



MaxPatrol O2

версия 2024.3

Руководство администратора

© Positive Technologies, 2024.

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

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

Документ может быть изменен без предварительного уведомления.

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

Дата редакции документа: 04.10.2024

Содержание

1.	Об этом документе.....	7
1.1.	Условные обозначения.....	7
1.2.	Другие источники информации о MaxPatrol O2.....	8
2.	О MaxPatrol O2	9
3.	Архитектура MaxPatrol O2	10
3.1.	Компоненты MaxPatrol O2	10
3.2.	Алгоритм работы MaxPatrol O2	12
4.	Развертывание MaxPatrol O2	14
4.1.	Комплект поставки.....	14
4.2.	Аппаратные требования	15
4.3.	Программные требования.....	15
4.4.	Подготовка к интеграции с MaxPatrol EDR	16
4.5.	Уведомления о вредоносной цепочке	17
4.6.	Об установке компонентов MaxPatrol O2 с помощью ролей	18
4.7.	Установка MaxPatrol O2	19
4.7.1.	Установка роли Deployer	20
4.7.2.	Установка роли SqlStorage.....	21
4.7.3.	Установка роли Base	22
4.7.4.	Установка роли Monitoring	22
4.7.5.	Установка роли Resources	23
4.7.6.	Установка роли Modelling	24
4.7.7.	Установка роли RmqMessageBus	25
4.7.8.	Установка роли O2 Base	26
4.7.9.	Установка роли Web	27
4.7.10.	Установка роли XdrAdapter.....	28
4.7.11.	Установка роли AdapterMP10Siem	29
4.8.	Настройка взаимодействия MaxPatrol O2 с MaxPatrol EDR.....	30
4.9.	Настройка MaxPatrol O2 для обеспечения его безопасной работы.....	30
4.10.	Установка доверенного сертификата для сайта MaxPatrol O2	32
5.	Обновление MaxPatrol O2.....	34
6.	Проверка работы MaxPatrol O2 после установки	36
7.	Учетные записи пользователей	37
7.1.	Создание учетной записи пользователя.....	37
7.2.	Назначение пользователю роли эксперта по ИБ.....	37
7.3.	Блокирование и разблокирование учетной записи	38
8.	О модели ресурсов в MaxPatrol O2	39
9.	Работа с недопустимыми событиями	40
9.1.	Добавление недопустимых событий.....	40
9.1.1.	Добавление начальной информации	41
9.1.2.	Создание сценария	41
9.1.3.	Создание группы ресурсов.....	41
9.1.4.	Синтаксис запросов для фильтрации ресурсов	42
9.1.4.1.	Используемые ресурсы	42

9.1.4.2.	Фильтрация по параметрам ресурсов	44
9.1.4.3.	Фильтрация по табличным спискам.....	45
9.1.5.	Экспорт данных об активах в табличный список	45
9.2.	Удаление недопустимого события.....	47
10.	Создание списка исключений из реагирования	48
11.	Интеграция с PT Threat Analyzer.....	50
11.1.	Подготовка к интеграции с PT Threat Analyzer	50
11.1.1.	Создание репутационного списка	50
11.1.2.	Добавление учетной записи	51
11.1.3.	Создание ключа API.....	51
11.2.	Настройка интеграции с PT Threat Analyzer	52
12.	Администрирование MaxPatrol O2.....	53
12.1.	Мониторинг состояния MaxPatrol O2.....	53
12.1.1.	Системный журнал	53
12.1.2.	Работа с дашбордами.....	54
12.2.	Просмотр и изменение параметров конфигурации MaxPatrol O2.....	54
12.2.1.	Просмотр конфигурации роли.....	55
12.2.2.	Изменение конфигурации роли	55
12.2.3.	Параметры базовой конфигурации ролей MaxPatrol O2	56
12.3.	Смена паролей служебных учетных записей.....	63
12.4.	Настройка уровня журналирования работы MaxPatrol O2.....	64
13.	Настройка модулей реагирования.....	66
13.1.	О модулях реагирования MaxPatrol O2.....	67
13.2.	Импорт модуля.....	67
13.3.	Добавление модуля в политику	68
13.4.	Назначение политики на группу агентов.....	69
13.5.	Установка агента на сервер EDR	69
13.6.	Блокировка запросов к объектам в Artifactory	70
13.6.1.	Настройка защиты Artifactory в PT AF 3 3.7	70
13.6.1.1.	Создание группы серверов	71
13.6.1.2.	Создание сервиса.....	71
13.6.1.3.	Создание политики безопасности	72
13.6.1.4.	Создание веб-приложения.....	72
13.6.2.	Создание учетной записи для подключения по SSH	73
13.6.3.	Настройка параметров модуля «Блокировка запросов к объектам в Artifactory»	73
13.6.4.	Разблокирование URL-адреса	74
13.7.	Блокировка по IP-адресу в Check Point GAiA	75
13.7.1.	Создание сетевой группы.....	76
13.7.2.	Получение идентификатора группы	76
13.7.3.	Создание правила для группы.....	77
13.7.4.	Создание профиля для блокировки трафика	78
13.7.5.	Создание учетной записи администратора	78
13.7.6.	Настройка параметров модуля «Блокировка по IP-адресу в Check Point GAiA».....	79
13.7.7.	Разблокирование IP-адреса	80
13.8.	Блокировка учетных записей в Active Directory.....	81

13.8.1.	Создание доменной группы пользователей	82
13.8.2.	Создание доменной учетной записи	82
13.8.3.	Добавление учетной записи в доменную группу пользователей	83
13.8.4.	Предоставление прав на управление учетными записями	83
13.8.5.	Экспорт корневого сертификата контроллера домена	84
13.8.6.	Настройка параметров модуля «Блокировка учетных записей в Active Directory»	85
13.8.7.	Разблокирование учетной записи Active Directory	87
13.9.	Блокировка учетных записей в Confluence	87
13.9.1.	Настройка параметров модуля «Блокировка учетных записей в Confluence»	88
13.9.2.	Разблокирование учетной записи Confluence	88
13.10.	Блокировка учетных записей в FreeIPA	89
13.10.1.	Создание роли для блокировки учетной записи	90
13.10.2.	Создание учетной записи FreeIPA	91
13.10.3.	Настройка параметров модуля «Блокировка учетных записей в FreeIPA»	91
13.10.4.	Разблокирование учетной записи FreeIPA	92
13.11.	Блокировка учетных записей в Passwork	93
13.11.1.	Создание учетной записи в БД Passwork	93
13.11.2.	Настройка параметров модуля «Блокировка учетных записей Passwork»	94
13.11.3.	Разблокирование учетной записи Passwork	95
13.12.	Блокировка учетных записей и отзыв токенов в GitLab	95
13.12.1.	Создание токена доступа	96
13.12.2.	Настройка параметров модуля «Блокировка учетной записи GitLab и отзыв токена доступа»	96
13.13.	Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost	97
13.13.1.	Создание токена доступа	97
13.13.2.	Настройка параметров модуля «Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost»	98
13.13.3.	Разблокирование учетной записи Mattermost	99
13.14.	Завершение SSH-сессий	99
13.15.	Завершение VPN-сессий в Cisco ASA	100
13.16.	Завершение сессий в OpenVPN	101
13.16.1.	Предварительная настройка OpenVPN	102
13.16.2.	Настройка параметров модуля «Завершение сессий в OpenVPN»	104
13.16.3.	Проверка работоспособности модуля «Завершение сессий в OpenVPN»	104
13.17.	Завершение сессий в Windows	105
13.18.	Завершение сессий и блокировка учетных записей в VMware vSphere	106
13.18.1.	Создание и настройка учетной записи vCenter Server	106
13.18.2.	Настройка параметров модуля «Завершение сессий и блокировка учетных записей в VMware vSphere»	107
13.19.	Отзыв сертификатов AD CS	108
13.19.1.	Создание списка доверенных сертификатов AD CS	108
13.19.2.	Возврат сертификата AD CS	109
13.20.	Отзыв токенов в Artifactory	109
13.20.1.	Создание токена доступа	110
13.20.2.	Настройка параметров модуля «Отзыв токенов в Artifactory»	110
13.21.	Перенаправление DNS-запросов в Active Directory (sinkholing)	111

13.22.	Снятие групповой политики с подразделения	111
13.23.	Удаление запланированных задач в Windows.....	112
13.24.	Удаление писем в Microsoft Exchange	112
13.24.1.	Создание доменной учетной записи	113
13.24.2.	Создание группы ролей для поиска и удаления содержимого почтовых ящиков	114
13.24.3.	Создание почтового ящика для карантина	114
13.24.4.	Создание папки в почтовом ящике	114
13.24.5.	Настройка параметров модуля «Удаление писем в Microsoft Exchange».....	114
13.24.6.	Отзыв или возврат токена доступа	115
13.24.7.	Удаление писем	116
13.25.	Удаление служб в Windows (блокировка в Linux)	116
13.26.	Проверка работоспособности модуля	117
14.	Диагностика и решение проблем	119
14.1.	Ошибка входа в MaxPatrol O2 после авторизации в PT MC.....	119
14.2.	Служба Chains останавливается через некоторое время после запуска.....	120
14.3.	Ошибка регистрации MaxPatrol O2 в PT MC.....	121
14.4.	MaxPatrol O2 не получает события из MaxPatrol 10 после обновления LogSpace	122
14.5.	Подсеть Docker-контейнера MaxPatrol O2 совпадает с одной из подсетей организации.....	122
15.	Техническая поддержка	125
	Приложение А. PDQL-запросы данных об активах.....	129
A.1.	Активы с операционной системой Windows	129
A.2.	Активы службы каталогов Active Directory.....	136
A.3.	Активы с операционной системой семейства Unix	137
A.4.	Активы с VMware vSphere.....	139
A.5.	Активы с GitLab	141
	Глоссарий.....	143

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

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о MaxPatrol O2 \(см. раздел 1.2\)](#)

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 ОК	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 \(см. раздел 15\)](#).

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 вредоносности. Использование технологий машинного обучения для оценки уровня опасности событий в цепочке.
- **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 по электронной почте или 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 \(см. раздел 3.2\)](#)

3.1. Компоненты MaxPatrol O2

Компонент AdapterMP10Siem

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. Также компонент получает из MaxPatrol 10 данные о нормализованных событиях, которые используются для обогащения событий, зарегистрированных в MaxPatrol O2.

Компонент O2 Base

Анализирует зарегистрированные события, выявляет целевые атаки в IT-инфраструктуре и обеспечивает реагирование на них. Компонент 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:

- Alerts — служба для обогащения зарегистрированных событий данными о связанных нормализованных событиях, хранящимися в MaxPatrol 10.
- 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 **Требуется внимания**.
- Responder — служба для создания сценария реагирования на цепочку событий. Также Responder отправляет команды на выполнение действий реагирования системе MaxPatrol Endpoint Detection and Response (далее также — MaxPatrol EDR) и получает от нее сообщения о результатах реагирования.

- 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.
- ApiGateway — служба для маршрутизации запросов к бэкенду.
- Registration — служба для регистрации MaxPatrol O2 в PT MC.
- Analytics — служба для сбора и отображения аналитической информации о работе продукта.
- Verdicts — служба для получения и обработки данных от Positive Technologies Threat Analyzer (далее также — PT Threat Analyzer).
- Notifications — служба для отправки уведомлений о возникновении вредоносной цепочки по электронной почте и в Telegram-чат для экспертов по ИБ.

Компонент Base

Обеспечивает взаимодействие микросервисов, используется для обнаружения микросервисов в распределенных системах.

Компонент Resources

Обеспечивает создание и обновление информации о ресурсах, задействованных в событиях, а также о недопустимых событиях, которые могут произойти в ИТ-инфраструктуре в результате атаки.

Компонент Modelling

Моделирует маршруты атаки в ИТ-инфраструктуре и рассчитывает кратчайший путь злоумышленника до реализации недопустимого события. Для работы использует информацию о ресурсах, недопустимых событиях и сетевой топологии.

Компонент XdrAdapter

Обеспечивает взаимодействие MaxPatrol O2 с системой MaxPatrol EDR. Компонент получает команду на запуск реагирования согласно сценарию, сформированному Base. XdrAdapter передает команду модулям 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 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 Monitoring

Собирает и хранит данные о работе MaxPatrol O2, а также предоставляет веб-интерфейс для просмотра и анализа этих данных.

Компонент RmqMessageBus

Компонент представляет собой брокер сообщений RabbitMQ, который реализует обмен данными между микросервисами.

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

Алгоритм работы MaxPatrol O2 следующий:

1. Компонент AdapterMP10Siem 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 O2 Base.
2. AdapterMP10Siem также запрашивает MaxPatrol 10 дополнительную информацию об активах организации — на ее основании позднее компонент Resources формирует модель ресурсов.
3. Компонент O2 Base создает в системе записи о событиях и объединяет события в цепочки по правилам, разработанным экспертами Positive Technologies. Также O2 Base по возможности выполняет обогащение событий информацией о связанных нормализованных событиях из MaxPatrol 10.
4. Компонент Resources создает и обновляет записи о ресурсах и недопустимых событиях.
5. Используя информацию о ресурсах, недопустимых событиях и сетевой топологии, компонент Modelling просчитывает возможные пути продвижения злоумышленника в инфраструктуре и выявляет кратчайший путь до реализации недопустимого события.
6. O2 Base вычисляет вредоносность каждого события цепочки, устанавливает роли ресурсов, задействованных в этих событиях, и на основании полученных данных рассчитывает вредоносность цепочки.
7. Если цепочка является вредоносной, O2 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.
8. С помощью компонента Web эксперт подключается к O2 Base для работы с системой.

9. 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 MaxPatrol EDR. Выполняя действия по сценарию, модули реагирования пресекают активность злоумышленника в инфраструктуре.

10. Компонент Monitoring обеспечивает возможность отслеживания работы MaxPatrol O2.

MaxPatrol O2 взаимодействует со следующими элементами IT-инфраструктуры:

- PT MC — авторизация и аутентификация пользователей с помощью сервиса PT MC;
- MaxPatrol 10 — получение данных о корреляционных и нормализованных событиях, а также об активах;
- MaxPatrol EDR — отправка команд на реагирование и получение информации о результатах реагирования;
- BAD (компонент MaxPatrol 10) — получение информации о наличии в IT-инфраструктуре аномальных событий;
- PT Threat Analyzer — получение репутационных списков;
- SMTP-сервер — отправка уведомлений о вредоносной цепочке на эл. почту;
- API Telegram — отправка уведомлений о вредоносной цепочке в Telegram-чат;
- DNS-сервер — разрешение доменных имен;
- NTP-сервер — синхронизация системного времени.

На рисунке ниже представлена схема взаимодействия MaxPatrol O2 с элементами IT-инфраструктуры и указаны порты взаимодействия.

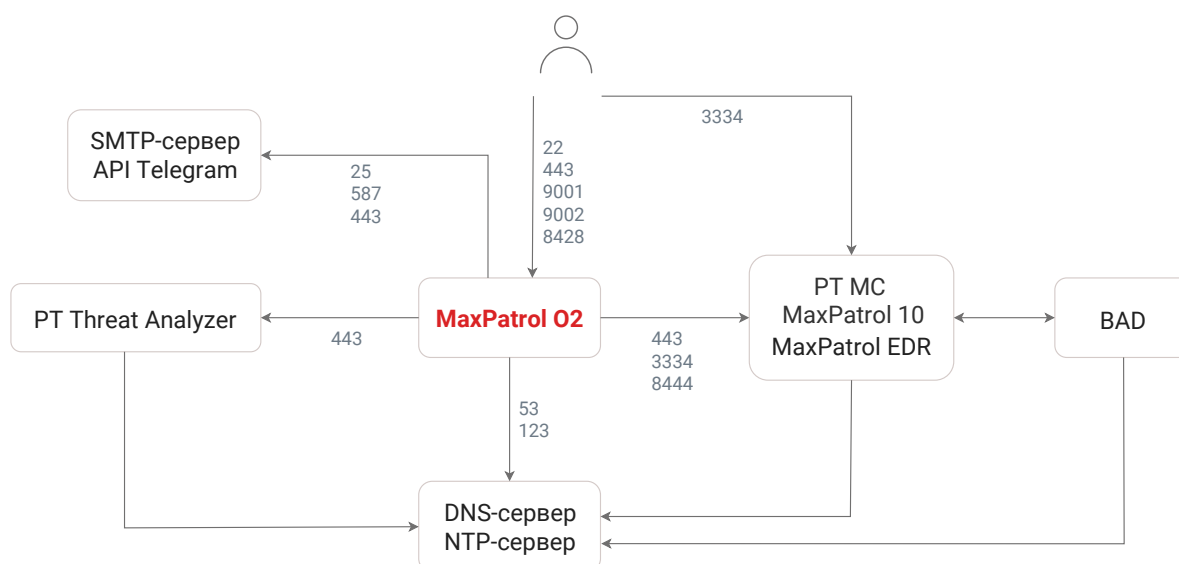


Рисунок 1. Схема взаимодействия MaxPatrol O2 с элементами IT-инфраструктуры

4. Развертывание MaxPatrol O2

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

1. Подготовка сетевой и IT-инфраструктуры к развертыванию MaxPatrol O2 согласно требованиям, приведенным в документе «Подготовка к внедрению».
2. Подготовка к настройке уведомлений о вредоносной цепочке.
3. Если MaxPatrol O2 будет взаимодействовать с MaxPatrol EDR — подготовка к интеграции с MaxPatrol EDR.
4. Установка MaxPatrol O2.
5. Если требуется — настройка взаимодействия MaxPatrol O2 с MaxPatrol EDR.
6. Настройка MaxPatrol O2 для обеспечения его безопасной работы.

В этом разделе

[Комплект поставки \(см. раздел 4.1\)](#)

[Аппаратные требования \(см. раздел 4.2\)](#)

[Программные требования \(см. раздел 4.3\)](#)

[Подготовка к интеграции с MaxPatrol EDR \(см. раздел 4.4\)](#)

[Уведомления о вредоносной цепочке \(см. раздел 4.5\)](#)

[Об установке компонентов MaxPatrol O2 с помощью ролей \(см. раздел 4.6\)](#)

[Установка MaxPatrol O2 \(см. раздел 4.7\)](#)

[Настройка взаимодействия MaxPatrol O2 с MaxPatrol EDR \(см. раздел 4.8\)](#)

[Настройка MaxPatrol O2 для обеспечения его безопасной работы \(см. раздел 4.9\)](#)

[Установка доверенного сертификата для сайта MaxPatrol O2 \(см. раздел 4.10\)](#)

4.1. Комплект поставки

MaxPatrol O2 поставляется в виде дистрибутива. Архив дистрибутива имеет имя `O2-Application_distro_<номер версии и сборки MaxPatrol O2>.tar`, например `O2-Application_distro_2024.3.10.7338.tar`.

Дистрибутив MaxPatrol O2 содержит четыре папки с дистрибутивами [ролей \(см. раздел 4.6\)](#). Название каждой папки соответствует названию приложения, которое создается после установки ролей из этой папки.

В состав дистрибутива MaxPatrol O2 входит:

- папка `Base-Application` с дистрибутивами ролей `Base`, `Modelling`, `Monitoring`, `Resources`, `SqlStorage`;
- папка `Deployment-Application` с дистрибутивом роли `Deployer`;
- папка `O2-Application` с дистрибутивами ролей `AdapterMP10Siem`, `O2 Base`, `RmqMessageBus`, `Web` и `XdrAdapter`.

См. также

[Об установке компонентов MaxPatrol O2 с помощью ролей \(см. раздел 4.6\)](#)

4.2. Аппаратные требования

Компоненты MaxPatrol O2 могут быть установлены на одном или двух серверах. Каждый сервер должен удовлетворять приведенным ниже аппаратным требованиям. Требования, предъявляемые к аппаратным ресурсам сервера, зависят от количества активов в MaxPatrol 10, с которыми будет взаимодействовать MaxPatrol O2.

Таблица 2. Аппаратные требования к серверу MaxPatrol O2

Компонент сервера	Низконагруженная система (менее 5000 активов)	Средненагруженная система (от 5000 до 10 000 активов)	Высоконагруженная система (от 10 000 до 50 000 активов)	Сверхнагруженная система (более 50 000 активов)
Центральный процессор	12 ядер с тактовой частотой 2,2 ГГц	24 ядра с тактовой частотой 2,2 ГГц	48 ядер с тактовой частотой 2,2 ГГц	64 ядра с тактовой частотой 2,2 ГГц
Память (ОЗУ)	32 ГБ	64 ГБ	128 ГБ	256 ГБ
Твердотельный накопитель (SSD)	1 ТБ	2 ТБ	5 ТБ	10 ТБ

4.3. Программные требования

MaxPatrol O2 поддерживает установку на чистую 64-разрядную ОС семейства Linux — Astra Linux Special Edition 1.7 (на базе ядра Linux версии 5.15 и выше) или Debian 10–12 (на базе ядра Linux версии 5.10 и выше).

Внимание! Перед развертыванием MaxPatrol O2 на Astra Linux Special Edition 1.7 необходимо на серверах компонентов выполнить действия, указанные в бюллетенях производителя № 2021-1126SE17 и № 2022-0318SE17MD (подробнее см. [в справочном центре Astra Linux](#)).

При установке MaxPatrol O2 на Astra Linux необходимо выбрать тип ядра generic. Другие типы ядра не поддерживаются. Если включен мандатный контроль целостности, для учетной записи, которая используется при установке компонентов системы, необходим максимальный уровень целостности.

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).

На серверах, где планируется развертывание продукта, рекомендуется установить следующие вспомогательные пакеты:

- curl;
- dnsutils;
- htop;
- iotop;
- jq;
- mc;
- net-tools;
- sudo;
- unzip.

Для работы в интерфейсе MaxPatrol O2 рекомендуется использовать последние версии браузеров Google Chrome, Microsoft Edge, Mozilla Firefox или Яндекс Браузер.

4.4. Подготовка к интеграции с MaxPatrol EDR

Для обеспечения автоматического реагирования на атаку вы можете интегрировать MaxPatrol O2 с MaxPatrol EDR.

Проверка возможности взаимодействия с MaxPatrol EDR через API

Перед развертыванием MaxPatrol O2 необходимо проверить, поддерживает ли экземпляр MaxPatrol EDR, установленный в IT-инфраструктуре, обмен данными с другими системами через API. Это можно проверить, просмотрев информацию о лицензии MaxPatrol EDR: если в лицензии в значении параметра `pt.edr.automation` указано `true`, то взаимодействие через API возможно.

Вы можете просмотреть информацию о лицензии с помощью сервиса Swagger UI.

► Чтобы просмотреть информацию о лицензии:

1. В адресной строке браузера введите: <IP-адрес или FQDN управляющего сервера MaxPatrol EDR>/api/edr/v1/swagger/index.html.
2. Выберите запрос **GET/licenses/**.
3. Нажмите **Try it out**.
4. Нажмите **Execute**.

В блоке **Responses** появится ответ на запрос, содержащий в поле `parameters` массив с параметрами лицензии.

Получение токена доступа к MaxPatrol EDR

При разворачивании MaxPatrol O2 вам потребуется настроить для него доступ к MaxPatrol EDR. Для настройки необходимо получить токен доступа к MaxPatrol EDR.

► Чтобы получить токен,

на управляющем сервере MaxPatrol EDR в каталоге `/opt/edr` выполните 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. Уведомления о вредоносной цепочке

Уведомления помогают оперативно узнавать о появлении вредоносной цепочки и вовремя реагировать на угрозу. При установке MaxPatrol O2 вы можете настроить отправку уведомлений по электронной почте или в Telegram-чат экспертов по ИБ. Уведомления будут отправляться при переходе цепочки событий из статуса **Собирается** в статус **Требуется внимания**.

Внимание! В MaxPatrol O2 должна быть настроена отправка уведомлений хотя бы одним способом — по электронной почте или через Telegram.

Для настройки уведомлений по электронной почте вам понадобится следующая информация:

- IP-адрес или FQDN SMTP-сервера;
- порт SMTP-сервера для входящих подключений от MaxPatrol O2;
- логин и пароль служебной учетной записи для подключения компонента Base к SMTP-серверу;
- электронный адрес отправителя, который будет указан в поле **От** письма с уведомлением.

Для настройки уведомлений в Telegram-чат вам нужно:

1. Создать Telegram-чат и добавить в него ответственных специалистов.
2. Создать Telegram-бота.
3. Добавить Telegram-бота в чат для экспертов.
4. Получить токен бота и идентификатор чата.

4.6. 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 (Base-Application, Deployment-Application и 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 Base-Application содержит роли Base, Modelling, Monitoring, Resources, SqlStorage;
- приложение Deployment-Application — роль Deployer;
- приложение O2-Application — роли AdapterMP10Siem, O2 Base, RmqMessageBus, Web, XdrAdapter.

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/base-application/base`.

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

4.7. 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 \(см. раздел 4.7.1\).](#)
4. [Установить роль SqlStorage \(см. раздел 4.7.2\).](#)
5. [Установить роль Base \(см. раздел 4.7.3\).](#)
6. [Установить роль Monitoring \(см. раздел 4.7.4\).](#)
7. [Установить роль Resources \(см. раздел 4.7.5\).](#)
8. [Установить роль Modelling \(см. раздел 4.7.6\).](#)
9. [Установить роль RmqMessageBus \(см. раздел 4.7.7\).](#)
10. [Установить роль O2 Base \(см. раздел 4.7.8\).](#)
11. [Установить роль Web \(см. раздел 4.7.9\).](#)

12. Установить роль XdrAdapter (см. раздел 4.7.10).
13. Установить роль AdapterMP10Siem (см. раздел 4.7.11).

Внимание! Установку ролей необходимо выполнять в приведенном выше порядке. Команды в интерфейсе терминала Linux необходимо выполнять от имени суперпользователя (root).

В этом разделе

- Установка роли Deployer (см. раздел 4.7.1)
- Установка роли SqlStorage (см. раздел 4.7.2)
- Установка роли Base (см. раздел 4.7.3)
- Установка роли Monitoring (см. раздел 4.7.4)
- Установка роли Resources (см. раздел 4.7.5)
- Установка роли Modelling (см. раздел 4.7.6)
- Установка роли RmqMessageBus (см. раздел 4.7.7)
- Установка роли O2 Base (см. раздел 4.7.8)
- Установка роли Web (см. раздел 4.7.9)
- Установка роли XdrAdapter (см. раздел 4.7.10)
- Установка роли AdapterMP10Siem (см. раздел 4.7.11)

4.7.1. 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. Нажмите **Yes**.
4. По завершении подготовки пакетов нажмите **Yes**.
5. Нажмите **I Accept**.
6. Выберите **Basic configuration**.
7. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль Deployer.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

8. Нажмите **ОК**.
9. По завершении установки нажмите **ОК**.

4.7.2. 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. Нажмите **Yes**.
4. Выберите **Create New Application**.
5. Нажмите **ОК**.

Вы можете изменить идентификатор приложения, заданный по умолчанию.

6. Выберите **Deploy New Instance**.
7. Нажмите **I Accept**.
8. Выберите доменное имя сервера MaxPatrol O2.
9. Нажмите **ОК**.
10. Выберите **Basic configuration**.

Примечание. Если требуется включить запись информации о работе роли SqlStorage в журналы служб, необходимо выбрать вариант **Advanced configuration** и установить флажок **EnableFilesLogCollection**.

11. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль SqlStorage.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

12. Укажите значение параметра `PgHardDiskType`, установив флажок **SSD**.
13. Нажмите **ОК**.
14. По завершении установки нажмите **ОК**.

4.7.3. 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. Нажмите **Yes**.
4. Выберите **base-application**.
5. Выберите **Deploy New Instance**.
6. Нажмите **I Accept**.
7. Выберите доменное имя сервера MaxPatrol O2.
8. Нажмите **OK**.
9. Выберите **Advanced configuration**.
10. 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. Параметр `ClientScore` должен иметь значение `idmgr.api <Значение ClientId>.api`.

11. Укажите значения параметров:

```
HostAddress: <IP-адрес или FQDN сервера, на который устанавливается роль Base>
MCAddress: https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью
Management and Configuration>:3334
MCHostAddress: <IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью
Management and Configuration>
SiemCoreUrl: https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core>
```
- Внимание!** Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.
12. Нажмите **OK**.
13. По завершении установки нажмите **OK**.

4.7.4. Установка роли Monitoring

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

► Чтобы установить роль:

1. Распакуйте архив `Monitoring_<Номер версии>.tar.gz`:

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

2. Запустите сценарий:

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

3. Нажмите **Yes**.

4. Выберите **base-application**.

5. Выберите **Deploy New Instance**.

6. Нажмите **I Accept**.

7. Выберите доменное имя сервера MaxPatrol O2.

8. Нажмите **OK**.

9. Выберите **Basic configuration**.

10. Укажите значения параметров:

`HostAddress`: <IP-адрес или FQDN сервера, на который устанавливается роль Monitoring>

`TracingCollectorHost`: <IP-адрес или FQDN сервера, на который устанавливается роль Monitoring>

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

11. Нажмите **OK**.

12. По завершении установки нажмите **OK**.

4.7.5. Установка роли Resources

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

► Чтобы установить роль:

1. Распакуйте архив `Resources_<Номер версии>.tar.gz`:

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

2. Запустите сценарий:

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

3. Нажмите **Yes**.

4. Выберите **base-application**.

5. Выберите **Deploy New Instance**.

6. Нажмите **I Accept**.

7. Выберите доменное имя сервера MaxPatrol O2.

8. Нажмите **OK**.
9. Выберите **Advanced configuration**.
10. 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. Параметр `ClientScore` должен иметь значение `idmgr.api <Значение ClientId>.api`.

11. Укажите значения параметров:

```
HostAddress: <IP-адрес или FQDN сервера, на который устанавливается роль Resources>
MCAddress: https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью
Management and Configuration>:3334
MCHostAddress: <IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью
Management and Configuration>
PostgreHost: <IP-адрес или FQDN сервера с установленной ролью SqlStorage>
SiemCoreUrl: https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core>
```

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

12. Нажмите **OK**.
13. По завершении установки нажмите **OK**.

4.7.6. Установка роли Modelling

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

► Чтобы установить роль:

1. Распакуйте архив `Modelling_<Номер версии>.tar.gz`:
`tar -xf Modelling_<Номер версии>.tar.gz`
2. Запустите сценарий:
`Modelling_<Номер версии>/install.sh`
3. Нажмите **Yes**.
4. Выберите **base-application**.
5. Выберите **Deploy New Instance**.
6. Нажмите **I Accept**.
7. Выберите доменное имя сервера MaxPatrol O2.
8. Нажмите **OK**.
9. Выберите **Advanced configuration**.
10. 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 РТ МС. Параметр `ClientScore` должен иметь значение `idmgr.api <Значение ClientId>.api`.

11. Укажите значения параметров:

`HostAddress`: <IP-адрес или FQDN сервера, на который устанавливается роль Modelling>
`MCAddress`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration>:3334`
`MCHostAddress`: <IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration>
`PostgreHost`: <IP-адрес или FQDN сервера с установленной ролью SqlStorage>
`SiemCoreUrl`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core>`

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

12. Нажмите **ОК**.

13. По завершении установки нажмите **ОК**.

4.7.7. 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 -xvf RmqMessageBus_<Номер версии>.tar.gz
```

2. Запустите сценарий:

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

3. Нажмите **Yes**.

4. Выберите **Create New Application**.

5. Нажмите **ОК**.

Вы можете изменить идентификатор приложения, заданный по умолчанию.

6. Выберите **Deploy New Instance**.

7. Нажмите **I Accept**.

8. Выберите доменное имя сервера MaxPatrol O2.

9. Нажмите **ОК**.

10. Выберите **Basic configuration**.

11. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль `RmqMessageBus`.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

12. Нажмите **ОК**.
13. По завершении установки нажмите **ОК**.

4.7.8. Установка роли O2 Base

Для установки роли вам потребуется архив `O2Base_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `O2Base_<Номер версии>.tar.gz`:

```
tar -xf O2Base_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
O2Base_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите **o2-application**.
5. Выберите **Deploy New Instance**.
6. Нажмите **I Accept**.
7. Выберите доменное имя сервера MaxPatrol O2.
8. Нажмите **ОК**.
9. Выберите **Advanced configuration**.
10. В качестве значения параметра `ApplicationDisplayName` укажите название экземпляра MaxPatrol O2.
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. Параметр `ClientScore` должен иметь значение `idmgr.api <Значение ClientId>.api`.

12. Укажите значения параметров:

`HostAddress`: <IP-адрес или FQDN сервера, на который устанавливается роль O2 Base>

`MCAddress`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration>:3334`

`PostgreHost`: <IP-адрес или FQDN сервера с установленной ролью `SqlStorage`>

`SiemCoreUrl`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core>`

`UIHostAddress`: <IP-адрес или FQDN сервера, на который планируется установить роль `Web`>

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

13. Если требуется настроить отправку уведомлений по электронной почте, укажите значения параметров:

EmailRecipients: ["<Адрес эл. почты получателя>"]

Примечание. Если нужно, чтобы уведомления отправлялись нескольким получателям, вы можете указать адреса через запятую, например EmailRecipients: ["username1@example.com", "username2@example.com"].

Smtphost: <IP-адрес или FQDN SMTP-сервера>

Smtppassword: <Пароль служебной учетной записи для подключения O2 Base к SMTP-серверу>

Smtpport: <Порт SMTP-сервера для входящих подключений от MaxPatrol O2>

Smtpsender: <Поле заголовка Sender>

Smtouser: <Логин служебной учетной записи для подключения Base к SMTP-серверу>

Примечание. Если для отправки уведомлений планируется использовать публичный почтовый сервис, значения параметров Smtpsender и Smtouser должны совпадать.

14. Если требуется настроить отправку уведомлений в Telegram, укажите значения параметров:

BotToken: <Токен Telegram-бота, добавленного в чат для экспертов>

ChatIds: <Идентификатор Telegram-чата для экспертов>

15. Нажмите **OK**.

16. По завершении установки нажмите **OK**.

4.7.9. 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. Нажмите **Yes**.

4. Выберите **o2-application**.

5. Выберите **Deploy New Instance**.

6. Нажмите **I Accept**.

7. Выберите доменное имя сервера MaxPatrol O2.

8. Нажмите **OK**.

9. Нажмите **I Accept**.

10. Выберите **Advanced configuration**.

11. В качестве значения параметра `ApiGatewayHost` укажите IP-адрес или FQDN сервера с установленной ролью O2 Base.
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 получать данные от BAD, установите флажок **FeatureFlagBadEnabled**.
14. Если требуется получать данные от PT Threat Analyzer, установите флажок **FeatureFlagTAEnabled**.
15. Укажите значения параметров:
`GrafanaServerRootUrl`: <IP-адрес или FQDN сервера с установленной ролью Monitoring>
`HostAddress`: <IP-адрес или FQDN сервера, на который устанавливается роль Web>
`MCAddress`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration>:3334`
`SiemCoreUrl`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core>`
16. Нажмите **OK**.
17. По завершении установки нажмите **OK**.

4.7.10. 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. Нажмите **Yes**.
4. Выберите **o2-application**.
5. Нажмите **OK**.
6. Выберите **Deploy New Instance**.
7. Нажмите **I Accept**.
8. Выберите доменное имя сервера MaxPatrol O2.
9. Нажмите **OK**.
10. Выберите **Advanced configuration**.
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 РТ МС. Параметр `ClientScore` должен иметь значение `idmgr.api <Значение ClientId>.api`.

12. 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 управляющего сервера MaxPatrol EDR>:8444/api/edr/v1`

`HostAddress: <IP-адрес или FQDN сервера, на который устанавливается роль XdrAdapter>`

`MCAddress: https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration>:3334`

`PostgreHost: <IP-адрес или FQDN сервера с установленной ролью SqlStorage>`

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

13. Нажмите **OK**.

14. По завершении установки нажмите **OK**.

4.7.11. Установка роли AdapterMP10Siem

Для установки роли вам потребуется архив `AdapterMP10Siem_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. Распакуйте архив `AdapterMP10Siem_<Номер версии>.tar.gz`:

```
tar -xvf AdapterMP10Siem_<Номер версии>.tar.gz
```

2. Запустите сценарий:

```
AdapterMP10Siem_<Номер версии>/install.sh
```

3. Нажмите **Yes**.

4. Выберите **o2-application**.

5. Выберите **Deploy New Instance**.

6. Нажмите **I Accept**.

7. Выберите доменное имя сервера MaxPatrol O2.

8. Нажмите **OK**.

9. Выберите **Advanced configuration**.

10. 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 РТ МС. Параметр `ClientScore` должен иметь значение `idmgr.api <Значение ClientId>.api mpx.api`.

11. Укажите значения параметров:

`HostAddress`: <IP-адрес или FQDN сервера, на который устанавливается роль `AdapterMP10Siem`>
`MCAddress`: `https://<IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Management and Configuration>:3334`
`PostgreHost`: <IP-адрес или FQDN сервера с установленной ролью `SqlStorage`>

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой.

12. Если требуется, в значении параметра `SiemAdapterStartTime` укажите время начала периода, с которого служба `SiemAdapter` начнет запрашивать корреляционные события из MaxPatrol 10, в формате ISO 8601 (UTC+0), например `2024-01-15T23:59:59Z`.
13. В качестве значения параметра `SiemCoreUrl` укажите IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью `Core`.
14. Нажмите **ОК**.
15. По завершении установки нажмите **ОК**.

4.8. Настройка взаимодействия MaxPatrol O2 с MaxPatrol EDR

Для настройки взаимодействия MaxPatrol O2 с MaxPatrol EDR необходимо добавить модуль `o2_dispatcher` в каждую группу [модулей реагирования](#) (см. [раздел 13](#)) MaxPatrol EDR, с которыми должен работать MaxPatrol O2.

4.9. Настройка MaxPatrol O2 для обеспечения его безопасной работы

После развертывания MaxPatrol O2 необходимо выполнить настройку системы для обеспечения ее безопасной работы.

► Чтобы настроить MaxPatrol O2:

1. На сервере MaxPatrol O2 разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m comment --comment "SSH admin access" -j ACCEPT
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, `remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24`.

2. На сервере MaxPatrol O2 разрешите доступ к веб-интерфейсу системы по порту 443 с рабочих станций пользователей:

```
iptables -F DOCKER-USER
iptables -I DOCKER-USER -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -I DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций> -p tcp -m conntrack --ctstate NEW --ctorigdstport 443 -m comment --comment "Web access" -j ACCEPT
```

3. На сервере MaxPatrol O2 разрешите доступ к веб-интерфейсу VictoriaMetrics по порту 8428 с рабочих станций пользователей, которым требуется доступ к метрикам:

```
iptables -I DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций> -p tcp -m conntrack --ctstate NEW --ctorigdstport 8428 -m comment --comment "victoria metrics access" -j ACCEPT
```

4. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed-roles/мс-application/<Название экземпляра роли SqlStorage>/images/storage-pgadmin/config/`, добавьте параметры:

```
PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True
PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
```

5. Пересоберите контейнер pgAdmin:

```
cd /var/lib/deployed-roles/мс-application/<Название экземпляра роли SqlStorage>/images/storage-pgadmin
docker-compose down
docker-compose up -d
iptables -I DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 9001 -m comment --comment "pgAdmin access" -j ACCEPT
```

6. Разрешите доступ к СУБД PostgreSQL с рабочих станций администраторов:

```
iptables -I DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 5432 -m comment --comment "PostgreSQL access" -j ACCEPT
```

7. Разрешите доступ к веб-интерфейсу Grafana с рабочих станций администраторов:

```
iptables -I DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 9002 -m comment --comment "grafana access" -j ACCEPT
```

8. На сервере MaxPatrol O2 заблокируйте все входящие соединения, кроме разрешенных:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT
```

9. Для сохранения созданных правил на сервере MaxPatrol O2 установите пакет `iptables-persistent`:

```
apt-get update
apt-get install iptables-persistent
```

Примечание. Порядок сохранения правил описан в [справочном центре Astra Linux](#).

10. Сохраните правила межсетевого экрана:
`netfilter-persistent save`
11. [Смените пароли служебных учетных записей \(см. раздел 12.3\)](#) в MaxPatrol O2.
12. [Установите собственные доверенные сертификаты \(см. раздел 4.10\)](#) для MaxPatrol O2.
13. Для каждого администратора MaxPatrol O2 создайте отдельную учетную запись:
`adduser <Логин администратора>`
14. На рабочих станциях администраторов MaxPatrol O2 сгенерируйте ключевую пару.
Примечание. Для генерации ключевой пары вы можете использовать утилиту `ssh-keygen`.
15. На сервере MaxPatrol O2 добавьте открытый ключ в файл `/home/<Логин администратора>/.ssh/authorized_keys`.
16. В файле `/etc/ssh/sshd_config` раскомментируйте и измените значения параметров:
`PubkeyAuthentication yes`
`RhostsRSAAuthentication no`
`HostbasedAuthentication no`
`PermitEmptyPasswords no`
`PasswordAuthentication no`
17. В файле `/etc/sudoers` измените значение параметра:
`<Логин администратора> ALL=(ALL) ALL`
18. В приложении Management and Configuration смените пароль учетной записи Administrator.
19. В приложении Management and Configuration для каждого пользователя MaxPatrol O2 [создайте учетную запись с ролью эксперта по ИБ \(см. раздел 7\)](#).

MaxPatrol O2 настроен.

4.10. Установка доверенного сертификата для сайта MaxPatrol O2

Вы можете установить пользовательский сертификат безопасности для MaxPatrol O2.

При развертывании MaxPatrol O2 для его сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения к сайту вы получите предупреждение о том, что создаваемое подключение не защищено.

Вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком `BEGIN RSA PRIVATE KEY` без дополнительных заголовков;

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

- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Subject Alternative Name (SAN) содержать запись об FQDN сервера компонента или его IP-адресе в зависимости от значения параметра `HostAddress` (оно может содержать как FQDN, так и IP-адрес).

► Чтобы установить пользовательский сертификат безопасности:

1. На сервере с установленными ролями Web и Monitoring разместите файлы сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей Web и Monitoring.
2. На сервере с установленной ролью Deployer разместите файлы сертификатов центров сертификации всей цепочки в каталоге `/opt/deployer/pki/trusted_ca/`.

3. Выполните команду:

```
dpkg-reconfigure deployer
```

4. Измените конфигурации (см. раздел 12.2.2) ролей Web и Monitoring:

```
SSLCertificatePemFileName: <Имя файла сертификата>
```

```
SSLKeyFileName: <Имя файла закрытого ключа>
```

Например:

```
SSLCertificatePemFileName: website.crt
```

```
SSLKeyFileName: website.key
```

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

5. Обновление MaxPatrol O2

Базовыми единицами установки и обновления MaxPatrol O2 являются [роли \(см. раздел 4.6\)](#). Для обновления системы вам нужно обратиться в Positive Technologies и получить дистрибутивы с новыми версиями ролей.

Для обновления MaxPatrol O2 необходимо:

1. Сохранить архив с дистрибутивом на сервер MaxPatrol O2.
2. Распаковать архив с дистрибутивом.
3. Обновить роль Deployer.
4. Обновить роль SqlStorage.
5. Обновить роль Base.
6. Обновить роль Monitoring.
7. Обновить роль Resources.
8. Обновить роль Modelling.
9. Обновить роль RmqMessageBus.
10. Обновить роль O2 Base.
11. Обновить роль Web.
12. Обновить роль XdrAdapter.
13. Обновить роль AdapterMP10SiemV25.

Внимание! Обновление ролей необходимо выполнять в приведенном выше порядке.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется файл с названием вида `install_<Название роли>_<Версия дистрибутива роли>.log`, содержащий информацию об обновлении роли. Вы можете передавать файл в рамках запроса в техническую поддержку для анализа проблем.

Обновление роли

► Чтобы обновить роль:

1. Распакуйте архив с дистрибутивом роли:
`tar -xf <Название архива>.tar.gz`
2. Запустите сценарий:
`<Название архива>/install.sh`
3. Нажмите **Yes**.
4. Нажмите **I Accept**.
5. Выберите **Skip configuration**.

6. Если требуется, подтвердите изменение конфигурации роли, нажав **OK**.

Примечание. Для изменения значения параметров необходимо нажать **Cancel** и выбрать вариант **Advanced configuration**.

7. Нажмите **OK**.
8. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

6. Проверка работы MaxPatrol O2 после установки

Проверку работы MaxPatrol O2 нужно выполнять при условии, что в MaxPatrol 10 есть корреляционные события, которые должен получать MaxPatrol O2 в соответствии с критериями фильтрации, установленными в конфигурационном файле службы Siemadapter. Информация о корреляционных событиях отображается в MaxPatrol 10 в разделе **События**.

Примечание. Вы можете просмотреть запрос для фильтрации событий по команде `docker exec -it $(docker container ls -q --filter name=siemadapter*) cat /usr/local/share/microservice/layers/mapping/events.yaml`. С помощью запроса вы можете отфильтровать записи о событиях в MaxPatrol 10.

MaxPatrol O2 работает корректно, если:

- на вкладке **Собирается** есть цепочки событий;
- на странице цепочки отображается схема атаки;
- в веб-интерфейсе MaxPatrol O2 отсутствуют сообщения об ошибках.

7. Учетные записи пользователей

Администратор создает учетные записи для пользователей MaxPatrol O2. Для предоставления пользователю доступа к интерфейсу продукта администратор назначает учетной записи пользователя роль эксперта по ИБ.

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

В этом разделе

[Создание учетной записи пользователя \(см. раздел 7.1\)](#)

[Назначение пользователю роли эксперта по ИБ \(см. раздел 7.2\)](#)

[Блокирование и разблокирование учетной записи \(см. раздел 7.3\)](#)

7.1. Создание учетной записи пользователя

► Чтобы создать учетную запись пользователя:

1. В главном меню нажмите  → **Management and Configuration**.
2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.
3. Нажмите **Добавить пользователя**.
4. Выберите тип аутентификации.
5. Если вы выбрали локальную аутентификацию, введите логин и пароль пользователя.
6. Если вы выбрали LDAP-аутентификацию, введите логин пользователя и по ссылке **Выбрать домен** выберите LDAP-подключение.
7. Нажмите кнопку **Создать**.

7.2. Назначение пользователю роли эксперта по ИБ

► Чтобы назначить пользователю роль эксперта по ИБ:

1. В главном меню нажмите  → **Management and Configuration**.
2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.
3. 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. Нажмите **Роли в приложениях**.

5. В раскрывающемся списке **MaxPatrol O2** установите флажок **Эксперт по ИБ**.
6. Нажмите **Сохранить**.

7.3. Блокирование и разблокирование учетной записи

- Чтобы заблокировать учетную запись пользователя:

1. В главном меню нажмите  → **Management and Configuration**.
2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.
3. 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. Нажмите **Заблокировать**.

Учетная запись заблокирована.

- Чтобы разблокировать учетную запись пользователя:

1. В главном меню нажмите  → **Management and Configuration**.
2. В панели **Пользователи по приложениям** выберите MaxPatrol O2.
3. 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. Нажмите **Разблокировать**.

Учетная запись разблокирована.

8. О модели ресурсов в MaxPatrol O2

В MaxPatrol O2 реализована модель ресурсов: все собранные сведения о ресурсах представлены в виде специальных объектов. С помощью набора этих объектов можно охарактеризовать любой ресурс. Объекты модели имеют атрибуты, которые идентифицируют и характеризуют объект в MaxPatrol O2.

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

Поля модели ресурсов могут быть использованы для формирования условия фильтрации [при добавлении недопустимых событий \(см. раздел 9.1\)](#) и [для создания списка исключений из реагирования \(см. раздел 10\)](#).

9. Работа с недопустимыми событиями

MaxPatrol O2 помогает обнаружить действия злоумышленников и предотвратить недопустимые события в IT-инфраструктуре организации. Недопустимым называется событие, в результате реализации которого становится невозможным достижение операционных и стратегических целей организации. Примеры недопустимых событий: хищение крупной суммы денег с банковского счета, утечка исходного кода разрабатываемого приложения, пожар в заводском цеху.

Вы можете добавить информацию о недопустимых событиях в MaxPatrol O2, чтобы отслеживать, насколько близок злоумышленник к их реализации. Если система выявляет угрозу наступления недопустимых событий, на схеме атаки отображается информация о ближайших из них.

Внимание! В текущей версии продукта поддерживается работа с недопустимыми событиями в ОС Windows и Unix, а также в Active Directory, VMware vCenter и GitLab.

Далее в этом разделе приведены инструкции по работе с недопустимыми событиями.

В этом разделе

[Добавление недопустимых событий \(см. раздел 9.1\)](#)

[Удаление недопустимого события \(см. раздел 9.2\)](#)

9.1. Добавление недопустимых событий

Для добавления недопустимого события в MaxPatrol O2 необходимо выполнить следующие шаги:

1. Добавить начальную информацию о недопустимом событии.
2. Создать сценарий реализации недопустимого события.
3. Создать группу ресурсов для сценария.

В этом разделе

[Добавление начальной информации \(см. раздел 9.1.1\)](#)

[Создание сценария \(см. раздел 9.1.2\)](#)

[Создание группы ресурсов \(см. раздел 9.1.3\)](#)

[Синтаксис запросов для фильтрации ресурсов \(см. раздел 9.1.4\)](#)

[Экспорт данных об активах в табличный список \(см. раздел 9.1.5\)](#)

9.1.1. Добавление начальной информации

► Чтобы добавить начальную информацию о недопустимом событии:

1. В главном меню нажмите .
2. Нажмите **Добавить**.
3. Введите название недопустимого события.
4. Введите имя и фамилию ответственного лица.
5. Нажмите **Сохранить**.

9.1.2. Создание сценария

Для одного недопустимого события вы можете создать несколько сценариев его реализации. Сценарий описывает способ получения злоумышленником несанкционированного доступа к целевой системе при попытке реализации недопустимого события. Например, для недопустимого события «Остановка производства» сценариями могут быть «Получение доступа к компьютеру оператора АСУ ТП» или «Внедрение вредоносного кода в компонент АСУ ТП». Выполнение злоумышленником хотя бы одного сценария означает реализацию недопустимого события.

► Чтобы создать сценарий реализации недопустимого события:

1. В главном меню нажмите .
2. Выберите недопустимое событие.
3. Нажмите **Добавить сценарий**.
4. Введите название сценария.
5. Нажмите **Сохранить**.

9.1.3. Создание группы ресурсов

Для одного сценария вы можете создать несколько групп ресурсов. Захват злоумышленником хотя бы одного ресурса из группы означает выполнение сценария и, как следствие, реализацию недопустимого события.

► Чтобы создать группу ресурсов:

1. В главном меню нажмите .
2. Выберите недопустимое событие.
3. Наведите курсор на название сценария и нажмите .

4. В поле **Фильтр по параметрам ресурсов** введите запрос к модели ресурсов MaxPatrol O2.
5. Если требуется, в поле **Фильтр по табличным спискам** введите запрос к табличному списку MaxPatrol O2.
6. Нажмите **Сохранить**.

9.1.4. Синтаксис запросов для фильтрации ресурсов

Вы можете создать группу ресурсов с помощью запроса: в соответствии с его условием выполняется отбор ресурсов в группу. Условие запроса формируется с помощью логических выражений, в которых объединяются ключевое слово или атрибут ресурса и его значение. Для составления выражений используются поля [модели ресурсов \(см. раздел 8\)](#) MaxPatrol O2. Значения атрибутов ресурсов можно получить с помощью PDQL-запросов к табличным спискам в MaxPatrol 10. Подробная информация о работе с табличными списками приведена в документации MaxPatrol 10.

В этом разделе

[Используемые ресурсы \(см. раздел 9.1.4.1\)](#)

[Фильтрация по параметрам ресурсов \(см. раздел 9.1.4.2\)](#)

[Фильтрация по табличным спискам \(см. раздел 9.1.4.3\)](#)

9.1.4.1. Используемые ресурсы

В текущей версии продукта поддерживается фильтрация ресурсов следующих типов: «Локальная учетная запись», «Доменная учетная запись», «Внутренний узел», «Доступ к компоненту на узле».

Таблица 3. Структура ресурсов

Тип ресурса	Атрибут ресурса	Поле в модели активов MaxPatrol 10	Описание
Локальная учетная запись (Credentials.LocalCredential)	Login	Host.User.Name	Имя учетной записи
	UserID	Host.User.ID	Идентификатор учетной записи: в Windows — SID, в Unix — UID, в ПО — уникальный идентификатор пользователя

Тип ресурса	Атрибут ресурса	Поле в модели активов MaxPatrol 10	Описание
	Component	—	Компонент актива, где создана учетная запись. Допустимые значения: Windows, Linux, GitLab, VMware vSphere
	Host.FQDN	Host.FQDN	Полное доменное имя актива, где создана учетная запись
	Host.HostID	Host.@id	Идентификатор актива, где создана учетная запись
Доменная учетная запись (Credentials.DomainCredential)	Login	ActiveDirectory.Domains.Users.SamAccountName	Имя учетной записи в Active Directory
	UserID	ActiveDirectory.Domains.Users.objectSid	Идентификатор учетной записи в Active Directory
	Domain	ActiveDirectory.Domains.Name	Имя домена учетной записи в Active Directory
Внутренний узел (Host.InternalHost)	HostID	Host.@id	Идентификатор актива
	FQDN	Host.FQDN	Полное доменное имя актива
	IPAddress	Host.Endpoints<IpEndpoint>.Address	IP-адрес актива
	Hostname	Host.Hostname	Имя актива
Доступ к компоненту на узле (Access.AccessToAssetComponent)	Component	—	Компонент актива. Допустимые значения: Windows, Linux, GitLab, VMware vSphere
	Host.FQDN	Host.FQDN	Полное доменное имя актива
	Host.HostID	Host.@id	Идентификатор актива

Тип ресурса	Атрибут ресурса	Поле в модели активнов MaxPatrol 10	Описание
	DomainCredential.Login	ActiveDirectory.Domains.Users.SamAccountName	Имя учетной записи с доступом к компоненту в Active Directory
	DomainCredential.UserID	ActiveDirectory.Domains.Users.objectSid	Идентификатор учетной записи с доступом к компоненту в Active Directory
	DomainCredential.Domain	ActiveDirectory.Domains.Name	Имя домена учетной записи с доступом к компоненту в Active Directory
	LocalCredential.Login	Host.User.Name	Имя учетной записи
	LocalCredential.UserID	Host.User.ID	Идентификатор учетной записи: в Windows — SID, в Unix — UID, в ПО — уникальный идентификатор пользователя

9.1.4.2. Фильтрация по параметрам ресурсов

Вы можете отфильтровать ресурсы по их параметрам.

В условии запроса должен быть указан тип ресурса. Тип ресурса задается с помощью ключевого слова `Type`, которое может иметь следующие значения:

- `Credentials.DomainCredential` — тип «Доменная учетная запись»;
- `Credentials.LocalCredential` — тип «Локальная учетная запись»;
- `Host.InternalHost` — тип «Внутренний узел»;
- `Access.AccessToAssetComponent` — тип «Доступ к компоненту на узле».

Синтаксис: `@Type = <Тип ресурса>`

Вы можете дополнительно отфильтровать ресурсы по их параметрам, используя поля модели ресурсов. Атрибут ресурса и его значение объединяются в выражении с помощью оператора равенства (=) или неравенства (!=).

Синтаксис: `@Type = <Тип ресурса> AND <Атрибут ресурса> <Оператор> <Значение>`

Вы можете добавлять в условие запроса несколько выражений с помощью операторов AND и OR, а также скобок. Операторы объединяют выражения, а скобки определяют порядок выполнения операций в запросе. Операторы работают регистронезависимо.

Примечание. Значение ключевого слова Type и строковые значения атрибутов ресурсов должны быть указаны в одинарных кавычках.

Примеры

Запрос @Type = 'Host.InternalHost' позволяет найти все внутренние узлы.

Запрос @Type = 'Credentials.DomainCredential' AND (Login = 's_admin' or Login = 'admin') позволяет найти доменные учетные записи с логинами s_admin или admin.

9.1.4.3. Фильтрация по табличным спискам

Вы можете отфильтровать ресурсы по табличным спискам. Для фильтрации используются табличные списки, в которые [экспортированы \(см. раздел 9.1.5\)](#) данные об активах MaxPatrol 10.

Синтаксис: <Атрибут ресурса> = \$<Название табличного списка>.<Название колонки табличного списка>.

В результате выполнения запроса будут найдены все ресурсы, для которых атрибут, указанный в выражении, имеет значение, соответствующее значению данных в ячейке табличного списка.

Вы можете добавлять в условие запроса несколько выражений с помощью операторов AND и OR, а также скобок. Операторы объединяют выражения, а скобки определяют порядок выполнения операций в запросе. Операторы работают регистронезависимо.

Примеры

Запрос Host.HostID = \$example_list.HostId позволяет найти узлы, для которых идентификатор узла (значение атрибута Host.HostId) совпадает со значением данных в колонке HostId в табличном списке example_list.

Запрос Login = \$example_list.Login AND Domain = \$example_list.Domain позволяет найти доменные учетные записи, для которых логин (значение атрибута Login) совпадает со значением данных в колонке Login в табличном списке example_list, и домен этих учетных записей (значение атрибута Domain) совпадает со значением данных в колонке Domain в табличном списке example_list.

9.1.5. Экспорт данных об активах в табличный список

Для фильтрации ресурсов по табличным спискам необходимо в MaxPatrol 10 создать группу активов, которые входят в состав целевых систем, и экспортировать данные об активах группы в табличный список. Если сведения об активах меняются, записи табличного списка автоматически обновляются.

Вы можете использовать данные о следующих активах:

- с операционной системой Windows;
- операционной системой семейства Unix;
- установленным VMware vSphere;
- установленным GitLab;
- об активах службы каталогов Active Directory.

Вы можете создать статическую или динамическую группу активов. В группу нужно добавить активы, которые входят в состав целевой системы — то есть доступ к которым может привести к реализации недопустимого события. Для удобства работы вы можете сгруппировать активы по целевым системам (например, «Система управления цепочками поставок») или по недопустимым событиям (например, «Захват сервера 1С»). Подробные инструкции по созданию группы см. в Руководстве оператора MaxPatrol 10.

► Чтобы экспортировать данные об активах в табличный список:

1. Выберите раздел **Активы**.
2. В панели **Группы** выберите **группы** (см. раздел 9.1.5), по активам которых должен быть сформирован табличный список.
3. Если требуется, в панели фильтрации настройте PDQL-запрос для фильтрации активов.
4. Нажмите  **Создать табличный список**.
5. Введите название табличного списка.
6. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения табличного списка в БД.

Примечание. Вы можете добавить табличный список в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**.

7. В раскрывающемся списке **Назначение** выберите **Данные об активах**.
8. Если требуется изменить список групп, по активам которых должен быть сформирован табличный список, в раскрывающемся списке **Группы активов** установите флажки напротив названий групп.
9. Если требуется добавить активы из вложенных групп, установите флажок **Включать вложенные группы**.
10. Измените PDQL-запрос к модели активов.

Примечание. PDQL-запросы для получения данных об активах приведены в приложении.

11. Нажмите **Обновить схему**.

12. Нажмите кнопку **Создать**.
13. На странице **Табличные списки** в панели **Доступные списки** выберите созданный табличный список и нажмите **Установить в SIEM**.

См. также

[Фильтрация по табличным спискам \(см. раздел 9.1.4.3\)](#)

9.2. Удаление недопустимого события

► Чтобы удалить недопустимое событие:

1. В главном меню нажмите .
2. Наведите курсор на строку с названием события и нажмите  → **Удалить**.

10. 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 \(см. раздел 8\)](#) MaxPatrol O2.

► Чтобы создать список исключений из реагирования:

1. На сервере MaxPatrol O2 с установленной ролью Base перейдите в каталог `/var/lib/deployed-roles/o2-application/o2base/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-application/o2base/images/responder.extended`.
5. Перезапустите службу Responder, выполнив команды:


```
docker-compose stop
docker-compose start
```

Список исключений из реагирования создан и вступил в силу.

Таблица 4. Формат файла CustomResourceList.yaml

Элемент структуры	Описание	Обязательность	Массив
<code>resourceTypes</code>	Тип ресурса	Нет	Да
<code>propertyName</code>	Параметр ресурса	Нет	Нет
<code>comparison</code>	Тип данных параметра <code>propertyValues</code> . Возможные значения: — <code>string</code>; — <code>winpath</code> — путь к файлу или папке в файловой системе Windows; — <code>unixpath</code> — путь к файлу или каталогу в файловой системе Unix	Нет	Нет

Элемент структуры	Описание	Обязательность	Массив
	Значение по умолчанию — <code>string</code>		
<code>propertyValues</code>	Значение параметра ресурса	Да, если указан параметр ресурса	Да

Необходимо соблюдать отступы строк в файле, как показано в примере ниже. 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:
  - 02.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: IPAddress
  comparison: string
  propertyValues:
    - 192.0.2.10
    - 192.0.2.135
# Правило для исключения процессов, у которых полный путь к исполняемому файлу в ОС
# семейства Unix — /usr/lib/systemd/system
- resourceTypes:
  - 02.LinuxProcess
  propertyName: Path
  comparison: unixpath
  propertyValues:
    - /usr/lib/systemd/system
```

11. Интеграция с PT Threat Analyzer

MaxPatrol O2 можно интегрировать с PT Threat Analyzer. При настроенной интеграции MaxPatrol O2 получает от PT Threat Analyzer сведения об угрозах информационной безопасности и индикаторах компрометации, обнаруженных в IT-инфраструктуре. Информация о вредоносном объекте (ресурсе или его параметре) отображается на схеме атаки и в панели о ресурсе.

В этом разделе

[Подготовка к интеграции с PT Threat Analyzer \(см. раздел 11.1\)](#)

[Настройка интеграции с PT Threat Analyzer \(см. раздел 11.2\)](#)

11.1. Подготовка к интеграции с PT Threat Analyzer

До настройки интеграции вам нужно выполнить следующие действия в PT Threat Analyzer:

1. Создать репутационные списки с информацией о вредоносных и доверенных объектах.
2. Добавить учетную запись для подключения к MaxPatrol O2 к PT Threat Analyzer.
3. Получить ключ API для созданной учетной записи.

В этом разделе

[Создание репутационного списка \(см. раздел 11.1.1\)](#)

[Добавление учетной записи \(см. раздел 11.1.2\)](#)

[Создание ключа API \(см. раздел 11.1.3\)](#)

11.1.1. Создание репутационного списка

В PT Threat Analyzer вам нужно создать два репутационных списка: один должен включать информацию о вредоносных объектах, другой — о доверенных.

► Чтобы создать репутационный список:

1. В главном меню выберите раздел **Репутационные списки**.
2. Нажмите **Добавить**.
3. Введите название репутационного списка.
4. Выберите уровень доступа к наблюдению.

Примечание. Каждой учетной записи в PT Threat Analyzer назначается свой уровень доступа к информации в системе. Вы можете регистрировать и просматривать репутационные списки с уровнем доступа не выше, чем уровень, назначенный учетной записи пользователя.

5. Если вы создаете список вредоносных объектов, в поле **Запрос** введите:
`ENT [DomainName, IPAddress, URL, File] {ENT {IsIOC} CONF 0.5 ANDNOT ENT {isTrusted} CONF 0.4}`
6. Если вы создаете список доверенных объектов, в поле **Запрос** введите:
`ENT [DomainName, IPAddress, URL, File] {IsTrusted} CONF 0.5`
7. Нажмите **Добавить**.
8. Включите репутационный список по кнопке в правой верхней части страницы.

Для настройки интеграции вам потребуются идентификаторы обоих списков.

11.1.2. Добавление учетной записи

► Чтобы добавить учетную запись в PT Threat Analyzer:

1. В главном меню выберите раздел **Пользователи**.
2. Нажмите **Добавить**.
3. Введите логин учетной записи, под которой MaxPatrol O2 будет выполнять вход в PT Threat Analyzer.
4. Введите имя учетной записи, которое будет отображаться в интерфейсе.
5. Введите адрес электронной почты для учетной записи.
6. Задайте пароль для входа в интерфейс вручную или сгенерируйте его автоматически по кнопке **Сгенерировать**.
7. Выберите уровень доступа к данным в PT Threat Analyzer.

Примечание. Данные, с уровнем доступа выше, чем назначенный пользователю, ему не отображаются.

8. Выберите роли **Инженер данных** и **Аналитик SOC**.

11.1.3. Создание ключа API

► Чтобы создать ключ API для учетной записи:

1. В главном меню выберите раздел **Пользователи**.
2. Выберите учетную запись.
3. В блоке **Ключ API** нажмите **Создать**.
4. Введите описание ключа API.
5. Включите параметр **Наследовать от пользователя**.
6. Задайте срок действия ключа API или включите параметр **Бессрочный**, чтобы ключ API действовал неограниченное время.

7. Нажмите **Создать**.

PT Threat Analyzer сгенерирует новый ключ API. Ключ отображается только один раз, поэтому необходимо скопировать его.

8. Нажмите **Скопировать в буфер обмена и закрыть**.

11.2. Настройка интеграции с PT Threat Analyzer

► Чтобы настроить интеграцию:

1. Откройте на редактирование конфигурационный файл `custom.env` службы Verdicts:

```
nano /var/lib/deployed-roles/o2-application/o2base/images/verdicts.extended/config/custom.env
```

2. Добавьте в файл строки:

```
ThreatAnalyzer_BaseAddress=<IP-адрес или FQDN PT Threat Analyzer>
ThreatAnalyzer_ApiKey=<Значение ключа API>
ThreatAnalyzer_TrustedListId=<Идентификатор репутационного списка вредоносных объектов>
ThreatAnalyzer_IsIocListId=<Идентификатор репутационного списка доверенных объектов>
```

3. Перезапустите службу Verdicts:

```
docker-compose -f /var/lib/deployed-roles/o2-application/o2base/images/verdicts.extended/
docker-compose.yaml up -d
```

12. Администрирование MaxPatrol O2

Раздел содержит справочную информацию и инструкции для администрирования MaxPatrol O2 после развертывания.

В этом разделе

[Мониторинг состояния MaxPatrol O2 \(см. раздел 12.1\)](#)

[Просмотр и изменение параметров конфигурации MaxPatrol O2 \(см. раздел 12.2\)](#)

[Смена паролей служебных учетных записей \(см. раздел 12.3\)](#)

[Настройка уровня журналирования работы MaxPatrol O2 \(см. раздел 12.4\)](#)

12.1. Мониторинг состояния MaxPatrol O2

Вы можете отслеживать работу служб MaxPatrol O2, анализируя информацию о системных событиях, данные трассировки и специальные метрики. Для мониторинга состояния MaxPatrol O2 вместе с продуктом устанавливаются следующие сервисы:

- OpenTelemetry — для сбора информации о системных событиях, данных трассировки и метрик;
- ClickHouse — для хранения системного журнала и данных трассировки;
- VictoriaMetrics — для хранения метрик;
- Grafana — для визуализации, мониторинга и анализа информации о системных событиях и метрик;
- Jaeger — для визуализации данных трассировки.

Веб-интерфейс Grafana доступен по адресу `https://<IP-адрес сервера MaxPatrol O2 с установленной ролью Monitoring>:9002`, веб-интерфейс Jaeger — по адресу `https://<IP-адрес сервера MaxPatrol O2 с установленной ролью Monitoring>:16686`. По умолчанию имя пользователя `admin`, пароль `P@ssw0rd`.

В этом разделе

[Системный журнал \(см. раздел 12.1.1\)](#)

[Работа с дашбордами \(см. раздел 12.1.2\)](#)

12.1.1. Системный журнал

Вы можете просматривать информацию о работе системы с помощью сервиса Grafana. Страница журнала открывается сразу после входа в веб-интерфейс Grafana. По умолчанию в журнале отображаются 100 записей за последние пять минут.

Для работы с журналом можно использовать фильтры. Панель фильтрации расположена в верхней части страницы журнала. Для поиска информации о конкретных системных событиях доступны следующие фильтры:

- **Service** — по службе MaxPatrol O2;
- **Limit** — по количеству отображаемых записей;
- **Level** — по уровню журналирования;
- **Body** — по наличию в записи текста, введенного в поле;
- **Traceid** — по наличию для записи идентификатора трассировки, введенного в поле.

Примечание. Вы можете скопировать идентификатор трассировки из строки журнала (он отображается после названия службы).

Вы также можете выбрать период, за который отображаются записи журнала. Панель для выбора периода находится в правой верхней части страницы.

12.1.2. Работа с дашбордами

Дашборд в Grafana — это страница, на которой отображаются панели с графиками, диаграммами и прочей статистической информацией о работе продукта и операционной системы.

При установке MaxPatrol O2 в Grafana добавляются стандартные дашборды для мониторинга состояния продукта.

► Чтобы открыть дашборд:

1. Войдите в веб-интерфейс Grafana.
2. Нажмите  → **Manage**.
3. Выберите дашборд.

12.2. Просмотр и изменение параметров конфигурации MaxPatrol O2

Этот раздел содержит инструкции по просмотру и изменению параметров конфигурации ролей MaxPatrol O2, а также описание параметров базовой конфигурации ролей.

В этом разделе

[Просмотр конфигурации роли \(см. раздел 12.2.1\)](#)

[Изменение конфигурации роли \(см. раздел 12.2.2\)](#)

[Параметры базовой конфигурации ролей MaxPatrol O2 \(см. раздел 12.2.3\)](#)

12.2.1. Просмотр конфигурации роли

► Чтобы просмотреть конфигурацию роли:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_<Название роли>_<Номер версии>.tar.gz` из комплекта поставки:

```
tar -xf pt_<Название роли>_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_<Название роли>_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите идентификатор приложения роли.
5. Выберите идентификатор экземпляра роли.
6. Выберите **Advanced configuration**.

12.2.2. Изменение конфигурации роли

► Чтобы изменить конфигурацию роли:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_<Название роли>_<Номер версии>.tar.gz` из комплекта поставки:

```
tar -xf pt_<Название роли>_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_<Название роли>_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите идентификатор приложения роли.
5. Выберите идентификатор экземпляра роли.
6. Выберите **Advanced configuration**.
7. Измените значения параметров.
8. Нажмите **OK**.
9. Нажмите **Submit**.
10. Нажмите **OK**.
11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

12.2.3. Параметры базовой конфигурации ролей MaxPatrol O2

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

Таблица 5. Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost

Таблица 6. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
PgAdminPort	Порт для доступа к pgAdmin	9001
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения — HDD или SSD)	HDD
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

Таблица 7. Параметры конфигурации роли Base

Параметр	Описание	Значение по умолчанию
ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	secret

Параметр	Описание	Значение по умолчанию
EnableCentralLogCollection	Информация о работе роли Base записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLogToConsole	Информация о работе роли Base записывается в журналы Docker-контейнеров	Флажок снят
EnableLogToFiles	Информация о работе роли Base записывается в файлы журналов	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
LoggingThreshold	Уровень журналирования работы роли Base. Возможные значения: TRACE, DEBUG, INFO, WARNING, ERROR, CRITICAL	TRACE
MCHostAddress	IP-адрес или FQDN сервера PT MC	localhost
SiemCoreUrl	IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core	https://localhost

Таблица 8. Параметры конфигурации роли Monitoring

Параметр	Описание	Значение по умолчанию
CollectorServerHttpPort	Порт для доступа к коллектору OpenTelemetry по протоколу HTTP	4318
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
JaegerUiPort	Порт для доступа к веб-интерфейсу Jaeger	16686
MetricsHttpPort	Порт для доступа к веб-интерфейсу VictoriaMetrics	8428
PostgreHost	IP-адрес или FQDN сервера с установленной СУБД PostgreSQL	localhost
PostgrePort	Порт для доступа к СУБД PostgreSQL	5432
TracingCollectorHost	IP-адрес или FQDN сервера с установленной ролью Monitoring	localhost

Таблица 9. Параметры конфигурации роли Resources

Параметр	Описание	Значение по умолчанию
----------	----------	-----------------------

ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	secret
EnableCentralLogCollection	Информация о работе роли Resources записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLogToConsole	Информация о работе роли Resources записывается в журнал Docker-контейнера	Флажок снят
EnableLogToFiles	Информация о работе роли Resources записывается в файлы журнала	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
LoggingThreshold	Уровень журналирования работы роли Resources. Возможные значения: TRACE, DEBUG, INFO, WARNING, ERROR, CRITICAL	TRACE
PostgreHost	IP-адрес или FQDN сервера с установленной СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

Таблица 10. Параметры конфигурации роли Modelling

Параметр	Описание	Значение по умолчанию
ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	secret
EnableCentralLogCollection	Информация о работе роли Modelling записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLogToConsole	Информация о работе роли Modelling записывается в журнал Docker-контейнера	Флажок снят
EnableLogToFiles	Информация о работе роли Modelling записывается в файлы журнала	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
LoggingThreshold	Уровень журналирования работы роли Modelling. Возможные значения: TRACE, DEBUG, INFO, WARNING, ERROR, CRITICAL	TRACE

PostgreHost	IP-адрес или FQDN сервера с установленной СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

Таблица 11. Параметры конфигурации роли RmqMessageBus

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost

Таблица 12. Параметры конфигурации роли O2 Base

Параметр	Описание	Значение по умолчанию
ApplicationDisplayname	Название экземпляра приложения MaxPatrol O2 в PT MC	O2
BotToken	Токен Telegram-бота, добавленного в чат для экспертов	—
ChatIds	Идентификаторы Telegram-чатов для экспертов	—
ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	secret
EmailRecipients	Адреса электронной почты получателей уведомлений	—
EnableCentralLogCollection	Информация о работе роли Base записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLogToConsole	Информация о работе роли Base записывается в журналы Docker-контейнеров	Флажок снят
EnableLogToFiles	Информация о работе роли Base записывается в файлы журналов	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
LoggingThreshold	Уровень журналирования работы роли O2 Base. Возможные значения: TRACE, DEBUG, INFO, WARNING, ERROR, CRITICAL	TRACE

Параметр	Описание	Значение по умолчанию
PostgreHost	IP-адрес или FQDN сервера с установленной СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
Smtphost	IP-адрес или FQDN SMTP-сервера	—
Smtppassword	Пароль служебной учетной записи для подключения Base к SMTP-серверу	P@ssw0rd
Smtpsender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	sender@pt.ru
Smtplibuser	Логин служебной учетной записи для подключения Base к SMTP-серверу	user
UIHostAddress	IP-адрес или FQDN сервера с установленной ролью Web	localhost

Таблица 13. Параметры конфигурации роли Web

Параметр	Описание	Значение по умолчанию
BffFileLogging	Информация о работе службы BFF записывается в файл журнала	Флажок установлен
BffLogLevel	Уровень журналирования событий службы BFF. Возможные значения — debug, info, warning, error или critical	debug
ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	Secret
DISABLE_DATA_VALIDATION	Служба BFF не выполняет проверку типов данных, получаемых от других служб	Флажок установлен
EnableCentralLogCollection	Информация о работе роли Web записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLocalTelemetryLog	Информация о работе роли Web записывается в журналы Docker-контейнеров	Флажок снят
FeatureFlagBadEnabled	MaxPatrol O2 получает данные от BAD	Флажок снят

Параметр	Описание	Значение по умолчанию
FeatureFlagTAEnabled	MaxPatrol O2 получает данные от PT Threat Analyzer	Флажок снят
FeatureFlagDefaultGraphAttackPatterns	При переходе на страницу цепочки в веб-интерфейсе MaxPatrol O2 отображается схема «Паттерны атаки»	Флажок снят
FeatureFlagGraphToggle	В веб-интерфейсе MaxPatrol O2 поддерживается возможность работы со схемой «Паттерны атаки»	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
SiemCoreUrl	IP-адрес или FQDN сервера MaxPatrol 10 с установленной ролью Core	https://localhost

Таблица 14. Параметры конфигурации роли XdrAdapter

Параметр	Описание	Значение по умолчанию
ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	secret
EdrToken	Токен доступа к MaxPatrol EDR	—
EdrUri	IP-адрес или FQDN сервера MaxPatrol EDR с указанием протокола WebSocket и порта для входящих подключений от MaxPatrol O2	—
EnableCentralLogCollection	Информация о работе роли XdrAdapter записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLogToConsole	Информация о работе роли XdrAdapter записывается в журнал Docker-контейнера	Флажок снят
EnableLogToFiles	Информация о работе роли XdrAdapter записывается в файлы журнала	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
LoggingThreshold	Уровень журналирования работы роли XdrAdapter. Возможные значения: TRACE, DEBUG, INFO, WARNING, ERROR, CRITICAL	TRACE
PostgreHost	IP-адрес или FQDN сервера с установленной СУБД PostgreSQL	localhost

Параметр	Описание	Значение по умолчанию
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

Таблица 15. Параметры конфигурации роли AdapterMP10Siem

Параметр	Описание	Значение по умолчанию
ClientSecret	Ключ для регистрации приложения MaxPatrol O2 в PT MC	secret
DlqEnabled	Информация о корреляционных или нормализованных событиях, которую не удалось обработать, отправляется в базе данных в очередь недоставленных сообщений (DLQ)	Флажок установлен
EnableCentralLogCollection	Информация о работе роли AdapterMP10Siem записывается в базу данных под управлением СУБД ClickHouse	Флажок установлен
EnableLogToConsole	Информация о работе роли AdapterMP10Siem записывается в журнал Docker-контейнера	Флажок снят
EnableLogToFiles	Информация о работе роли AdapterMP10Siem записывается в файлы журнала	Флажок снят
HostAddress	IP-адрес или FQDN сервера, на который установлена роль	localhost
LoggingThreshold	Уровень журналирования работы роли AdapterMP10Siem. Возможные значения: TRACE, DEBUG, INFO, WARNING, ERROR, CRITICAL	TRACE
PostgreHost	IP-адрес или FQDN сервера с установленной СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

12.3. Смена паролей служебных учетных записей

Для выполнения своих функций компоненты MaxPatrol O2 могут использовать служебные учетные записи. Такие учетные записи не предназначены для выполнения пользователем действий в системе и необходимы для доступа компонентов к ее ресурсам. При развертывании MaxPatrol O2 логины и пароли служебных учетных записей устанавливаются значения по умолчанию.

Вы можете сменить пароли служебных учетных записей при установке ролей или после развертывания продукта. Команды для смены паролей необходимо вводить в интерфейсе терминала Linux от имени суперпользователя (root).

Смена пароля служебной учетной записи в Grafana

При развертывании MaxPatrol O2 в Grafana создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи — `admin`, пароль — `P@ssw0rd`.

► Чтобы сменить пароль служебной учетной записи в Grafana:

1. На сервере с установленной ролью Monitoring выполните команду:

```
docker exec -it $(docker ps | awk '/grafana/ {print $NF}') grafana-cli admin reset-admin-password <Новый пароль>
```

2. Измените конфигурацию роли Monitoring:

```
GrafanaAdminPassword: <Новый пароль>
```

Смена паролей служебных учетных записей в PostgreSQL

При развертывании MaxPatrol O2 в PostgreSQL создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи — `pt_system`, пароль — `P@ssw0rdP@ssw0rd`.

► Чтобы сменить пароль служебной учетной записи в PostgreSQL:

1. На сервере с установленной ролью SqlStorage выполните команду:

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

2. Измените конфигурацию роли SqlStorage:

```
PgPassword: <Новый пароль>
```

3. Подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью.

4. Измените конфигурации ролей AdapterMP10Siem, Modelling, Monitoring, O2 Base, Resources, XdrAdapter.

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

Примечание. В целях безопасности вы можете удалить строку с командой, выполненной на шаге 1, из файла `.bash_history`.

Смена пароля служебной учетной записи в RabbitMQ

Для работы с брокером сообщений RabbitMQ по умолчанию используются служебные учетные записи Administrator и pt_system, для которых установлен пароль P@ssw0rdP@ssw0rd.

► Чтобы сменить пароли служебных учетных записей для работы с RabbitMQ:

1. На сервере с установленной ролью RmqMessageBus выполните команды:


```
docker exec -it $(docker ps | awk '/messagebus-rabbitmq/ {print $NF}') rabbitmqctl change_password pt_system <Новый пароль>
docker exec -it $(docker ps | awk '/messagebus-rabbitmq/ {print $NF}') rabbitmqctl change_password Administrator <Новый пароль>
```
2. Измените конфигурацию роли RmqMessageBus:


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

Примечание. Вы можете установить неодинаковые пароли.

См. также

[Изменение конфигурации роли \(см. раздел 12.2.2\)](#)

12.4. Настройка уровня журналирования работы MaxPatrol O2

Вы можете настроить уровень журналирования работы ролей и отдельных служб MaxPatrol O2.

Примечание. Настройка доступна для ролей Resources, Modelling, O2 Base, AdapterMP10Siem, XdrAdapter.

Настройка уровня журналирования работы роли

► Чтобы настроить уровень журналирования:

1. На сервере с установленной ролью Deployer распакуйте архив pt_<Название роли>_<Номер версии>.tar.gz из комплекта поставки:


```
tar -xf pt_<Название роли>_<Номер версии>.tar.gz
```
2. Запустите сценарий:


```
pt_<Название роли>_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите идентификатор приложения роли.
5. Выберите идентификатор экземпляра роли.
6. Выберите **Advanced configuration**.
7. Измените значение параметра LoggingThreshold.

8. Нажмите **OK**.
9. Нажмите **Submit**.
10. Нажмите **OK**.
11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

Настройка уровня журналирования работы службы

► Чтобы настроить уровень журналирования:

1. На сервере MaxPatrol O2 откройте на редактирование файл `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol O2 MaxPatrol O2>/<Название экземпляра роли>/images/<Название службы>/config/custom.env`.

2. Добавьте в файл строку:

`Logging_Threshold=<Уровень журналирования>`

Примечание. Возможны значения FATAL, ERROR, WARN, INFO, DEBUG и TRACE. Для диагностики проблем рекомендуется установить значения DEBUG или TRACE.

3. Выполните команды:

```
cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol O2>/<Название экземпляра роли>/images/<Название службы>
docker-compose down
docker-compose up -d
```

13. Настройка модулей реагирования

Для пресечения обнаруженной вредоносной активности MaxPatrol O2 передает команду на реагирование в MaxPatrol EDR. Реагирование выполняется с помощью модулей, установленных на агентах. Подробнее об агентах см. в Руководстве администратора MaxPatrol EDR.

В MaxPatrol O2 автоматически поддерживается взаимодействие с модулями MaxPatrol EDR «Удаление файлов», «Изоляция узлов», «Завершение процессов». Вы можете импортировать в MaxPatrol EDR и настроить модули, поставляемые с MaxPatrol O2.

Внимание! Для корректной работы модулей необходимо [импортировать \(см. раздел 13.2\)](#) модуль o2_dispatcher, поставляемый с MaxPatrol O2, в MaxPatrol EDR и [добавить \(см. раздел 13.3\)](#) его в каждую политику, [назначенную на группу агентов \(см. раздел 13.4\)](#), с помощью которых должно выполняться реагирование.

Для большинства модулей предусмотрена [быстрая проверка их работоспособности \(см. раздел 13.26\)](#). Например, после настройки модуля вы можете проверить соединение с сервером, доступность служб или подключение к учетным записям, которые используются для реагирования.

В этом разделе приведена справочная информация о работе с модулями, а также даны инструкции по их настройке.

В этом разделе

[О модулях реагирования MaxPatrol O2 \(см. раздел 13.1\)](#)

[Импорт модуля \(см. раздел 13.2\)](#)

[Добавление модуля в политику \(см. раздел 13.3\)](#)

[Назначение политики на группу агентов \(см. раздел 13.4\)](#)

[Установка агента на сервер EDR \(см. раздел 13.5\)](#)

[Блокировка запросов к объектам в Artifactory \(см. раздел 13.6\)](#)

[Блокировка по IP-адресу в Check Point GAIa \(см. раздел 13.7\)](#)

[Блокировка учетных записей в Active Directory \(см. раздел 13.8\)](#)

[Блокировка учетных записей в Confluence \(см. раздел 13.9\)](#)

[Блокировка учетных записей в FreeIPA \(см. раздел 13.10\)](#)

[Блокировка учетных записей в Passwork \(см. раздел 13.11\)](#)

[Блокировка учетных записей и отзыв токенов в GitLab \(см. раздел 13.12\)](#)

[Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost \(см. раздел 13.13\)](#)

[Завершение SSH-сессий \(см. раздел 13.14\)](#)

- [Завершение VPN-сессий в Cisco ASA \(см. раздел 13.15\)](#)
- [Завершение сессий в OpenVPN \(см. раздел 13.16\)](#)
- [Завершение сессий в Windows \(см. раздел 13.17\)](#)
- [Завершение сессий и блокировка учетных записей в VMware vSphere \(см. раздел 13.18\)](#)
- [Отзыв сертификатов AD CS \(см. раздел 13.19\)](#)
- [Отзыв токенов в Artifactory \(см. раздел 13.20\)](#)
- [Перенаправление DNS-запросов в Active Directory \(sinkholing\) \(см. раздел 13.21\)](#)
- [Снятие групповой политики с подразделения \(см. раздел 13.22\)](#)
- [Удаление запланированных задач в Windows \(см. раздел 13.23\)](#)
- [Удаление писем в Microsoft Exchange \(см. раздел 13.24\)](#)
- [Удаление служб в Windows \(блокировка в Linux\) \(см. раздел 13.25\)](#)
- [Проверка работоспособности модуля \(см. раздел 13.26\)](#)

13.1. О модулях реагирования MaxPatrol O2

Модули, поставляемые с MaxPatrol O2, запускаются от имени учетной записи, которую использует агент. По умолчанию агенты под управлением Microsoft Windows запускаются от имени системной учетной записи (System), под управлением ОС семейства Unix — от имени учетной записи суперпользователя (root).

Модуль выполняет действие реагирования на конечном устройстве по команде эксперта или автоматически при регистрации определенного события. MaxPatrol EDR передает MaxPatrol O2 сведения о результатах реагирования. Ответ в формате JSON содержит список параметров модуля и статус выполнения действия (поле `status`). Если действие реагирования выполнено частично или не выполнено, ответ включает описание причины неуспешного запроса (поле `data.reason`). Возможные статусы выполнения действия:

- успешный — поле `status` имеет значение `success`, поле `data.reason` отсутствует;
- частично успешный — поле `status` имеет значение `success`, присутствует поле `data.reason`;
- неуспешный — поле `status` имеет значение отличное от `success`, присутствует поле `data.reason`.

13.2. Импорт модуля

Вы можете импортировать модуль на сервер MaxPatrol EDR из ZIP-архива. Архив может содержать несколько разных модулей и несколько версий каждого модуля. За одну операцию вы можете загрузить только один модуль, при этом возможен импорт сразу всех версий этого

модуля. Если загружаемая версия модуля уже есть на сервере, то импорт будет возможен только при условии перезаписи ее файлов и конфигурации. Размер архива не должен превышать 100 МБ.

► Чтобы импортировать модуль:

1. В главном меню выберите раздел **EDR** → **Модули**.
2. Нажмите **Импортировать**.
3. Выберите архив с файлами модуля.
4. Выберите модуль, который вы хотите импортировать.
5. Выберите версию модуля, которую вы хотите импортировать.
6. Если требуется перезаписать на сервере файлы и конфигурации загружаемых версий модуля, установите флажок **Перезаписать модуль**.

Если вы не установите этот флажок и на сервере уже есть хотя бы одна загружаемая версия модуля, то не импортируется ни одна из версий.

7. Нажмите **Импортировать**.

13.3. Добавление модуля в политику

Для выполнения инструкции в MaxPatrol EDR должна быть создана политика, в которую планируется добавить модуль. Подробнее о политиках см. в Руководстве администратора MaxPatrol EDR.

Примечание. Нельзя добавить модуль в политику, назначенную на группу агентов, если этот модуль уже добавлен в одну из политик, назначенную на ту же группу агентов.

► Чтобы добавить модуль в политику:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Доступны для добавления** выберите модуль.
4. Нажмите **Добавить**.

Если политика [назначена на группу \(см. раздел 13.4\)](#), то сразу после добавления модуля он будет автоматически установлен на всех агентах группы.

13.4. Назначение политики на группу агентов

Для установки модулей на агенты необходимо назначить политику на группу агентов. Одну политику можно назначить на множество групп. Вы не можете назначить политику на группу, если в этой политике есть модуль, который уже работает на агентах этой группы (входит в другую политику). В таких случаях вам нужно отключить модуль в другой политике или снять ее с группы.

► Чтобы назначить политику на группу:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. Нажмите .
4. В списке **Доступны для назначения** нажмите  напротив группы, на которую вы хотите назначить политику.

13.5. Установка агента на сервер EDR

Для работы модулей могут быть использованы агенты, установленные на сервере агентов, а не на конечном устройстве. Такие агенты работают только с модулями, которые выполняют реагирование с помощью серверной части.

Для установки агента на сервер используется сервис Swagger UI.

► Чтобы установить агент на сервер MaxPatrol EDR:

1. В адресной строке браузера введите адрес сервиса Swagger UI: <IP-адрес или FQDN управляющего сервера MaxPatrol EDR>/api/edr/v1/swagger/index.html.
2. Выберите запрос **POST/agents/**.
3. Нажмите **Try it out**.
4. В поле **service_hash** укажите идентификатор сервера агентов.

Примечание. Для получения идентификатора нужно в главном меню MaxPatrol 10 выбрать **EDR** → **Агенты** и скопировать идентификатор из URL-адреса: `https://<IP-адрес или FQDN управляющего сервера MaxPatrol 10>/#/edr/services/<Идентификатор сервера агентов>`.

5. В поле **json** введите:

```
{
  "arch": "amd64",
  "name": "0.0.0.0_server_only",
  "os": "linux"
}
```

6. Нажмите **Execute**.

13.6. Блокировка запросов к объектам в Artifactory

Модуль «Блокировка запросов к объектам в Artifactory» блокирует и [разблокирует](#) (см. [раздел 13.6.4](#)) переход по ссылке на объект в JFrog Artifactory с помощью PT AF.

Модуль выполняет реагирование с помощью серверной части под управлением Unix. Агенты должны быть установлены на конечных устройствах под управлением Unix или Windows.

Для настройки модуля необходимо:

1. Включить и настроить перенаправление запросов к JFrog Artifactory через PT AF. Включить в политике безопасности использование модуля защиты «Черные списки».
2. Создать учетную запись ОС на сервере PT AF для выполнения реагирования.
3. [Импортировать модуль](#) (см. [раздел 13.2](#)) в MaxPatrol EDR.
4. [Добавить модуль в политику](#) (см. [раздел 13.3](#)).
5. [Назначить политику на группу агентов](#) (см. [раздел 13.4](#)).
6. Настроить параметры модуля в политике.

В этом разделе

[Настройка защиты Artifactory в PT AF 3 3.7](#) (см. [раздел 13.6.1](#))

[Создание учетной записи для подключения по SSH](#) (см. [раздел 13.6.2](#))

[Настройка параметров модуля «Блокировка запросов к объектам в Artifactory»](#) (см. [раздел 13.6.3](#))

[Разблокирование URL-адреса](#) (см. [раздел 13.6.4](#))

13.6.1. Настройка защиты Artifactory в PT AF 3 3.7

Для блокирования URL-адресов, которые ведут к объектам Artifactory, необходимо включить защиту веб-приложения в PT AF — перенаправить запросы к Artifactory на узел, который защищен PT AF, и включить модуль защиты «Черные списки».

Примечание. Подробнее о работе с PT AF 3 [см. на справочном портале](#).

Для настройки защиты Artifactory в PT AF необходимо:

1. Создать группу серверов и указать в ней сервер Artifactory.
2. Создать сервис и добавить его в группу серверов.
3. Создать политику безопасности.
4. Создать веб-приложение.

В этом разделе

[Создание группы серверов \(см. раздел 13.6.1.1\)](#)

[Создание сервиса \(см. раздел 13.6.1.2\)](#)

[Создание политики безопасности \(см. раздел 13.6.1.3\)](#)

[Создание веб-приложения \(см. раздел 13.6.1.4\)](#)

13.6.1.1. Создание группы серверов

► Чтобы создать группу серверов:

1. В главном меню выберите **Конфигурация** → **Сеть** → **Группы серверов**.
2. Нажмите кнопку **Создать**.
3. Укажите название группы.
4. В блоке параметров **Защищаемый сервер** нажмите **Добавить**.
5. В поле **Узел** укажите IP-адрес или имя сервера Artifactory.
6. Укажите номер порта, на котором расположен сервер Artifactory.
7. В поле **Вес сервера** укажите частоту использования сервера.
8. Нажмите кнопку **Применить**.

13.6.1.2. Создание сервиса

► Чтобы создать сервис:

1. В главном меню выберите **Конфигурация** → **Сеть** → **Сервисы**.
2. Нажмите кнопку **Создать**.
3. Укажите название сервиса.
4. Выберите режим интеграции **Обратный прокси-сервер**.
5. Установите флажок **Активен**.
6. В блоке параметров **Серверы** нажмите **Добавить**.
7. Укажите алиас интерфейса, соответствующий одному или нескольким сетевым интерфейсам.
8. Укажите внешний порт для прослушивания, который PT AF будет слушать для того, чтобы проксировать HTTP-трафик.

Внимание! Для корректной работы PT AF не используйте порты, задействованные для внутренних нужд.

9. Укажите группу серверов, [созданную ранее](#) (см. раздел 13.6.1.1).
10. Выберите протокол группы серверов для связи с защищаемыми серверами.
11. Если Artifactory использует протокол ws или wss для взаимодействия с сервером, установите флажок **Включить прокси-сервер WebSocket**.
12. Если вы используете протокол **HTTPS**, установите флажок **Включить SSL** и укажите параметры SSL.

Примечание. Вы можете выбрать не более двух объектов SSL. При выборе двух объектов их типы должны различаться (ГОСТ и RSA).

13. Нажмите кнопку **Применить**.

13.6.1.3. Создание политики безопасности

► Чтобы создать политику безопасности:

1. В главном меню выберите **Конфигурация** → **Безопасность** → **Политики**.
2. Нажмите кнопку **Создать**.
3. Укажите имя политики.
4. Выберите шаблон **LAX (Generic)**.
5. Нажмите кнопку **Применить**.
6. В строке с созданной политикой нажмите .
7. Выберите вкладку **Модули**.
8. Установите флажок **Черные списки**.
9. Нажмите кнопку **Применить**.

13.6.1.4. Создание веб-приложения

► Чтобы создать веб-приложение:

1. В главном меню выберите **Конфигурация** → **Безопасность** → **Веб-приложения**.
2. Нажмите кнопку **Создать**.
3. Укажите название веб-приложения.
4. Выберите тип защищаемого сервера **Generic**.
5. Выберите сервис, [созданный ранее](#) (см. раздел 13.6.1.2).
6. Выберите политику безопасности, [которую создали ранее](#) (см. раздел 13.6.1.3).
7. Выберите режим защиты **Активное предотвращение**.

8. В блоке параметров **Узлы** нажмите **Добавить**.
9. Укажите FQDN сервера, на который необходимо перенаправлять запросы к Artifactory.
10. В блоке параметров **Расположение** нажмите **Добавить** и введите **/**.
11. Нажмите кнопку **Применить**.

13.6.2. Создание учетной записи для подключения по SSH

► Чтобы создать учетную запись для подключения по SSH:

1. Откройте интерфейс командной строки на сервере PT AF.
2. Создайте учетную запись:

```
useradd -m -g users -s /bin/bash <Логин>
passwd <Логин>
<Пароль>
```
3. Настройте права доступа к домашнему каталогу:

```
chmod 700 /home/<Логин>
```
4. Войдите от имени созданной учетной записи:

```
su - <Логин>
<Пароль>
```
5. Откройте конфигурационный файл службы sshd (`*/etc/ssh/sshd_config`).
6. В секцию `AllowUsers` добавьте созданную учетную запись.
7. Сохраните конфигурационный файл.

13.6.3. Настройка параметров модуля «Блокировка запросов к объектам в Artifactory»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Блокировка запросов к объектам в Artifactory».
4. В блоке параметров **connections** нажмите **Изменить**.
5. Нажмите кнопку **Добавить**.
6. В поле **connection_name** укажите название подключения к PT AF (используется для идентификации соединения в системных журналах).
7. В поле **connection_timeout_ms** укажите время ожидания ответа от сервера (в миллисекундах).

8. Если требуется, в блоке параметров **database** укажите имя БД для аутентификации, название БД, логин и пароль учетной записи для подключения к базе данных PT AF.
9. В поле **doorkeeper_password** укажите пароль учетной записи для доступа к PT AF по SSH (см. раздел 13.6.2).
10. В поле **doorkeeper_username** укажите логин учетной записи для доступа к PT AF по SSH (см. раздел 13.6.2).
11. Если используется командная оболочка WSC, в полях **doorkeeper_wsc_password** и **doorkeeper_wsc_username** укажите пароль и логин учетной записи для доступа к WSC.
12. Если используется приватный ключ, в поле **private_key** укажите его в формате PEM с алгоритмом шифрования RSA:

```
-----BEGIN RSA PRIVATE KEY-----
<Ключ>
-----END RSA PRIVATE KEY-----
```
13. Если используется приватный ключ, в поле **private_key_password** укажите пароль для доступа к нему по SSH.
14. Если используется публичный ключ для доступа по SSH, в поле **public_key** укажите его значение.
15. В поле **waf_address** укажите адрес для доступа к серверу PT AF по SSH.
16. В поле **waf_port** укажите порт для доступа к серверу PT AF по SSH.
17. Нажмите кнопку **Сохранить**.
18. Если требуется, в блоке параметров **security_key** укажите ключ безопасности для выполнения действий, которые требуют дополнительного уровня доступа.
19. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.6.4. Разблокирование URL-адреса

Вы можете вручную разблокировать URL-адрес объекта в Artifactory, который заблокировали ранее.

► Чтобы разблокировать URL-адрес:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать URL-адрес.
3. Выберите модуль «Блокировка запросов к объектам в Artifactory».
4. Нажмите .
5. Выберите действие с параметрами **pt_artifactory_blocker_unblock_urls**.
6. Укажите часть URL-адреса, который необходимо разблокировать.

Внимание! URL-адрес чувствителен к регистру и должен полностью совпадать с адресом, который был заблокирован.

7. Если при настройке модуля был задан ключ безопасности, укажите его в поле **security_key**.
8. Нажмите **Выполнить действие**.

13.7. Блокировка по IP-адресу в Check Point GAIa

Модуль «Блокировка по IP-адресу в Check Point GAIa» блокирует и [разблокирует](#) (см. [раздел 13.7.7](#)) сетевой трафик по IP-адресам в операционной системе Check Point GAIa.

Модуль выполняет реагирование с помощью серверной части под управлением Unix. Агенты должны быть установлены на конечных устройствах под управлением Unix или Windows.

Примечание. На компьютере, с которого будет выполняться настройка модуля, должна быть установлена программа SmartConsole. Инструкции необходимо выполнять от имени суперпользователя (root).

Для того, чтобы обеспечить реагирование с помощью модуля, на Check Point Security Management Server нужно:

1. Создать сетевые группы, в которые будут добавляться блокируемые IP-адреса.
2. Получить идентификаторы групп.
3. Создать правила блокировки трафика для групп.
4. Создать профиль для блокировки трафика.
5. Создать учетную запись, от имени которой будет выполняться реагирование.

Далее необходимо:

1. [Импортировать модуль](#) (см. [раздел 13.2](#)) в MaxPatrol EDR.
2. [Добавить модуль в политику](#) (см. [раздел 13.3](#)).
3. [Назначить политику на группу агентов](#) (см. [раздел 13.4](#)).
4. Настроить параметры модуля в политике.

В этом разделе

[Создание сетевой группы](#) (см. [раздел 13.7.1](#))

[Получение идентификатора группы](#) (см. [раздел 13.7.2](#))

[Создание правила для группы](#) (см. [раздел 13.7.3](#))

[Создание профиля для блокировки трафика](#) (см. [раздел 13.7.4](#))

[Создание учетной записи администратора](#) (см. [раздел 13.7.5](#))

Настройка параметров модуля «Блокировка по IP-адресу в Check Point GAIa»
(см. раздел 13.7.6)

Разблокирование IP-адреса (см. раздел 13.7.7)

13.7.1. Создание сетевой группы

Для настройки модуля необходимо создать три сетевые группы, в которые будут добавляться IP-адреса для блокировки входящего, исходящего и всего (входящего и исходящего) трафика.

► Чтобы создать сетевую группу:

1. Запустите SmartConsole.
2. Введите логин и пароль.
3. Укажите IP-адрес Check Point Security Management Server.
4. Нажмите **Login**.
5. На вкладке **Objects** нажмите **New** → **More** → **Network Object** → **Group** → **Network Group**.
6. Введите название группы для блокировки входящего трафика.
7. Нажмите **OK**.
8. Нажмите **Publish** и подтвердите публикацию.

Далее необходимо создать группу для блокировки исходящего трафика и группу для блокировки всего трафика, повторив шаги 5—8.

13.7.2. Получение идентификатора группы

► Чтобы получить идентификатор группы:

1. Запустите SmartConsole.
2. Введите логин и пароль.
3. Укажите IP-адрес Check Point Security Management Server.
4. Нажмите **Login**.
5. Выберите раздел **GATEWAYS & SERVERS**.
6. Нажмите **Actions** → **Open Shell**.
7. Введите логин и пароль, которые вы использовали для входа в SmartConsole.
8. Нажмите **Login**.
9. Выполните команду:

```
mgmt login user <Логин учетной записи>
```

10. Введите пароль учетной записи.

11. Выполните команду:

```
mgmt_cli -m <IP-адрес сервера, на котором была создана группа> -u <Логин учетной записи>
-r <Пароль учетной записи> show-group name <Название группы для блокировки входящего
трафика>
```

Ответ будет содержать поле `uid` с идентификатором группы.

Далее необходимо получить идентификаторы двух оставшихся групп, повторив шаг 11.

13.7.3. Создание правила для группы

Для каждой группы необходимо создать правило, с помощью которого в группу будут добавляться IP-адреса.

► Чтобы создать правила для групп:

1. Запустите SmartConsole.
2. Введите логин и пароль.
3. Укажите IP-адрес Check Point Security Management Server.
4. Нажмите **Login**.
5. Выберите раздел **SECURITY POLICIES**.
6. В списке правил выберите первую строку и нажмите .
7. В новой строке укажите название правила для блокировки входящего трафика.
8. Наведите курсор на поле **Destination** и нажмите .
9. Выберите группу для блокировки входящего трафика.
10. Наведите курсор на поле **Track**, нажмите ▼ → **Log**.
11. Нажмите .
12. В новой строке укажите название правила для блокировки исходящего и всего (входящего и исходящего) трафика.
13. Наведите курсор на поле **Destination** и нажмите .
14. Выберите группу для блокировки исходящего трафика и группу для блокировки всего трафика.
15. Наведите курсор на поле **Track**, нажмите ▼ → **Log**.
16. Нажмите **Publish** и подтвердите публикацию.

13.7.4. Создание профиля для блокировки трафика

► Чтобы создать профиль:

1. Запустите SmartConsole.
2. Введите логин и пароль.
3. Укажите IP-адрес Check Point Security Management Server.
4. Нажмите **Login**.
5. Выберите раздел **MANAGE & SETTINGS**.
6. Нажмите **Permissions & Administrators** → **Permission Profiles** → .
7. Введите название профиля.
8. В блоке параметров **Permissions** выберите вариант **Customized**.
9. Выберите вкладку **Access Control** и снимите флажки в блоках параметров:
 - **Policy** — **Application Control and URL Filtering**, **Content Awareness** и **Mobile Access**;
 - **Additional Policies** — все флажки;
 - **Actions** — **Application Control and URL Filtering Update**.
10. Выберите вкладку **Threat Prevention** и снимите флажки в блоках параметров:
 - **Policy** — все флажки;
 - **Permissions** — **Profiles** и **Protections**;
 - **Actions** — **IPS Update**.
11. Выберите вкладку **Others** и снимите все флажки, кроме **Common Objects** и **Check Point Users Database**.
12. В раскрывающемся списке напротив флажка **Common Objects** выберите **Write**.
13. Выберите вкладку **Management** и снимите флажок **High-Availability Operations**.
14. Нажмите **OK**.

13.7.5. Создание учетной записи администратора

► Чтобы создать учетную запись администратора:

1. Запустите SmartConsole.
2. Введите логин и пароль.
3. Укажите IP-адрес Check Point Security Management Server.
4. Нажмите **Login**.

5. Выберите раздел **MANAGE & SETTINGS**.
6. Нажмите **Permissions & Administrators** → **Administrators** →  → **New Administrator**.
7. Укажите имя пользователя, от имени которого будет выполняться реагирование.
8. В раскрывающемся списке **Authentication Method** выберите пункт **Check Point Password**.
9. Нажмите **Set New Password**.
10. Задайте пароль для учетной записи администратора и подтвердите его.
11. Снимите флажок **User must change password on next login**.
12. Нажмите **OK**.
13. В раскрывающемся списке **Permission Profile** выберите [профиль для блокировки трафика \(см. раздел 13.7.4\)](#).
14. Нажмите **OK**.
15. Нажмите **Publish** и подтвердите публикацию.

13.7.6. Настройка параметров модуля «Блокировка по IP-адресу в Check Point GAIa»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику, в которую добавлен модуль.
3. В списке **Включенные** выберите модуль «Блокировка по IP-адресу в Check Point GAIa».
4. В качестве значений параметров **doorkeeper_username** и **doorkeeper_password** укажите логин и пароль [учетной записи \(см. раздел 13.7.5\)](#), под которой будет выполняться реагирование.
5. Если требуется, в поле **api_key** введите API-ключ для подключения к Check Point Security Management Server.
6. Если требуется, в поле **block_lifetime_check_period_m** измените время, через которое будет выполняться проверка, не истек ли срок блокировки IP-адресов (в минутах). При нулевом значении параметра проверка не выполняется.
7. Если требуется, в поле **block_lifetime_m** измените время, в течение которого будут заблокированы IP-адреса (в минутах). При нулевом значении параметра время блокировки не ограничивается.
8. Если требуется, в поле **check_point_policy_package** измените название политики.
9. В поле **check_point_url** укажите IP-адрес и порт Check Point Security Management Server, например: <https://192.0.2.0:443>.

10. Если требуется, в поле **dummy_ip** измените IP-адрес, который создается автоматически для наполнения групп, используемых для блокировки трафика.
11. В поле **group_id_block_all** укажите идентификатор группы, в которую будут добавляться IP-адреса для блокировки всего трафика.
12. В поле **group_id_block_in** укажите идентификатор группы, в которую будут добавляться IP-адреса для блокировки входящего трафика.
13. В поле **group_id_block_out** укажите идентификатор группы, в которую будут добавляться IP-адреса для блокировки исходящего трафика.
14. Если требуется, в поле **max_ips_per_group** измените максимальное количество IP-адресов, которые могут быть добавлены в группу. При нулевом значении параметра количество IP-адресов в группе не ограничивается.

Если IP-адрес должен быть добавлен в группу, в которой лимит на количество IP-адресов уже достигнут, то из группы будет удален IP-адрес, который был заблокирован раньше остальных.
15. Если требуется, в поле **policy_installation_step_ms** измените время, через которое будет проверяется готовность к установке следующей политики для блокировки трафика (в миллисекундах).
16. Если требуется, в поле **policy_installation_timeout_ms** измените время ожидания установки политики (в миллисекундах).
17. Если требуется, в поле **request_timeout_ms** измените время ожидания ответа от Check Point Security Management Server (в миллисекундах). При нулевом значении время выполнения запроса не ограничивается; максимальное значение — 600000.
18. Если требуется, в блоке параметров **fixed_blocked_ips** нажмите **Добавить** и укажите IP-адреса, которые будут блокироваться навсегда.
19. Если требуется, в блоке параметров **trusted_ips** нажмите **Добавить** и укажите IP-адреса, которые не будут блокироваться при реагировании.
20. Нажмите **Сохранить**.

См. также

[Создание правила для группы \(см. раздел 13.7.3\)](#)

13.7.7. Разблокирование IP-адреса

Вы можете вручную разблокировать входящий и исходящий сетевой трафик для IP-адреса, который заблокировали ранее.

► Чтобы разблокировать IP-адрес:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать входящий и исходящий сетевой трафик для IP-адреса.
3. Выберите модуль «Блокировка по IP-адресу в Check Point GAIa».
4. Нажмите .
5. Выберите действие с параметрами **cpc_unblock_single_ip_in_all_groups**.
6. Укажите IP-адрес, который необходимо разблокировать.
7. Нажмите **Выполнить действие**.

13.8. Блокировка учетных записей в Active Directory

Модуль «Блокировка учетных записей в Active Directory» блокирует и [разблокирует](#) (см. [раздел 13.8.7](#)) учетные записи пользователей Active Directory. Для того, чтобы обеспечить реагирование с помощью модуля, на контроллере домена нужно:

1. Создать доменную группу учетных записей для выполнения реагирования.
2. Создать доменную учетную запись пользователя Active Directory, от имени которого будет выполняться реагирование.
3. Добавить учетную запись в доменную группу.
4. Предоставить учетной записи права на управление учетными записями в Active Directory.
5. Экспортировать сертификат контроллера домена.

Далее необходимо:

1. [Импортировать модуль](#) (см. [раздел 13.2](#)) в MaxPatrol EDR.
2. [Добавить модуль в политику](#) (см. [раздел 13.3](#)).
3. [Назначить политику на группу агентов](#) (см. [раздел 13.4](#)).
4. Настроить параметры модуля в политике.

В этом разделе

[Создание доменной группы пользователей](#) (см. [раздел 13.8.1](#))

[Создание доменной учетной записи](#) (см. [раздел 13.8.2](#))

[Добавление учетной записи в доменную группу пользователей](#) (см. [раздел 13.8.3](#))

[Предоставление прав на управление учетными записями](#) (см. [раздел 13.8.4](#))

[Экспорт корневого сертификата контроллера домена](#) (см. [раздел 13.8.5](#))

Настройка параметров модуля «Блокировка учетных записей в Active Directory»
(см. раздел 13.8.6)

Разблокирование учетной записи Active Directory (см. раздел 13.8.7)

13.8.1. Создание доменной группы пользователей

► Чтобы создать доменную группу пользователей:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.
3. В панели слева выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.
4. В главном меню выберите **Действие** → **Создать** → **Группа**.
5. В поле **Имя группы** введите название группы.
6. Нажмите **ОК**.

13.8.2. Создание доменной учетной записи

► Чтобы создать доменную учетную запись:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.
3. В панели слева выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.
4. В главном меню выберите **Действие** → **Создать** → **Пользователь**.
5. Введите имя пользователя.
6. В поле **Имя входа пользователя** введите логин учетной записи.
7. Нажмите **Далее**.
8. Введите пароль учетной записи и подтвердите его.
9. Снимите флажок **Требовать смены пароля при следующем входе в систему**.
10. Установите флажок **Срок действия пароля не ограничен**.
11. Нажмите **Далее**.
12. Нажмите **Готово**.

13.8.3. Добавление учетной записи в доменную группу пользователей

- ▶ Чтобы добавить доменную учетную запись в доменную группу пользователей:
 1. Откройте панель управления Windows.
 2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.
 3. В панели слева выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.
 4. Выберите учетную запись, которую нужно добавить в группу.
 5. В главном меню выберите **Действие** → **Свойства**.
 6. Выберите вкладку **Член групп**.
 7. Нажмите **Добавить**.
 8. В поле **Введите имена выбираемых объектов** введите название группы.
 9. Нажмите **ОК**.
 10. В списке **Член групп** выберите добавленную группу и нажмите **Задать основную группу**.
 11. В списке **Член групп** выберите группу **Domain Users** и нажмите **Удалить**.
 12. В окне **Свойства: <Логин>** нажмите **ОК**.

13.8.4. Предоставление прав на управление учетными записями

- ▶ Чтобы предоставить доменной учетной записи права на управление учетными записями Active Directory:
 1. Откройте панель управления Windows.
 2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory** → **<Имя домена>**.
 3. Откройте контекстное меню подразделения, содержащего учетную запись пользователя, которому требуется делегировать контроль, и выберите **Делегирование управления**.
 4. Нажмите **Далее**.
 5. Нажмите **Добавить**.
 6. Нажмите **Размещение**.

7. Выберите имя домена учетной записи пользователя, которому требуется делегировать управление.
8. Нажмите **Готово**.
9. В поле **Введите имена выбираемых объектов** введите имя учетной записи.
10. Нажмите **Проверить имена**.
11. Нажмите **ОК**.
12. Нажмите **Далее**.
13. Выберите **Создать особую задачу для делегирования**.
14. Нажмите **Далее**.
15. Выберите **Только следующим объектам в этой папке**.
16. В списке объектов установите флажок **Пользователь объектов**.
17. Установите флажок **Создать выбранные объекты в этой папке**.
18. Нажмите **Далее**.
19. Снимите флажок **Общие**.
20. Установите флажок **Разрешения для свойств**.
21. В списке **Разрешения** установите флажки **Read userAccountControl** и **Write userAccountControl**.
22. Нажмите **Далее**.
23. Нажмите **Завершить**.

13.8.5. Экспорт корневого сертификата контроллера домена

- Чтобы экспортировать корневой сертификат контроллера домена:

1. Выберите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `mmc` и нажмите **ОК**.
3. В главном меню выберите **Файл** → **Добавить или удалить оснастку**.
4. В списке доступных оснасток выберите **Сертификаты** → **Добавить**.
5. Выберите вариант **учетной записи компьютера**.
6. Нажмите **Далее**.
7. Выберите вариант **локальным компьютером**.
8. Нажмите **Готово**.

9. Нажмите **ОК**.
10. Выберите **Сертификаты (локальный компьютер) → Доверенные корневые центры сертификации → Сертификаты**.
11. Откройте контекстное меню корневого сертификата, которым подписан сертификат контроллера домена, и выберите **Все задачи → Экспорт**.
12. Нажмите **Далее**.
13. Выберите вариант **Файлы X.509 (.CER) в кодировке Base-64** и нажмите **Далее**.
14. Укажите имя файла сертификата и нажмите **Далее**.
15. Нажмите **Готово**.

Внимание! Сертификат должен содержать расширение X509v3 Basic Constraints, в котором параметр **CA** имеет значение **True**.

Далее необходимо сменить расширение файла сертификата с CER на PEM. Файл сертификата потребуется для настройки параметров модуля.

13.8.6. Настройка параметров модуля «Блокировка учетных записей в Active Directory»

Модуль «Блокировка учетных записей в Active Directory» может выполнять реагирование с помощью агентской и серверной части. Вы можете настроить параметры подключения к серверу Active Directory для агентской и серверной частей модуля или для одной из них.

До настройки параметров модуль должен быть [импортирован \(см. раздел 13.2\)](#) в MaxPatrol EDR и [добавлен в политику \(см. раздел 13.3\)](#), политика должна быть назначена на группу агентов (см. [раздел 13.4](#)).

► Чтобы настроить параметры модуля для реагирования с помощью агентской части:

1. В главном меню выберите **EDR → Политики**.
2. Выберите политику, в которую добавлен модуль.
3. В списке **Включенные** выберите модуль «Блокировка по IP-адресу в Active Directory».
4. В блоке параметров **agent_side_connections** нажмите **Изменить**.
5. Нажмите **Добавить**.
6. В поле **connection_name** укажите название соединения с агентской частью модуля (используется для идентификации соединения в системных журналах).
7. В поле **domain_server_name** укажите имя доменного сервера, которое будет использоваться при вызове команд на блокировку и разблокировку учетных записей.
8. В качестве значений параметров **domain_user_name** и **domain_user_password** укажите логин и пароль учетной записи пользователя, от имени которого будет выполняться реагирование.

Примечание. Если значение **domain_user_name** не указано, реагирование выполняется от имени системной учетной записи System.

9. Если требуется, в блоке параметров **security_key** нажмите **Изменить** и укажите ключ безопасности для выполнения действий, которые требуют дополнительного уровня доступа.
10. Нажмите **Сохранить**.
11. Если требуется, в блоке параметров **trusted_usernames** нажмите **Добавить** и укажите логины учетных записей, которые не нужно блокировать при реагировании.
12. Нажмите **Сохранить**.

Параметры модуля настроены.

► Чтобы настроить параметры модуля для реагирования с помощью серверной части:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику, в которую добавлен модуль.
3. В списке **Включенные** выберите модуль «Блокировка учетных записей в Active Directory».
4. Если требуется, в блоке параметров **security_key** нажмите **Изменить** и укажите ключ безопасности для выполнения действий, которые требуют дополнительного уровня доступа.
5. В блоке параметров **server_side_connections** нажмите **Изменить**.
6. Нажмите **Добавить**.
7. Скопируйте содержимое [файла сертификата \(см. раздел 13.8.5\)](#) в поле **certificate**.
8. Если требуется, в поле **connection_name** укажите название соединения с серверной частью модуля.
9. В поле **distinguished_name** укажите отличительное имя учетной записи пользователя, от имени которого будет выполняться реагирование, например CN=admin, CN=users, DC=company, DC=com.
10. В поле **distinguished_name_search** укажите фильтр для поиска этой учетной записи в Active Directory, например DC=company, DC=com.
11. Если требуется запретить TLS-шифрование подключения, в качестве значения параметра **enable_starttls** выберите вариант **Нет**.
12. В поле **ldap_uri** укажите URL сервера Active Directory в формате `ldap://<FQDN или IP-адрес сервера Active Directory>`.
13. В поле **user_password** укажите пароль учетной записи пользователя, от имени которого будет выполняться реагирование.
14. Нажмите **Сохранить**.

15. Если требуется, в блоке параметров **trusted_usernames** нажмите **Добавить** и укажите логины учетных записей, которые не нужно блокировать при реагировании.

16. Нажмите **Сохранить**.

Параметры модуля настроены.

См. также

[Импорт модуля \(см. раздел 13.2\)](#)

[Добавление модуля в политику \(см. раздел 13.3\)](#)

[Назначение политики на группу агентов \(см. раздел 13.4\)](#)

13.8.7. Разблокирование учетной записи Active Directory

Вы можете вручную разблокировать учетную запись Active Directory, которую заблокировали ранее.

► Чтобы разблокировать учетную запись Active Directory:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать учетную запись.
3. Выберите модуль «Блокировка учетных записей в Active Directory».
4. Нажмите .
5. Выберите действие с параметрами **adcn_unblock_user**.
6. Если требуется, укажите ключ безопасности.
7. Укажите логин учетной записи заблокированного пользователя.
8. Нажмите **Выполнить действие**.

13.9. Блокировка учетных записей в Confluence

Модуль «Блокировка учетных записей в Confluence» блокирует и [разблокирует \(см. раздел 13.9.2\)](#) учетные записи пользователей вики-системы Atlassian Confluence.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix или Windows.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

4. Настроить параметры модуля в политике.
5. Если версия Confluence от 7.7 до 8.2 — отключить режим безопасных сессий администратора. Для этого необходимо нажать  → **Основные настройки** → **Настройки безопасности** → **Изменить**, снять флажок **Безопасные сессии администратора**, нажать **Сохранить**.

В этом разделе

Настройка параметров модуля «Блокировка учетных записей в Confluence» (см. раздел 13.9.1)

Разблокирование учетной записи Confluence (см. раздел 13.9.2)

13.9.1. Настройка параметров модуля «Блокировка учетных записей в Confluence»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Блокировка учетных записей в Confluence».
4. В блоке параметров **doorkeeper_password** нажмите **Изменить**.
5. В поле **doorkeeper_password** укажите пароль учетной записи администратора.
6. Нажмите кнопку **Сохранить**.
7. В поле **confluence_url** укажите URL-адрес и порт сервера Confluence (например, `https://confluence.example.com:8080`).
8. В поле **doorkeeper_username** укажите логин учетной записи администратора.
9. В поле **timeout_ms** укажите максимальное время ожидания ответа сервера Confluence (в миллисекундах).
10. Если требуется, в блоке параметров **trusted_usernames** нажмите **Добавить** и укажите логины учетных записей, которые не нужно блокировать при реагировании.
11. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.9.2. Разблокирование учетной записи Confluence

Вы можете вручную разблокировать учетную запись Confluence, которую заблокировали ранее.

► Чтобы разблокировать учетную запись Confluence:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать учетную запись.
3. Выберите модуль «Блокировка учетных записей в Confluence».
4. Нажмите .
5. Выберите действие с параметрами **confl_unblock_user**.
6. Укажите логин учетной записи заблокированного пользователя.
7. Нажмите **Выполнить действие**.

Учетная запись пользователя разблокирована.

13.10. Блокировка учетных записей в FreeIPA

Модуль «Блокировка учетных записей в FreeIPA» блокирует и [разблокирует](#) (см. раздел 13.10.4) учетные записи службы каталогов FreeIPA.

Модуль выполняет реагирование с помощью агентской и серверной частей. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix.

Для настройки модуля необходимо:

1. Создать роль для блокировки учетных записей FreeIPA.
2. Создать учетную запись FreeIPA для реагирования в агентской части.
3. [Импортировать модуль](#) (см. раздел 13.2) в MaxPatrol EDR.
4. [Добавить модуль в политику](#) (см. раздел 13.3).
5. [Назначить политику на группу агентов](#) (см. раздел 13.4).
6. Настроить параметры модуля в политике.

В этом разделе

[Создание роли для блокировки учетной записи](#) (см. раздел 13.10.1)

[Создание учетной записи FreeIPA](#) (см. раздел 13.10.2)

[Настройка параметров модуля «Блокировка учетных записей в FreeIPA»](#) (см. раздел 13.10.3)

[Разблокирование учетной записи FreeIPA](#) (см. раздел 13.10.4)

13.10.1. Создание роли для блокировки учетной записи

► Чтобы создать роль для блокировки учетной записи FreeIPA:

1. В адресной строке браузера введите IP-адрес или доменное имя сервера.
2. Войдите в веб-интерфейс FreeIPA от имени учетной записи администратора.
3. В главном меню выберите **IPA-сервер**.
4. Нажмите **Управление доступом на основе ролей** → **Привилегии**.
5. Нажмите кнопку **Добавить**.
6. Укажите имя привилегии.
7. Нажмите **Добавить и изменить**.

Откроется страница **Привилегия: <Название>**.

8. Нажмите кнопку **Добавить**.

Откроется окно **Добавить привилегию '<Название>' в разрешения**.

9. В списке доступных разрешений выберите **System: Unlock User**.
10. Нажмите **>**.
11. Нажмите кнопку **Добавить**.
12. Нажмите **Управление доступом на основе ролей** → **Роли**.
13. Нажмите кнопку **Добавить**.
14. Укажите имя роли.
15. Нажмите **Добавить и изменить**.

Откроется страница **Роль: <Название>**.

16. Выберите вкладку **Привилегии**.

17. Нажмите кнопку **Добавить**.

Откроется окно **Добавить роль '<Название>' в привилегии**.

18. В списке доступных привилегий выберите привилегию, созданную ранее.
19. Нажмите **>**.
20. Нажмите кнопку **Добавить**.

Роль для блокировки учетной записи создана.

13.10.2. Создание учетной записи FreeIPA

► Чтобы создать учетную запись FreeIPA для реагирования:

1. В адресной строке браузера введите IP-адрес или доменное имя сервера.
2. Войдите в веб-интерфейс FreeIPA от имени учетной записи администратора.
3. В главном меню выберите **Идентификация**.
4. Нажмите **Пользователи** → **Активные пользователи**.
5. Нажмите кнопку **Добавить**.
6. Укажите логин и пароль учетной записи.
7. Укажите имя и фамилию пользователя.
8. Нажмите **Добавить и изменить**.

Откроется страница **Пользователь: <Название>**.

9. Выберите вкладку **Роли**.

10. Нажмите кнопку **Добавить**.

Откроется окно **Добавить пользователя '<Название>' в роли**.

11. В списке доступных ролей выберите роль, созданную ранее.
12. Нажмите ►.
13. Нажмите кнопку **Добавить**.

Учетная запись создана.

13.10.3. Настройка параметров модуля «Блокировка учетных записей в FreeIPA»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Блокировка учетных записей в FreeIPA».
4. В блоке параметров **agents_side_connections** нажмите **Изменить**.
5. Нажмите кнопку **Добавить**.
6. В поле **connection_name** укажите название соединения с агентской частью (используется для идентификации соединения в системных журналах).
7. В поле **doorkeeper_password** укажите пароль [учетной записи с правами на блокирование другой учетной записи](#) (см. раздел 13.10.2).

8. В поле **doorkeeper_username** укажите логин учетной записи.
 9. Если требуется, добавьте дополнительные учетные записи, от имени которых будет выполняться реагирование с помощью агентской части.
 10. Нажмите кнопку **Сохранить**.
 11. Если требуется, в блоке параметров **security_key** укажите ключ безопасности для выполнения действий, которые требуют дополнительного уровня доступа.
 12. В блоке параметров **server_side_connections** нажмите **Изменить**.
 13. Нажмите кнопку **Добавить**.
 14. В поле **connection_name** укажите название соединения с серверной частью (используется для идентификации соединения в системных журналах).
 15. В поле **connection_timeout_ms** укажите время ожидания ответа от сервера (в миллисекундах).
 16. В поле **doorkeeper_password** укажите пароль учетной записи для подключения по SSH, от имени которой будет выполняться реагирование (см. раздел 13.10.2).
 17. В поле **doorkeeper_username** укажите логин учетной записи для подключения по SSH, от имени которой будет выполняться реагирование.
 18. В поле **freeipa_address** укажите IP-адрес или FQDN сервера FreeIPA.
 19. В поле **freeipa_port** укажите порт сервера FreeIPA.
 20. Если требуется, добавьте дополнительные соединения в серверной части, с помощью которых будет выполняться реагирование.
 21. Нажмите кнопку **Сохранить**.
 22. Если требуется, в блоке параметров **trusted_usernames** нажмите **Добавить** и укажите логины учетных записей, которые не нужно блокировать при реагировании.
 23. Нажмите кнопку **Сохранить**.
- Модуль настроен.

13.10.4. Разблокирование учетной записи FreeIPA

Вы можете вручную разблокировать учетную запись FreeIPA, которую заблокировали ранее.

► Чтобы разблокировать учетную запись FreeIPA:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать учетную запись.
3. Выберите модуль «Блокировка учетных записей в FreeIPA».
4. Нажмите .

5. Выберите действие с параметрами **freeipa_blocker_unblock_user**.
6. Укажите логин учетной записи заблокированного пользователя.
7. Если при настройке модуля был задан ключ безопасности, укажите его в поле **security_key**.
8. Нажмите **Выполнить действие**.

Учетная запись пользователя разблокирована.

13.11. Блокировка учетных записей в Passwork

Модуль «Блокировка учетных записей в Passwork» блокирует и [разблокирует](#) (см. [раздел 13.11.3](#)) учетные записи в системе управления корпоративными паролями Passwork.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix.

Для настройки модуля необходимо:

1. Создать учетную запись БД Passwork для реагирования.
2. [Импортировать модуль](#) (см. [раздел 13.2](#)) в MaxPatrol EDR.
3. [Добавить модуль в политику](#) (см. [раздел 13.3](#)).
4. [Назначить политику на группу агентов](#) (см. [раздел 13.4](#)).
5. Настроить параметры модуля в политике.

В этом разделе

[Создание учетной записи в БД Passwork](#) (см. [раздел 13.11.1](#))

[Настройка параметров модуля «Блокировка учетных записей Passwork»](#) (см. [раздел 13.11.2](#))

[Разблокирование учетной записи Passwork](#) (см. [раздел 13.11.3](#))

13.11.1. Создание учетной записи в БД Passwork

► Чтобы создать учетную запись в базе данных Passwork:

1. Запустите MongoDB Shell от имени учетной записи администратора.
2. Перейдите в базу данных Passwork (по умолчанию — pwbox):

```
use <Название БД Passwork>
```
3. Создайте роль для реагирования:

```
db.createRole(
  {
    role: "<Название роли>",
    privileges: [
      {
```

```

        resource: {
            role: 'readWrite',
            db: '<Название БД Password>',
            collection: 'user'
        }, actions: ["find","update"]
    },
    roles: []
}
)

```

4. Перейдите в базу данных администратора:

```
use admin
```

5. Создайте учетную запись для реагирования:

```

db.createUser(
{user: '<Логин>',
  pwd: '<Пароль>',
  roles: [
    { role: '<Созданная роль>', db: '<Название БД Password>' }
  ]}
)

```

Учетная запись создана.

13.11.2. Настройка параметров модуля «Блокировка учетных записей Password»

- Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Блокировка учетных записей в Password».
4. В блоке параметров **database_name** нажмите **Изменить**.
5. В поле **database_name** укажите название базы данных Password (по умолчанию — **pwbox**).
6. Нажмите кнопку **Сохранить**.
7. В блоке параметров **doorkeeper** нажмите **Изменить**.
8. Укажите пароль и логин учетной записи, **от имени которой будет выполняться реагирование (см. раздел 13.11.1)**.
9. Нажмите кнопку **Сохранить**.
10. В поле **server_url** укажите адрес и порт сервера MongoDB (по умолчанию — **localhost:27017**).

11. Если требуется, в блоке параметров **trusted_usernames** нажмите **Добавить** и укажите логины учетных записей, которые не нужно блокировать при реагировании.
12. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.11.3. Разблокирование учетной записи Passwork

Вы можете вручную разблокировать учетную запись Passwork, которую заблокировали ранее.

► Чтобы разблокировать учетную запись Passwork:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать учетную запись.
3. Выберите модуль «Блокировка учетных записей в Passwork».
4. Нажмите .
5. Выберите действие с параметрами **pswb_unblock_user**.
6. Укажите логин учетной записи заблокированного пользователя.
7. Нажмите **Выполнить действие**.

Учетная запись пользователя разблокирована.

13.12. Блокировка учетных записей и отзыв токенов в GitLab

Модуль «Блокировка учетных записей и отзыв токенов в GitLab» блокирует учетные записи онлайн-сервиса GitLab и отзывает их токены доступа.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix или Windows.

Для настройки модуля необходимо:

1. Создать токен доступа для реагирования.
2. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
3. [Добавить модуль в политику \(см. раздел 13.3\)](#).
4. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
5. Настроить параметры модуля в политике.

В этом разделе

Создание токена доступа (см. раздел 13.12.1)

Настройка параметров модуля «Блокировка учетной записи GitLab и отзыв токена доступа» (см. раздел 13.12.2)

13.12.1. Создание токена доступа

Для блокировки учетных записей и удаления их токенов через API GitLab необходимо создать токен доступа для учетной записи администратора (подробнее см. на сайте docs.gitlab.com).

► Чтобы создать токен для реагирования:

1. Войдите в веб-интерфейс GitLab от имени учетной записи администратора.
2. Нажмите значок профиля и выберите **Edit Profile**.
Откроется страница с параметрами профиля.
3. В списке слева выберите пункт **Access Tokens**.
4. Нажмите **Add new token**.
5. В блоке параметров **Add a personal access token** укажите название токена.
6. В блоке параметров **Select scopes** установите флажок **api**.
7. Нажмите **Create personal access token**.

13.12.2. Настройка параметров модуля «Блокировка учетной записи GitLab и отзыв токена доступа»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Блокировка учетной записи GitLab и отзыв токена доступа».
4. В блоке параметров **token** нажмите **Изменить**.
5. В поле **token** укажите токен доступа [для реагирования \(см. раздел 13.12.1\)](#).
6. Нажмите кнопку **Сохранить**.
7. Если требуется, в блоке параметров **trusted_tokens** укажите названия доверенных токенов, которые не нужно отзывать при реагировании.
8. Если требуется, в блоке параметров **trusted_users** укажите логины учетных записей, у которых не нужно отзывать токены при реагировании.

9. В поле **url_gitlab** укажите URL-адрес API GitLab с версией (например, `https://gitlab.example.com/api/v4/`).

10. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.13. Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost

Модуль «Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost» блокирует учетные записи, завершает все сессии пользователей и отзывает их токены доступа в приложении для обмена мгновенными сообщениями Mattermost.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix или Windows.

Для настройки модуля необходимо:

1. Создать токен доступа для реагирования.
2. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
3. [Добавить модуль в политику \(см. раздел 13.3\)](#).
4. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
5. Настроить параметры модуля в политике.

В этом разделе

[Создание токена доступа \(см. раздел 13.13.1\)](#)

[Настройка параметров модуля «Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost» \(см. раздел 13.13.2\)](#)

[Разблокирование учетной записи Mattermost \(см. раздел 13.13.3\)](#)

13.13.1. Создание токена доступа

Токен необходим для блокировки учетных записей и удаления их токенов с помощью REST API.

Примечание. Инструкция разработана для Mattermost версии 9.10. При использовании других версий рекомендуется воспользоваться инструкциями на сайте mattermost.com.

► Чтобы создать токен для реагирования:

1. Войдите в веб-приложение Mattermost от имени учетной записи администратора.
2. Нажмите  → **Системная консоль**.
3. Выберите **Интеграции** → **Управление интеграцией**.

4. Включите возможность создания персональных токенов доступа.
5. Нажмите кнопку **Сохранить**.
6. Перезапустите веб-приложение и снова войдите от имени учетной записи администратора.
7. Нажмите значок профиля и выберите **Профиль**.
Откроется окно **Профиль**.
8. Выберите раздел **Безопасность**.
9. Выберите блок параметров **Персональные токены доступа** и нажмите **Создать токен**.
10. Укажите описание токена.
11. Нажмите кнопку **Сохранить**.
12. Нажмите **Да, создать**.

13.13.2. Настройка параметров модуля «Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost».
4. В блоке параметров **auth_token** нажмите **Изменить**.
5. В поле **auth_token** укажите [токен для реагирования \(см. раздел 13.13.1\)](#).
6. Нажмите кнопку **Сохранить**.
7. Если требуется, в блоке параметров **security_key** укажите ключ безопасности для выполнения действий, которые требуют дополнительного уровня доступа.
8. В поле **timeout_ms** укажите максимальное время ожидания ответа сервера Mattermost (в миллисекундах).
9. Если требуется, в блоке параметров **trusted_usernames** укажите учетные записи Mattermost, которые не нужно блокировать при реагировании, а также не нужно завершать их сессии и отзывать токены.

10. В поле **url_mattermost** укажите адрес и порт сервера Mattermost.

11. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.13.3. Разблокирование учетной записи Mattermost

Вы можете вручную разблокировать учетную запись Mattermost, которую заблокировали ранее.

► Чтобы разблокировать учетную запись Mattermost:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите разблокировать учетную запись.
3. Выберите модуль «Блокировка учетных записей, завершение сессий и отзыв токенов в Mattermost».
4. Нажмите .
5. Выберите действие с параметрами **mattermost_blocker_unblock_user**.
6. Если при настройке модуля был задан ключ безопасности, укажите его в поле **security_key**.
7. Укажите логин учетной записи заблокированного пользователя.
8. Нажмите **Выполнить действие**.

Учетная запись пользователя разблокирована.

13.14. Завершение SSH-сессий

Модуль «Завершение SSH-сессий» завершает активные SSH-сессии пользователей.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Настройка параметров модуля в политике не требуется, но вы можете указать список доверенных учетных записей, SSH-сессии которых не нужно завершать.

► Чтобы задать список доверенных учетных записей:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Завершение SSH-сессий».
4. В блоке параметров **trusted_usernames** нажмите **Изменить**.
5. Нажмите кнопку **Добавить**.
6. В поле **username 1** укажите логин учетной записи пользователя, SSH-сессии которого не требуется завершать.

Внимание! Логины учетных записей чувствительны к регистру.

7. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.15. Завершение VPN-сессий в Cisco ASA

Модуль «Завершение VPN-сессий в Cisco ASA» завершает VPN-сессии пользователей в Cisco ASA.

Модуль выполняет реагирование с помощью серверной части под управлением Unix. Агенты должны быть установлены на конечных устройствах под управлением Unix или Windows.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
4. Настроить параметры модуля в политике.

Настройка параметров модуля в политике

► Чтобы настроить параметры модуля в политике:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику, в которую добавлен модуль.
3. В списке **Включенные** выберите модуль «Завершение VPN-сессий в Cisco ASA».
4. В блоке параметров **cisco_asa_servers** нажмите **Изменить**.
5. Нажмите **Добавить**.
6. В поле **cisco_asa_ip** укажите IP-адрес сервера Cisco ASA.
7. В поле **cisco_asa_port** укажите порт сервера Cisco ASA.

8. Если требуется, в поле **connection_name** укажите название соединения с серверной частью модуля (используется для идентификации соединения в системных журналах).
9. Если требуется, в поле **connection_timeout_ms** укажите время ожидания ответа от сервера (в миллисекундах).
10. В полях **doorkeeper_username** и **doorkeeper_password** укажите логин и пароль учетной записи для подключения к Cisco ASA по SSH.

Внимание! Учетная запись должна иметь права администратора.

11. Если требуется, в поле **privileged_password** укажите пароль, который будет использоваться для повышения привилегий пользователя, от имени которого будет выполняться реагирование.

Примечание. В блоке параметров **trusted_usernames** вы можете нажать **Добавить** и указать логины пользователей, чьи сессии не будут завершаться при реагировании.

12. Нажмите **Сохранить**.

13.16. Завершение сессий в OpenVPN

Модуль «Завершение сессий в OpenVPN» завершает VPN-сессии пользователей частной виртуальной сети OpenVPN (без блокирования учетных записей). Модуль может выполнять реагирование одновременно на нескольких серверах OpenVPN. При наличии нескольких экземпляров OpenVPN на одном сервере реагирование выполняется отдельно для каждого экземпляра.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix.

Для настройки модуля необходимо:

1. Установить сервер OpenVPN.
2. Выполнить настройку OpenVPN.
3. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
4. [Добавить модуль в политику \(см. раздел 13.3\)](#).
5. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
6. Настроить параметры модуля в политике.

В этом разделе

[Предварительная настройка OpenVPN \(см. раздел 13.16.1\)](#)

[Настройка параметров модуля «Завершение сессий в OpenVPN» \(см. раздел 13.16.2\)](#)

[Проверка работоспособности модуля «Завершение сессий в OpenVPN» \(см. раздел 13.16.3\)](#)

13.16.1. Предварительная настройка OpenVPN

Перед началом работы с модулем «Завершение сессий в OpenVPN» необходимо выполнить настройку OpenVPN.

Настройка экземпляров OpenVPN

Для настройки экземпляров OpenVPN необходимо выполнить следующее:

1. Обеспечить подключение клиентов к экземплярам OpenVPN по разным портам. Подробные инструкции по настройке экземпляров OpenVPN приведены на сайте openvpn.net.

Примечание. Если номера портов совпадают, но протоколы различаются (UDP и TCP), то порты считаются разными.

2. Для каждого экземпляра OpenVPN указать разные диапазоны IP-адресов, к которым должны подключаться клиенты. Диапазоны IP-адресов нужно добавить в строку `server` в конфигурационном файле, расположенном в каталоге `/etc/openvpn/server`.
3. Включить журналирование активных сессий пользователей. Для этого в конфигурационные файлы экземпляров нужно добавить строку `status /var/log/openvpn/openvpn-status.log`.
4. Включить Management Interface на каждом экземпляре сервера.

Примечание. Вы можете проверить количество экземпляров OpenVPN с помощью команды `ip a`. Команда выводит информацию об интерфейсах виртуальных туннелей. Количество интерфейсов соответствует количеству экземпляров OpenVPN, запущенных на сервере (например, параметры `tun0` и `tun1` указывают на то, что на сервере запущены два экземпляра).

Настройка Management Interface

Завершение сессии пользователя на стороне сервера выполняется с помощью компонента Management Interface. Для обмена данными между компонентами необходимо установить пакет `socat` и включить TCP- или Unix-сокеты (подробности см. на сайте openvpn.net).

Пример конфигурации с сокетом Unix:

```
management /var/run/openvpn-management.socket 'unix'
```

Для ограничения доступа к интерфейсу при использовании Unix-сокета необходимо разрешить подключение от имени определенного пользователя (`username/uid`) и группы (`groupname/gid`). Пример команды на разрешение взаимодействия с интерфейсом только для суперпользователя (`root`):

```
--management-client-user root
--management-client-group root
```

В конфигурации TCP-сокета необходимо использовать адрес виртуального сетевого интерфейса `loopback` и пароль. Пароль необходимо сохранить в текстовом файле, а путь к нему указать в качестве третьего аргумента опции `management`. Пример конфигурации TCP-сокета с паролем:

```
management localhost 7506 /etc/openvpn/server/password
```

При использовании внешнего способа аутентификации (например, Radius, LDAP, PAM) необходимо включить функцию, которая позволит серверу использовать имя пользователя (`UserName`) вместо общего имени для центра сертификации (`CommonName`):

```
--username-as-common-name
```

Завершение соединений с Management Interface

OpenVPN поддерживает только одно активное подключение к Management Interface, поэтому для корректной работы модуля указанный в конфигурации порт Management Interface не должен быть занят другими процессами. Вы можете проверить наличие соединений с Management Interface по команде `sudo lsof -i: <Порт>`. Если соединения обнаружены, необходимо завершить их по команде `sudo kill <PID процесса>`.

Блокировка учетной записи локально

Для того чтобы пользователь не смог снова подключиться к серверу после завершения его сессии, нужно заблокировать его учетную запись локально.

► Чтобы заблокировать учетную запись OpenVPN локально:

1. На сервере OpenVPN создайте каталог `ccd`.
2. В каталоге `ccd` создайте текстовый файл, в качестве его названия укажите имя пользователя (`CommonName`), которого нужно заблокировать.
3. Откройте файл и добавьте строку `disable`.
4. В конфигурационные файлы всех экземпляров OpenVPN добавьте строку:
`client-config-dir <Путь к каталогу ccd>`

Разблокирование учетной записи локально

Вы можете разблокировать учетную запись OpenVPN, которую заблокировали ранее.

► Чтобы разблокировать учетную запись OpenVPN локально:

1. На сервере OpenVPN откройте каталог `ccd`.
2. Откройте текстовый файл с именем пользователя (`CommonName`), которого нужно разблокировать.
3. Закомментируйте строку `disable`.

13.16.2. Настройка параметров модуля «Завершение сессий в OpenVPN»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику, в которую добавлен модуль.
3. В списке **Включенные** выберите модуль «Завершение сессий в OpenVPN».
4. В блоке параметров **Конфигурация нескольких шлюзов OpenVPN** нажмите **Изменить**.
5. В блоке параметров **OpenVPN шлюзы** нажмите **Добавить**.
6. В поле **agentId** укажите идентификатор агента в MaxPatrol EDR.
7. Если требуется, в поле **fqdn** укажите полное доменное имя узла.
8. В блоке параметров **ips** укажите IP-адреса узлов OpenVPN.
9. В блоке параметров **OpenVPN экземпляры 1** в поле **password** укажите пароль для входа в экземпляр OpenVPN.
10. В поле **port** укажите номер порта, на котором расположен экземпляр OpenVPN.
11. Если вы используете несколько экземпляров OpenVPN, добавьте для каждого порт и пароль с помощью кнопки **Добавить**.
12. Если требуется, настройте другие шлюзы OpenVPN.
13. Нажмите **Сохранить**.

13.16.3. Проверка работоспособности модуля «Завершение сессий в OpenVPN»

После настройки модуля вы можете вручную проверить его работоспособность, чтобы убедиться, что параметры указаны верно.

► Чтобы проверить работоспособность модуля:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите проверить работоспособность модуля.
3. Выберите модуль «Завершение сессий в OpenVPN».
4. Нажмите .
5. Выберите действие с параметрами **openvpn_terminator_healthcheck**.
6. Укажите FQDN сервера OpenVPN.

Пример:

```
{"fqdn": "openvpn.com"}
```

- Укажите IP-адреса сервера OpenVPN.

Пример:

```
{"ip_addresses": ["192.0.2.255"]}
```

- Нажмите **Выполнить действие**.

MaxPatrol O2 отправит запрос с параметрами модуля на конечное устройство.

13.17. Завершение сессий в Windows

Модуль «Завершение сессий в Windows» завершает сессии пользователей Microsoft Windows.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением Windows.

Для настройки модуля необходимо:

- [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
- [Добавить модуль в политику \(см. раздел 13.3\)](#).
- [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Настройка параметров модуля в политике не требуется, но вы можете указать список идентификаторов сессий, которые не нужно завершать при реагировании.

► Чтобы задать список доверенных идентификаторов сессий:

- В главном меню выберите **EDR** → **Политики**.
- Выберите политику.
- В списке **Включенные** выберите модуль «Завершение сессий в Windows».
- В блоке параметров **trusted_login_ids** нажмите **Изменить**.
- Нажмите кнопку **Добавить**.
- В поле **login_id 1** укажите идентификатор сессии, которую не нужно завершать.

Примечание. Системная сессия с идентификатором 999 не может быть завершена по умолчанию.

- Нажмите кнопку **Сохранить**.

Модуль настроен.

13.18. Завершение сессий и блокировка учетных записей в VMware vSphere

Модуль «Завершение сессий и блокировка учетных записей в VMware vSphere» завершает сессии и блокирует учетные записи пользователей платформы виртуализации VMware vSphere. Модуль поддерживает работу одновременно на нескольких серверах vSphere (vCenter).

Модуль выполняет реагирование с помощью серверной части под управлением Unix. Агенты должны быть установлены на конечных устройствах под управлением Unix или Windows.

Для настройки модуля необходимо:

1. Создать и настроить учетную запись vCenter Server для реагирования.
2. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
3. [Добавить модуль в политику \(см. раздел 13.3\)](#).
4. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
5. Настроить параметры модуля в политике.

В этом разделе

[Создание и настройка учетной записи vCenter Server \(см. раздел 13.18.1\)](#)

[Настройка параметров модуля «Завершение сессий и блокировка учетных записей в VMware vSphere» \(см. раздел 13.18.2\)](#)

13.18.1. Создание и настройка учетной записи vCenter Server

Инструкция разработана для VMware vSphere версии 7.0. При использовании других версий рекомендуется воспользоваться [инструкциями вендора](#).

► Чтобы создать учетную запись vCenter Server:

1. В адресной строке браузера введите IP-адрес или доменное имя сервера.
Откроется страница **VM vSphere Client**.
2. Войдите под именем учетной записи администратора.
3. Выберите раздел **Administration**.
4. В иерархическом списке выберите **Single Sign On** → **Users and Groups**.
5. На вкладке **Users** в раскрывающемся списке **Domain** выберите SSO-домен VMware vCenter.
6. Нажмите **Add User**.

7. В поле **Username** введите логин учетной записи.
8. В поле **Password** введите пароль учетной записи и подтвердите его в поле **Confirm Password**.

Внимание! Логин и пароль учетной записи не должны содержать символы &, ;, ", ', ^, \, %, < и >.

9. Нажмите **ADD**.
10. В иерархическом списке выберите **Access Control** → **Global Permissions**.
11. Нажмите + (**Add Permission**).
12. В раскрывающемся списке **Domain** выберите SSO-домен VMware vCenter.
13. В поле **User/Group** укажите созданную учетную запись.
14. В раскрывающемся списке **Role** выберите **Administrator**.
15. Установите флажок **Propagate to children**.
16. Нажмите кнопку **OK**.

13.18.2. Настройка параметров модуля «Завершение сессий и блокировка учетных записей в VMware vSphere»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Завершение сессий и блокировка учетных записей в VMware vSphere».
4. В блоке параметров **vcenter_servers** нажмите **Изменить**.
5. Нажмите кнопку **Добавить**.
6. В блоке параметров **connection_info 1** в поле **doorkeeper_password** укажите пароль учетной записи администратора vCenter Server, [созданной ранее \(см. раздел 13.18.1\)](#).
7. В поле **doorkeeper_username** укажите логин учетной записи.
8. Если требуется, в поле **no_access_role_id** укажите идентификатор роли, которая будет присваиваться заблокированной учетной записи.
9. Если требуется, в поле **no_access_role_name** укажите название роли, которая будет присваиваться заблокированной учетной записи (по умолчанию — NoAccess).

Примечание. Если в системную роль NoAccess необходимо внести изменения, следует создать новую роль с такими же свойствами и указать ее идентификатор в поле **no_access_role_id** или название в **no_access_role_name**.

10. Если требуется, включите проверку SSL-сертификата при запросе на сервер.
 11. В поле **timeout_ms** укажите максимальное время ожидания ответа сервера vSphere (в миллисекундах).
 12. Если требуется, в блоке параметров **trusted_usernames** нажмите **Добавить** и укажите логины учетных записей, которые не нужно блокировать при реагировании.
 13. Если требуется, в поле **vcenter_fqdn** укажите FQDN сервера vCenter.
 14. Если требуется, в блоке параметров **vcenter_ips** укажите IP-адреса сервера vCenter.
- Внимание!** Для корректной работы модуля необходимо указать значение хотя бы одного параметра: **vcenter_fqdn** или **vcenter_ips**.
15. Если требуется, добавьте параметры других серверов vCenter.
 16. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.19. Отзыв сертификатов AD CS

Модуль «Отзыв сертификатов AD CS» отзывает сертификаты, выпущенные центром сертификации Active Directory.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением Windows.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Настройка параметров модуля в политике не требуется. Вы можете указать [список сертификатов \(см. раздел 13.19.1\)](#), которые не нужно отзывать.

В этом разделе

[Создание списка доверенных сертификатов AD CS \(см. раздел 13.19.1\)](#)

[Возврат сертификата AD CS \(см. раздел 13.19.2\)](#)

13.19.1. Создание списка доверенных сертификатов AD CS

► Чтобы создать список:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику, в которую добавлен модуль.

3. В списке **Включенные** выберите модуль «Отзыв сертификатов AD CS».
4. В блоке параметров **trusted_certificates** нажмите **Изменить**.
5. Нажмите **Добавить**.
6. В поле **trusted_certificates** укажите серийные номера сертификатов, которые не требуется отзывать.
7. Нажмите **Сохранить**.

13.19.2. Возврат сертификата AD CS

Вы можете вручную вернуть сертификат AD CS, который отозвали ранее.

► Чтобы вернуть сертификат:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите вернуть сертификат.
3. Выберите модуль «Отзыв сертификатов AD CS».
4. Нажмите .
5. Выберите действие с параметрами **ad_cs_certificate_revoker_unrevoke_certificate**.
6. Укажите серийный номер сертификата.
7. Нажмите **Выполнить действие**.

13.20. Отзыв токенов в Artifactory

Модуль «Отзыв токенов в Artifactory» отзывает токены пользователей системы хранения артефактов JFrog Artifactory.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix или Windows.

Для настройки модуля необходимо:

1. Создать токен доступа для реагирования.
2. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
3. [Добавить модуль в политику \(см. раздел 13.3\)](#).
4. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
5. Настроить параметры модуля в политике.

В этом разделе

Создание токена доступа (см. раздел 13.20.1)

Настройка параметров модуля «Отзыв токенов в Artifactory» (см. раздел 13.20.2)

13.20.1. Создание токена доступа

Токен необходим для отзыва токенов других пользователей с помощью REST API (подробнее см. на сайте jfrog.com).

► Чтобы создать токен для реагирования:

1. Войдите в веб-интерфейс Artifactory от имени учетной записи администратора.
2. Нажмите .
3. В разделе **Identity and Access** выберите пункт **Access Tokens**.
4. Нажмите **Generate Token**.
5. Выберите токен с ограничениями (**Scoped Token**).
6. В раскрывающемся списке **Token scope** выберите **Admin**.
7. В поле **User name** укажите имя пользователя.
8. Рядом с полем **Service** установите флажок **All**.
9. В раскрывающемся списке **Expiration time** выберите **Never**.
10. Нажмите **Generate**.
11. Нажмите **Copy**.

13.20.2. Настройка параметров модуля «Отзыв токенов в Artifactory»

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Отзыв токенов в Artifactory».
4. В блоке параметров **token** нажмите **Изменить**.
5. В поле **token** укажите [токен доступа для выполнения реагирования](#) (см. раздел 13.20.1).
6. Нажмите кнопку **Сохранить**.
7. Если требуется, в блоке параметров **trusted_users** укажите учетные записи, у которых не нужно отзывать токены при реагировании.

8. В поле **url_artifactory** укажите URL-адрес Artifactory (по умолчанию — `https://localhost`).

9. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.21. Перенаправление DNS-запросов в Active Directory (sinkholing)

Модуль «Перенаправление DNS-запросов в Active Directory (sinkholing)» перенаправляет трафик с подозрительных доменов на заданный немаршрутизируемый IP-адрес.

Внимание! Модуль выполняет реагирование на агентах, которые установлены на конечных устройствах под управлением операционной системы Windows Server со службой каталогов Active Directory.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Примечание. Настройка параметров модуля в политике не требуется.

13.22. Снятие групповой политики с подразделения

Модуль «Снятие групповой политики с подразделения» отвязывает групповую политику (GPO) от подразделения Active Directory (OU) и восстанавливает связь между ними.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением Windows.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Настройка параметров модуля в политике не требуется, но вы можете указать ключ безопасности для восстановления связи групповой политики с подразделением в параметре **security_key** в карточке модуля.

После снятия групповой политики с подразделения вы можете вручную восстановить связь между ними.

► Чтобы восстановить связь между групповой политикой и подразделением:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите восстановить связь между групповой политикой и подразделением.
3. Выберите модуль «Снятие групповой политики с подразделения».
4. Нажмите .
5. Выберите действие с параметрами **gpo_link_disabler_enable_link**.
6. Укажите идентификатор групповой политики, связь с которой необходимо восстановить.
7. Если при настройке модуля был задан ключ безопасности, укажите его в поле **security_key**.
8. Нажмите **Выполнить действие**.

13.23. Удаление запланированных задач в Windows

Модуль «Удаление запланированных задач в Windows» удаляет задачи из планировщика заданий Microsoft Windows.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением Windows.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Примечание. Настройка параметров модуля в политике не требуется.

13.24. Удаление писем в Microsoft Exchange

Модуль «Удаление писем в Microsoft Exchange» удаляет потенциально опасные письма на почтовом сервере Microsoft Exchange, а также [отзывает и возвращает токены доступа пользователей \(см. раздел 13.24.6\)](#).

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением Windows с установленным сервером Microsoft Exchange.

Для настройки модуля необходимо:

1. Создать доменную учетную запись Active Directory для реагирования.
2. Создать группу ролей с правами на поиск, перемещение и удаление содержимого из почтовых ящиков пользователей и добавить в нее доменную учетную запись.

3. Создать почтовый ящик карантина для перемещения копий удаленных писем.
4. Создать папку в почтовом ящике карантина для хранения копий удаленных писем.
5. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
6. [Добавить модуль в политику \(см. раздел 13.3\)](#).
7. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).
8. Настроить параметры модуля в политике.

В этом разделе

[Создание доменной учетной записи \(см. раздел 13.24.1\)](#)

[Создание группы ролей для поиска и удаления содержимого почтовых ящиков \(см. раздел 13.24.2\)](#)

[Создание почтового ящика для карантина \(см. раздел 13.24.3\)](#)

[Создание папки в почтовом ящике \(см. раздел 13.24.4\)](#)

[Настройка параметров модуля «Удаление писем в Microsoft Exchange» \(см. раздел 13.24.5\)](#)

[Отзыв или возврат токена доступа \(см. раздел 13.24.6\)](#)

[Удаление писем \(см. раздел 13.24.7\)](#)

13.24.1. Создание доменной учетной записи

► Чтобы создать доменную учетную запись:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.
3. В панели слева выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.
4. В главном меню выберите **Действие** → **Создать** → **Пользователь**.
5. Введите имя пользователя.
6. В поле **Имя входа пользователя** введите логин учетной записи.
7. Нажмите **Далее**.
8. Введите пароль учетной записи и подтвердите его.
9. Снимите флажок **Требовать смены пароля при следующем входе в систему**.
10. Установите флажок **Срок действия пароля не ограничен**.
11. Нажмите **Далее**.
12. Нажмите **Готово**.

13.24.2. Создание группы ролей для поиска и удаления содержимого почтовых ящиков

► Чтобы создать группу ролей для поиска и удаления писем:

1. Запустите Exchange Management Shell от имени учетной записи администратора.
2. Выполните команду:

```
New-RoleGroup -Name "<Название группы ролей>" -Roles "Mailbox Search", "Mailbox Import Export" -Members <Доменная учетная запись>
```

13.24.3. Создание почтового ящика для карантина

После удаления потенциально опасных писем с сервера Exchange их копии сохраняются для дальнейшего анализа. Для хранения таких копий необходимо создать почтовый ящик для карантина.

► Чтобы создать почтовый ящик для карантина:

1. Запустите консоль администрирования Exchange (EAC).
2. Выберите раздел **Почтовые ящики получателей**.
3. Нажмите **Создать** → **Почтовый ящик пользователя**.
4. В поле **Псевдоним** укажите псевдоним пользователя, который будет отображаться в адресе электронной почты до символа @.
5. В поле **Существующий пользователь** нажмите **Обзор** и выберите учетную запись.
6. Нажмите кнопку **Сохранить**.

13.24.4. Создание папки в почтовом ящике

► Чтобы создать папку в почтовом ящике для карантина:

1. Запустите Exchange Management Shell от имени доменной учетной записи, созданной ранее.
2. Выполните команду:

```
New-MailboxFolder -Parent :\ -Name <Название папки>
```

13.24.5. Настройка параметров модуля «Удаление писем в Microsoft Exchange»

Модуль «Удаление писем в Microsoft Exchange» выполняет реагирование с помощью агента.

► Чтобы настроить параметры модуля:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику.
Откроется карточка политики.
3. В списке **Включенные** выберите модуль «Удаление писем в Microsoft Exchange».
4. В блоке параметров **Пароль администратора Exchange-сервера** нажмите **Изменить**.
5. Укажите пароль учетной записи администратора сервера Microsoft Exchange.
6. Нажмите кнопку **Сохранить**.
7. В блоке параметров **Логин администратора Exchange-сервера** нажмите **Изменить**.
8. Укажите логин учетной записи.
9. Нажмите кнопку **Сохранить**.
10. В блоке параметров **Папка карантина** нажмите **Изменить**.
11. Укажите имя [папки для хранения удаленных писем \(см. раздел 13.24.4\)](#).
12. Нажмите кнопку **Сохранить**.
13. В блоке параметров **Почтовый ящик карантина** нажмите **Изменить**.
14. Укажите название [почтового ящика для хранения удаленных писем \(см. раздел 13.24.3\)](#).
15. Нажмите кнопку **Сохранить**.

Модуль настроен.

13.24.6. Отзыв или возврат токена доступа

Вы можете вручную отозвать токен доступа пользователя Microsoft Exchange или вернуть токен, который отзывали ранее. Действия модуля могут отозвать или вернуть токены OWA, IMAP, POP, EWS и ECP.

► Чтобы отозвать или вернуть токен доступа:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите отозвать или вернуть токен доступа.
3. Выберите модуль «Удаление писем в Microsoft Exchange».
4. Нажмите .
5. В блоке параметров **Действие с параметрами** выполните одно из следующих действий:
 - Если вы хотите отозвать токен, выберите **disable_owa_imap_pop_ews_ecp**.

- Если вы хотите вернуть токен, который был отозван ранее, выберите **enable_owa_imap_pop_ews_escr**.
6. Укажите учетную запись.
 7. Нажмите **Выполнить действие**.

13.24.7. Удаление писем

Вы можете вручную удалять письма с сервера Microsoft Exchange с определенными параметрами.

► Чтобы удалить письма:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, на котором установлен сервер Microsoft Exchange.
3. Выберите модуль «Удаление писем в Microsoft Exchange».
4. Нажмите .
5. Выберите действие с параметрами **delete_mails**.
6. Укажите фильтр для удаления писем с сервера со следующими параметрами:
 - **from** — SMTP-адрес, имя (Display Name) или псевдоним (Alias) отправителя писем, которые необходимо удалить;
 - **to** — SMTP-адрес, имя (Display Name) или псевдоним (Alias) получателя писем;
 - **subject** — тема письма (не может содержать спецсимволы).

Пример:

```
{"from":"Petr Petrov","subject":"Send passwords urgently","to":"Ivan Ivanov"}
```

7. Нажмите **Выполнить действие**.

13.25. Удаление служб в Windows (блокировка в Linux)

Модуль «Удаление служб в Windows (блокировка в Linux)» удаляет системные службы в Windows и блокирует в Linux.

Модуль выполняет реагирование с помощью агентской части. Агенты должны быть установлены на конечных устройствах под управлением ОС семейства Unix или Windows.

Для настройки модуля необходимо:

1. [Импортировать модуль \(см. раздел 13.2\)](#) в MaxPatrol EDR.
2. [Добавить модуль в политику \(см. раздел 13.3\)](#).
3. [Назначить политику на группу агентов \(см. раздел 13.4\)](#).

Настройка параметров модуля в политике не требуется. Вы можете составить список служб, которые не нужно блокировать (удалять).

Создание списка доверенных служб

► Чтобы создать список:

1. В главном меню выберите **EDR** → **Политики**.
2. Выберите политику, в которую добавлен модуль.
3. В списке **Включенные** выберите модуль «Удаление служб в Windows (блокировка в Linux)».
4. Если требуется создать список доверенных служб в Linux, выполните следующие действия:
 - В блоке параметров **trusted_services_linux** нажмите **Изменить**.
 - Нажмите **Добавить**.
 - Укажите название службы, которую не требуется блокировать.
5. Если требуется создать список доверенных служб в Windows, выполните следующие действия:
 - В блоке параметров **trusted_services_windows** нажмите **Изменить**.
 - Нажмите **Добавить**.
 - Укажите название службы, которую не требуется блокировать.
6. Нажмите **Сохранить**.

13.26. Проверка работоспособности модуля

После настройки модуля вы можете вручную проверить его работоспособность, чтобы убедиться, что параметры указаны верно.

Внимание! Инструкция разработана для всех модулей реагирования, кроме [модуля «Завершение сессий в OpenVPN»](#) (см. [раздел 13.16.3](#)).

► Чтобы проверить работоспособность модуля:

1. В главном меню выберите **EDR** → **Агенты**.
2. Выберите агент, в ОС которого вы хотите проверить работоспособность модуля.
3. Выберите модуль.
4. Нажмите .
5. Выберите быстрое действие **<Название модуля>_healthcheck**.

MaxPatrol O2 отправит запрос с параметрами модуля на конечное устройство.

14. Диагностика и решение проблем

В этом разделе приводятся инструкции по диагностике и решению проблем, возникающих при работе с MaxPatrol O2.

В этом разделе

[Ошибка входа в MaxPatrol O2 после авторизации в PT MC \(см. раздел 14.1\)](#)

[Служба Chains останавливается через некоторое время после запуска \(см. раздел 14.2\)](#)

[Ошибка регистрации MaxPatrol O2 в PT MC \(см. раздел 14.3\)](#)

[MaxPatrol O2 не получает события из MaxPatrol 10 после обновления LogSpace \(см. раздел 14.4\)](#)

[Подсеть Docker-контейнера MaxPatrol O2 совпадает с одной из подсетей организации \(см. раздел 14.5\)](#)

14.1. Ошибка входа в MaxPatrol O2 после авторизации в PT MC

После авторизации в PT MC при попытке входа в MaxPatrol O2 возникает ошибка. В журнале службы BFF отображается информация о том, что веб-токен JSON еще не активен.

Возможные причины

Время на серверах MaxPatrol O2 и PT MC не синхронизировано.

Решение

Для решения проблемы потребуется настроить синхронизацию системного времени на каждом сервере, где развернуты MaxPatrol O2 и PT MC, с NTP-серверами.

► Чтобы настроить синхронизацию системного времени сервера с NTP-серверами:

1. Обновите список пакетов:
`apt update`
2. Установите пакет NTP:
`apt install ntp`
3. Откройте файл `/etc/ntp.conf`:
`sudo nano /etc/ntp.conf`
4. Добавьте в файл строки:
`echo "<FQDN или IP-адрес NTP-сервера, который будет использоваться по умолчанию> prefer"`
`>> /etc/ntp.conf`
`echo "<FQDN или IP-адрес NTP-сервера>" >> /etc/ntp.conf`

5. Сохраните изменения и закройте файл.

6. Перезапустите службу NTP:

```
systemctl restart ntp
```

Вы можете проверить корректность настройки с помощью команды `ntpq -p`. В выводе команды отобразятся IP-адреса NTP-серверов и информация об их работе.

14.2. Служба Chains останавливается через некоторое время после запуска

После остановки службы Chains в журнале отображается информация о недостаточном объеме общей памяти и подсказка о необходимости увеличить значение параметра `max_pred_locks_per_transaction`.

Возможные причины

Количество объектов в базе данных, которые должны быть заблокированы в рамках одной транзакции, превышает значение параметра `max_pred_locks_per_transaction`, заданное в конфигурации роли `SqlStorage`.

Решение

Необходимо сменить значение параметра `max_pred_locks_per_transaction` на 512.

► Чтобы изменить значение параметра `max_pred_locks_per_transaction`:

1. Скопируйте конфигурационный файл `postgresql.conf.template` из Docker-контейнера `storage-postgres` в каталог `etc/postgresql`:

```
docker cp $(docker ps -q -f name= storage-postgres):/etc/postgresql/postgresql.conf.template ./
```

2. Откройте файл `postgresql.conf.template`:

```
sudo nano /etc/postgresql/postgresql.conf.template ./
```

3. Раскомментируйте параметр `max_pred_locks_per_transaction` и в качестве его значения укажите 512.

4. Сохраните файл `postgresql.conf.template`.

5. Скопируйте файл `postgresql.conf.template` в контейнер `storage-postgres`:

```
docker cp ./postgresql.conf.template $(docker ps -q -f name=storage-postgres):/etc/postgresql/postgresql.conf.template
```

6. Перезапустите контейнер:

```
docker restart $(docker ps -q -f name=storage-postgres)
```

При пересоздании контейнера значение параметра `max_pred_locks_per_transaction` заменится на значение по умолчанию (64). Для того чтобы заданное вами значение сохранилось, вы можете создать Docker-образ контейнера и пересоздать контейнер из этого образа.

► Чтобы создать образ контейнера `storage-postgres`:

1. Выведите в консоли содержимое файла с переменными окружения контейнера:
`cat /var/lib/deployed-roles/mc-application/sqlstorage/images/storage-postgres/.env`
2. В выводе команды скопируйте значение переменной `REGISTRY`.
3. Создайте образ контейнера:
`docker commit $(docker ps -q -f name=storage-postgres) <Значение переменной REGISTRY>/storage-postgres:2.3.2_custom`

► Чтобы пересоздать контейнер из образа:

1. Укажите имя образа в файле `docker-compose.yaml`:
`sed -i 's/storage-postgres:2.3.2/storage-postgres:2.3.2_custom/g' /var/lib/deployed-roles/mc-application/sqlstorage/images/storage-postgres/docker-compose.yaml`
2. Пересоздайте контейнер:
`docker compose -f /var/lib/deployed-roles/mc-application/sqlstorage/images/storage-postgres/docker-compose.yaml up -d`

14.3. Ошибка регистрации MaxPatrol O2 в PT MC

Не удастся войти в MaxPatrol O2. В журнале службы Registration отображается сообщение о том, что приложение еще не зарегистрировано.

Возможные причины

Значение параметра `ClientId` в конфигурации экземпляра MaxPatrol O2 совпадает со значением `ClientId` в конфигурации другого экземпляра MaxPatrol O2, зарегистрированного в PT MC.

Решение

Значение параметра `ClientId` должно быть уникальным для каждого экземпляра MaxPatrol O2, зарегистрированного в PT MC.

Для решения проблемы необходимо [изменить конфигурации \(см. раздел 12.2.2\)](#) ролей Resources, Modelling, O2 Base, Web, XdrAdapter и AdapterMP10Siem, указав в расширенных параметрах установки новое значение `ClientId`.

Необходимо также изменить значения следующих параметров:

- для ролей Resources, Modelling, O2 Base и XdrAdapter — `ClientScope: idmgr.api <Значение ClientId>.api`;
- для роли AdapterMP10Siem — `ClientScope: idmgr.api <Значение ClientId>.api mpx.api`;
- для роли Web — `0idcScope: openid profile email offline_access <Значение ClientId>.access.allow idmgr.api mpx.api <Значение ClientId>.api`.

14.4. MaxPatrol O2 не получает события из MaxPatrol 10 после обновления LogSpace

MaxPatrol O2 прекращает получать данные о событиях из MaxPatrol 10 после обновления хранилища событий LogSpace.

Возможные причины

При обновлении LogSpace в базе данных из таблицы `siem.cp` были не полностью удалены данные.

Решение

Для решения проблемы необходимо пересоздать таблицу `siem.cp`.

- Чтобы пересоздать таблицу `siem.cp`,

на сервере MaxPatrol 10 с установленной ролью Event Storage выполните команды:

```
systemctl stop siemserver-storage.service
logspace-client --query 'truncate table siem.cp'
logspace-client --query 'drop table siem.cp'
systemctl start siemserver-storage.service
```

14.5. Подсеть Docker-контейнера MaxPatrol O2 совпадает с одной из подсетей организации

Решение

Необходимо изменить подсеть Docker-контейнера MaxPatrol O2.

► Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol O2 остановите Docker-контейнеры:
`docker stop $(docker ps -qa)`
2. На всех серверах с установленным MaxPatrol O2 удалите Docker-контейнеры:
`docker rm $(docker ps -qa)`
3. На всех серверах с установленным MaxPatrol O2 удалите действующие параметры сети Docker:
`docker network prune`
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz`:
`tar -xf pt_deployer_<Номер версии>.tar.gz`
5. Запустите сценарий:
`pt_deployer_<Номер версии>/install.sh`
6. Нажмите **Yes**.
7. Выберите идентификатор приложения роли.
8. Выберите идентификатор экземпляра роли.
9. Выберите **Advanced configuration**.
10. В качестве значения параметра `CustomDockerAddressPool` укажите подсеть для Docker-контейнеров MaxPatrol O2, отличную от подсетей, используемых в вашей организации.

Внимание! Значение параметра должно относиться к одной из поддерживаемых частных подсетей: 10.0.0.0/8, 172.16.0.0/12 или 192.168.0.0/16.
11. В качестве значения параметра `CustomDockerNetworkSize` введите размер подсетей, которые будут выделяться из диапазона, указанного в параметре `CustomDockerAddressPool`.

Примечание. Рекомендуется использовать значение, не превышающее 25 бит.
12. Нажмите **OK**.
13. Нажмите **Submit**.
14. Нажмите **OK**.
15. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
16. На сервере с установленной ролью Deployer запустите обновление конфигурации установленных компонентов MaxPatrol O2.
`/opt/deployer/bin/Restart-Configuration.ps1 '*' -Verbose`

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

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

Изменение подсети Docker-контейнера при обновлении MaxPatrol O2

► Чтобы изменить подсеть Docker-контейнера при обновлении ролей MaxPatrol O2:

1. На всех серверах с установленным MaxPatrol O2 остановите Docker-контейнеры:
`docker stop $(docker ps -qa)`
2. На всех серверах с установленным MaxPatrol O2 удалите Docker-контейнеры:
`docker rm $(docker ps -qa)`
3. На всех серверах с установленным MaxPatrol O2 удалите действующие параметры сети Docker:
`docker network prune`
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz` с новой версией роли:
`tar -xf pt_deployer_<Номер версии>.tar.gz`
5. Запустите сценарий:
`pt_deployer_<Номер версии>/install.sh`
6. Нажмите **Yes**.
7. Выберите **Advanced configuration**.
8. В качестве значения параметра `CustomDockerAddressPool` укажите подсеть для Docker-контейнеров MaxPatrol O2, отличную от подсетей, используемых в вашей организации.

Внимание! Значение параметра должно относиться к одной из поддерживаемых частных подсетей: 10.0.0.0/8, 172.16.0.0/12 или 192.168.0.0/16.
9. В качестве значения параметра `CustomDockerNetworkSize` введите размер подсетей, которые будут выделяться из диапазона, указанного в параметре `CustomDockerAddressPool`.

Примечание. Рекомендуется использовать значение, не превышающее 25 бит.
10. Нажмите **OK**.
11. По завершении установки пакетов нажмите **OK**.
12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
13. Обновите остальные роли.

15. Техническая поддержка

Базовая техническая поддержка продуктов включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продуктов

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies предоставляет обновленные версии продуктов в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продуктов.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продуктов в рамках выпуска обновленных версий продукта

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по технической поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 16. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение А. PDQL-запросы данных об активах

Для добавления информации о недопустимых событиях (см. раздел 9.1) в MaxPatrol O2 вы можете использовать данные, полученные из табличных списков MaxPatrol 10. В этом разделе приводятся PDQL-запросы, с помощью которых можно отфильтровать информацию об активах для наполнения табличных списков.

В этом разделе

Активы с операционной системой Windows (см. раздел A.1)

Активы службы каталогов Active Directory (см. раздел A.2)

Активы с операционной системой семейства Unix (см. раздел A.3)

Активы с VMware vSphere (см. раздел A.4)

Активы с GitLab (см. раздел A.5)

A.1. Активы с операционной системой Windows

Вы можете отфильтровать данные об активах, на которых установлен Windows, с помощью PDQL-запросов, приведенных в этом разделе.

Для отбора данных по конкретному активу вы можете добавить в начало запроса строку `filter (WindowsHost.@Id = $HostID) |`, заменив `$HostID` на идентификатор узла Windows.

Для выполнения приведенных ниже запросов необходимо заменить переменную `$GroupSID` на идентификатор безопасности (SID) группы, в которую входят искомые пользователи.

Идентификаторы безопасности групп, которые могут использоваться для реализации недопустимых событий, следующие:

- администраторы — S-1-5-32-544;
- операторы архива — S-1-5-32-551;
- операторы печати — S-1-5-32-550 (только на контроллере домена);
- операторы сервера — S-1-5-32-549 (только на контроллере домена);
- операторы учета — S-1-5-32-548 (только на контроллере домена).

Полный список идентификаторов безопасности групп доступен на сайте microsoft.com.

Доменные пользователи, входящие в локальную группу

```
select(  
    WindowsHost.@Id,  
    WindowsHost.Groups.SID,  
    WindowsHost.Groups.Name,  
    WindowsHost.Groups.Members.SID,  
    WindowsHost.Groups.Members.Name,
```

```

        WindowsHost.Groups.Members.Type,
        WindowsHost.Groups.Members.IsLocal
    ) |
    filter(
        WindowsHost.Groups.SID = '$GroupSID'
        and WindowsHost.Groups.Members.IsLocal = False
        and WindowsHost.Groups.Members.Type = 'Account'
    ) |
    join(
        select(
            ActiveDirectory.Domains.Name,
            ActiveDirectory.Domains.Users.SamAccountName,
            ActiveDirectory.Domains.Users.objectsid,
            ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable
        ) |
        filter(
            ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable = False
        ) as DomainUser,
        WindowsHost.Groups.Members.SID =
        DomainUser.ActiveDirectory.Domains.Users.Objectsid
    ) |
    calc (
        lower(DomainUser.ActiveDirectory.Domains.Users.SamAccountName) as Login
    ) |
    filter (DomainUser.ActiveDirectory.Domains.Users.objectsid != null) |
    select(
        WindowsHost.@Id as HostId,
        DomainUser.ActiveDirectory.Domains.Name as Domain,
        Login,
        DomainUser.ActiveDirectory.Domains.Users.objectsid as UserID
    ) | limit (0)

```

Локальные пользователи, входящие в локальную группу

```

    select(
        WindowsHost.@Id,
        WindowsHost.Groups.SID,
        WindowsHost.Groups.Members.SID,
        WindowsHost.Groups.Members.Name,
        WindowsHost.Groups.Members.Type,
        WindowsHost.Groups.Members.IsLocal
    ) |
    filter (
        WindowsHost.Groups.SID = '$GroupSID'
        and WindowsHost.Groups.Members.Type = 'Account'
        and WindowsHost.Groups.Members.IsLocal = True
    ) |

```

```

calc (
    lower(WindowsHost.Groups.Members.Name) as Login
) |
select (
    WindowsHost.@Id as HostID,
    Login,
    WindowsHost.Groups.Members.SID as UserID
) | limit (0)

```

Доменные пользователи, входящие в доменную группу, которая включена в локальную группу

```

select(
    WindowsHost.@Id,
    WindowsHost.Groups.SID,
    WindowsHost.Groups.Name,
    WindowsHost.Groups.Members.SID,
    WindowsHost.Groups.Members.Name,
    WindowsHost.Groups.Members.Type,
    WindowsHost.Groups.Members.IsLocal
) |
filter(
    WindowsHost.Groups.SID = '$GroupSID'
    and WindowsHost.Groups.Members.IsLocal = False
    and WindowsHost.Groups.Members.Type = 'Group'
) |
join(
    select(
        ActiveDirectory.Domains.Name,
        ActiveDirectory.Domains.Groups.ObjectSid,
        ActiveDirectory.Domains.Groups.AllMembers.ObjectSid,
        ActiveDirectory.Domains.Groups.AllMembers.SamAccountName,
        ActiveDirectory.Domains.Groups.AllMembers.ObjectType
    ) |
        filter(
            ActiveDirectory.Domains.Groups.AllMembers.ObjectType = "DomainUser"
        ) as DomainUser,
    WindowsHost.Groups.Members.SID =
DomainUser.ActiveDirectory.Domains.Groups.ObjectSid
) |
calc (lower(DomainUser.ActiveDirectory.Domains.Name) as Domain) |
calc
(lower(DomainUser.ActiveDirectory.Domains.Groups.AllMembers.SamAccountName) as Login)
|
select(
    WindowsHost.@Id as HostID,
    Domain,

```

```

Login,
DomainUser.ActiveDirectory.Domains.Groups.AllMembers.ObjectSid as UserID
) | limit (0)

```

Для выполнения приведенных ниже запросов необходимо заменить переменную `$Privilege` на название привилегии, которая предоставлена искомым пользователям. Привилегии учетных записей, которые могут использоваться для реализации недопустимых событий, следующие:

- `SeBackupPrivilege` — позволяет извлечь содержимое файла, независимо от настройки списка контроля доступа (ACL).
- `SeCreateTokenPrivilege` — позволяет создать токен доступа для предоставления системных, административных и других важных полномочий.
- `SeDebugPrivilege` — позволяет выполнить отладку процессов, запущенных от имени другой учетной записи. Может применяться для внедрения в память процесса и проникновения на узел в обход средств контроля безопасности.
- `SeImpersonatePrivilege` — позволяет получить токен доступа и использовать его от имени другого пользователя. Может применяться для выполнения действий с системными полномочиями.
- `SeLoadDriverPrivilege` — позволяет загрузить и скачать драйверы устройств путем создания в реестре записи с определенными значениями `ImagePath` и `Type`.
- `SeRestorePrivilege` — позволяет изменить содержимое файла, независимо от настройки списка контроля доступа.
- `SeTakeOwnershipPrivilege` — позволяет стать владельцем объекта, даже если доступ к объекту явно запрещен.
- `SeTcbPrivilege` — позволяет процессу получить токен доступа пользователя, что обеспечивает процессу доступ к объектам, доступным пользователю.

Подробнее о привилегиях в Windows см. на сайте microsoft.com.

Доменные пользователи с привилегиями

```

select(
    WindowsHost.@Id as HostID,
    WindowsHost.Privileges.$Privilege
) |
join(
    select(
        ActiveDirectory.Domains.Name,
        ActiveDirectory.Domains.Users.SamAccountName,
        ActiveDirectory.Domains.Users.Objectsid as UserID,
        ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable
    ) |
    filter(
        ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable = False
    )
)

```

```

) as DomainUser,
    WindowsHost.Privileges.$Privilege = DomainUser.UserID
) |
filter(DomainUser.UserID)
| calc (lower(DomainUser.ActiveDirectory.Domains.Name) as Domain)
| calc (lower(DomainUser.ActiveDirectory.Domains.Users.SamAccountName) as Login)
| select(HostID, Domain, Login, DomainUser.UserID as UserID)
| limit (0)

```

Локальные пользователи с привилегиями

```

select(
    WindowsHost.@Id as HostID,
    WindowsHost.Privileges.$Privilege
) |
join(
    select(
        WindowsHost.@Id as HostID,
        WindowsHost.User.Name as Login,
        WindowsHost.User.ID as UserID) as HostUsers, HostID = HostUsers.HostID
) |
filter(
    WindowsHost.Privileges.$Privilege = HostUsers.UserID
) |
calc (lower(HostUsers.Login) as Login)
| select(HostID, Login, HostUsers.UserID as UserID) | limit (0)

```

Доменные пользователи, входящие в доменную группу с привилегиями

```

select(
    WindowsHost.@Id as HostID,
    WindowsHost.Privileges.$Privilege
) |
join(
    select(
        ActiveDirectory.Domains.Name,
        ActiveDirectory.Domains.Groups.ObjectSid,
        ActiveDirectory.Domains.Groups.AllMembers.ObjectSid,
        ActiveDirectory.Domains.Groups.AllMembers.SamAccountName,
        ActiveDirectory.Domains.Groups.AllMembers.ObjectType
    ) |
    filter(
        ActiveDirectory.Domains.Groups.AllMembers.ObjectType = "DomainUser"
    ) as DomainGroup,

```

```

        WindowsHost.Privileges.$Privilege =
DomainGroup.ActiveDirectory.Domains.Groups.ObjectSid
    ) |
    filter(
        DomainGroup.ActiveDirectory.Domains.Groups.ObjectSid
    ) |
    calc (lower(DomainGroup.ActiveDirectory.Domains.Name) as Domain) |
    calc
    (lower(DomainGroup.ActiveDirectory.Domains.Groups.AllMembers.SamAccountName) as Login
    ) |
    select(HostID, Domain, Login,
DomainGroup.ActiveDirectory.Domains.Groups.AllMembers.ObjectSid as UserID)
    | limit (0)

```

Доменные пользователи, которые являются членами доменной группы, входящей в локальную группу с привилегиями

```

select(
    WindowsHost.@Id as HostID,
    WindowsHost.Privileges.$Privilege
) |
join(
    select(
        WindowsHost.@Id as HostID,
        WindowsHost.Groups.SID as GroupSID,
        WindowsHost.Groups.Members.Name as MemberName,
        WindowsHost.Groups.Members.SID as MemberSID,
        WindowsHost.Groups.Members.Type as Type,
        WindowsHost.Groups.Members.isLocal as isLocal) as HostGroups, HostID =
HostGroups.HostID
    ) |
    filter(
        WindowsHost.Privileges.$Privilege = HostGroups.GroupSID
        and HostGroups.Type = 'Group'
        and HostGroups.isLocal = False
    ) |
    join(
        select(
            ActiveDirectory.Domains.Name,
            ActiveDirectory.Domains.Groups.ObjectSid as GroupID,
            ActiveDirectory.Domains.Groups.AllMembers.ObjectSid as UserID,
            ActiveDirectory.Domains.Groups.AllMembers.SamAccountName,
            ActiveDirectory.Domains.Groups.AllMembers.ObjectType
        ) |
        filter(
            ActiveDirectory.Domains.Groups.AllMembers.ObjectType = "DomainUser"
        ) as DomainGroup,

```

```

        HostGroups.MemberSID = DomainGroup.GroupID
    ) |
    calc (lower(DomainGroup.ActiveDirectory.Domains.Name) as Domain) |
    calc
    (lower(DomainGroup.ActiveDirectory.Domains.Groups.AllMembers.SamAccountName) as Login
    ) |
    select(HostID, Domain, Login, DomainGroup.UserID as UserID)
    | limit (0)

```

Доменные пользователи, входящие в локальную группу с привилегиями

```

select(
    WindowsHost.@Id as HostID,
    WindowsHost.Privileges.$Privilege) |
join(
    select(
        WindowsHost.@Id as HostID,
        WindowsHost.Groups.SID as GroupSID,
        WindowsHost.Groups.Members.Name as MemberName,
        WindowsHost.Groups.Members.SID as MemberSID,
        WindowsHost.Groups.Members.Type as Type,
        WindowsHost.Groups.Members.isLocal as isLocal) as HostGroups, HostID =
HostGroups.HostID
    ) |
filter(
    WindowsHost.Privileges.$Privilege = HostGroups.GroupSID
    and HostGroups.Type = 'Account'
    and HostGroups.isLocal = False
) |
join(
    select(
        ActiveDirectory.Domains.Name,
        ActiveDirectory.Domains.Users.SamAccountName,
        ActiveDirectory.Domains.Users.Objectsid as UserID,
        ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable
    ) |
    filter(
        ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable = False
    ) as DomainUser,
    HostGroups.MemberSID = DomainUser.UserID
    ) |
filter(DomainUser.UserID
) |
calc (lower(DomainUser.ActiveDirectory.Domains.Name) as Domain) |
calc (lower(DomainUser.ActiveDirectory.Domains.Users.SamAccountName) as Login) |

```

```
select(HostID, Domain, Login, DomainUser.UserID as UserID)
| limit (0)
```

Локальные пользователи, входящие в локальную группу с привилегиями

```
select(
  WindowsHost.@Id as HostID,
  WindowsHost.Privileges.$Privilege
) |
join(
  select(
    WindowsHost.@Id as HostID,
    WindowsHost.Groups.SID as GroupSID,
    WindowsHost.Groups.Members.Name as MemberName,
    WindowsHost.Groups.Members.SID as MemberSID,
    WindowsHost.Groups.Members.Type as Type,
    WindowsHost.Groups.Members.isLocal as isLocal) as HostGroups, HostID =
HostGroups.HostID
) |
filter(
  WindowsHost.Privileges.$Privilege = HostGroups.GroupSID
  and HostGroups.Type = 'Account'
  and HostGroups.isLocal = True
) |
calc (lower(HostGroups.MemberName) as Login)
| select(HostID, Login, HostGroups.MemberSID as UserID) | limit (0)
```

A.2. Активы службы каталогов Active Directory

Вы можете отфильтровать данные об активах службы каталогов Active Directory с помощью PDQL-запросов, приведенных в этом разделе.

Для выполнения запроса необходимо заменить переменную `$GroupSID` на идентификатор безопасности (SID) группы, в которую входят искомые пользователи. Идентификаторы безопасности групп, которые могут использоваться для реализации недопустимых событий, следующие:

- администраторы — S-1-5-32-544;
- операторы архива — S-1-5-32-551;
- операторы печати — S-1-5-32-550 (только на контроллере домена);
- операторы сервера — S-1-5-32-549 (только на контроллере домена);
- операторы учета — S-1-5-32-548 (только на контроллере домена).

Полный список идентификаторов безопасности групп доступен на сайте microsoft.com.

Для отбора активов в конкретном домене вы можете добавить в начало запроса строку `filter (ActiveDirectory.@id = $DomainID)`, заменив `$DomainID` на идентификатор домена.

```
select(
    ActiveDirectory.@id as DomainID,
    ActiveDirectory.Domains.Name,
    ActiveDirectory.Domains.Groups.ObjectSid as GroupSid,
    ActiveDirectory.Domains.Groups.AllMembers.ObjectSid as UserID,
    ActiveDirectory.Domains.Groups.AllMembers.SamAccountName,
    ActiveDirectory.Domains.Groups.AllMembers.ObjectType
) |
filter(GroupSid in ['$GroupSID'] and
ActiveDirectory.Domains.Groups.AllMembers.ObjectType = "DomainUser"
) |
calc(lower(ActiveDirectory.Domains.Name) as Domain) |
calc(lower(ActiveDirectory.Domains.Groups.AllMembers.SamAccountName) as Login) |
select(DomainID, Domain, Login, UserID) | unique() | limit(0)
```

А.3. Активы с операционной системой семейства Unix

Вы можете отфильтровать данные об активах с ОС семейства Unix с помощью PDQL-запросов, приведенных в этом разделе.

Пользователи группы

Для выполнения запроса необходимо заменить переменную `$Group` на имя группы, в которую входят искомые пользователи.

Для отбора данных по конкретному активу вы можете добавить в начало запроса строку `filter(UnixHost.@Id = $HostID).|`, заменив `$HostID` на идентификатор узла.

```
select(
    UnixHost.@Id as HostID,
    UnixHost.Groups.Name as GroupName,
    UnixHost.Groups.Users as GroupUsers
) | filter (GroupName = $Group and GroupUsers)
| join (select (UnixHost.@Id as HostID, UnixHost.User.Name as Login,
UnixHost.User.ID as UserID) as HostUsers, HostID = HostUsers.HostID
) |
filter(
    GroupUsers = HostUsers.Login
) | select (HostID, HostUsers.Login as Login, HostUsers.UserID as UserID) | limit (0)
```

Пользователи с правами суперпользователя (root)

Для отбора данных по конкретному активу вы можете добавить в первую строку запроса выражение `UnixHost.@Id = $HostID` в формате `filter (UnixHost.@Id = $HostID and UnixHost.Sudo.SudoConfig.UserSpecifications)`. Переменную `$HostID` необходимо заменить на идентификатор узла.

```
filter (UnixHost.Sudo.SudoConfig.UserSpecifications)
| select(
    UnixHost.@Id as HostID,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Users as Username,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.Hosts as Host,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.CmndSpecs.RunAsUsers as RunAsUser,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.CmndSpecs.RunAsGroup as RunAsGroup,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.CmndSpecs.Cmnd as Cmnd
) |
filter(
    Username != null
    and Host = "ALL"
    and RunAsUser = "ALL"
    and Cmnd = "ALL"
    and not Username like "%%"
) |
select(HostID, Username) | limit (0)
```

Пользователи группы, которой назначены права суперпользователя (root)

Для отбора данных по конкретному активу вы можете добавить в первую строку запроса выражение `UnixHost.@Id = $HostID` в формате `filter (UnixHost.@Id = $HostID and UnixHost.Sudo.SudoConfig.UserSpecifications)`. Переменную `$HostID` необходимо заменить на идентификатор узла.

```
filter(UnixHost.Sudo.SudoConfig.UserSpecifications and UnixHost.Groups)
| select(
    UnixHost.@Id as HostID,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Users as GroupName,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.Hosts as Host,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.CmndSpecs.RunAsUsers as RunAsUser,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.CmndSpecs.RunAsGroup as RunAsGroup,
    UnixHost.Sudo.SudoConfig.UserSpecifications.Values.CmndSpecs.Cmnd as Cmnd
) |
filter(Groupname != null
    and Host = "ALL")
```

```

    and RunAsUser = "ALL"
    and Cmd = "ALL"
    and Groupname like "\%"
) |
select(HostID, Groupname) |
    join(select(
        UnixHost.@Id as HostID,
        UnixHost.Groups.Name as GroupsName,
        UnixHost.Groups.Users as GroupsUsers
    ) |
        filter(GroupsUsers != null) |
    calc("%" + GroupsName as SudoGroupName) as Groups, (
        HostID = Groups.HostID
        and Groupname = Groups.SudoGroupName
    )) |
    filter (Groups.GroupsUsers != null) |
    select(HostID, Groups.GroupsUsers as Username) | limit (0)

```

A.4. Активы с VMware vSphere

Вы можете отфильтровать данные об активах с установленным VMware vSphere с помощью PDQL-запросов, приведенных в этом разделе.

Для выполнения запросов необходимо заменить переменную `$Privilege` на название привилегии, которая предоставлена искомым пользователям. Вы можете указать несколько привилегий через запятую. Привилегии, которые могут использоваться для реализации недопустимых событий, следующие:

- `CertificateAuthority.Administer` — управление сертификатами VMware vCenter Server с правами администратора;
- `CertificateManagement.Administer` — предоставление пользователям права на управление сертификатами VMware vCenter Server;
- `Datacenter.Create` — создание дата-центра;
- `Datacenter.Delete` — удаление дата-центра;
- `Datacenter.Reconfigure` — изменение дата-центра;
- `Datastore.Config` — настройка дата-центра;
- `Global.Settings` — просмотр и изменение параметров глобальной настройки VMware vCenter;
- `Sessions.ImpersonateUser` — выполнение действий от имени другого пользователя.

Для расширений VMware vSphere предусмотрены дополнительные привилегии. Подробнее о привилегиях в VMware vSphere см. на сайте vmware.com.

Для отбора данных по конкретному активу вы можете добавить в первое и второе условие фильтрации выражение `Host.@Id = $HostID` в формате `filter(Host.@Id = $HostID and Host.Softs<vCenterInstance>) |`. Переменную `$HostID` необходимо заменить на идентификатор узла.

Доменные пользователи с привилегиями

```
filter(Host.Softs<vCenterInstance>) |
select(
    Host.@Id as VcHostID,
    Host.Softs<vCenterInstance>.Roles.ID as RoleID,
    Host.Softs<vCenterInstance>.Roles.Privileges as RolePrivileges
) |
filter(RolePrivileges in [$Privilege]) |
join (
    filter(Host.Softs<vCenterInstance>) |
    select(
        Host.@Id as JoinedVcHostID,
        Host.Softs<vCenterInstance>.Users.Name as Login,
        Host.Softs<vCenterInstance>.Users.Domain as Domain,
        Host.Softs<vCenterInstance>.Users.IsGroup as IsGroup,
        Host.Softs<vCenterInstance>.Users.Permissions.RoleID as UserRoleID
    ),
    (VcHostID = JoinedVcHostID and RoleID = UserRoleID)
) |
filter(IsGroup = false and not Domain in ["VSPHERE.LOCAL", ""]) |
select(VcHostID, Login, Domain) |
unique() |
limit(0)
```

Локальные пользователи с привилегиями

```
filter(Host.Softs<vCenterInstance>) |
select(
    Host.@Id as VcHostID,
    Host.Softs<vCenterInstance>.Roles.ID as RoleID,
    Host.Softs<vCenterInstance>.Roles.Privileges as RolePrivileges
) |
filter(RolePrivileges in [$Privilege]) |
join (
    filter(Host.Softs<vCenterInstance>) |
    select(
        Host.@Id as JoinedVcHostID,
        Host.Softs<vCenterInstance>.Users.Name as Login,
        Host.Softs<vCenterInstance>.Users.Domain as Domain,
        Host.Softs<vCenterInstance>.Users.IsGroup as IsGroup,
```

```

        Host.Softs<vCenterInstance>.Users.Permissions.RoleID as UserRoleID
    ),
    (VcHostID = JoinedVcHostID and RoleID = UserRoleID)
) |
filter(IsGroup = false and Domain = "VSPHERE.LOCAL") |
select(VcHostID, Login) |
unique() |
limit(0)

```

А.5. Активы с GitLab

Вы можете отфильтровать данные об активах с установленным GitLab с помощью PDQL-запросов, приведенных в этом разделе.

Для отбора данных по конкретному активу вы можете добавить в первое условие фильтрации выражение `Host.@Id = $HostID` в формате `filter(Host.@Id = $HostID and Host.Softs<Gitlab>.Projects) |`. Переменную `$HostID` необходимо заменить на идентификатор узла.

Доменные пользователи с ролями Owner, Developer, Maintainer

```

filter(Host.Softs<Gitlab>.Projects) |
select(
    Host.@Id as HostID,
    Host.Softs<Gitlab>.Projects.AllMembers.ID as UserID,
    Host.Softs<Gitlab>.Projects.AllMembers.AccessLevel
) |
filter(Host.Softs<Gitlab>.Projects.AllMembers.AccessLevel in ['Owner', 'Developer', 'Maintainer'])
| join(
    select(
        Host.@Id as HostID,
        Host.Softs<Gitlab>.Users.LogonName as Login,
        Host.Softs<Gitlab>.Users.ID as UserID,
        Host.Softs<Gitlab>.Users.State as State,
        Host.Softs<Gitlab>.Users.Identities.Provider as IdProvider,
        Host.Softs<Gitlab>.Users.identities.Identity as IdIdentity) as Users, (HostID =
Users.HostID and UserID = Users.UserID))
|
filter(Users.State = "Active" and Users.IdProvider = "ldapmain")
| join(
    select(
        ActiveDirectory.Domains.Name as Domain,
        ActiveDirectory.Domains.Users.SamAccountName as Login,
        ActiveDirectory.Domains.Users.DistinguishedName as UserDN,
        ActiveDirectory.Domains.Users.ObjectSid as UserID,
        ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable

```

```

) |
filter(
    ActiveDirectory.Domains.Users.UserAccountControl.AccountDisable = False
) as Domain, (Users.IdIdentity = Domain.UserDN)
) |
select(HostID, Domain.Login as Login, Domain.UserID as UserID,
Domain.Domain as Domain) | unique() | limit(0)

```

Локальные пользователи с ролями Owner, Developer, Maintainer

```

filter(Host.Softs<Gitlab>.Projects) |
select(
    Host.@Id as HostID,
    Host.Softs<Gitlab>.Projects.AllMembers.ID as UserID,
    Host.Softs<Gitlab>.Projects.AllMembers.AccessLevel
) |
filter(Host.Softs<Gitlab>.Projects.AllMembers.AccessLevel in ['Owner', 'Developer', '
Maintainer'])
| join(
    select(
        Host.@Id as HostID,
        Host.Softs<Gitlab>.Users.LogonName as Login,
        Host.Softs<Gitlab>.Users.ID as UserID,
        Host.Softs<Gitlab>.Users.State as State,
        Host.Softs<Gitlab>.Users.Identities.Provider as IdProvider,
        Host.Softs<Gitlab>.Users.identities.Identity as IdIdentity) as Users, (HostID =
Users.HostID and UserID = Users.UserID))
|
filter(
    Users.State = "Active"
    and Users.IdProvider = null
) |
select(HostID, Users.Login as Login, Users.UserID as UserID) | unique() | limit(0)

```

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, возникшее в результате кибератаки, которое делает невозможным достижение операционных и (или) стратегических целей организации или приводит к значительному нарушению ее основной деятельности.

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 — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.