоматическом реагировании.
DeviceCustomString3	Наименование типа задачи: `enable_network_isolation`, `disable_network_isolation`, `enable_prevention`, `disable_prevention`, `run_process`.
DeviceCustomString3Label	`kedr response kind`

DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Правила корреляции

В файле, доступном по ссылке для скачивания, описаны правила корреляции, включенные в поставку. Приводятся сценарии, покрываемые правилами, условия их использования и необходимые источники событий.

Описанные в этом документе правила корреляции содержатся в файле SOC_package дистрибутива OSMP и защищены паролем SOC_package1. Одновременно возможно использование только одной версии набора SOC-правил: или русской, или английской.

Импортированные правила корреляции можно добавлять в используемые вашей организацией коррелляторы. Дополнительную информацию см. в разделе: Шаг 3. Корреляция.

Чтобы импортировать пакет правил корреляции в KUMA:

1. В Консоли KUMA перейдите в раздел **Параметры** → **Обновление хранилища** и для параметра **Источник обновлений** установите значение **Серверы обновлений "Лаборатории Касперского"**.

   Вы также можете настроить обновление хранилища.

2. Нажмите на **Запустить обновление**, чтобы сохранить параметры обновления и вручную запустить задачу *Обновление хранилища*.

3. Перейдите в **Диспетчер задач,** чтобы убедиться, что задача *Обновление хранилища* завершена.

4. Перейдите в раздел **Ресурсы** и нажмите на **Импортировать ресурсы**.

5. В окне **Импортировать ресурсы** выберите тенант, которому будут принадлежать импортируемые ресурсы.

6. В раскрывающемся списке **Импортировать ресурсы** выберите **Хранилище**, выберите пакет SOC Content и нажмите на **Импортировать**.

   Ресурсы из пакета SOC Content импортируются в KUMA. Дополнительные сведения об импорте см. в разделе Импорт ресурсов.

Скачать описание правил корреляции, содержащихся в файле SOC_package.xlsx.

Формат времени

KUMA поддерживает обработку информации, передающейся в поля Модели данных события с типом timestamp (EndTime, StartTime, DeviceCustomDate1, и т.д.) в следующих форматах:

- "May 8, 2009 5:57:51 PM",
- "oct 7, 1970",
- "oct 7, '70",
- "oct. 7, 1970",
- "oct. 7, 70",
- "Mon Jan 2 15:04:05 2006",
- "Mon Jan 2 15:04:05 MST 2006",
- "Mon Jan 02 15:04:05 -0700 2006",
- "Monday, 02-Jan-06 15:04:05 MST",
- "Mon, 02 Jan 2006 15:04:05 MST",
- "Tue, 11 Jul 2017 16:28:13 +0200 (CEST)",
- "Mon, 02 Jan 2006 15:04:05 -0700",
- "Mon 30 Sep 2018 09:09:09 PM UTC",
- "Mon Aug 10 15:44:11 UTC+0100 2015",
- "Thu, 4 Jan 2018 17:53:36 +0000",
- "Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)",
- "Sun, 3 Jan 2021 00:12:23 +0800 (GMT+08:00)",
- "September 17, 2012 10:09am",
- "September 17, 2012 at 10:09am PST-08",
- "September 17, 2012, 10:10:09",
- "October 7, 1970",
- "October 7th, 1970",
- "12 Feb 2006, 19:17",
- "12 Feb 2006 19:17",
- "14 May 2019 19:11:40.164",
- "7 oct 70",
- "7 oct 1970",
- "03 February 2013",

- "1 July 2013",
- "2013-Feb-03".

Формат dd/Mon/yyyy

- "06/Jan/2008:15:04:05 -0700",
- "06/Jan/2008 15:04:05 -0700".

Формат mm/dd/yyyy

- "3/31/2014",
- "03/31/2014",
- "08/21/71",
- "8/1/71",
- "4/8/2014 22:05",
- "04/08/2014 22:05",
- "4/8/14 22:05",
- "04/2/2014 03:00:51",
- "8/8/1965 12:00:00 AM",
- "8/8/1965 01:00:01 PM",
- "8/8/1965 01:00 PM",
- "8/8/1965 1:00 PM",
- "8/8/1965 12:00 AM",
- "4/02/2014 03:00:51",
- "03/19/2012 10:11:59",
- "03/19/2012 10:11:59.3186369".

Формат yyyy/mm/dd

- "2014/3/31",
- "2014/03/31",
- "2014/4/8 22:05",

- "2014/04/08 22:05",
- "2014/04/2 03:00:51",
- "2014/4/02 03:00:51",
- "2012/03/19 10:11:59",
- "2012/03/19 10:11:59.3186369".

Формат yyyy:mm:dd

- "2014:3:31",
- "2014:03:31",
- "2014:4:8 22:05",
- "2014:04:08 22:05",
- "2014:04:2 03:00:51",
- "2014:4:02 03:00:51",
- "2012:03:19 10:11:59",
- "2012:03:19 10:11:59.3186369".

Формат, содержащий китайские символы

"2014年04月08日"

Формат yyyy-mm-ddThh

- "2006-01-02T15:04:05+0000",
- "2009-08-12T22:15:09-07:00",
- "2009-08-12T22:15:09",
- "2009-08-12T22:15:09.988",
- "2009-08-12T22:15:09Z",
- "2017-07-19T03:21:51:897+0100",
- "2019-05-29T08:41-04" без указания секунд, 2 символа TZ.

Формат yyyy-mm-dd hh:mm:ss

- "2014-04-26 17:24:37.3186369",

- "2012-08-03 18:31:59.257000000",
- "2014-04-26 17:24:37.123",
- "2013-04-01 22:43",
- "2013-04-01 22:43:22",
- "2014-12-16 06:20:00 UTC",
- "2014-12-16 06:20:00 GMT",
- "2014-04-26 05:24:37 PM",
- "2014-04-26 13:13:43 +0800",
- "2014-04-26 13:13:43 +0800 +08",
- "2014-04-26 13:13:44 +09:00",
- "2012-08-03 18:31:59.257000000 +0000 UTC",
- "2015-09-30 18:48:56.35272715 +0000 UTC",
- "2015-02-18 00:12:00 +0000 GMT",
- "2015-02-18 00:12:00 +0000 UTC",
- "2015-02-08 03:02:00 +0300 MSK m=+0.000000001",
- "2015-02-08 03:02:00.001 +0300 MSK m=+0.000000001",
- "2017-07-19 03:21:51+00:00",
- "2014-04-26",
- "2014-04",
- "2014",
- "2014-05-11 08:20:13,787".

Формат yyyy-mm-dd-07:00

"2020-07-20+08:00"

Формат mm.dd.yyyy

- "3.31.2014",
- "03.31.2014",
- "08.21.71".

Формат yyyy.mm.dd

"2014.03.30"

Формат yyyymmdd и аналогичные

- "20140601",
- "20140722105203".

Формат yymmdd hh:mm:yy

"171113 14:14:20"

Формат Unix timestamp

- "1332151919",
- "1384216367189",
- "1384216367111222",
- "13842163671112223333".

Сопоставление полей предустановленных нормализаторов

В файле, доступном по ссылке для скачивания, представлено описание сопоставления полей предустановленных нормализаторов.

Скачать Описание сопоставления полей предустановленных нормализаторов.ZIP

Глоссарий

Bootstrap

Базовая среда выполнения, включающая кластер Kubernetes и компоненты инфраструктуры для работы Open Single Management Platform. Bootstrap входит в транспортный архив и автоматически устанавливается при развертывании Open Single Management Platform.

Kaspersky Deployment Toolkit

Утилита, используемая для развертывания и управления кластером Kubernetes, компонентами Open Single Management Platform и веб-плагинами управления. KDT работает на устройстве администратора и подключается к целевым устройствам с помощью SSH.

Агент

Сервисы KUMA, которые используются для получения событий на удаленных устройствах и пересылки их коллекторам KUMA.

Актив

Устройство или пользователь защищаемой инфраструктуры. Если на активе обнаружен алерт или инцидент, вы можете выполнить действия по реагированию для этого актива.

Алгоритм плейбука

Алгоритм, включающий последовательность действий по реагированию, которые помогают анализировать и обрабатывать алерты или инциденты.

Алерт

Событие в ИТ-инфраструктуре организации, которое было отмечено Open Single Management Platform как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуре организации.

Граф расследования

Инструмент для визуального анализа, который показывает отношения между событиями, алертами, инцидентами, наблюдаемыми объектами и активами (устройствами). На графе расследования отображается подробная информация об инциденте: соответствующие алерты, пользователи, активы и их общие свойства.

Действия по реагированию

Действия, запускаемые в плейбуках.

Дистрибутив

Архив, содержащий транспортный архив с компонентами Open Single Management Platform и Лицензионными соглашениями для Open Single Management Platform и KDT, а также архив с утилитой KDT и шаблонами конфигурационного файла и файлом инвентаря KUMA.

Инцидент

Контейнер алертов, который обычно указывает на истинно положительное обнаружение проблемы в ИТ-инфраструктуре организации. Инцидент может содержать один или несколько алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему.

Кластер Kubernetes

Набор устройств, объединенных с помощью Kubernetes в один вычислительный ресурс. Кластер Kubernetes используется для работы компонентов Open Single Management Platform (кроме сервисов KUMA). Кластер Kubernetes может включать в себя как целевые устройства, так и устройство администратора.

Коллектор

Сервис KUMA, который получает сообщения от источников событий, обрабатывает их, а затем передает их в хранилище, коррелятор и/или сторонние службы для идентификации алертов.

Контекст

Набор параметров доступа, определяющих кластер Kubernetes, с которым пользователь может выбрать взаимодействие. Контекст также включает данные для подключения к кластеру с помощью KDT.

Конфигурационный файл

Файл в формате YAML, содержащий список целевых устройств для развертывания Open Single Management Platform и набор параметров для установки компонентов Open Single Management Platform. Конфигурационный файл используется KDT.

Коррелятор

Сервис KUMA, анализирующий нормализованные события.

Мультитенантность

Режим, который позволяет главному администратору предоставлять функциональность Open Single Management Platform нескольким клиентам независимо или разделять активы и параметры приложения и объекты для разных офисов. Также режим мультитенантности позволяет копировать и наследовать параметры и объекты тенанта от родительского тенанта, а также автоматически распространять лицензионный ключ Open Single Management Platform для всех тенантов в иерархии.

Наблюдаемые объекты

Объекты, связанные с алертом и инцидентом, такие как хеши MD5 и SHA256, IP-адрес, веб-адрес, имя домена, имя пользователя или имя устройства.

Нормализованное событие

Событие, которое обрабатывается в соответствии с нормализованной моделью данных событий KUMA.

Плейбук

Объект, который реагирует на алерты или инциденты в соответствии с заданным алгоритмом (алгоритмом плейбука). Плейбуки позволяют автоматизировать рабочие процессы и сокращать время, необходимое для обработки алертов и инцидентов.

Пользовательские действия

KDT – это команда, позволяющая выполнять дополнительные операции, специфичные для компонентов Open Single Management Platform (кроме установки, обновления, удаления).

Правила сегментации

Правила, которые позволяют автоматически разделять связанные алерты на отдельные инциденты в зависимости от заданных условий.

Правило корреляции

Ресурс KUMA, используемый для распознавания определенных последовательностей обработанных событий и выполнения заданных действий после распознавания.

Реестр

Компонент инфраструктуры, в котором хранятся контейнеры приложений и который используется для установки и хранения компонентов Open Single Management Platform.

Сервисы KUMA

Основные компоненты KUMA, которые помогают системе управлять событиями. Сервисы позволяют получать события из источников событий и в дальнейшем приводить их к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа. Сервисы KUMA (агенты, коллекторы, корреляторы и хранилища) устанавливаются на устройства, расположенные вне кластера Kubernetes.

Событие

События информационной безопасности, зарегистрированные на контролируемых элементах ИТ-инфраструктуры организации. Например, события включают попытки входа в систему, взаимодействия с базой данных и многоадресную рассылку информации. Каждое отдельное событие может показаться бессмысленным, но, если рассматривать их вместе, они формируют более широкую картину сетевой активности, которая помогает идентифицировать угрозы безопасности.

Тенант

Логический объект, соответствующий организационной единице (клиенту или офису), которой предоставляется функциональность Open Single Management Platform. Каждый тенант может включать в себя активы, пользователей и их права доступа, события, алерты, инциденты, плейбуки, а также интеграцию с другими приложениями, службами и решениями "Лаборатории Касперского". Также тенант определяет набор доступных операций с включенными объектами.

Транспортный архив

Архив, который содержит компоненты Open Single Management Platform и веб-плагинов управления и Лицензионные соглашения Open Single Management Platform и KDT. Транспортный архив включен в дистрибутив.

Узел

Физическая или виртуальная машина, на которой будет развернут Open Single Management Platform. Есть первичный и рабочий узлы. Первичный узел предназначен для управления кластером, хранения метаданных и распределения рабочей нагрузки. Рабочие узлы предназначены для выполнения рабочей нагрузки компонентов Open Single Management Platform.

Устройство администратора

Физическая или виртуальная машина, которая используется для развертывания и управления кластером Kubernetes и Open Single Management Platform с помощью KDT. KDT работает на устройстве администратора. Если устройство администратора не включено в кластер Kubernetes, оно будет использоваться только для развертывания. Если устройство администратора включено в кластер, оно также будет действовать как целевое устройство, которое используется для работы компонентов Open Single Management Platform.

Файл инвентаря KUMA

Файл в формате YAML, который содержит параметры для установки сервисов KUMA, не включенных в кластер Kubernetes. Путь к файлу инвентаря KUMA включен в конфигурационный файл, который используется KDT для развертывания Open Single Management Platform.

Хранилище

Сервис KUMA, который используется для хранения нормализованных событий, чтобы к ним можно было быстро и постоянно получать доступ из KUMA с целью извлечения аналитических данных.

Целевые устройства

Физические или виртуальные машины, на которых устанавливается Open Single Management Platform. Целевые устройства включены в кластер Kubernetes. Компоненты Open Single Management Platform работают на этих устройствах.

Цепочка развития угрозы

Последовательность шагов, позволяющих отслеживать стадии кибератаки. Цепочка развития угроз позволяет проанализировать причины возникновения угрозы. Для создания цепочки развития угрозы управляемое приложение передает данные с устройства на Сервер администрирования с помощью Агента администрирования.

Информация о стороннем коде

Информация о стороннем коде содержится в файлах legal_notices_ksmp.txt и legal_notices_kuma.txt на устройстве, которое выступает в роли узла оператора. Файлы находятся в директории /home/kdt/ пользователя, который запускает установку Open Single Management Platform.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash, PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD, AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS, and AWS Marketplace являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Apache, and Apache Cassandra являются либо зарегистрированными товарными знаками, либо товарными знаками Apache Software Foundation.

Apple, App Store, AppleScript, Carbon, FileVault, iPhone, Mac, Mac OS, macOS, OS X, Safari, QuickTime – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

LTS, and Ubuntu являются зарегистрированными товарными знаками Canonical Ltd.

Check Point NGFW – товарный знак или зарегистрированный товарный знак Check Point Software Technologies Ltd. или аффилированных компаний.

Cisco, IOS, and Snort являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix, XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Citrix NetScaler является зарегистрированным товарным знаком или товарным знаком компании Cloud Software Group, Inc. и/или ее дочерних компаний в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

CorelDRAW – товарный знак или зарегистрированный в Канаде, США и/или других странах товарный знак Corel Corporation и/или ее дочерних компаний.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Elasticsearch – зарегистрированный в США и других странах товарный знак Elasticsearch BV.

F5 – товарный знак F5 Networks, Inc. в США и в некоторых других странах.

Firebird – зарегистрированный товарный знак Firebird Foundation.

Fortinet, FortiGate, FortiMail, FortiSOAR – товарные знаки или зарегистрированные в США и/или других странах товарные знаки Fortinet, Inc.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Maps, Google Play, Google Public DNS – товарные знаки Google LLC.

HUAWEI, EulerOS, Huawei Eudemon являются товарными знаками Huawei Technologies Co., Ltd.

ViPNet является зарегистрированным товарным знаком компании "ИнфоТеКС".

IBM, Guardium, InfoSphere, QRadar – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Insider – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Node.js – товарный знак Joyent, Inc.

Juniper, Juniper Networks, and JUNOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Juniper Networks, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Kubernetes является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Microsoft, Access, Active Directory, ActiveSync, ActiveX, BitLocker, Excel, Halo, Hyper-V, InfoPath, Internet Explorer, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, SQL Server, Tahoma, Visio, Win32, Windows, Windows Media, Windows Mobile, Windows Phone, Windows PowerShell, Windows Server, Windows Vista являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

Mozilla, Firefox являются товарными знаками Mozilla Foundation в США и других странах.

NetApp – товарный знак или зарегистрированный в США и/или других странах товарный знак NetApp, Inc.

Netskope, логотип Netskope и другие названия продуктов Netskope, упомянутые в настоящем документе, являются товарными знаками Netskope, Inc. и/или одной из ее дочерних компаний и могут быть зарегистрированы в Ведомстве по патентам и товарным знакам США и в других странах.

NetWare – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Novell – товарный знак Novell Enterprises Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Oracle, Java, and JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

PROOFPOINT является товарным знаком Proofpoint, Inc. в США и других странах.

Chef – товарный знак или зарегистрированный в США и/или других странах товарный знак Progress Software Corporation и/или одной из дочерних или аффилированных компаний.

Puppet – товарный знак или зарегистрированный товарный знак Puppet, Inc.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

Red Hat, CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

The Trademark BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Samsung – товарный знак компании SAMSUNG в США или других странах.

Sendmail и другие наименования и названия продуктов – товарные знаки или зарегистрированные товарные знаки Sendmail, Inc.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Splunk – товарный знак и зарегистрированный в США и других странах товарный знак Splunk, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

OpenAPI – товарный знак компании The Linux Foundation.

Trend Micro является товарным знаком или зарегистрированным товарным знаком Trend Micro Incorporated.

Наименования, изображения и логотипы, идентифицирующие продукты и услуги UserGate, являются фирменными знаками UserGate и/или ее дочерних компаний или филиалов, а сами продукты являются собственностью UserGate.

VMware, VMware ESXi, VMware Horizon, VMware vCenter, VMware vSphere, VMware Workstation – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

ClickHouse – товарный знак компании YANDEX LLC.

Zabbix – зарегистрированный товарный знак Zabbix SIA.