MaxPatrol O2 версия 2023.4

Руководство администратора

Дата редакции документа: 14.11.2023

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию MaxPatrol O2. Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку, первоначальную настройку и администрирование MaxPatrol O2.

Комплект документации MaxPatrol O2 включает в себя следующие документы:

— Этот документ.

— Руководство пользователя — содержит пошаговые инструкции и справочную информацию об использовании продукта для защиты информационных активов организации.

В этом разделе

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о MaxPatrol O2

Вы можете найти дополнительную информацию о MaxPatrol O2 на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 11).

2. О MaxPatrol O2

MaxPatrol O2 — система, предназначенная для автоматического обнаружения действий злоумышленников и предотвращения недопустимых событий в IT-инфраструктуре организации.

MaxPatrol O2 упрощает работу экспертов по ИБ: на одной странице веб-интерфейса эксперт видит последовательность хакерских действий и набор рекомендаций по пресечению активности злоумышленника. MaxPatrol O2 позволяет своевременно и точно реагировать на угрозу, что дает возможность свести к минимуму неблагоприятное влияние на сетевую инфраструктуру.

Ключевые функции MaxPatrol O2:

- **Автоматическое выявление цепочки подозрительных событий.** Анализ событий ИБ, происходящих в инфраструктуре организации, выявление связей между ними и определение ресурсов, затронутых в событиях. Формирование цепочек событий и оценка уровня их опасности.
- **Визуализация данных для анализа цепочек событий.** Подробная информация о событиях и ресурсах цепочки представлена на схеме атаки и временной шкале, а также в карточке цепочки. Кроме того, на странице цепочки отображается информация о ближайших недопустимых событиях, которые могут быть реализованы злоумышленником при развитии атаки. По итогам анализа эксперт принимает решение о том, требуется ли дальнейшее реагирование.
- **Запуск реагирования по сценарию.** Формирование сценария реагирования на вредоносную цепочку событий. Сценарий реагирования содержит список действий, направленных на пресечение активности злоумышленника. Сценарий может быть изменен экспертом до начала реагирования.
- **Автоматизированный контроль реагирования.** Предлагается набор статусов, с помощью которых эксперт управляет реагированием на события ИБ и отслеживает, остановлена ли атака в результате такого реагирования.
- **Отправка уведомлений.** Оповещение экспертов о возникновении вредоносной цепочки через Telegram.

3. Архитектура MaxPatrol O2

MaxPatrol O2 имеет сервис-ориентированный тип архитектуры и состоит из микросервисов, сгруппированных в программные компоненты. В этом разделе описаны компоненты MaxPatrol O2 и приведен алгоритм работы системы.

В этом разделе

Компоненты MaxPatrol O2 (см. раздел 3.1)

Алгоритм работы MaxPatrol O2 и схема взаимодействия компонентов (см. раздел 3.2)

3.1. Компоненты MaxPatrol O2

Компонент AdapterMP10SiemV25

Получает данные о корреляционных событиях из системы Positive Technologies MaxPatrol 10 (далее также — MaxPatrol 10), фильтрует и обрабатывает их. В результате обработки выделяется информация, необходимая для создания в MaxPatrol O2 записей о подозрительном событии и задействованных в нем ресурсах.

Компонент Base

Анализирует зарегистрированные события, выявляет целевые атаки в IT-инфраструктуре и обеспечивает реагирование на них. Base также взаимодействует с системой управления пользователями и доступом Positive Technologies Management and Configuration (далее также — PT MC), которая реализует механизм единого входа в системы Positive Technologies, развернутые в инфраструктуре организации.

В состав компонента входят перечисленные ниже микросервисы.

Resources — служба для создания и обновления записей о ресурсах, задействованных в событиях. В качестве источника информации служба использует данные, полученные от компонента AdapterMP10SiemV25, а также сведения о ресурсах из модели активов MaxPatrol 10.

Alerts — служба для обогащения зарегистрированных событий данными о связанных нормализованных событиях, хранящимися в MaxPatrol 10.

Risks — служба для создания и обновления записей о недопустимых событиях, которые могут произойти в IT-инфраструктуре в результате атаки. Сведения о недопустимом событии включают сценарии реализации этого события и критерии выполнения сценария.

Threat Modelling Engine (TME) — служба для моделирования маршрутов атаки в IT-инфраструктуре и расчета кратчайшего пути хакера до реализации недопустимого события. Для работы TME использует информацию о ресурсах, недопустимых событиях и сетевой топологии.

Chains — служба для формирования цепочек из связанных событий по правилам, установленным экспертами Positive Technologies.

Hacker Decision-making Informer (HDMI) — служба для расчета уровня опасности цепочки. Если уровень опасности превышает заданное пороговое значение, HDMI автоматически переводит цепочку в статус **Требует внимания**.

Responder — служба для создания сценария реагирования на цепочку событий. Также Responder отправляет команды на выполнение действий реагирования системе Positive Technologies Extended Detection and Response (далее также — PT XDR) и получает от нее сообщения о результатах реагирования.

> **Примечание.** Если для работы MaxPatrol O2 используется MaxPatrol 10 версии 26.1, реагирование выполняется в системе MaxPatrol Endpoint Detection and Response (далее также — MaxPatrol EDR).

Chains.Queries — служба для сбора информации о цепочках событий и подготовки цепочек для отображения в веб-интерфейсе MaxPatrol O2. Информация агрегируется из служб Chains, HDMI и Responder.

Notifications — служба для отправки уведомлений о возникновении вредоносной цепочки по электронной почте и в Telegram-чат для экспертов по ИБ.

Компонент XdrAdapter

Обеспечивает взаимодействие MaxPatrol O2 с системой PT XDR (MaxPatrol EDR). Компонент получает команду на запуск реагирования согласно сценарию, сформированному Base. XdrAdapter передает команду модулям PT XDR (MaxPatrol EDR), которые выполняют действия по устранению угрозы, например завершают процессы, блокируют сетевой трафик или удаляют файлы. Также XdrAdapter сообщает Base о результатах реагирования.

Компонент RmqMessageBus

Компонент представляет собой брокер сообщений RabbitMQ, который реализует обмен данными между компонентами Base и XdrAdapter.

Компонент Web

Обеспечивает работу пользователя с MaxPatrol O2: предоставляет пользовательский графический интерфейс и поддерживает обмен данными между интерфейсом приложения и службами компонента Base.

Компонент Web взаимодействует с PT MC для журналирования действий пользователей.

Компонент SqlStorage

Обеспечивает централизованное хранение информации, необходимой MaxPatrol O2 на всех этапах работы. Информация хранится в базе данных под управлением СУБД PostgreSQL.

3.2. Алгоритм работы MaxPatrol O2 и схема взаимодействия компонентов

Алгоритм работы MaxPatrol O2:

1. Компонент AdapterMP10SiemV25 запрашивает данные о корреляционных событиях из MaxPatrol 10. Фильтрует полученные данные и извлекает из них информацию для регистрации в MaxPatrol O2 подозрительных событий и ресурсов, задействованных в событиях. Информация передается компоненту Base.
2. AdapterMP10SiemV25 также запрашивает MaxPatrol 10 дополнительную информацию об активах организации — на ее основании позднее компонент Base формирует модель ресурсов.
3. Компонент Base создает в системе записи о событиях и задействованных в них ресурсах и объединяет события в цепочки по правилам, разработанным экспертами Positive Technologies. Также Base по возможности выполняет обогащение событий информацией о связанных нормализованных событиях из MaxPatrol 10.
4. Используя информацию о ресурсах, недопустимых событиях и сетевой топологии, компонент Base просчитывает возможные пути продвижения злоумышленника в инфраструктуре и выявляет кратчайший путь до реализации недопустимого события.
5. Base вычисляет вредоносность каждого события цепочки, устанавливает роли ресурсов, задействованных в этих событиях, и на основании полученных данных рассчитывает вредоносность цепочки.
6. Если цепочка является вредоносной, Base уведомляет эксперта о ее появлении и создает сценарий реагирования на угрозу. Сценарий содержит список действий, которые должны быть выполнены на ресурсах, вовлеченных в события цепочки, для остановки атаки.
7. Эксперт просматривает цепочки событий, анализирует агрегированную в них информацию и принимает решение о реагировании на угрозу. Компонент XdrAdapter передает команду на запуск реагирования в систему PT XDR (MaxPatrol EDR). Выполняя действия по сценарию, модули реагирования пресекают активность злоумышленника в инфраструктуре.

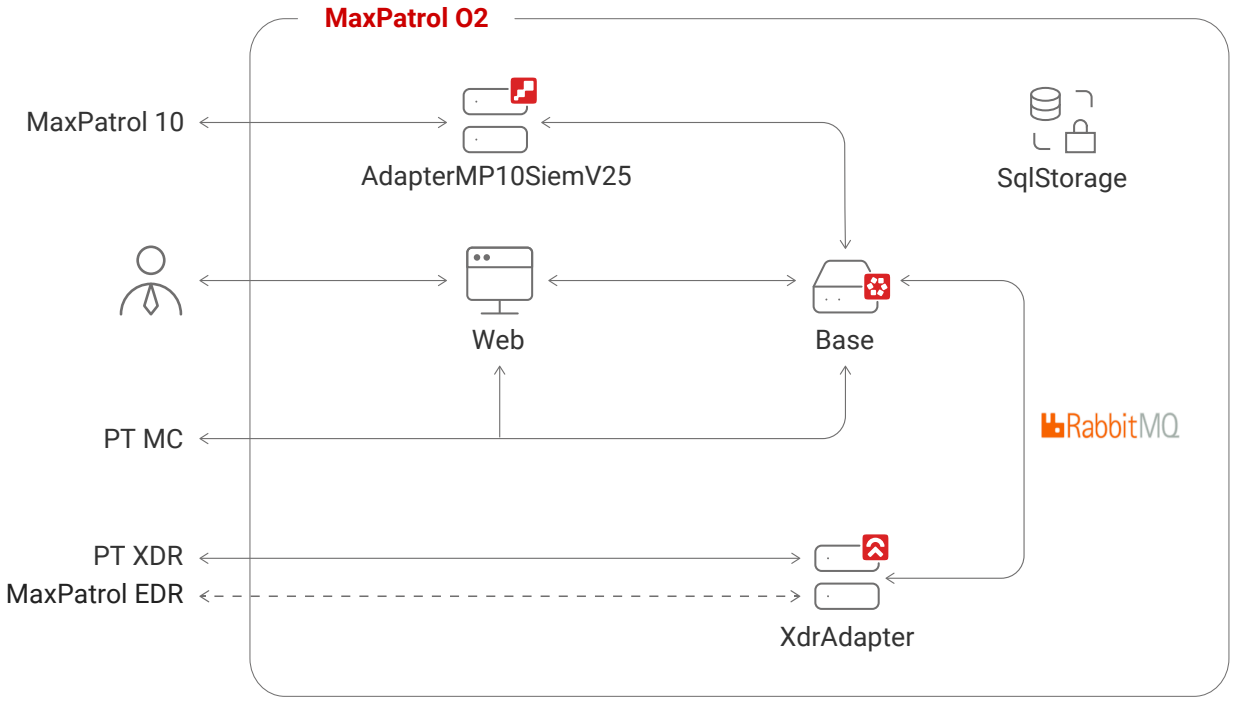

Рисунок 1. Взаимодействие компонентов O2

4. Развертывание MaxPatrol O2

Развертывание MaxPatrol O2 в IT-инфраструктуре организации состоит из следующих этапов:

1. Подготовка к развертыванию MaxPatrol O2.
2. Установка MaxPatrol O2.
3. Если в конфигурации роли AdapterMP10SiemV25 в качестве значения параметра `SiemAdapterEventStreamType` будет выбран вариант `GetEventsPolling` — настройка MaxPatrol 10 для работы с MaxPatrol O2.
4. Если для работы с MaxPatrol O2 будет использоваться MaxPatrol 10 версии 25.0 — создание табличных списков MaxPatrol O2 в MaxPatrol 10, а также их установка в конвейеры обработки событий.
5. Настройка взаимодействия MaxPatrol O2 с PT XDR (или MaxPatrol EDR).

В этом разделе

4.1. Комплект поставки

MaxPatrol O2 поставляется в виде дистрибутива. Объем дистрибутива для текущей версии продукта — 2,53 ГБ.

Архив дистрибутива имеет имя `O2-Application_distro_<номер версии и сборки MaxPatrol O2>.tar`, например `O2-Application_distro_0.9.17.3060.tar`.

Дистрибутив MaxPatrol O2 содержит три папки с дистрибутивами ролей (см. раздел 4.5). Название каждой папки соответствует названию приложения, которое создается после установки ролей из этой папки.

В состав дистрибутива MaxPatrol O2 входит:

— папка `Deployment-Application` с дистрибутивом роли Deployer;

— папка `MC-Application` с дистрибутивами ролей ManagementAndConfiguration и SqlStorage;

— папка `O2-Application` с дистрибутивами ролей Base, AdapterMP10SiemV25, XdrAdapter, Web и RmqMessageBus.

4.2. Аппаратные и программные требования

Компоненты системы MaxPatrol O2 необходимо устанавливать на двух серверах, удовлетворяющих приведенным ниже требованиям.

Таблица 2. Аппаратные требования к серверу MaxPatrol O2

Компонент сервера	Рекомендуемые требования
Процессор	64 ядра с тактовой частотой 2,2 ГГц, архитектура — x86-64
Память (ОЗУ)	256 ГБ
Дисковое пространство	10 ТБ SSD (6 × 1,92 ТБ SSD, объединенных в массив RAID 5) 24 ТБ HDD (6 × 8 ТБ 7,2 K RPM HDD, объединенных в массив RAID 10)
Сетевые подключения	2 × 1 Гбит/с, RJ-45 2 × 10 Гбит/с, SFP+

MaxPatrol O2 поддерживает установку на чистую 64-разрядную операционную систему семейства Linux — Debian 10 или Astra Linux 1.7.

Для установки или обновления Debian необходимо использовать полный установочный образ. Он содержит необходимый набор пакетов и не требует подключения к интернету (подробнее см. на сайте debian.org).

Пользовательский интерфейс MaxPatrol O2 работает в браузерах:

— Google Chrome версий 99.0 и выше;

— Mozilla Firefox версий 97.0 и выше.

4.3. Подготовка к развертыванию MaxPatrol O2 с установкой MaxPatrol 10 версии от 25.0 до 26.0

Перед развертыванием MaxPatrol O2 необходимо:

1. Выполнить развертывание MaxPatrol 10 версии от 25.0 до 26.0, PT MC и PT XDR в инфраструктуре организации.
2. Установить операционную систему Debian 10 или Astra Linux 1.7 на серверы, где планируется развертывание MaxPatrol O2.
3. Обеспечить доступ к серверам MaxPatrol 10, PT MC, PT XDR и MaxPatrol O2 по протоколу HTTP. По умолчанию для подключения к PT MC используется порт 3334, для подключения к PT XDR — порт 443.
4. Обеспечить доступ к серверам MaxPatrol 10, PT MC, PT XDR и MaxPatrol O2 по протоколу SSH.
5. Синхронизировать время на серверах MaxPatrol 10, PT MC, PT XDR и MaxPatrol O2.
6. Установить на серверы MaxPatrol O2 вспомогательные пакеты unzip и curl с помощью команд:
   ```
   apt-get install unzip
   apt-get install curl
   ```
7. Получить токен доступа к PT XDR.

   Примечание. Для получения токена доступа необходимо на сервере PT XDR в каталоге `/opt/edr` выполнить команду `./register_client --privileges pt.edr.ui.services.api.view,pt.edr.ui.groups.api.view,pt.edr.ui.modules.interactive,pt.edr.ui.agents.api.view,pt.edr.ui.policies.api.view --client-id <Идентификатор экземпляра MaxPatrol O2, который будет использовать токен>`.

4.4. Подготовка к развертыванию MaxPatrol O2 с установкой MaxPatrol 10 версии выше 26.0

Перед развертыванием MaxPatrol O2 необходимо:

1. Выполнить развертывание MaxPatrol 10 версии 26.1, PT MC и MaxPatrol EDR в инфраструктуре организации.
2. Установить операционную систему Debian 10 или Astra Linux 1.7 на серверы, где планируется развертывание MaxPatrol O2.
3. Обеспечить доступ к серверам MaxPatrol 10, PT MC и MaxPatrol O2 по протоколу HTTP. По умолчанию для подключения к PT MC используется порт 3334.
4. Обеспечить доступ к серверам MaxPatrol 10, PT MC и MaxPatrol O2 по протоколу SSH. Если конфигурация MaxPatrol EDR многосерверная — обеспечить доступ к серверу агентов MaxPatrol EDR по протоколу SSH.

5. Синхронизировать время на серверах MaxPatrol 10, PT MC и MaxPatrol O2.
6. Установить на серверы MaxPatrol O2 вспомогательные пакеты unzip и curl с помощью команд:
```
apt-get install unzip
apt-get install curl
```
7. Получить токен доступа к MaxPatrol EDR.

   Примечание. Для получения токена доступа необходимо на сервере MaxPatrol 10 с установленным компонентом MaxPatrol 10 Core в каталоге `/opt/edr` выполнить команду `./register_client --privileges pt.edr.ui.services.api.view,pt.edr.ui.groups.api.view,pt.edr.ui.modules.interactive,pt.edr.ui.agents.api.view,pt.edr.ui.policies.api.view --client-id <Идентификатор экземпляра MaxPatrol O2, который будет использовать токен>`.

4.5. Об установке компонентов MaxPatrol O2 с помощью ролей

Роль является базовой единицей развертывания MaxPatrol O2 и представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Каждая роль поставляется в виде отдельного архива, который может содержать Docker-образы или deb-пакеты.

При развертывании системы создаются экземпляры ролей, которые распределяются по приложениям определенного типа (Deployment-Application, MC-Application, O2-Application). Такая архитектура позволяет гибко и удобно развертывать систему, а также обновлять и настраивать ее в дальнейшем. Тип приложения определяется составом входящих в него экземпляров ролей:

— приложение Deployment-Application содержит только роль Deployer;

— приложение MC-Application — только роли ManagementAndConfiguration и SqlStorage;

— приложение O2-Application — только роли Base, AdapterMP10SiemV25, XdrAdapter, Web и RmqMessageBus.

Примечание. При развертывании системы можно создать несколько приложений одного типа (например, несколько приложений O2-Application), однако такие конфигурации не поддерживаются производителем.

Управление развертыванием обеспечивается ролью Deployer, которая построена на базе системы управления конфигурациями SaltStack. Ее модуль Salt Master обеспечивает общее управление установкой ролей (созданием их экземпляров), модули Salt Minion — установку ролей на каждый сервер системы.

В общем случае установка роли делится на следующие этапы:

1. Распаковка архива и запуск сценария установки.

Внимание! Сценарий установки `install.sh` необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

2. Выбор приложения для установки роли. Вам потребуется или выбрать ранее созданное приложение необходимого типа, или создать новое, если приложение необходимого типа отсутствует. При создании приложения нужно ввести его идентификатор, который среди прочего будет использоваться в качестве имени каталога для размещения файлов всех экземпляров ролей, входящих в состав данного приложения.

   Примечание. Вы можете использовать идентификаторы, предлагаемые системой по умолчанию. Например, если для приложения O2-Application использовать предлагаемый по умолчанию идентификатор `o2-application`, файлы всех экземпляров ролей этого приложения будут размещены в каталоге `/var/lib/deployed-roles/o2-application`.

3. Ввод названия экземпляра роли и выбор сервера для ее установки. Введенное название среди прочего будет использоваться в качестве имени каталога для размещения файлов создаваемого экземпляра роли (например, файлов журналов и файлов конфигурации).

   Примечание. Вы можете использовать названия, предлагаемые системой по умолчанию. Например, если для роли Base использовать предлагаемое по умолчанию название `base`, файлы этого экземпляра роли будут размещены в каталоге `/var/lib/deployed-roles/o2-application/base`.

4. Проверка и изменение параметров конфигурации.
5. Запуск установки.

4.6. Установка MaxPatrol O2

Для установки MaxPatrol O2 необходимо:

1. Сохранить архив с дистрибутивом на сервер, где будет устанавливаться MaxPatrol O2.
2. Распаковать архив с дистрибутивом.
3. Установить роль Deployer (см. раздел 4.6.1).
4. Установить роль SqlStorage (см. раздел 4.6.2).
5. Установить роль RmqMessageBus (см. раздел 4.6.3).
6. Установить роль Base (см. раздел 4.6.4).
7. Установить роль Web (см. раздел 4.6.5).
8. Установить роль XdrAdapter (см. раздел 4.6.6).
9. Установить роль AdapterMP10SiemV25 (см. раздел 4.6.7).

   Внимание! Установку ролей необходимо выполнять в приведенном выше порядке.

В этом разделе

См. также

Установка роли XdrAdapter (см. раздел 4.6.6)

4.6.1. Установка роли Deployer

Для установки роли вам потребуется архив `pt_Deployer_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `pt_Deployer_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_Deployer_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_Deployer_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите кнопку **I Accept**, чтобы принять их.

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

   Откроется страница со списком основных параметров.
6. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль Deployer.
7. Нажмите кнопку **OK**.

   Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
8. Нажмите кнопку **OK**.

Роль установлена.

4.6.2. Установка роли SqlStorage

Для установки роли вам потребуется архив `pt_SqlStorage_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `pt_SqlStorage_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_SqlStorage_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_SqlStorage_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MaxPatrol O2.
9. В открывшемся окне введите название экземпляра роли SqlStorage и нажмите кнопку **OK**.

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

    Откроется страница со списком основных параметров.
11. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль SqlStorage.
12. Нажмите кнопку **OK**.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

4.6.3. Установка роли RmqMessageBus

Для установки роли вам потребуется архив `RmqMessageBus_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `RmqMessageBus_<Номер версии>.tar.gz`:
   ```
   tar -xf RmqMessageBus_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   RmqMessageBus_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения O2 Application и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MaxPatrol O2.
9. В открывшемся окне введите название экземпляра роли RmqMessageBus и нажмите кнопку **OK**.

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

    Откроется страница со списком основных параметров.
11. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль RmqMessageBus.
12. Нажмите кнопку **OK**.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.

Роль установлена.

4.6.4. Установка роли Base

Для установки роли вам потребуется архив `Base_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `Base_<Номер версии>.tar.gz`:
   ```
   tar -xf Base_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   Base_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения O2 Application и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MaxPatrol O2.
9. В открывшемся окне введите название экземпляра роли Base и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Advanced configuration**.

    Откроется страница со списком расширенных параметров.
11. В качестве значения параметра `ApplicationDisplayName` укажите название экземпляра MaxPatrol O2.
12. Если требуется, измените значение параметра `ClientId`.

    Внимание! Если в организации установлено несколько экземпляров MaxPatrol O2, значение параметра `ClientId` должно быть уникальным для каждого экземпляра, зарегистрированного в PT MC.
13. Если требуется, включите журналирование работы роли Base в Docker-контейнерах, установив флажок **EnableLogToConsole**.
14. Если MaxPatrol O2 будет взаимодействовать с MaxPatrol 10 версии 26.1 и с PT MC версии 101.0 или ниже, включите журналирование работы роли Base в файлы служб, установив флажок **EnableLogToFiles**.

15. В качестве значения параметра `MCAddress` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration.
16. В качестве значения параметра `SiemCoreUrl` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core.
17. В качестве значения параметров `HostAddress`, `PostgreHost`, `UIHostAddress` укажите IP-адрес или FQDN сервера MaxPatrol O2, на который устанавливается роль Base.
18. Нажмите кнопку **OK**.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
19. Нажмите кнопку **OK**.

Роль установлена.

4.6.5. Установка роли Web

Для установки роли вам потребуется архив `Web_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `Web_<Номер версии>.tar.gz`:
   ```
   tar -xf Web_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   Web_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения O2 Application и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MaxPatrol O2.
9. В открывшемся окне введите название экземпляра роли Web и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Advanced configuration**.

    Откроется страница со списком расширенных параметров.

11. Если требуется, измените значение параметра `ClientId`.

    Внимание! Если в организации установлено несколько экземпляров MaxPatrol O2, значение параметра `ClientId` должно быть уникальным для каждого экземпляра, зарегистрированного в PT MC.

12. В качестве значения параметра `MCAddress` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration.

13. В качестве значения параметра `SiemCoreUrl` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core.

14. В качестве значения параметров `ApiGatewayHost` и `HostAddress` укажите IP-адрес или FQDN сервера MaxPatrol O2, на который устанавливается роль Web.

15. Нажмите кнопку **OK**.

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

16. Нажмите кнопку **OK**.

Роль установлена.

4.6.6. Установка роли XdrAdapter

Для установки роли вам потребуется архив `XdrAdapter_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `XdrAdapter_<Номер версии>.tar.gz`:
   ```
   tar -xf XdrAdapter_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   XdrAdapter_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.

4. Выберите вариант **Create New Application**.

5. В открывшемся окне введите идентификатор приложения O2 Application и нажмите кнопку **OK**.

6. В окне **Instance selection** выберите вариант **Deploy New Instance**.

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

8. В открывшемся окне выберите вариант с доменным именем сервера MaxPatrol O2.

9. В открывшемся окне введите название экземпляра роли XdrAdapter и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.

10. Выберите вариант **Advanced configuration**.

    Откроется страница со списком расширенных параметров.

11. Если требуется, измените значение параметра `ClientId`.

    Внимание! Если в организации установлено несколько экземпляров MaxPatrol O2, значение параметра `ClientId` должно быть уникальным для каждого экземпляра, зарегистрированного в PT MC.

12. Если требуется, включите журналирование работы роли XdrAdapter в Docker-контейнере, установив флажок **EnableLogToConsole**.

13. Если MaxPatrol O2 будет взаимодействовать с MaxPatrol 10 версии 26.1 и с PT MC версии 101.0 или ниже, включите журналирование работы роли XdrAdapter в файлы служб, установив флажок **EnableLogToFiles**.

14. Если MaxPatrol O2 будет взаимодействовать с MaxPatrol 10 версии от 25.0 до 26.0, укажите значения параметров:

    ```
    EdrToken: '<Токен доступа к PT XDR, полученный при подготовке к развертыванию MaxPatrol O2>'
    EdrUri: <Протокол WebSocket (ws или wss)>://<IP-адрес или FQDN управляющего сервера PT XDR>
    ```

15. Если MaxPatrol O2 будет взаимодействовать с MaxPatrol 10 версии выше 26.0, укажите значения параметров:

    ```
    EdrToken: '<Токен доступа к MaxPatrol EDR, полученный при подготовке к развертыванию MaxPatrol O2>'
    EdrUri: <Протокол WebSocket (ws или wss)>://<IP-адрес или FQDN сервера MaxPatrol 10 с установленным компонентом MaxPatrol 10 Core>
    ```

16. В качестве значения параметра `MCAddress` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration.

17. В качестве значения параметра `SiemCoreUrl` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core.

18. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера MaxPatrol O2, на который устанавливается роль XdrAdapter.

19. Нажмите кнопку **OK**.

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

20. Нажмите кнопку **OK**.

Роль установлена.

4.6.7. Установка роли AdapterMP10SiemV25

Для установки роли вам потребуется архив `AdapterMP10SiemV25_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `AdapterMP10SiemV25_<Номер версии>.tar.gz`:
   ```
   tar -xf AdapterMP10SiemV25_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   AdapterMP10SiemV25_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения O2 Application и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MaxPatrol O2.
9. В открывшемся окне введите название экземпляра роли AdapterMP10SiemV25 и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Advanced configuration**.

    Откроется страница со списком расширенных параметров.
11. Если требуется, измените значение параметра `ClientId`.

    Внимание! Если в организации установлено несколько экземпляров MaxPatrol O2, значение параметра `ClientId` должно быть уникальным для каждого экземпляра, зарегистрированного в PT MC.
12. Если требуется, включите журналирование работы роли AdapterMP10SiemV25 в Docker-контейнере, установив флажок **EnableLogToConsole**.
13. В качестве значения параметра `MCAddress` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration.
14. В качестве значения параметра `SiemCoreUrl` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core.

15. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера MaxPatrol O2, на который устанавливается роль AdapterMP10SiemV25.
16. Нажмите кнопку **OK**.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
17. Нажмите кнопку **OK**.

Роль установлена.

4.7. Настройка MaxPatrol 10 для работы с MaxPatrol O2

Если в конфигурации роли AdapterMP10SiemV25 в качестве значения параметра `SiemAdapterEventStreamType` выбран вариант `GetEventsPolling`, необходимо настроить взаимодействие MaxPatrol O2 и MaxPatrol 10. Настройка выполняется на сервере MaxPatrol 10 с установленным компонентом MaxPatrol 10 Core.

Действия по настройке MaxPatrol 10 в Windows необходимо выполнять от имени администратора, в Debian — от имени суперпользователя (root).

► Чтобы настроить MaxPatrol 10:

1. Создайте файл `events.conf` со следующим содержимым:

```
location /siem-events/ {
rewrite /siem-events/(.+) /$1 break;
#Настройка доступа к адресам клиента
proxy_set_header Host $http_host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $scheme;
proxy_set_header X-Forwarded-Host $host:$server_port;
proxy_set_header X-Forwarded-Server $host;
#Настройка WebSocket
proxy_http_version 1.1;
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection $connection_upgrade;
#Проксирование запроса
proxy_pass https://<IP-адрес или FQDN сервера MaxPatrol 10>:8013
}
```

   Внимание! Если версия MaxPatrol 10 ниже 26.0, необходимо в значении параметра `proxy_pass` указать протокол HTTP, например: `proxy_pass http://<IP-адрес или FQDN сервера MaxPatrol 10>:8013`

2. Сохраните файл по адресу:

   - Если на сервере установлена Windows: `C:\ProgramData\Positive Technologies\MaxPatrol 10 Core\Config\ReverseProxy.Nginx\nginx-server`

- Если на сервере установлена Debian: `/var/lib/deployed-roles/mp10-application/core/config/reverse.proxy.nginx/nginx-server/`

3. Выполните одно из следующих действий:

   - Если на сервере установлена Windows, перезапустите службу Core.ReverseProxy.Nginx.Host.
   - Если на сервере установлена Debian, перезапустите контейнер ui-core-web.MP10-Application.Core.

MaxPatrol 10 настроен для работы с MaxPatrol O2.

4.8. Табличные списки MaxPatrol O2 в MaxPatrol 10

Если для работы с MaxPatrol O2 будет использоваться MaxPatrol 10 версии 25.0, необходимо вручную создать табличные списки MaxPatrol O2 в MaxPatrol 10 и установить их в конвейеры обработки событий. В MaxPatrol 10 версии 25.1 или выше табличные списки MaxPatrol O2 будут созданы и установлены в конвейеры обработки событий автоматически.

Информация, необходимая для создания табличных списков MaxPatrol O2 (перечень списков, их названия, а также PDQL-запросы, на основе которых будут сформированы списки), содержится в файле `ResourceAssetsMapping_0.0.0.1.yaml`. Файл расположен в Docker-контейнере с названием вида `resources.o2-application.base-<Имя экземпляра>`. Вы можете узнать название контейнера по команде `docker ps | awk '/ resource/ {print $NF}'`.

> **Примечание.** Для удобного просмотра файла вы можете скопировать его из контейнера в каталог пользователя, выполнив команду: `docker cp $(docker ps | awk '/resource/ {print $NF}'):/usr/local/bin/microservice/Layers/ResourceAssetsMapping_0.0.0.1.yaml /<Путь к каталогу>`.

Подробнее о создании табличных списков для данных об активах и об их установке в конвейеры обработки событий см. в Руководстве оператора MaxPatrol 10.

4.9. Настройка взаимодействия MaxPatrol O2 с PT XDR

Для настройки взаимодействия MaxPatrol O2 с PT XDR необходимо обеспечить доступ к PT XDR и добавить модуль `o2_dispatcher` в каждую группу модулей реагирования PT XDR, с которыми должен работать MaxPatrol O2. Подробнее о работе с модулями реагирования PT XDR см. в Руководстве администратора PT XDR.

4.10. Настройка взаимодействия MaxPatrol O2 с MaxPatrol EDR

Для настройки взаимодействия MaxPatrol O2 с MaxPatrol EDR необходимо обеспечить доступ к MaxPatrol EDR и добавить модуль `o2_dispatcher` в каждую группу модулей реагирования MaxPatrol EDR, с которыми должен работать MaxPatrol O2. Подробнее о работе с модулями реагирования MaxPatrol EDR см. в Руководстве администратора MaxPatrol EDR.

4.11. Параметры базовой конфигурации ролей MaxPatrol O2

В этом разделе приведены описания параметров и их значения по умолчанию.

Таблица 3. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
`PostrgeHost`	IP-адрес или FQDN сервера, с установленной СУБД PostgreSQL	`localhost`
`PostgreUserName`	Логин служебной учетной записи для доступа к СУБД PostgreSQL	`pt_system`
`PostgrePassword`	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	`P@ssw0rdP@ssw0rd`

Таблица 4. Параметры конфигурации роли RmqMessageBus

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью RmqMessageBus	`localhost`
`MCHostAddress`	IP-адрес или FQDN сервера PT MC	`localhost`
`ClientSecret`	Ключ для регистрации приложения RmqMessageBus в PT MC	`secret`
`EnableLogToConsole`	Регистрируются ли системные события в журналах Docker-контейнеров RmqMessageBus	`False`
`EnableLogToFiles`	Регистрируются ли системные события в журналах служб RmqMessageBus	`False`
`EnableCentralLogCollection`	Регистрируются ли системные события в Grafana	`True`

Параметр	Описание	Значение по умолчанию
DlqEnabled	Отправляются ли корреляционные и нормализованные события, которые не удалось обработать, в очередь DLQ	False

Таблица 5. Параметры конфигурации роли Base

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера с установленной ролью Base	localhost
MCHostAddress	IP-адрес или FQDN сервера PT MC	localhost
UIHostAddress	IP-адрес или FQDN сервера с установленной ролью Web	localhost
ApplicationDisplayName	Название экземпляра приложения MaxPatrol O2 в PT MC	MaxPatrol O2
SiemCoreUrl	IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core	https://localhost
ClientSecret	Ключ для регистрации приложения Base в PT MC	secret
EnableLogToConsole	Регистрируются ли системные события в журналах Docker-контейнеров Base	False
EnableLogToFiles	Регистрируются ли системные события в журналах служб Base	False
EnableCentralLogCollection	Регистрируются ли системные события в Grafana	True
BotToken	Токен Telegram-бота, добавленного в чат для экспертов	—
ChatIds	Идентификатор Telegram-чата для экспертов	"[ ]"
SmtpPort	Порт SMTP-сервера для входящих подключений от Base	25
SmtpHost	IP-адрес или FQDN SMTP-сервера	—
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	sender@pt.ru
SmtpUser	Логин служебной учетной записи для подключения Base к SMTP-серверу	user

Параметр	Описание	Значение по умолчанию
`SmtpPassword`	Пароль служебной учетной записи для подключения Base к SMTP-серверу	`P@ssw0rd`
`EmailRecipients`	Адрес электронной почты получателя	`"[ ]"`
`DlqEnabled`	Отправляются ли корреляционные и нормализованные события, которые не удалось обработать, в очередь DLQ	`False`

Таблица 6. Параметры конфигурации роли Web

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью Web	`localhost`
`MCHostAddress`	IP-адрес или FQDN сервера PT MC	`localhost`
`BffFileLogging`	Регистрируются ли события службы BFF в журнале службы	`True`
`BffLogLevel`	Уровень журналирования событий службы BFF. Возможные значения — `debug`, `info`, `warning`, `error` или `critical`	`debug`
`SiemCoreUrl`	IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core	`https://localhost`
`FeatureFlagGraphNew`	Отображается ли на схеме атаки последовательность связей между процессами, задействованными в событии цепочки	`False`
`ClientSecret`	Ключ для регистрации приложения Web в PT MC	`secret`

Таблица 7. Параметры конфигурации роли XdrAdapter

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью XdrAdapter	`localhost`
`MCHostAddress`	IP-адрес или FQDN сервера PT MC	`localhost`
`ClientSecret`	Ключ для регистрации приложения XdrAdapter в PT MC	`secret`
`EnableLogToConsole`	Регистрируются ли системные события в журналах Docker-контейнеров XdrAdapter	`False`

Параметр	Описание	Значение по умолчанию
`EnableLogToFiles`	Регистрируются ли системные события в журналах служб XdrAdapter	`False`
`EnableCentralLogCollection`	Регистрируются ли системные события в Grafana	`True`
`EdrUri`	IP-адрес или FQDN сервера MaxPatrol EDR с указанием протокола WebSocket и порта для входящих подключений от MaxPatrol O2	–
`EdrToken`	Токен доступа к MaxPatrol EDR	–
`DlqEnabled`	Отправляются ли корреляционные и нормализованные события, которые не удалось обработать, в очередь DLQ	`False`

Таблица 8. Параметры конфигурации роли AdapterMP10SiemV25

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью AdapterMP10SiemV25	`localhost`
`MCHostAddress`	IP-адрес или FQDN сервера PT MC	`localhost`
`SiemCoreUrl`	IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core	`https://localhost`
`ClientSecret`	Ключ для регистрации приложения AdapterMP10SiemV25 в PT MC	`secret`
`EnableLogToConsole`	Регистрируются ли системные события в журналах Docker-контейнеров AdapterMP10SiemV25	`False`
`EnableLogToFiles`	Регистрируются ли системные события в журналах служб AdapterMP10SiemV25	`False`
`EnableCentralLogCollection`	Регистрируются ли системные события в Grafana	`True`
`DlqEnabled`	Отправляются ли корреляционные и нормализованные события, которые не удалось обработать, в очередь DLQ	`False`

5. Вход в MaxPatrol O2

Пользовательский интерфейс MaxPatrol O2 доступен в браузере. Вход зарегистрированного пользователя в MaxPatrol O2 выполняется через сервис PT MC, который обеспечивает механизм единого входа (технология single sign-on) в системы Positive Technologies.

► Чтобы войти в MaxPatrol O2:

1. В адресной строке браузера введите IP-адрес или FQDN сервера с установленным компонентом Web.

   Откроется страница входа в PT MC.

2. В поле **Логин** введите Administrator.
3. В поле **Password** введите P@ssw0rd.
4. Нажмите кнопку **Войти**.

   Откроется страница **Цепочки**.

6. Проверка работы MaxPatrol O2 после установки

Проверка работы MaxPatrol O2 должна выполняться при условии, что в MaxPatrol 10 есть события, соответствующие критериям фильтрации, установленным в конфигурационном файле `events.yaml` службы Siemadapter.

► Чтобы проверить работу MaxPatrol O2 после установки,

войдите в веб-интерфейс MaxPatrol O2.

Откроется страница **Цепочки**. Если цепочки событий отображаются, то MaxPatrol O2 работает нормально.

Вы также можете проверить, что в базе данных Alerts есть записи о получении событий из MaxPatrol 10. Для проверки нужно выполнить команду:

```
docker exec -it $(docker ps | awk '/storage-postgres/ {print $NF}') psql -U pt_system
-d alerts -c 'select "Id", "DetectedAt", "SourceId" from read_models."Alerts" order
by "DetectedAt" desc limit 100;'
```

Ответ сервера должен содержать записи о получении событий из MaxPatrol 10.

Если включено журналирование работы служб MaxPatrol O2 в Docker-контейнерах, вы можете проверить наличие ошибок в работе служб, выполнив команды:

```
sudo docker logs <Название контейнера siemadapter> | grep ERROR
sudo docker logs <Название контейнера resources> | grep ERROR
sudo docker logs <Название контейнера alerts> | grep ERROR
sudo docker logs <Название контейнера chains> | grep ERROR
sudo docker logs <Название контейнера web api> | grep ERROR
sudo docker logs <Название контейнера edr> | grep ERROR
sudo docker logs <Название контейнера enrichments> | grep ERROR
sudo docker logs <Название контейнера consul> | grep ERROR
sudo docker logs <Название контейнера hdmi> | grep ERROR
```

Примечание. Информацию о работе каждой службы можно посмотреть в журнале службы. Файл журнала находится в каталоге с названием вида `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/log/<Название службы>`.

При наличии ошибок обратитесь в службу технической поддержки Positive Technologies.

7. Учетные записи пользователей

При развертывании MaxPatrol O2 автоматически создается учетная запись администратора системы. Эту учетную запись невозможно заблокировать, также невозможно изменить ее логин.

Администратор создает учетные записи для пользователей MaxPatrol O2. После создания учетная запись не может быть удалена. Если требуется запретить пользователю вход в систему, необходимо заблокировать его учетную запись.

Для предоставления пользователю доступа к интерфейсу MaxPatrol O2 администратор назначает учетной записи пользователя роль эксперта по ИБ.

Примечание. Учетная запись администратора по умолчанию имеет роль эксперта по ИБ.

В этом разделе

7.1. Создание учетной записи пользователя

► Чтобы создать учетную запись пользователя:

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

   Откроется страница **Пользователи**.

2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.

   В панели **Пользователи <Название приложения>** отобразится список пользователей MaxPatrol O2.

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

   Откроется страница **Новый пользователь**.

4. В блоке параметров **Учетные данные** выберите тип аутентификации.

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

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

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

Учетная запись пользователя создана.

7.2. Назначение пользователю роли эксперта по ИБ

► Чтобы назначить пользователю роль эксперта по ИБ:

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

   Откроется страница **Пользователи**.
2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.

   В панели **Пользователи <Название приложения>** отобразится список пользователей MaxPatrol O2.
3. В списке выберите пользователя, учетной записи которого необходимо назначить роль эксперта по ИБ.

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

   Откроется окно **Роли пользователя <Логин>**.
5. В раскрывающемся списке **MaxPatrol O2** установите флажок **Эксперт по ИБ**.
6. Нажмите кнопку **Сохранить**.

Роль эксперта по ИБ назначена.

7.3. Блокирование и разблокирование учетной записи

► Чтобы заблокировать учетную запись пользователя:

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

   Откроется страница **Пользователи**.
2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.

   В панели **Пользователи <Название приложения>** отобразится список пользователей MaxPatrol O2.
3. В списке выберите пользователя, учетную запись которого необходимо заблокировать.

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

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

Учетная запись заблокирована.

► Чтобы разблокировать учетную запись пользователя:

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

   Откроется страница **Пользователи**.

2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.

   В панели **Пользователи <Название приложения>** отобразится список пользователей MaxPatrol O2.

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

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

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

Учетная запись разблокирована.

8. Создание списка исключений из реагирования

Вы можете создать список ресурсов, в отношении которых не должно выполняться реагирование. Список создается с помощью правил: ресурсы, попадающие под правило, не включаются в сценарий реагирования.

Для добавления правил вы можете использовать описание модели ресурсов MaxPatrol O2. Эта модель описана в файлах `DomainModel.xml`, расположенных в Docker-контейнерах служб MaxPatrol O2. Для удобного просмотра файла вы можете скопировать его из контейнера в каталог пользователя, выполнив команду `docker cp <Идентификатор или название контейнера>:/usr/local/share/microservice/layers/DomainModel.xml/<Путь к каталогу>/DomainModel.xml`.

► Чтобы создать список исключений из реагирования:

1. На сервере MaxPatrol O2 с установленной ролью Base перейдите в каталог `/var/lib/deployed-roles/O2/Base/data/responder/data`.
2. Создайте файл `CustomResourcesList.yaml`.
3. Добавьте в файл правила исключения из реагирования по формату, приведенному ниже.
4. Перейдите в каталог `/var/lib/deployed-roles/O2/Base/images/responder.extended`.
5. Перезапустите службу Responder, выполнив команды:

```
docker-compose stop
docker-compose up
```

Список исключений из реагирования создан и вступил в силу.

Таблица 9. Формат файла CustomResourceList.yaml

Элемент структуры	Описание	Обязательность	Массив
`resourceTypes`	Тип ресурса	Нет	Да
`propertyName`	Параметр ресурса	Нет	Нет

Элемент структуры	Описание	Обязательность	Массив
comparison	Тип данных параметра propertyValues. Возможные значения: — string; — winpath — путь к файлу или папке в файловой системе Windows; — unixpath — путь к файлу или каталогу в файловой системе Unix Значение по умолчанию — string	Нет	Нет
propertyValues	Значение параметра ресурса	Да, если указан параметр ресурса	Да

Значения элементов регистрозависимы, то есть при обработке файла CustomResourcesList.yaml не игнорируется регистр символов.

Пример файла CustomResourcesList.yaml:

```
# Правило для исключения файла с именем example.exe
- resourceTypes:
    - O2.File
  propertyName: Name
  comparison: string
  propertyValues:
    - example.exe
# Правило для исключения внутренних узлов с IP-адресами 192.0.2.10 и 192.0.2.135
-  resourceTypes:
    - Host.InternalHost
- propertyName: IPAddresses
  comparison: string
  propertyValue:
    - 192.0.2.10
    - 192.0.2.135
# Правило для исключения процессов, у которых полный путь к исполняемому файлу в Unix
- /usr/lib/systemd/system
-  resourceTypes:
```

```
  - O2.Process
propertyName: ExePath
comparison: unixpath
propertyValues:
  - /usr/lib/systemd/system
```

9. Журналирование работы MaxPatrol O2

Журналирование работы MaxPatrol O2 позволяет получать информацию, необходимую для поиска и устранения неисправностей в работе системы.

В этом разделе приведена основная информация о журналировании работы MaxPatrol O2.

В этом разделе

9.1. Система журналирования

Если MaxPatrol O2 работает с PT MC версии 101.0 или ниже, информация о системных событиях записывается в журналы служб. Журналы служб расположены в каталогах с названием вида `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol O2>/<Название экземпляра роли/log/<Название службы>`.

Если MaxPatrol O2 работает с PT MC версии 101.1 или выше:

- Информация о работе служб, входящих в состав ролей Base, AdapterMP10SiemV25 и XdrAdapter, сохраняется в СУБД ClickHouse.
- Информация о работе служб, входящих в состав остальных ролей MaxPatrol O2, записывается в журналы служб.

Вы можете отключить журналирование системных событий в ClickHouse. Для этого при установке или обновлении ролей установите флажок **EnableLogToFiles** и снимите флажок **EnableCentralLogCollection**. Информация о системных событиях будет записываться в журналы служб MaxPatrol O2.

9.2. Интеграция с Grafana

Для просмотра записей о системных событиях в ClickHouse используется сервис Grafana.

Grafana устанавливается автоматически при развертывании PT MC версии 101.1 или выше.

После установки веб-интерфейс Grafana доступен по адресу https://<IP-адрес сервера MaxPatrol O2 с установленной ролью O2 Base>:9002. Вместо IP-адреса вы можете использовать имя узла (hostname). По умолчанию имя пользователя admin, пароль P@ssw0rd.

Подробные инструкции по работе с Grafana приведены на сайте вендора.

10. Настройка уведомлений о появлении вредоносной цепочки

Вы можете настроить отправку уведомлений о появлении вредоносной цепочки по электронной почте и в Telegram-чат экспертов по ИБ. Уведомления будут отправляться при переходе цепочки событий из статуса **Собирается** в статус **Требует внимания**. После просмотра уведомления эксперт может приступить к работе с вредоносной цепочкой в интерфейсе MaxPatrol O2 и своевременно принять решение о реагировании на угрозу.

В этом разделе

10.1. Настройка отправки уведомлений по электронной почте

► Чтобы настроить отправку уведомлений о появлении вредоносной цепочки по электронной почте:

1. На сервере MaxPatrol O2 с установленной ролью Base распакуйте архив с дистрибутивом роли Base:
   ```
   tar -xf Base_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   Base_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. В открывшемся окне выберите вариант с идентификатором приложения роли.
5. В открывшемся окне выберите вариант с названием экземпляра роли Base.

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

   Откроется страница со списком расширенных параметров.
7. Укажите значения параметров:
   ```
   SmtpHost: <IP-адрес или FQDN SMTP-сервера>
   SmtpPassword: <Пароль служебной учетной записи для подключения Base к SMTP-серверу>
   SmtpPort: <Порт SMTP-сервера для входящих подключений от MaxPatrol O2>
   EmailSettingsRecipients: ["<Адрес электронной почты получателя>"]
   ```

Примечание. Если уведомления должны отправляться нескольким получателям, в значении массива укажите адреса электронной почты получателей через запятую, например `EmailSettingsRecipients: ["username1@example.com", "username2@example.com"]`.

```
SmtpSender: <Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте>
SmtpUser: <Логин служебной учетной записи для подключения Base к SMTP-серверу>
```

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

8. Нажмите кнопку **OK**.
9. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

   Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Отправка уведомлений по электронной почте настроена.

10.2. Настройка отправки уведомлений в Telegram

До настройки отправки уведомлений в Telegram необходимо выполнить следующие действия:

1. Создать Telegram чат и добавить в него ответственных специалистов.
2. Создать Telegram-бота.
3. Добавить Telegram-бота в чат для экспертов.

► Чтобы настроить отправку уведомлений о появлении вредоносной цепочки в Telegram:

1. На сервере MaxPatrol O2 с установленной ролью Base распакуйте архив с дистрибутивом роли Base:

   ```
   tar -xf Base_<Номер версии>.tar.gz
   ```
2. Перейдите в каталог с распакованными файлами роли Base.
3. Запустите сценарий:

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

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

Откроется страница со списком расширенных параметров.

8. Укажите значения параметров:

   ```
   BotToken: "<Токен Telegram-бота>"
   ChatIds: ["<Идентификатор Telegram-чата>"]
   ```

   Примечание. Если уведомления должны отправляться в несколько Telegram-чатов, в значении массива укажите идентификаторы чатов через запятую, например: `TelegramSettings_ChatIds: ["-875016703", "-455115454", "-484868181"]`.

9. Нажмите кнопку **OK**.

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

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

11. Нажмите кнопку **OK**.

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

Отправка уведомлений в Telegram настроена.

11. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

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

Вы можете получать техническую поддержку на портале.

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

В этом разделе

11.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

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

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

11.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

11.3. Как служба технической поддержки работает с запросами

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

В этом разделе

11.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

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

11.3.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

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

11.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 10).

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

Таблица 10. Время реакции на запрос и время его обработки

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

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

11.3.4. Выполнение работ по запросу

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

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

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

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

Работы по запросу считаются выполненными, если:

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

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

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

— проблема классифицирована как неподдерживаемая.

Глоссарий

атакованный ресурс

Подвергшийся атаке ресурс, для которого отсутствует подтверждение, что он захвачен.

атакующий ресурс

Ресурс, используемый в атаке на другие ресурсы. Может быть внешним или внутренним (захваченным злоумышленником).

захваченный ресурс

Ресурс, к которому злоумышленник получил доступ и может использовать его для неправомерных действий.

корреляционное событие

Результат срабатывания правил СЗИ из-за подозрительных или вредоносных действий.

корреляция событий

Процесс обнаружения нарушений ИБ на основе анализа потока событий от источников. Виды и сочетания событий, характерные для различных видов нарушений, указываются в заранее созданных правилах.

недопустимое событие

Событие, делающее невозможным достижение операционных и (или) стратегических целей или приводящее к значительному нарушению основной деятельности организации в результате кибератаки.

ресурс

Объект ИТ-инфраструктуры, защищаемой или внешней, который злоумышленник может использовать в атаке.

событие

Идентифицированное возникновение определенного состояния системы, сервиса или сети.

тактика

Тактическая цель злоумышленника, причина совершения действия. Компонент матриц Mitre Att&ck.

техника

Конкретный способ реализации тактики злоумышленником. Компонент матриц Mitre Att&ck.

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 185 тысяч акционеров.