



MaxPatrol Carbon

версия 2026.2

Руководство администратора

© Positive Technologies, 2026.

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

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

Документ может быть изменен без предварительного уведомления.

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

Дата редакции документа: 18.09.2026

Содержание

1.	Об этом документе.....	5
1.1.	Условные обозначения.....	5
1.2.	Другие источники информации о MaxPatrol Carbon.....	6
2.	О MaxPatrol Carbon.....	7
3.	Архитектура MaxPatrol Carbon.....	8
4.	Алгоритм работы MaxPatrol Carbon.....	11
5.	Аппаратные и программные требования.....	12
5.1.	Требования к аппаратному обеспечению.....	12
5.2.	Требования к программному обеспечению.....	13
5.3.	Требования к сетевой инфраструктуре.....	13
5.4.	Требования к интеграции MaxPatrol Carbon с другими продуктами Positive Technologies.....	16
6.	Развертывание MaxPatrol Carbon.....	17
6.1.	Установка роли Deployer.....	18
6.2.	Установка роли SqlStorage.....	19
6.3.	Установка роли Carbon.....	20
6.4.	Установка роли Web.....	22
6.5.	Установка роли Monitoring.....	22
6.6.	Установка роли VmStorageBusiness.....	23
6.7.	Установка роли RmqMessageBus.....	24
6.8.	Установка роли EtcdKeyValueStorage.....	25
6.9.	Установка доверенного сертификата для сайта MaxPatrol Carbon.....	26
7.	Обновление MaxPatrol Carbon.....	28
7.1.	Обновление роли Deployer.....	29
7.2.	Обновление роли SqlStorage.....	29
7.3.	Обновление роли Carbon.....	30
7.4.	Обновление роли Web.....	30
7.5.	Обновление роли Monitoring.....	31
7.6.	Обновление роли VmStorageBusiness.....	31
7.7.	Обновление роли RmqMessageBus.....	32
7.8.	Обновление роли EtcdKeyValueStorage.....	32
8.	Проверка работы MaxPatrol Carbon после установки или обновления.....	34
9.	Первоначальная настройка MaxPatrol Carbon.....	35
10.	О модели компонентов в MaxPatrol Carbon.....	37
10.1.	Синтаксис запросов для фильтрации компонентов.....	37
10.2.	Экспорт данных об активах в табличный список.....	40
11.	Решение проблем.....	42
11.1.	Устранение проблем при установке и обновлении MaxPatrol Carbon.....	42
11.2.	Устранение проблем при входе в MaxPatrol Carbon.....	45
11.3.	Устранение проблем, связанных с регистрацией MaxPatrol Carbon в PT MC.....	48
	Приложение А. PDQL-запросы данных об активах.....	50
A.1.	Активы с Windows.....	50
A.2.	Активы службы каталогов Active Directory.....	57
A.3.	Активы с ОС семейства Unix.....	58

A.4.	Активы с VMware vCenter Server	60
A.5.	Активы с GitLab	62
A.6.	Активы с OpenVPN	63
Глоссарий.....		65

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию MaxPatrol Carbon (далее также — MaxPatrol Carbon). Руководство не содержит инструкций по использованию основных функций продукта.

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

Комплект документации MaxPatrol Carbon включает:

- Этот документ.
- Руководство пользователя — содержит пошаговые инструкции и справочную информацию об использовании продукта.
- Документ «Подготовка к внедрению» — содержит справочную информацию и инструкции по подготовке инфраструктуры к развертыванию продукта.
- Документ «Сканирование активов» — содержит справочную информацию и инструкции по сканированию инфраструктуры организации.
- Документ «Типы действий злоумышленника: описание и данные для их применения в инфраструктуре» — содержит описание типов действий злоумышленника и рекомендации по оценке данных, необходимых для их применения.

В этом разделе

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

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

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

Пример	Описание
Нажмите OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <code>Stop-Service</code>	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 Carbon

Вы можете найти дополнительную информацию о MaxPatrol Carbon на справочном портале help.ptsecurity.com и на [Позитивном портале](#). Через Позитивный портал вы также можете обратиться в техническую поддержку.

2. О MaxPatrol Carbon

MaxPatrol Carbon — система, предназначенная для анализа ИТ-инфраструктуры организации, моделирования возможных действий злоумышленников и формирования рекомендаций для предотвращения недопустимых событий и усложнения сценариев их реализации. Помогает оценить инфраструктуру с точки зрения возможности проникновения и принять решения по исправлению проблем.

MaxPatrol Carbon получает данные об ИТ-инфраструктуре и изменениях в ней из MaxPatrol VM и MaxPatrol Topology (а также из MaxPatrol SIEM и MaxPatrol HCC — при наличии этих продуктов).

MaxPatrol Carbon рассчитывает модель возможных действий злоумышленника, строит графическое отображение этих действий и предлагает рекомендации по их предотвращению.

Ключевые функции MaxPatrol Carbon:

- Анализ возможных передвижений злоумышленника по ИТ-инфраструктуре на основе информации об этой инфраструктуре, ее уязвимостях и сетевой топологии.
- Возможность указать компоненты, которые могут являться точками входа злоумышленника, и компоненты, доступ к которым может приводить к недопустимым событиям.
- Построение и отображение в интерфейсе возможных маршрутов атак, оценка маршрутов с точки зрения их сложности, времени на прохождение злоумышленником (time to attack, TTA), времени на обнаружение злоумышленника (time to detect, TTD).
- Формирование рекомендаций для предотвращения недопустимых событий и усложнения сценариев их реализации. Возможность переходить к выполнению рекомендаций или отклонять их.
- Отображение сводной информации о безопасности ИТ-инфраструктуры на дашбордах, формирование статистики и отчетов.

При развертывании MaxPatrol Carbon автоматически устанавливается приложение для визуализации данных Grafana (подробная информация о Grafana приведена на сайте docs.grafana.org). В веб-интерфейсе Grafana добавляются несколько дашбордов, на которых отображаются графики и диаграммы со статистической информацией о работе продукта и операционной системы.

3. Архитектура MaxPatrol Carbon

MaxPatrol Carbon имеет сервис-ориентированный тип архитектуры и состоит из микросервисов, сгруппированных в программные компоненты.

На рисунке ниже представлена схема взаимодействия компонентов MaxPatrol Carbon и указаны порты взаимодействия.

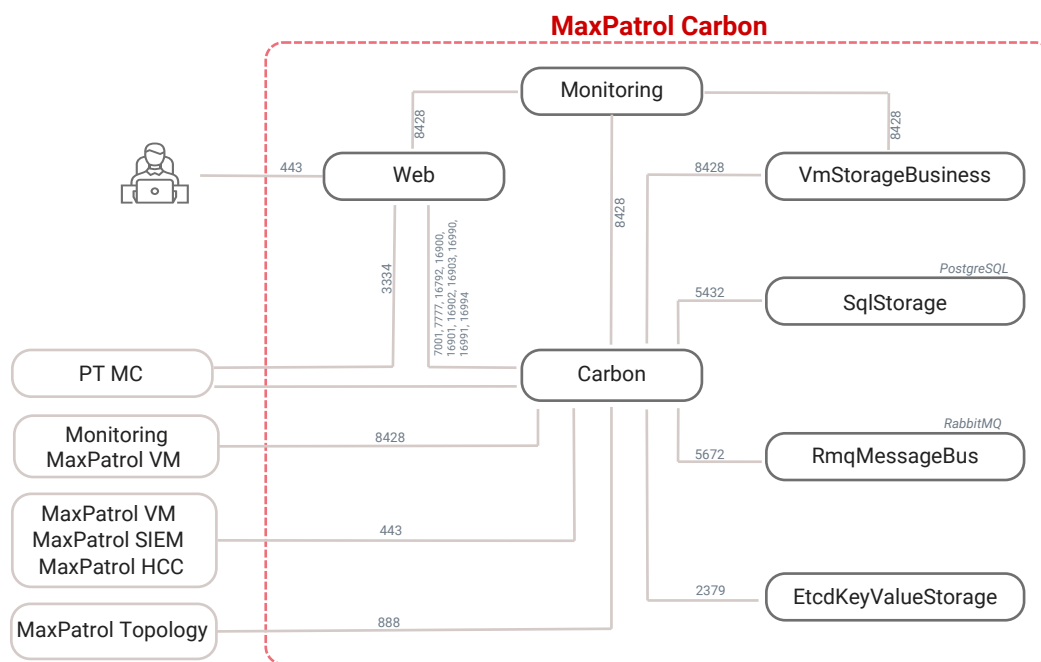


Рисунок 1. Схема взаимодействия компонентов

Описание портов взаимодействия приведено в [требованиях к сетевой инфраструктуре \(см. раздел 5.3\)](#) MaxPatrol Carbon.

Для обеспечения ключевых функций MaxPatrol Carbon в инфраструктуре, где развернут продукт, необходимо установить MaxPatrol VM и MaxPatrol Topology. Дополнительно могут быть установлены другие продукты, приведенные на схеме.

Компонент Web

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

Взаимодействует с системой управления пользователями и доступом PT MC (Positive Technologies Management and Configuration), которая реализует механизм единого входа в системы Positive Technologies, развернутые в ИТ-инфраструктуре организации.

Содержит микросервис Carbon.Api (BFF), который обеспечивает получение данных от серверной части продукта.

Компонент Monitoring

Собирает данные о работе MaxPatrol Carbon и предоставляет веб-интерфейс для просмотра и анализа этих данных.

Компонент VmStorageBusiness

Обеспечивает хранение и визуализацию технических и бизнес-метрик MaxPatrol Carbon.

Компонент Carbon

Реализует основные функции продукта и обеспечивает взаимодействие микросервисов, а также используется для обнаружения микросервисов в распределенных системах.

Содержит следующие микросервисы:

- Carbon — формирует рекомендации для предотвращения недопустимых событий и усложнения сценариев их реализации, ранжирует рекомендации по степени важности.
- Carbon.Core — хранит граф возможностей злоумышленника, участвует в формировании графа и управляет историей его изменения.
- Carbon.Reports — формирует отчеты.
- Carbon.Dashboards — обеспечивает получение данных для дашбордов.
- Carbon.Hcc.Adapter — обеспечивает интеграцию MaxPatrol Carbon и MaxPatrol HCC для проверки соответствия активов требованиям информационной безопасности.
- Carbon.Risks — создает и обновляет данные о компонентах, задействованных в недопустимых событиях.
- Carbon.Routes — строит возможные маршруты атаки, рассчитывает TTA и TTD, ранжирует маршруты по степени важности.
- Carbon.Search — обеспечивает полнотекстовый поиск компонентов.
- Carbon.Siem.Adapter — получает из MaxPatrol SIEM данные об источниках событий, установленных на активах, а также о состоянии мониторинга этих источников. На основе полученных данных формирует и обновляет в базе данных записи о каждом источнике. Взаимодействие обеспечивает брокер сообщений RabbitMQ.
- EntryPoints — получает данные о точках входа.
- MinPath — рассчитывает кратчайшие пути реализации недопустимых событий.
- Priviledges — формирует и обновляет данные о привилегиях учетных записей.
- Registration — обеспечивает регистрацию MaxPatrol Carbon в PT MC (для аутентификации пользователей).
- Threat Modelling Engine (TME) — формирует граф возможных действий злоумышленника в инфраструктуре. Граф представляет собой совокупность активов, их компонентов и всех возможных действий с ними.

Компонент EtcdKeyValueStorage

Обеспечивает хранение установленных пользователем параметров, например режима расчета ТТА и ТТД.

Компонент SqlStorage

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

Компонент RmqMessageBus

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

4. Алгоритм работы MaxPatrol Carbon

Алгоритм работы MaxPatrol Carbon:

1. С помощью компонента Web пользователь вводит данные о точках входа и недопустимых событиях в инфраструктуре.
2. Компонент Carbon формирует и обновляет компонентную модель и сведения о компонентах, задействованных в событиях.
3. На основе данных MaxPatrol VM и MaxPatrol Topology о сетевой топологии и достижимости активов компонент Carbon формирует граф возможных действий злоумышленника в инфраструктуре. На основе графа и указанных пользователем точек входа и недопустимых событий рассчитывает кратчайшие пути реализации этих событий.
4. Компонент Carbon формирует и обновляет сведения о привилегиях учетных записей, используя информацию из MaxPatrol VM.
5. Компонент Carbon выстраивает возможные маршруты атаки — (пути продвижения злоумышленника от точек входа до недопустимых событий), рассчитывает ТТА и TTD, а также ранжирует маршруты по степени важности. Для этого используются: сведения о компонентах инфраструктуры и привилегиях учетных записей, а также построенный граф.
6. Компонент Carbon формирует рекомендации для предотвращения недопустимых событий и усложнения сценариев их реализации, ранжирует рекомендации по степени важности. Для формирования рекомендаций используются стандарты и правила для проверки соответствия активов требованиям информационной безопасности из MaxPatrol HCC, для ранжирования — сведения об уязвимостях из MaxPatrol VM.
7. Компонент Carbon передает данные о маршрутах и рекомендациях компоненту Monitoring для формирования метрик и их отображения в веб-интерфейсе продукта (в том числе на дашбордах) с помощью компонента Web.
8. Пользователь просматривает маршруты и рекомендации, назначает приоритеты, принимает решение о выполнении или отклонении рекомендаций. Компонент Carbon получает от MaxPatrol VM актуальные данные, фиксирует изменения в инфраструктуре и обновляет маршруты и рекомендации.
9. Пользователь просматривает и настраивает общие параметры работы с продуктом через веб-интерфейс.

5. Аппаратные и программные требования

В этом разделе приведены требования к аппаратному и программному обеспечению серверов MaxPatrol Carbon, а также требования к интеграции MaxPatrol Carbon с другими продуктами Positive Technologies.

В этом разделе

[Требования к аппаратному обеспечению \(см. раздел 5.1\)](#)

[Требования к программному обеспечению \(см. раздел 5.2\)](#)

[Требования к сетевой инфраструктуре \(см. раздел 5.3\)](#)

[Требования к интеграции MaxPatrol Carbon с другими продуктами Positive Technologies \(см. раздел 5.4\)](#)

5.1. Требования к аппаратному обеспечению

Сервер, на котором выполняется развертывание MaxPatrol Carbon, должен удовлетворять требованиям, приведенным в таблице ниже.

Таблица 2. Требования к аппаратному обеспечению

Параметр	Минимальное значение
Центральный процессор	16 ядер с тактовой частотой 2,4 ГГц
Память (ОЗУ)	64 ГБ
Твердотельный накопитель (SSD)	1 ТБ

Объем дискового пространства для MaxPatrol Carbon и его резервных копий определяется в зависимости от количества активов.

Таблица 3. Объем дискового пространства, необходимый для MaxPatrol Carbon

Количество активов	Для установки, ГБ	Для резервной копии, ГБ
1 000	500	50
2 000	750	75
5 000	1 000	100
10 000	1 500	150
20 000	2 000	200
50 000	3 000	300
100 000	5 000	500

Для работы в интерфейсе MaxPatrol Carbon рекомендуется использовать разрешение монитора не менее 1920×1080 пикселей.

5.2. Требования к программному обеспечению

MaxPatrol Carbon поддерживает установку на чистую 64-разрядную серверную версию ОС семейства Linux – Debian 10–12 (на базе ядра Linux версии 5.10 или выше) или Astra Linux Special Edition 1.7.5–1.7.7 (на базе ядра Linux версии 5.15 или выше) в режиме защищенности «Воронеж».

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

На сервере, где планируется развертывание продукта, рекомендуется установить следующие вспомогательные пакеты: `curl`, `dnsutils`, `http`, `iotop`, `jq`, `mc`, `net-tools`, `sudo`, `unzip`.

Для работы в интерфейсе MaxPatrol Carbon рекомендуется использовать браузер Google Chrome последней версии.

5.3. Требования к сетевой инфраструктуре

Взаимодействие MaxPatrol Carbon с элементами IT-инфраструктуры

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

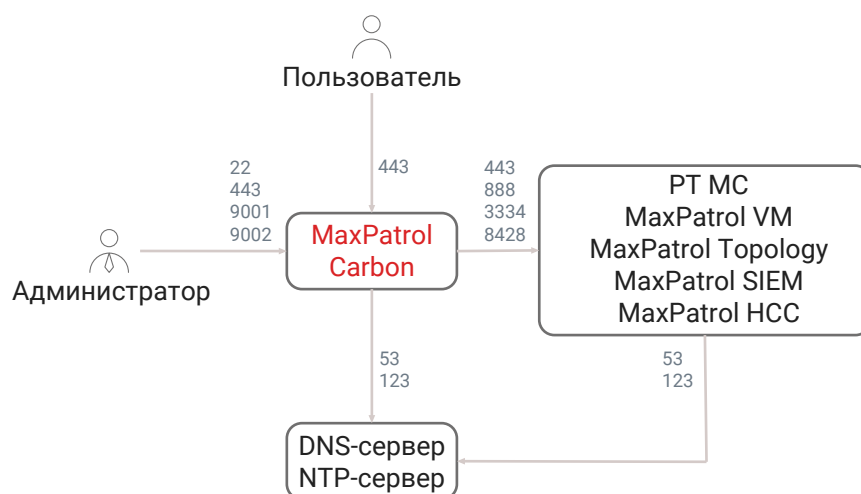


Рисунок 2. Схема взаимодействия MaxPatrol Carbon с элементами IT-инфраструктуры

Для обеспечения ключевых функций MaxPatrol Carbon в инфраструктуре, где развернут продукт, необходимо установить MaxPatrol VM и MaxPatrol Topology. Дополнительно могут быть установлены другие продукты, приведенные на схеме.

Для обеспечения сетевого взаимодействия MaxPatrol Carbon с элементами IT-инфраструктуры необходимо разрешить входящие и исходящие подключения по портам, представленным в таблице.

Доступ MaxPatrol Carbon к другим продуктам рекомендуется организовать без использования межсетевых экранов.

Таблица 4. Порты взаимодействия MaxPatrol Carbon с элементами IT-инфраструктуры

Подключение	Порт	Протокол	Назначение
Рабочая станция пользователя → Сервер MaxPatrol Carbon	443	HTTPS	Доступ к веб-интерфейсу MaxPatrol Carbon
Рабочая станция администратора → Сервер MaxPatrol Carbon	22	SSH	Управление MaxPatrol Carbon
	443	HTTPS	Доступ к веб-интерфейсу MaxPatrol Carbon
	9001	HTTPS	Доступ к платформе pgAdmin для работы с СУБД PostgreSQL
	9002	HTTPS	Доступ к Grafana
Сервер MaxPatrol Carbon → Сервер MaxPatrol Topology	888	HTTPS	Доступ к MaxPatrol Topology. Для взаимодействия с MaxPatrol Topology может использоваться любой незаполненный порт (см. Руководство по установке MaxPatrol Topology). По умолчанию указан порт 888
Сервер MaxPatrol Carbon → Сервер MaxPatrol VM, MaxPatrol SIEM и MaxPatrol HCC	443	HTTPS	Доступ к MaxPatrol VM, MaxPatrol SIEM и MaxPatrol HCC
	8711	TCP	
	8428	HTTPS	Доступ к сервису VictoriaMetrics MaxPatrol VM
Сервер MaxPatrol Carbon → Сервер PT MC	3334	HTTPS	Доступ к PT MC
Сервер MaxPatrol Carbon, Сервер PT MC, MaxPatrol VM,	53	TCP, UDP	Разрешение доменных имен

Подключение	Порт	Протокол	Назначение
MaxPatrol SIEM, MaxPatrol HCC → DNS-сервер			
Сервер MaxPatrol Carbon, Сервер PT MC, MaxPatrol VM, MaxPatrol SIEM, MaxPatrol HCC → NTP-сервер	123	TCP, UDP	Синхронизация времени

Взаимодействие компонентов MaxPatrol Carbon

Состав и схема взаимодействия компонентов приведены [при описании архитектуры \(см. раздел 3\)](#) MaxPatrol Carbon.

Для обеспечения сетевого взаимодействия компонентов MaxPatrol Carbon необходимо разрешить входящие и исходящие подключения по портам, представленным в таблице.

Таблица 5. Компоненты MaxPatrol Carbon и порты взаимодействия

Источник	Получатель	Порт	Протокол
Рабочая станция пользователя	Web	443	HTTPS
Web	Carbon	— 7001 (микросервис Registration); — 7777 (микросервис Carbon.Api); — 16900 (микросервис Carbon); — 16901 (микросервис Carbon.Siem.Adapter); — 16902 (микросервис Carbon.Hcc.Adapter); — 16903 (микросервис Carbon.Dashboards); — 15364 (микросервис EntryPoints);	TCP

Источник	Получатель	Порт	Протокол
		— 16991 (микросервис Carbon.Search); — 16994 (микросервис Carbon.Routes)	
Web и Carbon	PT MC	3334	HTTPS
Carbon	MaxPatrol VM, MaxPatrol SIEM	443	HTTPS
	Monitoring (MaxPatrol VM)	8428	HTTPS
	VmStorageBusiness	8428	HTTPS
	SqlStorage	5432	TCP
	RmqMessageBus	5672	TCP
	EtcdKeyValueStorage	2379	TCP

5.4. Требования к интеграции MaxPatrol Carbon с другими продуктами Positive Technologies

Для работы MaxPatrol Carbon необходимо в инфраструктуре, где будет развернут продукт, установить MaxPatrol VM и MaxPatrol Topology.

MaxPatrol Carbon взаимодействует с MaxPatrol 10 версии 27.2 или выше.

6. Развертывание MaxPatrol Carbon

MaxPatrol Carbon поставляется в виде архива с дистрибутивом с расширением .tar, который содержит папки с дистрибутивами ролей.

Роль является базовой единицей развертывания MaxPatrol Carbon 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.

В настоящее время поддерживается односерверное развертывание MaxPatrol Carbon (все роли устанавливаются на один сервер).

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

- приложение Deployment-Application содержит роль Deployer;
- приложение Carbon-Application содержит роли SqlStorage, Carbon, Web, Monitoring, VmStorageBusiness, RmqMessageBus и EtcdKeyValueStorage.

Управление развертыванием обеспечивается ролью Deployer.

В общем случае установка роли включает следующие этапы:

1. Распаковка архива с дистрибутивом.
2. Запуск сценария установки.
3. Выбор приложения для установки роли.
4. Ввод названия экземпляра роли и выбор сервера для ее установки.
5. Проверка и изменение параметров конфигурации.
6. Запуск установки.

Внимание! Перед установкой MaxPatrol Carbon рекомендуется установить MaxPatrol Topology (см. Руководство по установке MaxPatrol Topology). MaxPatrol Carbon и MaxPatrol Topology необходимо устанавливать на разные узлы.

Для установки MaxPatrol Carbon необходимо:

1. Сохранить архив с дистрибутивом на сервер, на котором будет устанавливаться MaxPatrol Carbon.
2. Распаковать архив с дистрибутивом:


```
tar -xf Carbon-Application_distro_<Номер версии>.tar
```
3. В каждом из каталогов приложений распаковать архивы с ролями:


```
for i in *.tar.gz; do tar -xvzf "$i"; done
```

4. Из приложения Deployment-Application установить роль Deployer.
5. Из приложения Carbon-Application установить роли SqlStorage, Carbon, Web, Monitoring, VmStorageBusiness, RmqMessageBus, EtcdKeyValueStorage.

Внимание! Рекомендуется устанавливать роли в приведенном выше порядке. Команды в интерфейсе терминала Linux требуется выполнять от имени суперпользователя (root).

Примечание. Если в IT-инфраструктуре используется FQDN, в значениях параметров ролей рекомендуется указывать его, а не IP-адрес.

В этом разделе

[Установка роли Deployer \(см. раздел 6.1\)](#)

[Установка роли SqlStorage \(см. раздел 6.2\)](#)

[Установка роли Carbon \(см. раздел 6.3\)](#)

[Установка роли Web \(см. раздел 6.4\)](#)

[Установка роли Monitoring \(см. раздел 6.5\)](#)

[Установка роли VmStorageBusiness \(см. раздел 6.6\)](#)

[Установка роли RmqMessageBus \(см. раздел 6.7\)](#)

[Установка роли EtcdKeyValueStorage \(см. раздел 6.8\)](#)

[Установка доверенного сертификата для сайта MaxPatrol Carbon \(см. раздел 6.9\)](#)

6.1. Установка роли Deployer

Роль Deployer обеспечивает корректную установку остальных ролей MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог Deployment-Application_<Номер версии>/pt_deployer_<Номер версии>.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
5. Выберите **Basic configuration**.

6. Укажите значение параметра:

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

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

7. Нажмите **OK**.

6.2. Установка роли SqlStorage

Роль SqlStorage обеспечивает хранение данных в MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

- ▶ Чтобы установить роль:

1. Перейдите в каталог Carbon-Application_<Номер версии>/SqlStorage_<Номер версии>.
2. Запустите сценарий:
./install.sh
3. Выберите **Create New Application**.
4. Введите идентификатор приложения Carbon.
5. Нажмите **OK**.
6. Выберите **Deploy New Instance**.
7. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
9. Введите название экземпляра роли sqlstorage.
10. Нажмите **OK**.
11. Выберите **Basic configuration**.
Примечание. Чтобы включить запись данных о работе роли в журналы служб, вы можете выбрать **Advanced configuration** и установить флажок **EnableFilesLogCollection**.
12. Укажите значения параметров, приведенные в таблице ниже.
13. Нажмите **OK**.

Таблица 6. Параметры конфигурации роли SqlStorage

Параметр	Вариант конфигурации	Описание
EnableFilesLogCollection	Advanced configuration	Включена ли запись журналов в файл вместо их централизованного сбора
PgUser	Advanced configuration. Basic configuration	Логин учетной записи, от имени которой выполняется подключение к БД PostgreSQL
PgPassword	Advanced configuration. Basic configuration	Пароль учетной записи, от имени которой выполняется подключение к БД PostgreSQL
PgHardDiskType	Advanced configuration. Basic configuration	HDD или SSD (в зависимости от типа дисковой подсистемы, используемой на сервере MaxPatrol Carbon). Примечание. Вы можете определить тип дисковой подсистемы с помощью команды <code>sudo lsblk -d -o name,rota</code> (результат 0 означает SSD, 1 — HDD)

6.3. Установка роли Carbon

Роль Carbon обеспечивает реализацию основных функций MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/Carbon_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите **Deploy New Instance**.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
8. Введите название экземпляра роли carbon.
9. Нажмите **OK**.
10. Выполните одно из действий:
 - Если требуется базовая настройка роли, выберите **Basic configuration**.
 - Если требуется расширенная настройка роли, выберите **Advanced configuration**.
11. Укажите значения параметров, приведенные в таблице ниже.
12. Нажмите **OK**.

Таблица 7. Параметры конфигурации роли Carbon

Параметр	Вариант конфигурации	Описание
ApplicationDisplayName	Advanced configuration. Basic configuration	Название экземпляра приложения MaxPatrol Carbon в PT MC
ClientId	Advanced configuration	ClientId инсталляции. Внимание! Если в вашей организации установлено несколько экземпляров MaxPatrol Carbon, значение параметра ClientId должно быть уникальным для каждого экземпляра, зарегистрированного в PT MC
EnableLogToFiles	Advanced configuration	Запись данных о работе роли в журналы служб включена (True) или выключена (False)
MCUrl	Advanced configuration. Basic configuration	Адрес сервера MaxPatrol 10 с установленной ролью Management and Configuration
NccUrl	Advanced configuration. Basic configuration	Адрес сервера MaxPatrol Topology с установленной ролью NCC
SiemCoreUrl	Advanced configuration. Basic configuration	https://<IP-адрес или FQDN сервера с установленным компонентом MP 10 Core>
TopologyApiScope	Advanced configuration. Basic configuration	<ClientId сервисов топологии>.api (см. Руководство по установке MaxPatrol Topology)

Параметр	Вариант конфигурации	Описание
TopologyUrl	Advanced configuration. Basic configuration	https://<IP-адрес или FQDN сервера MaxPatrol Topology>:<Порт, используемый для взаимодействия с MaxPatrol Topology> (см. Руководство по установке MaxPatrol Topology)

6.4. Установка роли Web

Роль Web обеспечивает работу пользовательского интерфейса MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/Web_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
8. Введите название экземпляра роли web.
9. Нажмите **OK**.
10. Выберите **Basic configuration**.
11. Нажмите **OK**.

6.5. Установка роли Monitoring

Роль Monitoring обеспечивает хранение и визуализацию технических и бизнес-метрик MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/Monitoring_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
8. Введите название экземпляра роли `monitoring`.
9. Нажмите **OK**.
10. Выберите **Basic configuration**.
11. Укажите значения параметров, приведенные в таблице ниже.
12. Нажмите **OK**.
13. Нажмите **Confirm**.

Таблица 8. Параметры конфигурации роли Monitoring

Параметр	Описание
TelegramBotToken	Токен Telegram-бота, добавленного в чат (если требуется отправка сообщений в Telegram)
SupportChatId	Идентификатор Telegram-чата (если требуется отправка сообщений в Telegram)

6.6. Установка роли VmStorageBusiness

Роль VmStorageBusiness обеспечивает хранение и визуализацию технических и бизнес-метрик MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/VmStorageBusiness_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите идентификатор приложения **Carbon**.
5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
8. Введите название экземпляра роли `vmstoragebusiness`.
9. Выберите **Basic configuration**.
10. Нажмите **OK**.
11. Нажмите **Confirm**.

6.7. Установка роли RmqMessageBus

Роль RmqMessageBus обеспечивает обмен данными между микросервисами MaxPatrol Carbon.

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/RmqMessageBus_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
8. Введите название экземпляра роли `rmqmessagebus`.

9. Нажмите **OK**.
10. Выберите **Basic configuration**.
11. Укажите значения параметров, приведенные в таблице ниже.
12. Нажмите **OK**.
13. Нажмите **Confirm**.

Таблица 9. Параметры конфигурации роли

Параметр	Описание
RMQUser	Логин учетной записи, от имени которой будет выполняться подключение к веб-интерфейсу RabbitMQ
RMQPassword	Пароль учетной записи, от имени которой будет выполняться подключение к веб-интерфейсу RabbitMQ

6.8. Установка роли EtcKeyKeyValueStorage

Роль EtcKeyKeyValueStorage обеспечивает хранение данных в формате «ключ — значение».

Перед установкой роли необходимо [распаковать архив с дистрибутивом и архив роли \(см. раздел 6\)](#).

► Чтобы установить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/EtcKeyKeyValueStorage_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Create New Application**.
5. Выберите **Carbon**.
6. Выберите **Deploy New Instance**.
7. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. Выберите вариант с доменным именем сервера MaxPatrol Carbon.
9. Введите название экземпляра роли `etcdkeyvaluestorage`.
10. Нажмите **OK**.
11. Выберите **Basic configuration**.

12. В параметре **EtcRootPassword** укажите пароль, с помощью которого будет выполняться подключение к веб-интерфейсу ETCD Keeper.
13. Нажмите **OK**.

6.9. Установка доверенного сертификата для сайта MaxPatrol Carbon

При развертывании MaxPatrol Carbon для его сайта автоматически устанавливается самоподписанный сертификат безопасности, 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 ключ, зашифрованный с помощью алгоритма RSA, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.

- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Extended Key Usage (EKU) содержать записи `serverAuth` и `clientAuth`;
- 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 доверенный сертификат:

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 ролей Web и Monitoring:


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

Например:

```
SSLCertificatePemFileName: website.crt
```

```
SSLKeyFileName: website.key
```

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

7. Обновление MaxPatrol Carbon

Обновление MaxPatrol Carbon осуществляется с использованием дистрибутива.

Внимание! Для корректного обновления продукта не допускается удаление каталогов /opt/deployer и /opt/saltstack на сервере MaxPatrol Carbon.

Для обновления MaxPatrol Carbon необходимо:

1. Обратиться в Positive Technologies и получить архив с дистрибутивом с новыми версиями ролей.
2. Сохранить архив с дистрибутивом на сервер MaxPatrol Carbon (с установленной ролью Deployer).
3. Распаковать архив с дистрибутивом:
`tar -xf Carbon-Application_distro_<Номер версии>.tar`
4. В каждом из каталогов приложений распаковать архивы с ролями:
`for i in *.tar.gz; do tar -xvzf "$i"; done`
5. Обновить роль Deployer.
6. Обновить роль SqlStorage.
7. Обновить роль Carbon.
8. Обновить роль Web.
9. Обновить роль Monitoring.
10. Обновить роль VmStorageBusiness.
11. Обновить роль RmqMessageBus.
12. Обновить роль EtcKeyValueStorage.

Внимание! Роли необходимо обновлять в приведенном выше порядке. Команды в интерфейсе терминала Linux требуется выполнять от имени суперпользователя (root).

Примечание. Если в IT-инфраструктуре используется FQDN, в значениях параметров ролей рекомендуется указывать его, а не IP-адрес.

В этом разделе

[Обновление роли Deployer \(см. раздел 7.1\)](#)

[Обновление роли SqlStorage \(см. раздел 7.2\)](#)

[Обновление роли Carbon \(см. раздел 7.3\)](#)

[Обновление роли Web \(см. раздел 7.4\)](#)

[Обновление роли Monitoring \(см. раздел 7.5\)](#)

[Обновление роли VmStorageBusiness \(см. раздел 7.6\)](#)

[Обновление роли RmqMessageBus \(см. раздел 7.7\)](#)

[Обновление роли EtcdKeyValueStorage \(см. раздел 7.8\)](#)

7.1. Обновление роли Deployer

Перед обновлением роли необходимо [распаковать архив с дистрибутивом](#) и архив с новой версией роли ([см. раздел 7](#)).

► Чтобы обновить роль:

1. Перейдите в каталог `Deployment-Application_<Номер версии>/pt_deployer_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
5. Выберите **Basic configuration**.
6. Если требуется, измените значения параметров роли, указанные [в разделе об ее установке \(см. раздел 6.1\)](#).
7. Нажмите **OK**.

7.2. Обновление роли SqlStorage

Перед обновлением роли необходимо [распаковать архив с дистрибутивом](#) и архив с новой версией роли ([см. раздел 7](#)).

► Чтобы обновить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/SqlStorage_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите вариант с названием экземпляра роли `SqlStorage`.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Basic configuration**.

Примечание. Чтобы включить запись данных о работе роли в журналы служб, вы можете выбрать **Advanced configuration** и установить флажок **EnableFilesLogCollection**.

8. Если требуется, измените значения параметров роли, указанные в разделе об ее установке (см. раздел 6.2).
9. Нажмите **OK**.

7.3. Обновление роли Carbon

Перед обновлением роли необходимо распаковать архив с дистрибутивом и архив с новой версией роли (см. раздел 7).

► Чтобы обновить роль:

1. Перейдите в каталог Carbon-Application_<Номер версии>/Carbon_<Номер версии>.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите вариант с названием экземпляра роли Carbon.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Basic configuration**.
8. Если требуется, измените значения параметров роли, указанные в разделе об ее установке (см. раздел 6.3).
9. Нажмите **OK**.

7.4. Обновление роли Web

Перед обновлением роли необходимо распаковать архив с дистрибутивом и архив с новой версией роли (см. раздел 7).

► Чтобы обновить роль:

1. Перейдите в каталог Carbon-Application_<Номер версии>/Web_<Номер версии>.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.

5. Выберите вариант с названием экземпляра роли Web.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Basic configuration**.
8. Нажмите **OK**.

7.5. Обновление роли Monitoring

Перед обновлением роли необходимо [распаковать архив с дистрибутивом](#) и [архив с новой версией роли \(см. раздел 7\)](#).

► Чтобы обновить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/Monitoring_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите вариант с названием экземпляра роли Monitoring.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Basic configuration**.
8. Если требуется, измените значения параметров роли, указанные [в разделе об ее установке роли \(см. раздел 6.5\)](#).
9. Нажмите **OK**.

7.6. Обновление роли VmStorageBusiness

Перед обновлением роли необходимо [распаковать архив с дистрибутивом](#) и [архив с новой версией роли \(см. раздел 7\)](#).

► Чтобы обновить роль:

1. Перейдите в каталог `Carbon-Application_<Номер версии>/VmStorageBusiness_<Номер версии>`.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.

4. Выберите **Carbon**.
5. Выберите вариант с названием экземпляра роли VmStorageBusiness.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Skip configuration**.

7.7. Обновление роли RmqMessageBus

Перед обновлением роли необходимо [распаковать архив с дистрибутивом](#) и [архив с новой версией роли](#) (см. раздел 7).

► Чтобы обновить роль:

1. Перейдите в каталог Carbon-Application_<Номер версии>/RmqMessageBus_<Номер версии>.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите вариант с названием экземпляра роли RmqMessageBus.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Skip configuration**.

7.8. Обновление роли EtdcKeyValueStorage

Перед обновлением роли необходимо [распаковать архив с дистрибутивом](#) и [архив с новой версией роли](#) (см. раздел 7).

► Чтобы обновить роль:

1. Перейдите в каталог Carbon-Application_<Номер версии>/EtdcKeyValueStorage_<Номер версии>.
2. Запустите сценарий:
`./install.sh`
3. Нажмите **Yes**.
4. Выберите **Carbon**.
5. Выберите вариант с названием экземпляра роли EtdcKeyValueStorage.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Skip configuration**.

8. Проверка работы MaxPatrol Carbon после установки или обновления

После установки или обновления MaxPatrol Carbon вы можете выполнить базовую проверку его работоспособности:

1. Убедиться, что все Docker-контейнеры находятся в статусе Up и нет циклически перезапускаемых контейнеров. Для этого необходимо выполнить команду:

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

2. Убедиться, что в веб-интерфейсе MaxPatrol Carbon нет сообщений об ошибках.

Для входа в веб-интерфейс MaxPatrol Carbon нужно в адресной строке браузера ввести `https://<IP-адрес или FQDN сервера MaxPatrol Carbon>`.

3. В браузере перейти к инструментам разработчика и убедиться, что на вкладках сети и консоли нет сообщений об ошибках.

4. В веб-интерфейсе Grafana убедиться, что в метриках сервисов MaxPatrol Carbon нет сообщений об ошибках.

Для входа в веб-интерфейс Grafana в адресной строке браузера нужно ввести `https://<IP-адрес или FQDN сервера MaxPatrol Carbon>:9002`.

По умолчанию имя пользователя — `admin`, пароль — `P@ssw0rd`.

5. Убедиться, что граф возможных действий злоумышленника в инфраструктуре построен. Для этого нужно открыть веб-интерфейс Grafana, перейти к дашборду **General** → **Служба ТМЕ** и открыть вкладку **Граф**.

Если граф построен, на панелях вкладки отображаются действия и компоненты, а также статус **Расчет выполнен**.

6. Проверить наличие компонентов в БД MaxPatrol Carbon. Для этого необходимо выполнить запрос:

```
SELECT COUNT(id) FROM public.components;
```

7. Проверить наличие рекомендаций. Для этого в веб-интерфейсе MaxPatrol Carbon необходимо открыть страницу **Рекомендации** или выполнить запрос:

```
SELECT COUNT(id) FROM carbon.recommendations.recommendations;
```

8. Убедиться, что в файле `ResourceAssetsMapping.yaml` PDQL-запросы не содержат адресов внутренних подсетей (параметр `Address`). Для перехода к файлу нужно выполнить команду:
- ```
file=$(docker exec $(docker ps -q -f name=resources.base) bash -c "ls /usr/local/share/microservice/layers/ | grep ResourceAssetsMapping") && \
docker cp $(docker ps -q -f name=resources.base):/usr/local/share/microservice/layers/$file ./file
```

## 9. Первоначальная настройка MaxPatrol Carbon

На этапе подготовки к работе MaxPatrol Carbon необходимо выполнить сканирование активов (см. документы «Подготовка к работе MaxPatrol Carbon» и «Сканирование активов») и настроить взаимодействие MaxPatrol Carbon и MaxPatrol Topology (см. Руководство по установке MaxPatrol Topology).

### Взаимодействие с MaxPatrol Topology

MaxPatrol Topology — это компонент платформы MP 10 Core, предназначенный для оценки топологии, расчета достижимости целевых активов и визуализации инфраструктуры (см. Руководство по установке MaxPatrol Topology).

Вы можете настроить взаимодействие MaxPatrol Carbon и MaxPatrol Topology во время установки MaxPatrol Carbon или после нее.

- ▶ Чтобы настроить взаимодействие MaxPatrol Carbon и MaxPatrol Topology во время установки MaxPatrol Carbon,

укажите значения параметров конфигурации `TopologyApiScope` и `TopologyUrl`.

**Примечание.** Подробнее о параметрах конфигурации см. в Руководстве по установке MaxPatrol Topology.

- ▶ Чтобы настроить взаимодействие MaxPatrol Carbon и MaxPatrol Topology после установки MaxPatrol Carbon:

1. Откройте конфигурационный файл `/var/lib/deployed-roles/carbon-app/modelling/images/tme.extended/config/custom.env`.

2. Укажите значение параметра:

`Authentication_Scope = idmgr.api <ClientID инсталляции MaxPatrol Carbon>.api mpx.api <ClientID инсталляции MaxPatrol Topology>.api`

3. Укажите значение параметра (порт по умолчанию — 888):

`TopologyServicesSettings_TopologyUrl = https://<IP-адрес или FQDN сервера с MaxPatrol Topology>:<Порт, используемый для взаимодействия с MaxPatrol Topology>`

4. Заново соберите контейнер `tme`, выполнив команду:

`cd /var/lib/deployed-roles/carbon-app/modelling/images/tme.extended/ && docker-compose up -d`

5. Получите токен PT MC, выполнив запрос:

`curl --location --request POST 'https://<IP-адрес или FQDN сервера с установленным компонентом MP 10 Core>:3334/connect/token' \`  
`--header 'Content-Type: application/x-www-form-urlencoded' \`  
`--data-urlencode 'grant_type=client_credentials' \`  
`--data-urlencode 'client_secret= <Секретный ключ клиента MaxPatrol Carbon>' \`  
`--data-urlencode 'client_id= <ClientId инсталляции MaxPatrol Carbon>' \`

```
--data-urlencode 'scope=idmgr.api <ClientId инсталляции MaxPatrol Carbon>.api mpx.api' \
--insecure
```

6. Рассчитайте достижимость целевых активов и графа возможных действий злоумышленника в инфраструктуре, выполнив запрос:

```
curl -X POST 'https:// <IP-адрес или FQDN сервера с установленным MaxPatrol Carbon>:16792/
api/tme/v2/reachability/calculate_for_all' \
--header 'Authorization: Bearer <Токен PT MC, полученный в ответе на предыдущий запрос>' \
--insecure
```

## Построение маршрутов

Для реализации [ключевых функций продукта \(см. раздел 2\)](#) необходимо указать недопустимые события и точки входа (см. разделы «Работа с недопустимыми событиями» и «Работа с точками входа» Руководства пользователя MaxPatrol Carbon).

На основе данных о компонентах и сетевой топологии, полученных в результате сканирования активов, в системе автоматически рассчитывается [граф возможных действий злоумышленника в инфраструктуре \(см. раздел 3\)](#). На основе графа и указанных точек входа и недопустимых событий автоматически строятся возможные маршруты злоумышленника. Они отображаются в MaxPatrol Carbon на странице **Маршруты**.

В зависимости от ожидаемой активности и умений злоумышленников вы можете установить режим расчета TTA и TTD, нажав в главном меню значок .

Time to attack (TTA) — это время, за которое злоумышленник может пройти маршрут. Time to detect (TTD) — это время на обнаружение злоумышленника при его проникновении в инфраструктуру.

В MaxPatrol Carbon расчет TTA и TTD выполняется для агрессивного, умеренного и спокойного режимов действий злоумышленника. Например, TTA маршрута для агрессивного режима может быть равно 26 минут, для умеренного — 30 минут, для спокойного — 36 минут; TTD маршрута для агрессивного режима может быть равно 30 минут, для умеренного — 40 минут, для спокойного — 48 минут.

### См. также

[Архитектура MaxPatrol Carbon \(см. раздел 3\)](#)

## 10. О модели компонентов в MaxPatrol Carbon

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

Модель описана в файлах `DomainModel.xml`, расположенных в Docker-контейнерах служб MaxPatrol Carbon. 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`.

Вы можете использовать поля модели для формирования условия фильтрации при добавлении точек входа и недопустимых событий.

### В этом разделе

[Синтаксис запросов для фильтрации компонентов \(см. раздел 10.1\)](#)

[Экспорт данных об активах в табличный список \(см. раздел 10.2\)](#)

### 10.1. Синтаксис запросов для фильтрации компонентов

Вы можете добавить группу компонентов с помощью запроса: в соответствии с его условием выполняется отбор компонентов в группу. Условие запроса формируется с помощью логических выражений, в которых объединяются ключевое слово или атрибут компонента и его значение. Для составления выражений используются поля [модели компонентов](#) (см. раздел 10) MaxPatrol Carbon.

В текущей версии MaxPatrol Carbon поддерживается фильтрация компонентов, приведенных в таблице ниже.

Таблица 10. Типы компонентов

| Тип компонента                                                       | Атрибут компонента | Поле в модели данных MaxPatrol VM | Описание                                                                                     |
|----------------------------------------------------------------------|--------------------|-----------------------------------|----------------------------------------------------------------------------------------------|
| Локальная учетная запись<br><code>Credentials.LocalCredential</code> | Login              | <code>Host.User.Name</code>       | Имя учетной записи                                                                           |
|                                                                      | UserID             | <code>Host.User.ID</code>         | Идентификатор учетной записи пользователя.<br><br>В Windows — SID, в ОС семейства Unix — UID |

| Тип компонента                                          | Атрибут компонента | Поле в модели данных MaxPatrol VM            | Описание                                                                                                  |
|---------------------------------------------------------|--------------------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------|
|                                                         | Component          | —                                            | Компонент актива, на котором создана учетная запись. Допустимые значения: Windows, Linux, GitLab, vCenter |
|                                                         | Host.FQDN          | Host.FQDN                                    | Полное доменное имя актива, на котором создана учетная запись                                             |
|                                                         | Host.HostID        | Host.@id                                     | Идентификатор актива, на котором создана учетная запись                                                   |
|                                                         | Host.Hostname      | Host.Hostname                                | Имя актива, на котором создана учетная запись                                                             |
|                                                         | Host.IPAddress     | Host.Endpoints<Ip Endpoint>.Address          | IP-адрес актива, на котором создана учетная запись                                                        |
| Доменная учетная запись<br>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<br>Host.Host                            | HostID             | Host.@id                                     | Идентификатор актива                                                                                      |
|                                                         | FQDN               | Host.FQDN                                    | Полное доменное имя актива                                                                                |
|                                                         | Hostname           | Host.Hostname                                | Имя актива                                                                                                |
|                                                         | IPAddress          | Host.Endpoints<Ip Endpoint>.Address          | IP-адрес актива                                                                                           |
| Внешняя сеть<br>TME.ExternalNetwork                     | Name               | —                                            | Имя сети                                                                                                  |
|                                                         | Address.Address    | —                                            | Адрес сети                                                                                                |

| Тип компонента                                                                                | Атрибут компонента             | Поле в модели данных MaxPatrol VM                                                                                                                                    | Описание                      |
|-----------------------------------------------------------------------------------------------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                                                                                               | Address.Prefix                 | —                                                                                                                                                                    | Префикс сети                  |
| Диапазон адресов VPN TME.VPNPool<br><br><b>Примечание.</b> Поддерживается OpenVPN и Cisco ASA | AddressPool.Name               | Host.Softs<OpenVPN>.Configs<ServerConfig>.AddressPools.Name или Host.Softs<OpenVPN>.Configs<ServerConfig>.Clients.ClientName                                         | Название диапазона IP-адресов |
|                                                                                               | AddressPool.Addresses.Values   | Host.Softs<OpenVPN>.Configs<ServerConfig>.Clients.IfConfig.ClientAddress.Address или Host.Softs<OpenVPN>.Configs<ServerConfig>.AddressPools.Addresses.Values.Address | IP-адреса                     |
|                                                                                               | AddressPool.Addresses.Operator | Host.Softs<OpenVPN>.Configs<ServerConfig>.AddressPools.Addresses.Operator                                                                                            | Оператор                      |
|                                                                                               | Application.Name               | Host.Softs<OpenVPN>.Name                                                                                                                                             | Имя приложения                |
|                                                                                               | Application.Host.FQDN          | Host.FQDN                                                                                                                                                            | Полное доменное имя актива    |
|                                                                                               | Application.Host.HostID        | Host.@id                                                                                                                                                             | Идентификатор актива          |

Синтаксис запросов для фильтрации компонентов по типам: @Type = <Тип компонента>. Для типа компонента «внутренний узел», кроме условия @Type = 'Host.Host', необходимо указывать одно или несколько условий для атрибутов.

Синтаксис запросов для фильтрации компонентов с использованием атрибутов (полей модели компонентов): @Type = '<Тип компонента>' AND <Атрибут компонента> <Оператор> <Значение>. Атрибут компонентов и его значение объединяются в выражении с помощью оператора равенства (=) или неравенства (!=).

Вы можете [добавлять в условие запроса \(см. приложение A\)](#) 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.

Значение ключевого слова Type и строковые значения атрибутов необходимо указывать в одинарных кавычках.

Пример запроса для фильтрации внутренних узлов с дополнительным условием для атрибута HostID: @Type = 'Host.Host' AND HostID='1051492c-95xx-4b61-8bc2-ecb388f86bc5'.

Пример запроса для фильтрации доменных учетных записей с логинами s\_admin или admin: @Type = 'Credentials.DomainCredential' AND (Login = 's\_admin' or Login = 'admin').

## Фильтрация компонентов по табличным спискам

Если в инфраструктуре установлен MaxPatrol SIEM, вы можете отфильтровать компоненты по табличным спискам, в которые экспортированы данные об активах.

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

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

Вы можете [добавлять в условие запроса \(см. приложение A\)](#) 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.

## 10.2. Экспорт данных об активах в табличный список

Если в инфраструктуре установлен MaxPatrol SIEM, для фильтрации компонентов по табличным спискам необходимо в MaxPatrol SIEM 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 vCenter Server;
- установленным GitLab;
- установленным OpenVPN;
- 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 SIEM.

► Чтобы экспортировать данные об активах в табличный список:

1. В главном меню выберите **Активы**.
2. В панели **Группы** выберите группы, 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**.

В новой вкладке браузера откроется веб-интерфейс Knowledge Base на странице **Новый табличный список**.

5. Введите название табличного списка.
6. 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. Измените PDQL-запрос к модели активов.

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

10. Нажмите **Обновить схему**.
11. Нажмите **Создать**.
12. Нажмите **Установить в SIEM**.

## 11. Решение проблем

В этом разделе приведены инструкции по решению проблем и устранению ошибок, возникающих при работе с MaxPatrol Carbon.

### В этом разделе

[Устранение проблем при установке и обновлении MaxPatrol Carbon \(см. раздел 11.1\)](#)

[Устранение проблем при входе в MaxPatrol Carbon \(см. раздел 11.2\)](#)

[Устранение проблем, связанных с регистрацией MaxPatrol Carbon в PT MC \(см. раздел 11.3\)](#)

### 11.1. Устранение проблем при установке и обновлении MaxPatrol Carbon

В процессе установки или обновления MaxPatrol Carbon могут появляться:

- ошибки установки пакетов;
- ошибки в работе утилиты docker-compose;
- ошибки, связанные с отсутствием совместимой версии устанавливаемого пакета или с отсутствием установленного зависимого пакета;
- ошибки, связанные с наличием поврежденного пакета в ОС;
- ошибки, связанные с отсутствием прав на изменение системных каталогов в результате монтирования дополнительных разделов при подготовке виртуальной машины;
- ошибки, связанные с особенностями работы гипервизора с конкретной ОС.

Большинство этих ошибок проявляется [при установке роли Deployer \(см. раздел 6.1\)](#). В редких случаях — при установке других ролей. Ошибки обычно возникают из-за некорректных значений параметров роли (например, некорректный IP-адрес, FQDN или порт, несуществующий каталог или путь к файлу сертификата).

Результат выполнения команд записывается в журнал установки. Он создается автоматически в каталоге, из которого был запущен скрипт `./install.sh`. Имя журнала представлено в виде `install_<Название и версия роли>.log` (например, `install_Deployer_1.25.4136.log`).

Для просмотра сведений об ошибках вы можете скачать журнал установки, открыть его в текстовом редакторе (например, Notepad++ или Visual Studio Code) и найти записи, содержащие строку `Result: False`. Для воспроизведения ошибки вы можете копировать команду, которая завершилась с ошибкой, и выполнить ее в терминале.

## Ошибки при установке или обновлении роли Deployer

**Проблема № 1:** при установке или обновлении роли Deployer появляется ошибка, связанная с тем, что не найдено лицензионное соглашение (EULA) из-за невозможности определить язык ОС:

```
Submit-EulaConfirmation: /opt/deployer/bin/Start-Configuration.ps1:246
Line |
246 | ... ot ($Silent -or (Submit-EulaConfirmation -RolePackageId $Package))) {
 | ~~~~~
 | Cannot bind argument to parameter 'Language' because it is an empty string.
Write-Error: Failed to apply deployment configuration on target host
```

Возможная причина: на сервере установлена локаль C.UTF-8.

**Примечание.** Вы можете вывести список доступных локалей, выполнив команду `locale -a`.

Решение: установить локаль `en_US.UTF-8`, выполнив следующие шаги:

1. Добавить локаль: выполнить команду `nano /etc/locale.gen`, раскомментировать строку `en_US.UTF-8` и сохранить изменения.
2. Сгенерировать локали, выполнив команду `locale-gen`.
3. Вывести список доступных локалей, выполнив команду `locale -a`, и убедиться, что в выводе команды отображается локаль `en_US.UTF-8`.
4. В файл `/etc/default/locale` добавить строку `LANG=en_US.UTF-8`.
5. Перезагрузить сервер.
6. Повторно запустить установку или обновление роли Deployer.

**Проблема № 2:** при выполнении проверок, встроенных в роль Deployer, появляется сообщение об ошибке «Unsupported OS distribution generic».

Возможная причина: наличие файла `/etc/cloud-release`.

Решение: на сервере MaxPatrol Carbon удалить файл `/etc/cloud-release` (с помощью команды `sudo rm /etc/cloud-release`) и повторно запустить установку или обновление роли Deployer.

**Проблема № 3:** при установке роли Deployer на Astra Linux версии 1.7.5 отображается сообщение об ошибке `Failed to apply deployment configuration <Deployer (Deployer <Версия роли>) on carbon-astra>`, а в журнале установки отображается запись `PermissionError: [Errno 13] Permission denied: '/tmp/__salt.tmp.*'`.

Возможная причина: в Astra Linux версии 1.7.5 используется Python версии 3.7.3.

Решение: для полноценного устранения проблемы необходимо обновить Python до версии 3.7.4.

Если нет возможности обновить Python, вы можете проверить, проявляется ли проблема для файла `/etc/hosts`, выполнив команду `getfattr -d -m - -e hex /etc/hosts`. Если это так, вывод команды будет содержать:

```
getfattr: Removing leading '/' from absolute path names
file: etc/hosts
security.PDPL=0x01000000003f0000000000000000000000000000000000000000000000000000
```

В этом случае для решения проблемы нужно выполнить команду `setfattr -x security.PDPL /etc/hosts`.

## Ошибка при установке или обновлении роли Monitoring

Проблема: при установке или обновлении роли Monitoring появляется следующая ошибка:

```
An exception occurred in this state: Traceback (most recent call last):
File \"/opt/saltstack/salt/lib/python3.10/site-packages/salt/modules/file.py\", line
4114, in stats
 pstat = os.lstat(path)
FileNotFoundError: [Errno 2] No such file or directory: '/var/lib/deployed-roles/
carbon-app/monitoring-sac9/data/clickhouse/store/f24/f2406ecf-dca3-4a66-a15d-
d085c9c3ccd7/202503_1735517_1735517_0/count.txt'
```

Решение: удалить содержимое каталога `/var/lib/deployed-roles/carbon-app/monitoring/data/clickhouse/` (с помощью команды `rm -rf /var/lib/deployed-roles/carbon-app/monitoring/data/clickhouse/`) и повторно запустить установку или обновление роли Monitoring.

## Ошибка, связанная с отсутствием установленной роли при ее обновлении

Проблема: в процессе обновления той или иной роли в окне выбора экземпляра роли (**Instance selection**) отображается сообщение `Select the role instance to configure/update`, при этом список ранее установленных ролей отсутствует, а при выборе варианта **Deploy New Instance** отображается окно с сообщением `No hosts available with no role <Название роли> installed`.

Возможная причина: осуществляется обновление на более старую версию MaxPatrol Carbon (например, установлена сборка 2025.6.18, а обновление выполняется на сборку 2025.5.9), и ее невозможно выбрать.

► Чтобы устранить проблему:

1. Запустите [установку роли \(см. раздел 6\)](#) и выполните все шаги до выбора экземпляра роли (окно **Instance selection**).
2. В окне **Instance selection** нажмите **Cancel**.
3. Перейдите в каталог `/var/lib/deployer/role_instances/<Название роли>`.
4. Откройте файл `instance.yaml`.

5. В параметре `RolePackageId` укажите версию, которую необходимо установить (например, `Base_2025_5_9`).

**Внимание!** Перечисленные действия необходимо выполнять последовательно, не допускается вносить изменения в файл заранее: сначала необходимо запустить и отменить установку роли (шаги 1–2), и только после этого внести изменения в файл (шаги 3–5). Если вы внесете изменения в файл заранее, в процессе установки роли возникнет сбой на сервере.

6. Сохраните изменения и закройте файл.
7. Запустите установку роли снова.

## 11.2. Устранение проблем при входе в MaxPatrol Carbon

### Сообщение об ошибке `JWT not active yet`

Проблема: после входа в PT MC отображается сообщение об ошибке `JWT not active yet`.

Возможная причина: рассинхронизация времени на серверах PT MC и MaxPatrol Carbon.

Решение: для корректной синхронизации времени на всех узлах кластера необходимо добавить записи о NTP-серверах в конфигурационный файл.

Для Debian:

```
Установить службу ntp:
apt update
apt install ntp -f -y
Добавить NTP-серверы в конфигурационный файл:
echo "<FQDN или IP-адрес NTP-сервера>" >> /etc/ntp.conf
Перезапустить службу ntp:
systemctl restart ntp
Вывести список NTP-серверов:
ntpq -p
```

Если при выполнении команды `apt update` возникает ошибка, связанная с недоступностью зеркала, необходимо в файле `/etc/apt/sources.list` раскомментировать или добавить зеркала.

Если при выполнении команды `systemctl restart ntp` отображается сообщение `Failed to restart ntp.service: Unit ntp.service is masked`, необходимо выполнить команду:

```
systemctl unmask ntp.service
```

Для Astra Linux:

```
Удалить пакеты ntp и chronyd:
sudo apt purge ntp
sudo apt purge chrony
Включить автоматическую синхронизацию времени:
sudo timedatectl set-ntp true
```

```
Запустить службу systemd-timesyncd:
sudo systemctl start systemd-timesyncd
Проверить статус службы systemd-timesyncd:
systemctl status systemd-timesyncd
Проверить время:
timedatectl
Если System clock synchronized: no, то необходимо добавить
NTP-серверы в файл /etc/systemd/timesyncd.conf
```

## Сообщение об ошибке JWT expired

Проблема: после входа в РТ МС отображается сообщение об ошибке JWT expired.

Возможная причина: истек срок действия токена авторизации.

Решение: заново войти в РТ МС.

## Сообщение об ошибке Failed to discover OpenID issuer: Error: connect ECONNREFUSED

Проблема: после входа в РТ МС отображается сообщение об ошибке Failed to discover OpenID issuer: Error: connect ECONNREFUSED.

Возможная причина: сервер РТ МС выключен.

Решение: включить сервер РТ МС.

## Сообщение об ошибке Failed to discover OpenID issuer: Error: connect EHOSTUNREACH

Проблема: после входа в РТ МС отображается сообщение об ошибке Failed to discover OpenID issuer: Error: connect EHOSTUNREACH.

Возможная причина: сервер РТ МС стал недоступен, то есть перестал отвечать на запросы.

Решение: запустить сервер РТ МС, чтобы он стал доступен.

## Сообщение об ошибке Failed to discover OpenID issuer: Error: getaddrinfo EAI\_AGAIN

Проблема: после входа в РТ МС отображается сообщение об ошибке Failed to discover OpenID issuer: Error: getaddrinfo EAI\_AGAIN.

Возможная причина: не удалось установить соединение с сервером РТ МС.

Решение: на сервере MaxPatrol Carbon добавить записи о DNS-серверах в файл /etc/resolv.conf и перезапустить службу networking.

Пример записей о DNS-серверах с IP-адресами 10.0.0.101 и 10.0.0.102, добавленных в файл `/etc/resolv.conf`:

```
nameserver 10.0.0.101
nameserver 10.0.0.102
```

Команда для перезапуска службы `networking`:

```
sudo service networking restart
```

**Примечание.** После добавления записей о DNS-серверах в файл `/etc/resolv.conf` и перезапуска службы `networking` исправление ошибки может занять некоторое время.

## Сообщение об ошибке `Failed to discover OpenID issuer: Error: getaddrinfo ENOTFOUND`

Проблема: после входа в PT MC отображается сообщение об ошибке `Failed to discover OpenID issuer: Error: getaddrinfo ENOTFOUND`.

Возможные причины:

1. Сервер PT MC выключен.
2. В конфигурационных файлах микросервисов MaxPatrol Carbon адрес сервера PT MC указан некорректно.

Решение:

1. Включить сервер PT MC.
2. Проверить и исправить адрес сервера PT MC в конфигурационных файлах микросервисов MaxPatrol Carbon. Вероятно, адрес был указан некорректно при установке роли Base, и необходимо проверить значения параметров `MCAAddress` и `MCHostAddress`.

## Сообщение об ошибке `Failed to discover OpenID issuer: OPErr: expected 200 OK, got: 502 Bad Gateway`

Проблема: после входа в PT MC отображается сообщение об ошибке `Failed to discover OpenID issuer: OPErr: expected 200 OK, got: 502 Bad Gateway`.

Возможная причина: закончилось свободное дисковое пространство на сервере MaxPatrol Carbon.

Решение: подключиться к серверу MaxPatrol Carbon по SSH и освободить дисковое пространство (например, удалить ненужные файлы и каталоги, удалить старые записи БД ClickHouse, удалить Docker-образы старых пакетов).

Вы можете вывести список самых объемных каталогов с помощью команды `cd / && du --exclude=proc -hs * | sort -hr | head -n 20`. Обычно самыми объемными являются каталоги `/var` и `/home`. Если в каталоге `/home` есть большие файлы (например, файлы инсталлятора или архивы со старыми резервными копиями), рекомендуется удалить их. Если в каталоге `/var/lib/deployer/role_packages` есть папки со старыми версиями пакетов ролей (номер версии указан в названии папки), их также рекомендуется удалить.

► Чтобы удалить папки со старыми версиями пакетов ролей:

1. В конфигурационном файле `/etc/opt/deployer/deployer.yaml` измените значения параметров:  
`AutoCleanPackages: true` # Очистка старых пакетов ролей  
`AutoCleanRetainCount: 0` # Сколько старых пакетов необходимо оставить  
 Значение 0 означает, что все старые пакеты будут удалены и останутся только пакеты текущей версии.
2. Запустите скрипт для удаления пакетов:  
`deployer package clean`
3. Убедитесь, что в открывшемся окне представлен список старых пакетов, которые требуется удалить, и подтвердите удаление.

**Примечание.** Чтобы проверить, что пакеты удалены, вы можете выполнить команду `ls -l /var/lib/deployer/role_packages`.

Для удаления старых записей БД ClickHouse вы можете использовать следующие команды:

```
Удалить записи старше 7 дней:
find /var/lib/deployed-roles/ -type f -name "*.log" -mtime +7 -exec rm -rf {} \;
Очистить БД ClickHouse:
docker stop $(docker ps -f "name=carbon-app.monitoring" -q) && \
rm -rf /var/lib/deployed-roles/carbon-app/monitoring/data/clickhouse && \
docker start $(docker ps -a -f status=exited -q)
```

Docker-образы всех пакетов хранятся в каталоге `/var/lib/docker`. Вы можете собрать идентификаторы образов старых пакетов (версия пакетов указана в столбце TAG) и удалить их:

```
Вывести список Docker-образов, отсортированный по имени образа
(для более удобного просмотра всех версий одного пакета):
docker images | sort -k 1
Удалить образы:
docker rmi -f <Идентификатор образа 1> <Идентификатор образа 2> <Идентификатор образа 3>
```

Вы также можете удалить все неиспользуемые образы, у которых нет активных контейнеров, с помощью команды `docker image prune -a`.

## 11.3. Устранение проблем, связанных с регистрацией MaxPatrol Carbon в PT MC

### Возможные причины

1. Отсутствует сетевая достижимость между узлами MaxPatrol Carbon и PT MC.
2. MaxPatrol Carbon не зарегистрирован в PT MC или был удален из него.

## Решение

1. Проверьте доступность между узлами MaxPatrol Carbon и PT MC, параметры портов и правила межсетевого экрана.
2. Повторно зарегистрируйте MaxPatrol Carbon в PT MC.

► Чтобы проверить доступность между MaxPatrol Carbon и PT MC:

1. Выполните проверку доступности на узле MaxPatrol Carbon:  
`ping -c 3 mpx-host.ptsecurity.com`
2. Выполните проверку доступности на узле PT MC:  
`ping -c 3 carbon-host.ptsecurity.com`
3. Если один из узлов недоступен, обратитесь к сетевому администратору.
4. Если проверки прошли успешно, просмотрите информацию о портах 80, 443 и 3334:  
`netstat -tulnp | grep -E "80|443|3334"`
5. Просмотрите текущие правила межсетевого экрана:  
`iptables -L -n`
6. Если порты и `iptables` настроены корректно, обратитесь к сетевому администратору.

Если MaxPatrol Carbon не зарегистрирован в PT MC или был удален из него, нужно зарегистрироваться снова.

► Чтобы зарегистрировать приложение MaxPatrol Carbon в PT MC:

1. Создайте резервную копию базы данных микросервиса Registration:  
`docker exec -i $(docker ps -f "name=storage-postgres" -q) /bin/bash -c "PGPASSWORD=P@ssw0rdP@ssw0rd pg_dump -U pt_system registration" > ~/dump_registration.sql`
2. Остановите контейнер Registration:  
`docker stop $(docker ps -f "name=registration" -q)`
3. Удалите БД Registration:  
`docker exec -i $(docker ps -f "name=storage-postgres" -q) /bin/bash -c 'dropdb registration --force -U pt_system'`
4. Запустите установку [роли Carbon \(см. раздел 6.3\)](#):  
`cd Carbon-Application_<Номер версии>/Carbon_<Номер версии>  
./install.sh`
5. В процессе установки выберите **Advanced configuration**.
6. Укажите новое значение параметра `ClientId`.
7. Подтвердите реконфигурацию ролей.
8. Завершите установку роли Carbon.

## Приложение А. PDQL-запросы данных об активах

Для добавления информации о точках входа и недопустимых событиях в MaxPatrol Carbon вы можете использовать данные, полученные из табличных списков MaxPatrol SIEM. В этом разделе приводятся PDQL-запросы, с помощью которых можно отфильтровать информацию об активах для наполнения табличных списков.

### В этом разделе

[Активы с Windows \(см. приложение A.1\)](#)

[Активы службы каталогов Active Directory \(см. приложение A.2\)](#)

[Активы с ОС семейства Unix \(см. приложение A.3\)](#)

[Активы с VMware vCenter Server \(см. приложение A.4\)](#)

[Активы с GitLab \(см. приложение A.5\)](#)

[Активы с OpenVPN \(см. приложение A.6\)](#)

### A.1. Активы с Windows

Вы можете отфильтровать данные об активах, на которых установлена 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](https://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](https://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](https://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)
```

## A.3. Активы с ОС 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 vCenter Server

Вы можете отфильтровать данные об активах с установленным VMware vCenter Server 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 Server;
- `Sessions.ImpersonateUser` — выполнение действий от имени другого пользователя.

Для расширений VMware vCenter Server предусмотрены дополнительные привилегии. Подробнее о привилегиях в VMware vCenter Server см. на сайте [vmware.com](https://www.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)

```

## A.6. Активы с OpenVPN

Вы можете отфильтровать данные об активах с OpenVPN, которые нужно экспортировать в табличный список, с помощью PDQL-запросов, приведенных в этом разделе.

Для отбора активов на конкретном узле вы можете добавить `Host.@Id = $HostID` в первое условие фильтрации в виде `filter(Host.@Id = $HostID and Host.Softs<OpenVPN>.Configs<ServerConfig>) |`. Переменную `$HostID` необходимо заменить на идентификатор узла.

## Получение списка активов, выделяющих динамические диапазоны адресов (без привязки к пользователям)

```
filter(Host.Softs<OpenVPN>.Configs<ServerConfig>) |
select(
 Host.@Id as HostID,
 Host.Softs<OpenVPN>.Configs<ServerConfig>.AddressPools.Name as PoolName,
 Host.Softs<OpenVPN>.Configs<ServerConfig>.Port as Instance,
 Host.Softs<OpenVPN>.Configs<ServerConfig>.AddressPools.Addresses.Operator as
 Operator,
 compact(Host.Softs<OpenVPN>.Configs<ServerConfig>.AddressPools.Addresses.Values) as
 Address
) |
calc("OpenVPN" as Component) |
filter(
 Address != NULL
 and Operator != 'eq'
) |
select(HostID, Component, Instance, PoolName, Operator, Address)
```

## Получение списка активов, выделяющих статические адреса (с привязкой к пользователям)

```
filter(Host.Softs<OpenVPN>.Configs<ServerConfig>) |
select(
 Host.@Id as HostID,
 Host.Softs<OpenVPN>.Configs<ServerConfig>.Clients.ClientName as PoolName,
 Host.Softs<OpenVPN>.Configs<ServerConfig>.Port as Instance,
 Host.Softs<OpenVPN>.Configs<ServerConfig>.Clients.IfConfig.ClientAddress.Address
 as Address
) |
calc("OpenVPN" as Component) |
calc("eq" as Operator) |
filter (
 Address != NULL
 and Address != 0.0.0.0
) |
select(HostID, Component, Instance, PoolName, Operator, Address)
```

# Глоссарий

## **граф**

Представление инфраструктуры в виде множества связей, состоящих из активов, их компонентов (ПО, портов, уязвимостей, учетных записей) и возможных действий злоумышленников.

## **действие**

Описание возможного действия злоумышленника по захвату (компрометации) целевых компонентов активов при наличии компонентов-источников.

## **маршрут**

Уникальная упорядоченная последовательность компонентов активов и действий от точки входа до компонента, позволяющего выполнить сценарий реализации недопустимого события.

## **рекомендация**

Набор изменений, которые необходимо выполнить в IT-инфраструктуре для предотвращения недопустимых событий и усложнения сценариев их реализации.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.