



MaxPatrol 360

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: 11.08.2026

Содержание

1.	Об этом документе.....	5
2.	Обзор MaxPatrol 360	6
3.	Развертывание MaxPatrol 360	8
3.1.	Аппаратные и программные требования	10
3.2.	Настройка ядра Astra Linux типа hardened	11
3.3.	Установка роли Deployer	11
3.4.	Установка компонента PT MC	12
3.4.1.	Установка роли SqlStorage	13
3.4.2.	Установка роли LogConnector	14
3.4.3.	Установка роли Observability	15
3.4.4.	Установка роли Grafana	16
3.4.5.	Установка роли PT MC	17
3.5.	Установка компонента Knowledge Base	19
3.6.	Установка компонента ReportingPortal	20
3.7.	Установка компонента MaxPatrol 360	22
3.7.1.	Установка роли Central Management Console	22
3.7.2.	Установка ролей Incident Management, Playbooks и Requests	23
3.8.	Активация PT MC	24
3.9.	Подтверждение регистрации приложения MaxPatrol 360	25
3.10.	Активация лицензии	26
3.11.	Деактивация лицензии	26
4.	Обновление MaxPatrol 360	28
4.1.	Обновление роли Deployer	29
4.2.	Обновление компонента PT MC	30
4.2.1.	Обновление роли SqlStorage	30
4.2.2.	Обновление роли LogConnector	32
4.2.3.	Обновление роли Observability	33
4.2.4.	Обновление роли Grafana	34
4.2.5.	Обновление роли Management and Configuration	35
4.3.	Обновление компонента Knowledge Base	36
4.4.	Обновление компонента ReportingPortal	37
4.5.	Обновление компонента MaxPatrol 360	38
5.	Импорт объектов экспертизы в Knowledge Base	40
6.	Настройка DNS-сервера для перехода между тенантами в интерфейсе MaxPatrol 360	41
7.	Установка доверенного сертификата для сайта MaxPatrol 360	43
8.	Изменение конфигурации роли	45
9.	Резервное копирование и восстановление данных MaxPatrol 360	46
9.1.	Создание резервной копии данных	46
9.2.	Восстановление данных из резервной копии	47
9.3.	Расположение пользовательских сертификатов	49
10.	Пользователи и права доступа	51

11. Настройка компонентов после изменения IP-адресов или FQDN их серверов	52
Приложение. Параметры конфигурации ролей MaxPatrol 360.....	54
Глоссарий.....	81

1. Об этом документе

Руководство содержит справочную информацию и инструкции по развертыванию, настройке и администрированию MaxPatrol 360.

Документ адресован специалистам, выполняющим установку, первоначальную настройку и администрирование MaxPatrol 360.

Комплект документации MaxPatrol 360 включает в себя следующие документы:

- Этот документ.
- Руководство пользователя — содержит пошаговые инструкции и справочную информацию об использовании продукта для защиты информационных активов организации (тенанта).
- Руководство разработчика — содержит информацию для интеграции MaxPatrol 360 со сторонними приложениями.

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

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

2. Обзор MaxPatrol 360

Что такое MaxPatrol 360

MaxPatrol 360 представляет собой систему централизованного управления инцидентами для организаций любого масштаба — от корпоративных центров мониторинга безопасности до поставщиков услуг в области ИБ.

MaxPatrol 360 помогает выстроить полный цикл работы с инцидентами, зарегистрированными на тенантах (предприятиях с установленным MaxPatrol 10), обеспечивая сбор данных об инцидентах, их анализ и расследование. Единая система управления инцидентами позволяет достичь высокого уровня прозрачности процессов и эффективности работы с инцидентами, что значительно повышает защищенность IT-инфраструктуры тенантов.

Ключевые особенности MaxPatrol 360:

- единый веб-интерфейс для централизованного управления инцидентами в структурах любого масштаба;
- возможность интеграции с внешними системами для получения информации об инцидентах;
- распространение экспертной логики для обнаружения инцидентов;
- использование ролевой модели доступа для защиты данных.

Основные возможности

MaxPatrol 360 позволяет:

- собирать сведения об инцидентах, зафиксированных на тенантах, а также регистрировать инциденты вручную;
- назначать ответственных за работу с инцидентами, обрабатывать инцидент и сохранять результаты работы в его карточке;
- направлять уведомления об инцидентах в MAX, Telegram или по электронной почте;
- направлять уведомления об инцидентах в систему ГосСОПКА;
- направлять запросы по инцидентам в систему ФинЦЕРТ;
- управлять тенантами, настраивать доступ к ним и просматривать приложения на тенантах;
- создавать пакеты распространения экспертизы из наборов для установки Knowledge Base, доставлять пакеты на выбранные тенанты и устанавливать объекты экспертизы в конвейеры тенантов;
- отправлять сервис-провайдеру и тенанту запросы для решения задач, не требующих немедленного реагирования;
- автоматизировать рутинные операции, связанные с обработкой инцидента, с помощью сценариев;

- настраивать интеграции с внешними системами для автоматизации работы с инцидентами;
- отслеживать состояние безопасности IT-инфраструктуры tenants с помощью дашборда **Инциденты**.

3. Развертывание MaxPatrol 360

MaxPatrol 360 поставляется в виде архива, который содержит папки с дистрибутивами [ролей](#) (см. [раздел 3](#)).

Для установки MaxPatrol 360 необходимо:

1. Скопировать архив с дистрибутивом на сервер, где будет устанавливаться MaxPatrol 360, и распаковать архив.
2. Последовательно установить на сервер компоненты MaxPatrol 360 из комплекта поставки: Deployer → PT MC → Knowledge Base → ReportingPortal → MaxPatrol 360.

Внимание! MaxPatrol 360 поддерживает работу с MaxPatrol 10 версий 27.2—27.6.

Работа компонентов ReportingPortal, Playbooks и Dashboards поддерживается только при наличии соответствующей лицензии.

3. [Активировать](#) (см. [раздел 3.8](#)) PT MC.
4. [Подтвердить регистрацию приложения](#) (см. [раздел 3.9](#)) MaxPatrol 360 в PT MC.
5. [Активировать лицензию](#) (см. [раздел 3.10](#)) MaxPatrol 360.
6. [Импортировать объекты экспертизы](#) (см. [раздел 5](#)) в Knowledge Base.
7. Если требуется переключаться между тенантами в веб-интерфейсе MaxPatrol 360 — [настроить DNS-сервер](#) (см. [раздел 6](#)).

Подготовка к развертыванию

Перед установкой MaxPatrol 360 необходимо проверить, что сервер MaxPatrol 360 соответствует аппаратным и программным требованиям.

При использовании FQDN в качестве адресов компонентов MaxPatrol 360 необходимо настроить и обеспечить доступность DNS для корректного разрешения имен узлов в IP-адреса. Работа с локальным DNS, например systemd-resolved или dnsmasq, не поддерживается.

Если предполагается установка MaxPatrol 360 на ядро Astra Linux типа hardened, то для корректной работы Docker-контейнеров перед установкой необходимо выполнить [настройку ядра](#) (см. [раздел 3.2](#)).

Об установке компонентов MaxPatrol 360 с помощью ролей

Роль является базовой единицей развертывания MaxPatrol 360 и представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Каждая роль поставляется в виде отдельного архива, который может содержать Docker-образы или deb-пакеты.

При развертывании системы создаются экземпляры ролей, которые распределяются по приложениям определенного типа. 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 Management and Configuration содержит роли SqlStorage, LogConnector, Observability, Grafana и Management and Configuration;
- приложение Knowledge Base содержит роль Knowledge Base;
- приложение Reporting Portal содержит роль Dashboards;
- приложение MaxPatrol 360 содержит роли Central Management Console, Incident Management, Playbooks и Requests.

В общем случае установка роли делится на следующие этапы:

1. Распаковка архива и запуск сценария установки.

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

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

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

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

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

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

В этом разделе

[Аппаратные и программные требования \(см. раздел 3.1\)](#)

[Настройка ядра Astra Linux типа hardened \(см. раздел 3.2\)](#)

[Установка роли Deployer \(см. раздел 3.3\)](#)

[Установка компонента PT MC \(см. раздел 3.4\)](#)

[Установка компонента Knowledge Base \(см. раздел 3.5\)](#)

[Установка компонента ReportingPortal \(см. раздел 3.6\)](#)

[Установка компонента MaxPatrol 360 \(см. раздел 3.7\)](#)

[Активация PT MC \(см. раздел 3.8\)](#)

[Подтверждение регистрации приложения MaxPatrol 360 \(см. раздел 3.9\)](#)

[Активация лицензии \(см. раздел 3.10\)](#)

[Деактивация лицензии \(см. раздел 3.11\)](#)

3.1. Аппаратные и программные требования

Аппаратные требования

MaxPatrol 360 может быть установлен как на физическом сервере, так и в виртуальной среде.

Внимание! Установка компонентов системы возможна только на серверы с процессорами, поддерживающими инструкции SSE 4.2.

Таблица 2. Аппаратные требования к серверу MaxPatrol 360

Компонент сервера	Минимальные требования
Количество логических ядер в системе виртуализации ¹	10
Память (ОЗУ)	26 ГБ
Твердотельный накопитель (SSD)	200 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

Программные требования

Все компоненты MaxPatrol 360 поддерживают установку на 64-разрядные версии следующих ОС:

- Astra Linux Special Edition 1.7.5—1.7.9 и 1.8.4 (на базе ядра Linux версии 5.15 и выше);
- Debian 11 и 12 (на базе ядра Linux версии 5.10 и выше).

Для работы в интерфейсе MaxPatrol 360 рекомендуется использовать последние версии браузеров Google Chrome, Mozilla Firefox, Microsoft Edge или Яндекс Браузер.

¹ Соответствует количеству потоков в физических ядрах процессора с включенной технологией Hyper-Threading. Рекомендуется использовать процессоры Intel Xeon Scalable второго поколения и выше или их аналоги.

3.2. Настройка ядра Astra Linux типа hardened

Для корректной работы Docker-контейнеров с операционной системой Astra Linux с типом ядра hardened необходимо, чтобы в Docker использовались компоненты cgroups версии 1. Для этого до установки MaxPatrol 360 необходимо настроить ядра типа hardened на всех серверах с Astra Linux.

► Чтобы настроить ядро Astra Linux:

1. Откройте конфигурационный файл `/etc/default/grub`.
2. В строку `GRUB_CMDLINE_LINUX_HARDENED` добавьте параметр `systemd.unified_cgroup_hierarchy` со значением 0.

Например:

```
GRUB_CMDLINE_LINUX_HARDENED="slub_debug=P page_poison=1 slab_nomerge
user.max_user_namespaces=0 kernel.kptr_restrict=1 vsyscall=none
systemd.unified_cgroup_hierarchy=0"
```

3. Сохраните файл и выполните команду:
`update-grub`
4. Перезагрузите сервер.

Вы можете проверить, применились ли изменения, выполнив команду `cat /proc/cmdline`: в параметрах ядра появится добавленная строка. Если на сервере уже установлен Docker, узнать используемую версию контрольной группы можно с помощью команды `docker info`: если изменения применились, параметр `Cgroup Driver` будет иметь значение `systemd`, а параметр `Cgroup Version` — 1.

3.3. Установка роли Deployer

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

Внимание! Для корректной работы MaxPatrol 360 необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в вашей организации. По умолчанию система виртуализации Docker использует подсеть 172.17.0.0/12. Если эта подсеть уже используется вашим оборудованием, вы можете изменить подсеть во время развертывания MaxPatrol 360 при установке роли Deployer. Для этого в наборе конфигурационных параметров **Advanced configuration** необходимо указать в качестве значения параметра `CustomDockerAddressPool` подсеть, отличную от используемых в вашей организации, а в качестве значения параметра `CustomDockerNetworkSize` — размер подсетей, которые будут выделяться из диапазона, указанного в параметре `CustomDockerAddressPool`. При указании размера подсетей рекомендуется использовать значение, не превышающее 25 бит.

► Чтобы установить роль:

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

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

```
pt_deployer_<Номер версии>/install.sh --os-packages-path <Полный путь к каталогу с распакованным дистрибутивом продукта>/os_packages
```
3. Нажмите **Yes**.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
5. Выберите **Basic configuration**.
6. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль Deployer.

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

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.4. Установка компонента PT MC

PT MC устанавливается с помощью ролей в следующем порядке: `SqlStorage` → `LogConnector` → `Observability` → `Management and Configuration`.

В этом разделе

[Установка роли `SqlStorage` \(см. раздел 3.4.1\)](#)

[Установка роли `LogConnector` \(см. раздел 3.4.2\)](#)

[Установка роли `Observability` \(см. раздел 3.4.3\)](#)

[Установка роли `Grafana` \(см. раздел 3.4.4\)](#)

[Установка роли PT MC \(см. раздел 3.4.5\)](#)

3.4.1. Установка роли SqlStorage

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

► Чтобы установить роль:

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

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

```
pt_sqlstorage_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки.
4. Выберите **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и 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, на который устанавливается роль.
9. Введите название экземпляра роли SqlStorage и нажмите **OK**.
10. Выберите вариант **Basic configuration**.
11. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль SqlStorage.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.

12. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

13. Нажмите **OK**.

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.4.2. Установка роли LogConnector

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

► Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив

`pt_logconnector_<Номер версии>.tar.gz`:

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

2. Запустите сценарий:

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

3. Нажмите **Yes**.

Начнутся распаковка и подготовка пакетов, необходимых для установки.

4. Выберите вариант с идентификатором приложения `Management and Configuration`.

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, на который устанавливается роль.

8. Введите название экземпляра роли `LogConnector` и нажмите **OK**.

9. Выберите вариант **Basic configuration**.

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

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.

11. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.4.3. Установка роли Observability

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

► Чтобы установить роль:

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

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

```
pt_observability_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения `Management and Configuration`.
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, на который устанавливается роль.
8. Введите название экземпляра роли `Observability` и нажмите **OK**.
9. Выберите вариант **Basic configuration**.
10. В качестве значений параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера, на который устанавливается роль `Observability`.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.
11. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение **Warning** или **Error**.

Примечание. Если в результате проверки отобразилось сообщение **Warning**, вы можете продолжить установку, нажав клавишу **Y**. Чтобы включить режим установки, при котором сообщения **Warning** будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

12. Нажмите **OK**.

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.4.4. Установка роли Grafana

Установка роли Grafana не является обязательной, но рекомендуется для доступа к средству визуализации и мониторинга данных Grafana.

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

► Чтобы установить роль Grafana:

1. На сервере с установленной ролью **Deployer** распакуйте архив `pt_grafana_<Номер версии>.tar.gz`:

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

```
pt_grafana_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения **Management and Configuration**.
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 **PT MC**.
8. Введите название экземпляра роли Grafana и нажмите **OK**.
9. Выберите вариант **Basic configuration**.

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

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.

11. Нажмите **ОК**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

12. Нажмите **ОК**.

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

После установки роли Grafana вы можете просматривать ключевые показатели приложений и метрики серверов, на которых установлены компоненты MaxPatrol 360. Метрики отображаются на дашбордах Grafana по адресу: `https://<IP-адрес или FQDN сервера компонента>:9002`.

Для первого входа в веб-интерфейс Grafana необходимо ввести логин и пароль учетной записи (по умолчанию `admin` и `P@ssw0rd`). Вы можете [изменить \(см. раздел 8\)](#) эти значения в параметрах роли `GrafanaAdminLogin` и `GrafanaAdminPassword` соответственно.

3.4.5. Установка роли PT MC

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

► Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_managementandconfiguration_<Номер версии>.tar.gz`:
`tar -xf pt_managementandconfiguration_<Номер версии>.tar.gz`
2. Запустите сценарий:
`pt_managementandconfiguration_<Номер версии>/install.sh`
3. Нажмите **Yes**.
- Начнутся распаковка и подготовка пакетов, необходимых для установки.
4. Выберите вариант с идентификатором приложения Management and Configuration.
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, на который устанавливается роль.
8. Введите название экземпляра роли Management and Configuration и нажмите **OK**.
9. Выберите вариант **Basic configuration**.
10. В качестве значений параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера, на который устанавливается роль Management and Configuration.
- Внимание!** Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.
11. В качестве значения параметра `DefaultLocale` выберите язык веб-интерфейса приложения Management and Configuration.
12. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.5. Установка компонента Knowledge Base

Компонент устанавливается с помощью роли Knowledge Base. Для установки роли вам потребуется архив `pt_kb_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

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

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

```
pt_kb_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
 Начнутся распаковка и подготовка пакетов, необходимых для установки.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Knowledge Base и 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, на который устанавливается роль.
9. В открывшемся окне введите название экземпляра роли Knowledge Base и нажмите **OK**.
10. Выберите **Advanced configuration**.
11. В качестве значения параметра `DefaultLocale` выберите язык интерфейса приложения Knowledge Base.
12. Укажите значения параметров:

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

Внимание! Если в параметре `DeploymentType` указать значение `siem`, то компонент Knowledge Base не будет работать.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.
13. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

14. Нажмите **OK**.

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

Компонент Knowledge Base в составе MaxPatrol 360 поставляется без базы знаний SIEM Content, поэтому после завершения установки необходимо [создать базу знаний и импортировать в нее объекты экспертизы \(см. раздел 5\)](#).

3.6. Установка компонента ReportingPortal

Компонент устанавливается с помощью роли `ReportingPortal`. Для установки роли вам потребуется архив `pt_reportingportal_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

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

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

```
pt_reportingportal_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения `Reporting Portal` и 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, на который устанавливается роль.

9. В открывшемся окне введите название экземпляра роли ReportingPortal и нажмите **OK**.
10. Выберите **Advanced configuration**.
11. Снимите флажок **EnablePullModel**.

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

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Необходимо указать IP-адрес или FQDN сервера.

13. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение Warning или Error.

Примечание. Если в результате проверки отобразилось сообщение Warning, вы можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения Warning будут автоматически игнорироваться, необходимо использовать ключ --silent при запуске сценария install.sh.

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

14. Нажмите **OK**.

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий install.sh, формируется каталог installReports с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

Компонент Reporting Portal обеспечивает работу с дашбордом **Инциденты**, на котором представлена статистическая информация об инцидентах, выявленных на тенантах.

Для корректной работы дашборда приложение Reporting Portal должно содержать датасеты, приведенные ниже. Для просмотра датасетов нужно в главном меню MaxPatrol 360 нажать ☰ → **Reporting Portal**, затем в главном меню Reporting Portal нажать кнопку **Датасеты**.

Внимание! Для корректной работы датасетов должна быть запущена служба IncidentReadModel.

Датасеты, необходимые для работы дашборда:

- dataschema_Incidents_time_to_qualify;
- dataschema_Incidents_queue_wait_time;
- dataschema_Incidents_time_to_contain;

- `dataschema_Incidents_time_to_transmit;`
- `dataschema_Incidents_incident_events.`

3.7. Установка компонента MaxPatrol 360

MaxPatrol 360 устанавливается с помощью ролей в следующем порядке: Central Management Console → Incident Management → Playbooks → Requests.

В этом разделе

[Установка роли Central Management Console \(см. раздел 3.7.1\)](#)

[Установка ролей Incident Management, Playbooks и Requests \(см. раздел 3.7.2\)](#)

3.7.1. Установка роли Central Management Console

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

► Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_cmc_<Номер версии>.tar.gz`:
`tar -xf pt_cmc_<Номер версии>.tar.gz`
2. Запустите сценарий:
`pt_cmc_<Номер версии>/install.sh`
3. Нажмите **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки.
4. Выберите **Create New Application**.
5. Введите идентификатор приложения MaxPatrol 360.
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, на который устанавливается роль.
9. Введите название экземпляра роли Central Management Console и нажмите **OK**.
10. Выберите **Advanced configuration**.
11. Если требуется переключаться между тенантами в веб-интерфейсе MaxPatrol 360, снимите флажок **DisableTenantLocator**.

12. Укажите значения параметров:

HostAddress: <IP-адрес или FQDN сервера, на который устанавливается роль Central Management Console>

PostgreHost: <IP-адрес или FQDN сервера с установленной СУБД PostgreSQL>

PostgrePort: <Порт для доступа к СУБД PostgreSQL>

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

13. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение Warning или Error.

Примечание. Если в результате проверки отобразилось сообщение Warning, вы можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения Warning будут автоматически игнорироваться, необходимо использовать ключ --silent при запуске сценария install.sh.

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

14. Нажмите **OK**.

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий install.sh, формируется каталог installReports с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.7.2. Установка ролей Incident Management, Playbooks и Requests

Для установки каждой из ролей Incident Management, Playbooks и Requests нужно выполнить инструкцию, приведенную в этом разделе. Для установки роли вам потребуется ее архив из комплекта поставки.

► Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив с дистрибутивом роли:
`tar -xf <Название архива>.tar.gz`
2. Запустите сценарий:
`<Название архива>/install.sh`
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения MaxPatrol 360.

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, на который устанавливается роль.
8. Введите название экземпляра роли и нажмите **OK**.
9. Выберите **Skip configuration**.
10. Нажмите **OK**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

В результате установки роли (в том числе и неуспешной) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.8. Активация PT MC

Активация выполняется в интерфейсе PT MC. Перед началом активации необходимо войти в PT MC по ссылке `https://<IP-адрес или FQDN сервера PT MC>/mc`. Для входа вам потребуются логин и пароль служебной учетной записи с ролью администратора; также необходимо знать тип учетной записи (локальная или доменная).

Для активации PT MC вам потребуется ZIP-файл ключа инсталляции.

Онлайн-активация

- Чтобы активировать PT MC при наличии доступа к серверу обновлений `update.ptsecurity.com`:

1. На странице **Активация платформы** выберите ZIP-файл ключа инсталляции.
2. Нажмите **Активировать**.

Офлайн-активация

- Чтобы активировать РТ МС при отсутствии доступа к серверу обновлений update.ptsecurity.com:

1. Внизу страницы **Активация платформы** нажмите **Перейти к офлайн-активации**.
2. На странице **Загрузка ключа инсталляции** выберите ZIP-файл ключа инсталляции.
3. Нажмите **Далее**.
4. Нажмите **Скачать файл**.

Начнется скачивание файла фингерпринта.

5. Отправьте файл фингерпринта сотруднику вашей компании, ответственному за работу с лицензиями.

Ответственный сотрудник передаст файл фингерпринта менеджеру Positive Technologies, представителю компании-интегратора или в службу технической поддержки. После этого ответственный сотрудник передаст вам ZIP-файл с лицензиями, который необходимо использовать на следующем шаге активации.

6. Нажмите **Далее**.
7. Выберите ZIP-файл с лицензиями, полученный от ответственного сотрудника.
8. Нажмите **Далее**.

3.9. Подтверждение регистрации приложения MaxPatrol 360

После установки MaxPatrol 360 вам нужно подтвердить регистрацию приложения MaxPatrol 360 в РТ МС.

- Чтобы подтвердить регистрацию приложения:

1. В главном меню нажмите  → **Management and Configuration**.
2. В главном меню нажмите .
3. На схеме площадок выберите **MaxPatrol 360**.
4. Нажмите **Подтвердить**.

После подтверждения регистрации сессия автоматически завершается. Чтобы продолжить работу, нужно повторить вход в РТ МС.

3.10. Активация лицензии

Для работы MaxPatrol 360 необходимо активировать его лицензию. До активации лицензии нужно активировать РТ МС, а также подтвердить регистрацию приложения MaxPatrol 360 в РТ МС.

Для того чтобы активировать лицензию, нужно добавить ее в РТ МС и привязать к приложению MaxPatrol 360.

► Чтобы добавить лицензию при наличии доступа к интернету:

1. В главном меню нажмите  → **Management and Configuration**.
2. В главном меню нажмите .
3. Нажмите **Обновить список лицензий**.

Для добавления лицензии вручную вам потребуется архив с лицензией из комплекта поставки.

► Чтобы добавить лицензию без доступа к интернету:

1. В главном меню нажмите  → **Management and Configuration**.
2. В главном меню нажмите .
3. Нажмите **Добавить**.
4. Выберите архив с лицензией.
5. Нажмите **Добавить**.

► Чтобы привязать лицензию:

1. В главном меню нажмите  → **Management and Configuration**.
2. В главном меню нажмите .
3. В строке лицензии MaxPatrol 360 нажмите **Привязать**.
4. Нажмите **Привязать**.

3.11. Деактивация лицензии

► Чтобы деактивировать лицензию:

1. В главном меню нажмите  → **Management and Configuration**.
2. В главном меню нажмите .
3. Выберите лицензию.
4. В панели инструментов нажмите  → **Деактивировать платформу**.

5. Установите флажок **Я понимаю, что могу потерять доступ к приложениям и их данным.**
6. Нажмите **Деактивировать.**

4. Обновление MaxPatrol 360

Базовыми единицами установки и обновления MaxPatrol 360 являются роли. Для обновления системы нужно обратиться в Positive Technologies и получить дистрибутивы с новыми версиями ролей.

Перед обновлением необходимо на сервере MaxPatrol 360 выполнить следующие команды:

```
rm /etc/apt/sources.list.d/deployer_role_packages.list
rm /etc/apt/sources.list.d/os_specific_packages.list
```

Если MaxPatrol 360 установлен в качестве отдельной системы, то для обновления необходимо:

1. Сохранить архив с дистрибутивом на сервер MaxPatrol 360.
2. Распаковать архив с дистрибутивом.
3. Обновить роль Deployer.
4. Обновить компонент PT MC.
5. Обновить компонент Knowledge Base.
6. Обновить компонент ReportingPortal.
7. Обновить компонент MaxPatrol 360.
8. [Деактивировать \(см. раздел 3.11\)](#) текущую лицензию, а затем [активировать \(см. раздел 3.10\)](#) новую.

Внимание! Обновление ролей и компонентов необходимо выполнять в приведенном выше порядке.

Если MaxPatrol 360 установлен с действующим MaxPatrol 10 (обе системы используют один экземпляр PT MC), то для обновления необходимо:

1. Обновить компоненты MaxPatrol 10. Инструкции по обновлению компонентов приведены в Руководстве администратора MaxPatrol 10.
2. Если MaxPatrol 360 и MaxPatrol 10 установлены на разных серверах — обновить компоненты ReportingPortal и MaxPatrol 360 из комплекта поставки MaxPatrol 360.
3. Если системы установлены на одном сервере — обновить роль Deployer и компоненты ReportingPortal и MaxPatrol 360 из комплекта поставки MaxPatrol 360.
4. [Деактивировать \(см. раздел 3.11\)](#) текущую лицензию, а затем [активировать \(см. раздел 3.10\)](#) новую.

В этом разделе

[Обновление роли Deployer \(см. раздел 4.1\)](#)

[Обновление компонента PT MC \(см. раздел 4.2\)](#)

[Обновление компонента Knowledge Base \(см. раздел 4.3\)](#)

[Обновление компонента ReportingPortal \(см. раздел 4.4\)](#)

[Обновление компонента MaxPatrol 360 \(см. раздел 4.5\)](#)

См. также

[Деактивация лицензии \(см. раздел 3.11\)](#)

[Активация лицензии \(см. раздел 3.10\)](#)

4.1. Обновление роли Deployer

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

► Чтобы обновить роль:

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

```
tar -xzf pt_deployer_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_deployer_<Номер версии>/install.sh --os-packages-path <Полный путь к каталогу с распакованным дистрибутивом продукта>/os_packages
```
3. Нажмите **Yes**.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
5. Выберите **Basic configuration**.
6. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который установлена роль Deployer.
7. Нажмите **OK**.

Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
8. Нажмите **OK**.
9. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
10. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.2. Обновление компонента PT MC

Для обновления компонента PT MC необходимо:

1. Обновить роль SqlStorage.
2. Обновить роль LogConnector.
3. Обновить роль Observability.
4. Обновить роль Grafana.
5. Обновить роль Management and Configuration.

Для корректной работы MaxPatrol 360 значения одноименных параметров ролей Observability и Grafana должны совпадать. Если вы ранее устанавливали собственные значения для параметров роли Observability и такие параметры используются в роли Grafana, необходимо указать те же значения для параметров этой роли. Для этого перед обновлением PT MC необходимо выполнить следующие действия:

1. Создать манифест с помощью команды `deployer instance export -AppId "*" .` В результате выполнения команды в текущем каталоге появится файл `export_manifest.yaml` с информацией обо всех экземплярах ролей.
2. Открыть файл и в блоке `appId: mc-application appType: MC-Application instances:` найти информацию о роли Observability.
3. Если блок `params` для роли Observability содержит параметры, которые используются в роли Grafana, указать значения этих параметров при последующей установке роли Grafana. Список параметров роли вы можете посмотреть в разделе «Параметры конфигурации ролей MaxPatrol 360».

В этом разделе

[Обновление роли SqlStorage \(см. раздел 4.2.1\)](#)

[Обновление роли LogConnector \(см. раздел 4.2.2\)](#)

[Обновление роли Observability \(см. раздел 4.2.3\)](#)

[Обновление роли Grafana \(см. раздел 4.2.4\)](#)

[Обновление роли Management and Configuration \(см. раздел 4.2.5\)](#)

См. также

[Установка роли Grafana \(см. раздел 3.4.4\)](#)

4.2.1. Обновление роли SqlStorage

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

► Чтобы обновить роль:

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

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

```
pt_sqlstorage_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. Выберите вариант с названием экземпляра роли SqlStorage.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант **Basic configuration**.
8. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль SqlStorage.
9. Нажмите **OK**.
10. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

11. Нажмите **OK**.
12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
13. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.2.2. Обновление роли LogConnector

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

► Чтобы обновить роль:

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

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

```
pt_logconnector_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. Выберите вариант с названием экземпляра роли LogConnector.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант **Basic configuration**.
8. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на котором установлена роль LogConnector.
9. Нажмите **OK**.
10. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

11. Нажмите **OK**.
12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
13. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.2.3. Обновление роли Observability

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

► Чтобы обновить роль:

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

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

```
pt_observability_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. Выберите вариант с названием экземпляра роли Observability.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант **Basic configuration**.
8. В качестве значений параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера, на который устанавливается роль Observability.
9. Нажмите **OK**.
10. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

11. Нажмите **OK**.

12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
13. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.2.4. Обновление роли Grafana

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

► Чтобы обновить роль:

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

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

```
pt_grafana_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. Выберите вариант с названием экземпляра роли Grafana.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Basic configuration**.
8. Нажмите **OK**.
9. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав `Continue`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

10. Нажмите **OK**.

11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
12. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.2.5. Обновление роли Management and Configuration

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

► Чтобы обновить роль:

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

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

```
pt_managementandconfiguration_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. Выберите вариант с названием экземпляра роли Management and Configuration.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант **Basic configuration**.
8. В качестве значений параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера, на котором установлена роль Management and Configuration.
9. В качестве значения параметра `DefaultLocale` выберите язык веб-интерфейса приложения Management and Configuration.
10. Нажмите **OK**.
11. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

12. Нажмите **OK**.
13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
14. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.3. Обновление компонента Knowledge Base

Для обновления компонента необходимо обновить роль Knowledge Base. Для обновления роли вам потребуется архив `pt_kb_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы обновить роль:

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

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

```
pt_kb_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения Knowledge Base.
5. Выберите вариант с названием экземпляра роли Knowledge Base.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Advanced configuration**.
8. В качестве значения параметра `DefaultLocale` выберите язык интерфейса приложения Knowledge Base.
9. Укажите значения параметров:

```
DeploymentType: production
HostAddress: <IP-адрес или FQDN сервера, на который устанавливается роль>
PostgreHost: <IP-адрес или FQDN сервера, на который устанавливается роль>
```
10. Нажмите **OK**.

11. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

12. Нажмите **OK**.
13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
14. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.4. Обновление компонента ReportingPortal

Для обновления компонента необходимо обновить роль `ReportingPortal`. Для обновления роли вам потребуется архив `pt_reportingportal_<Номер версии>.tar.gz` из комплекта поставки.

До обновления роли необходимо в приложении `Reporting Portal` удалить все дашборды и диаграммы.

► Чтобы обновить роль:

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

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

```
pt_reportingportal_<Номер версии>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения `Reporting Portal`.
5. Выберите вариант с названием экземпляра роли `ReportingPortal`.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Skip configuration**.
8. Нажмите **OK**.
9. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение **Warning** или **Error**.

Примечание. Если в результате проверки отобразилось сообщение **Warning**, вы можете продолжить установку, нажав клавишу **Y**. Чтобы включить режим установки, при котором сообщения **Warning** будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

10. Нажмите **OK**.
11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
12. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.5. Обновление компонента MaxPatrol 360

Для обновления компонента необходимо обновить следующие роли:

1. Central Management Console;
2. Incident Management;
3. Playbooks;
4. Requests.

Внимание! Перед обновлением роли Incident Management рекомендуется выполнить резервное копирование данных.

► Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив с дистрибутивом роли `<Название архива>.tar.gz`:

```
tar -xf <Название архива>.tar.gz
```
2. Запустите сценарий:

```
<Название архива>/install.sh
```
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения MaxPatrol 360.
5. Выберите вариант с названием экземпляра роли.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Skip configuration**.
8. Нажмите **OK**.
9. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется проверка сервера на соответствие программным и аппаратным требованиям. Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

10. Нажмите **OK**.
11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
12. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в формате HTML и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

Существующие до обновления MaxPatrol 360 данные об инцидентах, событиях и уведомлениях в ГосСОПКА будут доступны в новой версии. Инциденты, поступившие за время обновления из MaxPatrol 10, также будут сохранены. Все события и инциденты, добавленные во время обновления вручную, не сохраняются. Конфигурационные файлы роли Incident Management не сохраняются, кроме файла службы `incidentmanagement.connectors.mpx`.

5. Импорт объектов экспертизы в Knowledge Base

Перед выполнением инструкции необходимо скопировать на сервер с установленной ролью Knowledge Base файл с расширением `.kb` с объектами экспертизы для импорта.

► Чтобы импортировать объекты экспертизы в Knowledge Base:

1. На сервере с установленной ролью Knowledge Base перейдите в каталог утилиты `kbtools`:

```
cd /var/lib/deployed-roles/<Идентификатор приложения Knowledge Base>/<Название экземпляра роли Knowledge Base>/tools/kbtools/
```

Например:

```
cd /var/lib/deployed-roles/kb-application/kb/tools/kbtools/
```

2. Если MaxPatrol 360 был установлен в качестве отдельной системы, создайте базу знаний для импорта объектов:

```
./kbtools createRootdb --db siem_content --db_name "SIEM Content" --kbHost <IP-адрес или FQDN сервера с Knowledge Base> --login <Логин для подключения к Knowledge Base> --password <Пароль для подключения к Knowledge Base>
```

Примечание. Создавать, изменять и удалять базы знаний могут только пользователи с правами администратора в Knowledge Base.

3. Импортируйте объекты в базу знаний:

```
./kbtools importPackage --db <Идентификатор базы знаний> --kbHost <IP-адрес или FQDN сервера с Knowledge Base> --login <Логин для подключения к Knowledge Base> --password <Пароль для подключения к Knowledge Base> --source <Путь к файлу с импортируемыми объектами>.<Название файла с импортируемыми объектами>.kb --mode ReplaceOrigin --ImportPtOrigin --ImportMacros --ImportTaxonomy
```

Например:

```
./kbtools importPackage --db siem_content --kbHost kb.company.ru --login <Логин> --password <Пароль> --source /var/lib/deployed-roles/kb-application/kb/tools/Siem_content_new.kb --mode ReplaceOrigin --ImportPtOrigin --ImportMacros --ImportTaxonomy
```

4. Выберите версию SDK для валидации объектов экспертизы по инструкции ниже.

► Чтобы выбрать версию SDK для валидации:

1. В веб-интерфейсе Knowledge Base в главном меню выберите **SIEM** → **Выбор версии SDK**.
2. В центральной панели выберите версию SDK.
3. Нажмите **Установить SDK для валидации**.
4. Нажмите **Обновить**.

6. Настройка DNS-сервера для перехода между тенантами в интерфейсе MaxPatrol 360

В веб-интерфейсе MaxPatrol 360 поддерживается бесшовный переход между тенантами, для которых настроен сбор инцидентов из MaxPatrol 10, с помощью специальной панели навигации.

Для перехода между тенантами в MaxPatrol 360 нужно разрешить переходы по адресам вида <Поддомен>.<Доменное имя сервера с ролью Central Management Console>. Для этого необходимо добавить в параметры DNS-сервера wildcard-запись вида *.<Доменное имя сервера с ролью Central Management Console>.

► Чтобы настроить DNS-сервер:

1. Определите доменное имя сервера с ролью Central Management Console с помощью команды:

```
deployer params get | grep -Po '(?<=HostAddress=)(?!localhost$)^[^$]+' | head -n1
```

Например, доменное имя сервера с ролью Central Management Console — `cmc.example.com`, его IP-адрес — `192.0.2.5`, а в качестве DNS-сервера используется PowerDNS, доступный по адресу `powerdns.example.com`.

2. Если на сервере отсутствует утилита `nslookup`, установите ее:
`sudo apt-get install dnsutils -y`
3. Проверьте, разрешен ли при текущих параметрах DNS-сервера переход по адресам вида <Поддомен>.<Доменное имя сервера с ролью Central Management Console>:
`nslookup <Поддомен>.<Доменное имя сервера с ролью Central Management Console>`

Например:

```
nslookup subdomain.cmc.example.com
```

4. Если в ответе вернулось сообщение о том, что указанный домен не существует, добавьте в параметры DNS-сервера ресурсную запись типа «A» для адресов вида *.<Доменное имя сервера с ролью Central Management Console>:

```
curl -X PATCH \
  -H "X-API-Key: ${POWERDNS_API_KEY}" \
  -H "Content-Type: application/json" \
  -d '{"rrsets":[{"name": "*. <Доменное имя сервера с ролью Central Management Console>.", "type": "A", "changetype": "REPLACE", "ttl": 3600, "records": [{"content": "<IP-адрес сервера с ролью Central Management Console>", "disabled": false}]}]}' \
  <FQDN сервера DNS>/api/v1/servers/localhost/z/<Доменная зона сервера с ролью Central Management Console>
```

Например:

```
curl -X PATCH \
  -H "X-API-Key: ${POWERDNS_API_KEY}" \
  -H "Content-Type: application/json" \
```

```
-d '{"rrsets":
[{"name": "*.cmc.example.com.", "type": "A", "changetype": "REPLACE", "ttl": 3600, "records":
[{"content": "192.0.2.5", "disabled": false}]}]}' \
powerdns.example.com/api/v1/servers/localhost/z/example.com
```

Вы можете проверить корректность внесенных изменений, выполнив команду:

```
nslookup <Поддомен>.<Доменное имя сервера с ролью Central Management Console>
```

Например:

```
nslookup subdomain.cmc.example.com
```

Если ресурсная запись была успешно добавлена в параметры DNS-сервера, в командной строке отобразятся доменное имя и IP-адрес запрашиваемого узла.

Установка самоподписанного корневого сертификата, поставляемого с MaxPatrol 360

При работе с сайтами приложений tenants в интерфейсе MaxPatrol 360 используется листовой сертификат, который входит в комплект поставки продукта. Поэтому при попытке перейти к приложению из карточки tenants вы получите предупреждение о том, что создаваемое подключение не защищено. Чтобы избежать этого, вы можете установить в хранилище доверенных корневых сертификатов ОС самоподписанный корневой сертификат, поставляемый с MaxPatrol 360.

Для того чтобы скачать файл корневого сертификата, нужно в главном меню выбрать  и в панели инструментов нажать  → **Скачать сертификат**.

Если вы планируете использовать [собственные доверенные сертификаты \(см. раздел 7\)](#), устанавливать корневой сертификат, поставляемый с MaxPatrol 360, не требуется.

7. Установка доверенного сертификата для сайта MaxPatrol 360

Для работы с сайтом MaxPatrol 360 вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-2 (SHA-256, SHA-384, SHA-512);
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM (синтаксис PKCS #1, длина не менее 2048 бит, заголовок `BEGIN RSA PRIVATE KEY` без дополнительных заголовков);

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

- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Extended Key Usage (EKU) содержать записи `serverAuth` и `clientAuth`;
- в расширении Subject Alternative Name (SAN) содержать wildcard-запись вида `*.<Доменное имя сервера с ролью Central Management Console>`;
- иметь расширение `.crt`;
- 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).

Во время выполнения команды импорта доверенные корневые сертификаты автоматически проверяются на соответствие требованиям безопасности. Выявленные несоответствия отображаются в терминале. Автоматизация проверки позволяет исключить риск установки потенциально небезопасных сертификатов.

Внимание! Если в сертификате указан URL-адрес списка отозванных сертификатов, необходимо обеспечить к нему доступ из контейнеров приложений, иначе система не сможет считать сертификат доверенным. Для проверки доступа вы можете перейти к указанному адресу в Docker-контейнере каждого приложения.

► Чтобы установить доверенный сертификат:

1. На сервере с установленной ролью Deployer выполните команду:

```
deployer cacert import <Путь к корневому сертификату> <Путь к промежуточному сертификату
1> ... <Путь к промежуточному сертификату N> -verbose
```

Внимание! Путь к корневому сертификату необходимо указать первым. Пути к промежуточным сертификатам можно указать в любом порядке.

2. Выполните команду для импорта файлов доверенного сертификата и ключа сертификата на серверы с установленными ролями SqlStorage, Observability, Grafana, Management and Configuration, ReportingPortal, Knowledge Base, Central Management Console, Incident Management, Playbooks и Requests:

```
deployer cert import -certpath <Путь к файлу доверенного сертификата> -keypath <Путь к файлу закрытого ключа> -id <Идентификатор экземпляра роли>
```

Например:

```
deployer cert import -certpath ./user-cmc.crt -keypath ./user-cmc.key -id cmc-1
```

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

Примечание. Вы можете получить список экземпляров и типов ролей компонентов с помощью команды `deployer instance list`.

3. Измените конфигурации ролей SqlStorage, Observability, Grafana, Management and Configuration, ReportingPortal, Knowledge Base и Incident Management:

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

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

Например:

```
SSLCertificatePemFileName: website.crt
```

```
SSLKeyFileName: website.key
```

4. Измените конфигурацию роли Central Management Console:

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

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

```
TenantLocatorCertFileName: <Имя файла сертификата>
```

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

Например:

```
SSLCertificatePemFileName: website.crt
```

```
SSLKeyFileName: website.key
```

```
TenantLocatorCertFileName: website.crt
```

```
TenantLocatorKeyFileName: website.key
```

8. Изменение конфигурации роли

Конфигурация компонента включает в себя параметры конфигураций ролей, с помощью которых компонент был установлен. Для изменения конфигурации компонента необходимо изменить конфигурацию той или иной роли.

Вы можете изменить конфигурацию роли с помощью сценария `install.sh`, который необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

► Чтобы изменить конфигурацию приложения:

1. Перейдите в каталог с распакованным архивом роли.
2. Запустите сценарий:
`<Название архива>/install.sh`
3. Нажмите **Yes**.
4. Выберите вариант с идентификатором приложения роли.
5. Выберите вариант с идентификатором экземпляра роли.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Advanced configuration**.
8. Измените значения параметров.
9. Нажмите **OK**.
10. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
11. Нажмите **OK**.
12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

9. Резервное копирование и восстановление данных MaxPatrol 360

Вы можете создать резервную копию данных MaxPatrol 360, а затем восстановить эти данные с помощью сценариев. При создании резервной копии данных и при их последующем восстановлении должны совпадать версии компонентов и языки интерфейса ОС.

В резервной копии данных MaxPatrol 360 сохраняются только конфигурационные файлы приложения, например файлы для интеграции с MaxPatrol 10 и ГосСОПКА, а также ссылки на внешние источники и поля событий из карточки инцидента. Данные об инцидентах сохраняются в резервной копии данных роли SqlStorage.

Внимание! Перед созданием резервной копии данных MaxPatrol 360 необходимо остановить все задачи на сбор данных MaxPatrol 10, а также убедиться, что на период создания резервной копии не запланирован запуск задач по расписанию.

Для резервного копирования данных каждой роли вам потребуется сценарий `backup.sh`, а для восстановления данных каждой роли — сценарий `restore.sh`. Сценарии необходимо запускать в интерфейсе терминала Linux от имени суперпользователя (root).

Данные необходимо восстанавливать на сервере с чистой операционной системой.

В этом разделе

[Создание резервной копии данных \(см. раздел 9.1\)](#)

[Восстановление данных из резервной копии \(см. раздел 9.2\)](#)

[Расположение пользовательских сертификатов \(см. раздел 9.3\)](#)

9.1. Создание резервной копии данных

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

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

Примечание. Чтобы избежать ошибок в ходе восстановления данных из резервной копии, при сохранении копий файлов пользовательских сертификатов их необходимо отличать от системных. Для этого вы можете воспользоваться [поиском пользовательских сертификатов \(см. раздел 9.3\)](#).

- Чтобы создать резервную копию данных роли,

запустите сценарий резервного копирования:

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

Например:

```
/var/lib/deployed-roles/im-application/incidentma-7hcn/backup.sh /home
```

Архив backup.tar с резервной копией будет сохранен в каталоге /<Путь к каталогу для резервной копии>/<Идентификатор приложения>/<Название экземпляра роли>/.

Например:

```
/home/im-application/incidentma-7hcn/backup.tar
```

Порядок резервного копирования

Порядок резервного копирования ролей при сохранении данных MaxPatrol 360 зависит от варианта установки.

Таблица 3. Порядок резервного копирования ролей

Вариант установки	На сервере MaxPatrol 360	На удаленном сервере
MaxPatrol 360 установлен на сервер MaxPatrol 10	MP SIEM Server → MP 10 Core → Knowledge Base → SqlStorage → Deployer → Incident Management	—
MaxPatrol 360 установлен на сервер с ролью Deployer	Deployer → Incident Management	MP SIEM Server → MP 10 Core → Knowledge Base → SqlStorage → Deployer
MaxPatrol 360 установлен на сервер PT MC	SqlStorage → Deployer → Incident Management	MP SIEM Server → MP 10 Core → Knowledge Base → SqlStorage → Deployer

9.2. Восстановление данных из резервной копии

В ходе восстановления данных из резервной копии необходимо добавить:

- файлы сертификатов роли Deployer — в каталоги /opt/deployer/pki/ и /opt/deployer/pki/trusted_ca/;
- файлы сертификатов для остальных ролей — в каталог /var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs.

MaxPatrol 360 на сервере MaxPatrol 10

► Чтобы восстановить данные роли Incident Management:

1. Восстановите данные компонентов MaxPatrol 10 в соответствии с инструкцией из раздела «Восстановление данных компонентов MaxPatrol 10 на Linux из резервной копии» Руководства администратора MaxPatrol 10.
2. Установите роль Incident Management с помощью сценария:
`deployer package install -Path <Путь к файлам дистрибутива роли>/incidentmanagement_<Номер версии>.tar.gz`
3. Восстановите данные роли Incident Management:
`/var/lib/deployed-roles/<Идентификатор приложения Incident Management>/<Название экземпляра роли Incident Management>/restore.sh <Путь к архиву с файлами резервной копии>`
 Например:
`/var/lib/deployed-roles/im-application/incidentma-knfd/restore.sh /home/`

MaxPatrol 360 на сервере с ролью Deployer

► Чтобы восстановить данные роли Incident Management:

1. Восстановите данные компонентов MaxPatrol 10 на удаленном сервере в соответствии с инструкцией из раздела «Восстановление данных компонентов MaxPatrol 10 на Linux из резервной копии» Руководства администратора MaxPatrol 10.
2. Установите роль Deployer.
3. Восстановите данные роли Deployer:
`/var/lib/deployed-roles/<Идентификатор приложения Deployer>/<Название экземпляра роли Deployer>/restore.sh <Путь к архиву с файлами резервной копии>`
 Например:
`/var/lib/deployed-roles/Deployment-Application/Deployer/restore.sh /home/deploy-app/Deployer/backup.tar`
4. В каталоге `/var/lib/deployer/role_instances/<Название роли Incident Management>` в файле `instance.yaml` в качестве значения параметра `HostId` укажите идентификатор Salt Minion.
5. В каталоге `/var/lib/deployer/role_instances/<Название экземпляра роли Incident Management>` в файлах `params.yaml` и `params.default.yaml` в качестве значений параметров, содержащих FQDN, укажите FQDN сервера, на который будет установлена роль Incident Management.

Примечание. Вы можете использовать команду `find /var/lib/deployer/ -name "params*.yaml" -exec sed -i 's/<FQDN сервера, на который была установлена роль>/<FQDN сервера, на который будет установлена роль>/' {} \;` для быстрой замены значений параметров.

6. Установите роль Incident Management с помощью сценария:

```
deployer package install -Path <Путь к файлам дистрибутива роли>/incidentmanagement_<Номер версии>.tar.gz
```

7. Восстановите данные роли Incident Management:

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

Например:

```
/var/lib/deployed-roles/im-application/incidentma-knfd/restore.sh /home/
```

MaxPatrol 360 на сервере PT MC

- ▶ Чтобы восстановить данные роли Incident Management:

1. Восстановите данные PT MC в соответствии с инструкцией из раздела «Восстановление данных PT MC на Linux из резервной копии» Руководства администратора PT MC.

2. Установите роль Incident Management с помощью сценария:

```
deployer package install -Path <Путь к файлам дистрибутива роли>/incidentmanagement_<Номер версии>.tar.gz
```

3. Восстановите данные роли Incident Management:

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

Например:

```
/var/lib/deployed-roles/im-application/incidentma-knfd/restore.sh /home/
```

9.3. Расположение пользовательских сертификатов

При резервном копировании и восстановлении данных вам могут потребоваться файлы пользовательских сертификатов. Вы можете найти их в списке параметров всех установленных ролей.

- ▶ Чтобы отобразить параметры ролей,

на сервере с установленной ролью Deployer выполните команду:

```
deployer params get
```

В полученном списке параметров требуется найти разделы с заголовком `UserDefined` для каждой роли. Файлы с расширениями `.key`, `.pem` или `.crt` в этих разделах — это файлы пользовательских сертификатов.

Примечание. Список параметров роли может не содержать файлов пользовательских сертификатов, если пользовательские сертификаты для нее не создавались.

Сервер, на котором сохранен сертификат, указан в начале каждого списка параметров в строке вида: `<Название роли> (<Название роли> <Версия системы>) on <Название сервера> params`.

Путь к найденным файлам сертификатов указан в подразделе `InstanceDefined` в значении параметра `CertificatesDir` каждой роли, для которой был добавлен сертификат:
`CertificatesDir=/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs.`

10. Пользователи и права доступа

В MaxPatrol 360 реализована ролевая модель управления доступом. В общем случае пользователю могут быть назначены одна или несколько ролей. Каждая роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции в системе.

При развертывании системы ее компоненты передают в РТ МС данные о доступных привилегиях и стандартных ролях. Роли и привилегии распределены по приложениям, которым соответствует определенный набор функций системы. Если пользователь имеет несколько ролей в приложении, права доступа суммируются.

По умолчанию MaxPatrol 360 содержит стандартные роли приложений Central Management Console (**Администратор**, **Оператор подключений** и **Оператор экспертизы**) и Incident Management (**Администратор** и **Аудитор**).

При развертывании MaxPatrol 360 автоматически создается учетная запись (логин — Administrator, пароль — P@ssw0rd) с ролью **Администратор** со всеми возможными привилегиями. Эту учетную запись невозможно заблокировать, ее логин невозможно изменить. После входа в систему рекомендуется сменить пароль этой учетной записи на более сложный.

11. Настройка компонентов после изменения IP-адресов или FQDN их серверов

Для взаимодействия между собой компоненты MaxPatrol 360 используют IP-адреса или FQDN серверов, на которых они установлены. Эти сетевые параметры указываются администратором при установке компонента и сохраняются в его конфигурации. Если во время работы системы IP-адрес или FQDN сервера изменился, взаимодействие между компонентами нарушится, поскольку в конфигурации компонента будет храниться прежнее значение параметра.

Для восстановления взаимодействия необходимо в качестве значений параметров компонентов указать актуальные IP-адреса или FQDN серверов. Необходимо также в параметрах подключения MaxPatrol 360 к MaxPatrol 10 указать новый IP-адрес или FQDN сервера, с которого MaxPatrol 360 должен получать информацию об инцидентах.

Внимание! После указания новых IP-адресов или FQDN серверов в параметрах компонентов MaxPatrol 10 необходимо [деактивировать](#) РТ МС.

Внимание! Если компоненты MaxPatrol 10 развернуты на нескольких площадках, перед сменой IP-адресов необходимо разорвать связи между площадками. После смены IP-адресов связи можно восстановить.

Настройка роли Deployer

Если был изменен IP-адрес или FQDN сервера, на котором установлена роль Deployer, необходимо выполнить следующие действия:

1. На сервере каждого Salt Minion в файле `/etc/salt/minion.d/deployer.conf` указать в качестве значения параметра `master` актуальный IP-адрес или FQDN сервера с ролью Deployer и выполнить команду `systemctl restart salt-minion`.
- Внимание!** Использование сценария `deploy_minion.sh` или утилиты `deploy_minion.ps1` для изменения конфигурации Salt Minion сделает работу MaxPatrol 360 невозможной и потребует переустановки всей системы.
2. [Изменить конфигурацию \(см. раздел 8\)](#) роли Deployer, указав актуальное значение параметра `HostAddress`.
3. Выполнить команду для изменения конфигурации роли `deployer instance reconfigure -type Deployer`.
4. Выполнить команду `openssl s_client -connect localhost:5000 -showcerts </dev/null 2>/dev/null | openssl x509 -noout -ext subjectAltName`. Результат должен содержать DNS-имена и IP-адреса, соответствующие текущим настройкам DNS, или измененный IP-адрес — в зависимости от настройки доступа к системе.

Настройка компонентов после изменения адреса сервера MP 10 Core, PT MC и Knowledge Base

Если был изменен IP-адрес или FQDN сервера компонентов MP 10 Core, PT MC и Knowledge Base, необходимо указать актуальные значения следующих параметров:

- `HostAddress`, `KBAddress` и `MCAddress` компонента MP 10 Core;
- `HostAddress`, `MCAddress` и `CoreAddress` компонента Knowledge Base;
- `HostAddress` компонента PT MC;
- `CoreAddress` компонента MP SIEM Server на Linux.

Приложение. Параметры конфигурации ролей MaxPatrol 360

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

Роль Deployer

Таблица 4. Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
CertificateKeyGenerationAlgorithm	Алгоритм шифрования для генерации ключей сертификатов: — rsa — алгоритм RSA; — ec — алгоритм ECC	rsa
CertificateVendorEmail	Адрес электронной почты вендора. Примечание. Этот параметр может быть изменен только при первой установке продукта	pt@ptsecurity.com
CertificateVendorLocality	Город, где располагается главный офис вендора. Примечание. Этот параметр может быть изменен только при первой установке продукта	Moscow
CertificateVendorName	Название вендора. Примечание. Этот параметр может быть изменен только при первой установке продукта	Positive Technologies
CustomDockerAddressPool	Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию. Рекомендуется использовать подсеть с маской /20 или шире в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	—
CustomDockerNetworkSize	Размер подсетей, которые будут выделяться из диапазона, указанного в параметре CustomDockerAddressPool. Реко-	—

Параметр	Описание	Значение по умолчанию
	мендуется использовать значение, не превышающее 24 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра <code>CustomDockerAddressPool</code> , как минимум на 4 бит	
<code>DockerDaemonNoNewPrivileges</code>	Демон Docker запускает (флажок установлен) или не запускает (флажок снят) контейнеры с системным флагом <code>no-new-privileges</code>	Флажок установлен
<code>DockerNsUserName</code>	Имя пользователя в ОС сервера, от имени которого будут запускаться контейнеризированные приложения	<code>dockerns</code>
<code>HostAddress</code>	IP-адрес или FQDN сервера с установленной ролью <code>Deployer</code>	—
<code>Network</code>	Название виртуальной сети Docker роли <code>Deployer</code>	<code>registry-network</code>
<code>NetworkDriver</code>	Тип виртуальной сети Docker роли <code>Deployer</code>	<code>bridge</code>
<code>RegistryPort</code>	Номер порта для доступа к локальному реестру Docker-образов	<code>5000</code>

Роль `SqlStorage`

Таблица 5. Параметры конфигурации роли `SqlStorage`

Параметр	Описание	Значение по умолчанию
<code>CACertificateFileName</code>	Имя файла корневого сертификата	<code>rootCA.crt</code>
<code>CollectorAgentHttpPort</code>	Порт доступа к коллектору <code>OpenTelemetry</code> для роли <code>SqlStorage</code> по протоколу HTTP	<code>4319</code>
<code>CollectorAgentSyslogUdpPort</code>	Порт для прослушивания журналов <code>syslog</code> по протоколу UDP	<code>54528</code>
<code>DockerBindHost</code>	IP-адрес или FQDN сервера с локальным реестром Docker-образов	<code>0.0.0.0</code>

Параметр	Описание	Значение по умолчанию
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	Адрес и порт сервера MP 10 Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (флажок установлен) или выключена (флажок снят)	Флажок снят
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
Network	Название виртуальной сети Docker роли SqlStorage	storage-network.sqlstorage
NetworkDriver	Тип виртуальной сети Docker роли SqlStorage	bridge
PgAdminPort	Порт для доступа к pgAdmin	9001
PgAnalyzeScaleFactor	Доля от числа кортежей в таблице, которая прибавляется к значению параметра PgAnalyzeThreshold при расчете порога срабатывания команды ANALYZE. Например, если значение PgAnalyzeThreshold равно 200 000, а значение параметра PgAnalyzeScaleFactor равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет $200\,000 + 100\,000 = 300\,000$ кортежей	0.0
PgAnalyzeThreshold	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	200000
PgChecksums	Включение контрольных сумм на страницах данных СУБД PostgreSQL. Возможные значения: <code>auto</code>, <code>on</code>, <code>off</code>. Если выбрано значение <code>auto</code>, контрольные суммы при первичной установке роли SqlStorage включаются, а при обновлении или переустановке роли — остаются без изменений. Примечание. При обновлении или изменении конфигурации роли SqlStorage подсчет контрольных сумм может занять длительное	auto

Параметр	Описание	Значение по умолчанию
	время. До завершения процесса база данных не будет запущена и продолжение работы будет невозможно	
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранения (возможные значения — HDD или SSD)	HDD
PgInitArgs	Параметры инициализации кластера PostgreSQL	-- locale='en_US.UTF8'
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения — panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgMasterPasswordRequired	Запрос мастер-пароля для СУБД PostgreSQL включен (флажок установлен) или выключен (флажок снят)	Флажок снят
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL. Внимание! Не рекомендуется использовать в паролях служебных учетных записей в PostgreSQL следующие символы: # \ / ' " ; \$	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgServerMode	Режим сервера для экземпляра СУБД PostgreSQL включен (флажок установлен) или выключен (флажок снят)	Флажок снят
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgTimeZone	Часовой пояс для экземпляра СУБД PostgreSQL	Europe/Moscow
PgUpgradeJobs	Количество одновременных процессов или потоков, используемых для pg_upgrade	4

Параметр	Описание	Значение по умолчанию
PgUpgradeVerbose	Детализированное ведение журнала для <code>pg_upgrade</code> включено (флажок установлен) или выключено (флажок снят)	Флажок снят
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgVacuumNapTime	Минимальная задержка между двумя запусками автоочистки для отдельной базы данных	20min
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB
SeccompEnabled	Профиль безопасности в Docker-контейнере роли включен (флажок установлен) или выключен (флажок снят)	Флажок снят
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key

Роль LogConnector

Таблица 6. Параметры конфигурации роли LogConnector

Параметр	Описание	Значение по умолчанию
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	—
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к серверу СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432
PostgreUserName	Логин служебной учетной записи для доступа к серверу СУБД PostgreSQL	pt_system

Параметр	Описание	Значение по умолчанию
SeccompEnabled	Профиль безопасности в Docker-контейнере роли включен (флажок установлен) или выключен (флажок снят)	Флажок снят
TelemetryCollectCron	Время начала ежедневного сбора телеметрии. По умолчанию — 04:00 в текущей временной зоне	0 0 4 * * ? *
TelemetryConnectAuthority	FQDN сервера MaxPatrol 360 с указанием порта	—
TelemetryCronScheduleEnabled	Данные телеметрии отправляются (флажок установлен) или не отправляются (флажок снят) на сервер приема телеметрии	Флажок установлен
TelemetryExportDataPath	Путь к каталогу для экспорта данных телеметрии	/tmp/telemetry/files
TelemetryTrackerDataPath	Путь к каталогу для отправки данных телеметрии	./observability/telemetry/files
TelemetryType	Типы собираемых данных телеметрии	CFG, API, STATE, UAL

Роль Observability

Таблица 7. Параметры конфигурации роли Observability

Параметр	Описание	Значение по умолчанию
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorServerHttpPort	Порт для доступа к серверу сбора журналов по протоколу HTTP	4318
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	localhost:5000
ExportEnabledFrom	Разрешенное начальное время отправки телеметрии	04:00:00
ExportEnabledTo	Разрешенное конечное время отправки телеметрии	05:00:00

Параметр	Описание	Значение по умолчанию
FlusUri	Адрес сервера приема телеметрии	https://update.ptsecurity.com/
HostAddress	IP-адрес или FQDN сервера с установленной ролью Observability	localhost
JobExecutingInterval	Интервал запуска работ внутри сервиса Telemetry.Tracker	00:05:00
MetricsHttpPort	Порт для доступа к метрическим данным	8428
MetricsPassword	Пароль для доступа к метрическим данным	P@ssw0rd
MetricsRetention	Время сохранения метрических данных в базе данных	90d
MetricsUser	Логин для доступа к метрическим данным	admin
Network	Название виртуальной сети Docker роли Observability	observability-network
NetworkDriver	Тип виртуальной сети Docker роли Observability	bridge
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к серверу СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432
PostgreUserName	Логин служебной учетной записи для доступа к серверу СУБД PostgreSQL	pt_system
SeccompEnabled	Профиль безопасности в Docker-контейнере роли включен (флажок установлен) или выключен (флажок снят)	Флажок снят
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key
TelemetryFileSize	Максимальный размер файла телеметрии в мегабайтах	50
TelemetryPackSize	Максимальный размер архива в мегабайтах, который можно отправить на сервер приема телеметрии	35

Параметр	Описание	Значение по умолчанию
TimeZone	Используемый часовой пояс	Europe/Moscow

Роль Grafana

Таблица 8. Параметры конфигурации роли Grafana

Параметр	Описание	Значение по умолчанию
CommonCollectorServerAddress	HTTP-адрес сервера Telemetry Collector	https://localhost:4318
DefaultLocale	Интерфейс PT MC отображается на русском (ru-RU) или английском (en-US) языке	ru-Ru
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	localhost:5000
GrafanaAdminLogin	Логин для подключения к интерфейсу Grafana	admin
GrafanaAdminPassword	Пароль для подключения к интерфейсу Grafana	P@ssw0rd
GrafanaAuthAnonymousEnabled	Анонимный доступ к веб-интерфейсу включен (флажок установлен) или выключен (флажок снят)	Флажок снят
GrafanaServerHttpPort	Порт для доступа к интерфейсу Grafana по протоколу HTTP	9002
GrafanaServerRootUrl	Базовый URL для доступа к веб-интерфейсу Grafana	%(protocol)s://%(domain)s:%(http_port)s/grafana
GrafanaServerSubPathEnabled	Доступ к веб-интерфейсу Grafana по базовому URL с префиксом включен (флажок установлен) или выключен (флажок снят)	Флажок установлен
GrafanaServerSubUri	Путь для подключения к серверу Grafana	grafana
HostAddress	IP-адрес или FQDN сервера с установленной ролью Grafana	localhost

Параметр	Описание	Значение по умолчанию
MetricsAddress	Адрес для доступа к данным VictoriaMetrics	https://storage-victoriametrics:8428
MetricsUser	Логин для доступа к данным VictoriaMetrics	admin
MetricsPassword	Пароль для доступа к данным VictoriaMetrics	P@ssw0rd
MCAddress	IP-адрес или FQDN сервера PT MC	https://localhost:4318
Network	Название виртуальной сети Docker роли Grafana	observability-network
NetworkDriver	Тип виртуальной сети Docker роли Grafana	Bridge
SeccompEnabled	Профиль безопасности в Docker-контейнере роли включен (флажок установлен) или выключен (флажок снят)	Флажок снят
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key
TimeZone	Используемый часовой пояс	Europe/Moscow

Роль Management and Configuration

Таблица 9. Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
ActionLogBatchSize	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service одновременно отправляет службе MC User Action Logging Service	100
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
ApiGatewayPort	Порт для доступа к шлюзу API	8709

Параметр	Описание	Значение по умолчанию
ApproveRegistrationEnabled	Подтверждение регистрации приложений, установленных неавторизованными пользователями, включено (флажок установлен) или выключено (флажок снят)	Флажок снят
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
ClientId	Идентификатор приложения Management and Configuration	idmgr
ClientSecret	Ключ доступа к приложению Management and Configuration	—
CollectorAgentHttpPort	Порт доступа к коллектору OpenTelemetry для роли Management and Configuration по протоколу HTTP	4319
DefaultLocale	Интерфейс PT MC отображается на русском (ru-RU) или английском (en-US) языке	ru-Ru
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	Адрес и порт сервера компонента MP 10 Core
EmailNotificationRetryCount	Максимальное количество попыток отправки сообщения на сервер	10
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на сервер (в секундах)	60
EnableLogToConsole	Режим отправки журналов в командной строке включен (флажок установлен) или выключен (флажок снят)	Флажок снят
EnableLogToFiles	Запись журналов в файлы включена (флажок установлен) или выключена (флажок снят)	Флажок установлен
HostAddress	IP-адрес или FQDN сервера PT MC	—
IamCookieLifetime	Время жизни неактивной сессии в MaxPatrol 360 (в часах)	168
IamPort	Порт для подключения к сервису IAM (управление пользователями и доступом)	3334
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000

Параметр	Описание	Значение по умолчанию
LmPort	Порт для доступа к службе журналирования работы микросервисов LogManager	8997
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000
MasterRedirectEnabled	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
McPortalPort	Порт для доступа к сервису MC Portal	8710
MetricsAddress	Адрес для доступа к метрическим данным	—
MetricsHttpPort	Порт для доступа к метрическим данным	8428
MetricsPassword	Пароль для доступа к метрическим данным	P@ssw0rd
MetricsUser	Логин для доступа к метрическим данным	admin
Network	Название виртуальной сети Docker роли Management and Configuration	mc-network.managementandconfiguration-1
NetworkDriver	Тип виртуальной сети Docker роли Management and Configuration	bridge
NginxLogRotateCount	Максимальное количество файлов журналов для сервера nginx	14
NginxLogRotateSize	Максимальный размер файла в журнале сервера nginx (G для гигабайтов, M для мегабайтов, K для килобайтов)	50M
NotificationsPort	Порт для доступа к сервису уведомлений	8736
PackageManagementPort	Номер порта сервиса управления пакетами Package Management	8585
PackagesSourceUri	Адрес сервера обновлений	—
PostgreHost	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
PostgrePassword	Пароль служебной учетной записи для доступа PT MC к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432

Параметр	Описание	Значение по умолчанию
PostgreUserName	Логин служебной учетной записи для доступа PT MC к СУБД PostgreSQL	pt_system
ProxyPassword	Пароль для доступа к прокси-серверу	—
ProxyUrl	URL прокси-сервера	—
ProxyUserName	Логин для доступа к прокси-серверу	—
ReverseProxyPort	Порт для доступа к компоненту ReverseProxy	3334
RmPort	Порт для доступа к сервису RegistrationManager (регистрация приложений)	8998
SeccompEnabled	Профиль безопасности в Docker-контейнере роли включен (флажок установлен) или выключен (флажок снят)	Флажок снят
Smtphost	IP-адрес или FQDN SMTP-сервера	localhost
SmtIgnoreCertificateValidation	PT MC проверяет (флажок снят) или не проверяет (флажок установлен) валидность сертификата при подключении к SMTP-серверу	Флажок снят
SmtPassword	Пароль служебной учетной записи для подключения к SMTP-серверу	—
SmtPort	Порт SMTP-сервера для входящих подключений от PT MC	25
SmtSecureSocketOptions	Варианты шифрования при подключении к SMTP-серверу: — None — шифрование не используется; — Auto — почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется; — SslOnConnect — протоколы SSL или TLS используются при соединении;	Auto

Параметр	Описание	Значение по умолчанию
	— <code>StartTls</code> — протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается; — <code>StartTlsWhenAvailable</code> — протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS	
<code>SmtptSender</code>	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.local>
<code>SmtptUser</code>	Логин служебной учетной записи для подключения к SMTP-серверу	—
<code>SSLCertificatePemFileName</code>	Имя файла сертификата SSL в формате PEM	—
<code>SSLKeyFileName</code>	Имя файла закрытого ключа SSL-сертификата	—
<code>TimeZone</code>	Используемый часовой пояс	Europe/Moscow
<code>TmApplicationId</code>	Идентификатор приложения Management and Configuration	—
<code>TmPort</code>	Порт для доступа к сервису tenants	8703
<code>TmSiteAlias</code>	Псевдоним площадки	SITE
<code>TmSiteId</code>	Идентификатор площадки	—
<code>TmTenantManagerId</code>	Идентификатор службы MC Tenant Manager Service	—
<code>TriggersPort</code>	Порт для доступа к сервису Triggers (управление триггерами)	8834
<code>UalPort</code>	Порт для доступа к сервису для хранения и отображения действий пользователей	8704
<code>UserIdleLogoutEnabled</code>	Сессия пользователя завершается (флажок установлен) или не завершается (флажок снят) при его бездействии в системе	Флажок снят
<code>UseProxy</code>	Для онлайн-активации используется (флажок установлен) или не используется (флажок снят) прокси-сервер	Флажок снят

Роль Knowledge Base

Таблица 10. Параметры конфигурации роли Knowledge Base

Параметр	Описание	Значение по умолчанию
ClientId	Идентификатор для регистрации приложения Knowledge Base в PT MC	ptkb
ClientSecret	Ключ для регистрации приложения Knowledge Base в PT MC	secret
CoreAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
DefaultLocale	Интерфейс Knowledge Base отображается на русском (ru-RU) или английском (en-US) языке	ru-Ru
DeploymentType	Тип развертывания Knowledge Base	—
DetectOutOfSyncWithSIEM	Knowledge Base определяет (флажок установлен) или не определяет (флажок снят) отсутствие синхронизации с MP SIEM Server	Флажок установлен
DisplayName	Название приложения Knowledge Base в PT MC	Knowledge Base
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
EditableOrigins	Поставщик, атрибуты объектов которого можно изменять	Local
HostAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
MCAddress	IP-адрес или FQDN сервера PT MC	—
OriginNameENG	Полное название поставщика для объектов Knowledge Base на английском языке	Local system
OriginNameRUS	Полное название поставщика для объектов Knowledge Base на русском языке	Локальная система
OriginNickName	Псевдоним поставщика для объектов Knowledge Base	LOC
OriginSystemName	Поставщик объектов Knowledge Base	Local
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@ssw0rdP@ssw0rd

Параметр	Описание	Значение по умолчанию
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
SeccompEnabled	Профиль безопасности в Docker-контейнере роли включен (флажок установлен) или выключен (флажок снят)	Флажок снят
ShowDiffObjectId	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят
SiemPackageSourceContentDatabase	Название БД, которая автоматически обновляется с помощью PT UCS	siem_content
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>
SmtpUseDefaultCredentials	Режим аутентификации SMTP-сервера: флажок установлен — для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtpUser и SmtpPassword); флажок снят — для аутентификации используются логин и пароль, указанные в параметрах SmtpUser и SmtpPassword	Флажок установлен
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—

Параметр	Описание	Значение по умолчанию
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics

Роль ReportingPortal

Таблица 11. Параметры конфигурации роли ReportingPortal

Параметр	Описание	Значение по умолчанию
ApiGatewayPort	Порт для доступа к шлюзу API	8192
CACertFile, CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CertFile	Имя файла серверного сертификата	Portal.crt
ClickHouseHost	IP-адрес или FQDN сервера с установленной ролью ReportingPortal для доступа к ClickHouse	localhost
ClickHouseHttpPort	Порт для доступа к ClickHouse по протоколу HTTP	8123
ClickHouseNativePort	Порт для доступа к ClickHouse по протоколу, который используется по умолчанию	9000
ClickHouseHttpsPort	Порт для доступа к ClickHouse по протоколу HTTPS	8443
ClickHouseNativeSecurePort	Порт для доступа к ClickHouse по протоколу, который используется по умолчанию, с шифрованием соединения	9440
ClickHouseUserName	Логин служебной учетной записи для подключения к ClickHouse	default
ClickHouseUserPassword	Пароль служебной учетной записи для подключения к ClickHouse	P@ssw0rd
ClientId	Идентификатор приложения Reporting Portal	rp

Параметр	Описание	Значение по умолчанию
ClientSecret	Автоматически генерируемый секрет в формате GUID, который используется для регистрации приложения Reporting Portal в PT MC	—
CollectorAgentHttpPort	Порт доступа к коллектору OpenTelemetry для роли ReportingPortal по протоколу HTTP	4320
ConsulAgentToken	Токен, который сервисы роли используют для доступа к серверу Consul. Создается автоматически при первом запуске Consul	—
ConsulDatacenter	Идентификатор центра обработки данных Consul	RP-dc
ConsulDnsPort	DNS-порт сервера Consul	8611
ConsulHttpsPort	HTTP-порт сервера Consul	8512
ConsulLanPort	Ethernet-порт сервера Consul	8311
ConsulMasterToken	Токен, который дает сервисам роли неограниченный доступ к Consul	—
ConsulRpcPort	RPC-порт сервера Consul	8310
ConsulSecret	32-битный ключ шифрования стандарта Base64 для обмена данными между агентами Consul	—
ConsulUi	Интерфейс пользователя Consul включен (флажок установлен) или выключен (флажок снят)	Флажок снят
ConsulWanPort	WAN-порт сервера Consul	8312
DataPipelinePort	Порт, используемый сервисом Data Pipeline	8788
DataReceiverPort	Порт, используемый сервисом Data Receiver	8789
DefaultLocale	Язык интерфейса приложения Reporting Portal: русский (ru-RU) или английский (en-US)	ru-RU
DeploymentMode	Режим развертывания приложения Reporting Portal	standalone

Параметр	Описание	Значение по умолчанию
DisplayName	Название приложения Reporting Portal в PT MC	Reporting Portal
DockerRegistry	Номер порта для доступа к локальному реестру Docker-образов	localhost:5000
EnablePullModel	Сбор данных по pull-модели включен (флажок установлен) или выключен (флажок снят)	Флажок установлен
EtlMetricsPort	Порт, используемый сервисом ETL Metrics	8785
HostAddress	IP-адрес или FQDN сервера с установленной ролью ReportingPortal	localhost
KeyFile	Имя файла закрытого ключа сертификата	Portal.key
MEMORY_HIGH_WATERMARK_GB	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах). Примечание. Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10
MCAddress	IP-адрес или FQDN сервера PT MC	https://localhost:3334
MCTokenCheckInterval	Частота проверки токена доступа к PT MC (в секундах)	300
Network	Название виртуальной сети Docker роли ReportingPortal	rp-network
NetworkDriver	Тип виртуальной сети Docker роли ReportingPortal	bridge
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений	5432

Параметр	Описание	Значение по умолчанию
PostgreUserName	Логин служебной учетной записи для подключения к СУБД PostgreSQL	pt_system
RabbitMqHostName	IP-адрес или FQDN сервера с установленной службой RabbitMQ	rp-rabbitmq
ReportingPortalPortalPort	Порт, используемый сервисом Portal	8713
ReverseProxyPort	Порт для доступа к компоненту ReverseProxy	8887
RMQAdminPassword	Пароль служебной учетной записи администратора RabbitMQ	P@ssw0rd
RMQAdminUser	Логин служебной учетной записи администратора RabbitMQ	Administrator
RMQPassword	Пароль служебной учетной записи для доступа к RabbitMQ	P@ssw0rd
RMQUser	Логин служебной учетной записи для доступа к RabbitMQ	rp
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). Примечание. Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
RMQVirtualHost	Имя виртуального узла RabbitMQ	rp
RPCustomGroupsPort	Порт, используемый сервисом Custom Groups	8786
SecuritySettingsEnabled	Вкладка Безопасность в главном меню MaxPatrol 360 отображается (флажок установлен) или не отображается (флажок снят)	Флажок снят
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SupersetAppPrefix	Префикс, который является частью URL приложения Superset	' /superset '

Параметр	Описание	Значение по умолчанию
SSLKeyFileName	Имя файла закрытого ключа сертификата SSL	Portal.key
SupersetSecretKey	Ключ доступа к приложению Superset	00000000-0000-0000-0000-00000000
TimeZone	Используемый часовой пояс	Europe/Moscow
TriggerHttpTimeoutInSeconds	Максимальное время ожидания HTTP-запроса, используемого для сбора метрик	14400
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). Примечание. Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Роль Central Management Console

Таблица 12. Параметры конфигурации роли Central Management Console

Параметр	Описание	Значение по умолчанию
AllowUseHeadKbOriginsAsCmcOrigins	Возможность использовать код поставщика, дублирующий префикс объектов экспертизы в базе данных Knowledge Base, включена (флажок установлен) или выключена (флажок снят)	Флажок снят
CACertificateFileName	Имя корневого сертификата	rootCA.crt
ClientId	Идентификатор приложения Central Management Console	cmc
ClientSecret	Автоматически генерируемый секрет в формате GUID, который используется для регистрации MaxPatrol 360 в PT MC	—

Параметр	Описание	Значение по умолчанию
ConsulAgentToken	Токен, который службы используют для доступа к серверу Consul. Создается автоматически при первом запуске Consul	—
ConsulDatacenter	Идентификатор центра обработки данных Consul	CMC-dc
ConsulDnsPort	DNS-порт сервера Consul	8631
ConsulHttpPort	HTTP-порт сервера Consul	8532
ConsulLanPort	Ethernet-порт сервера Consul	8331
ConsulMasterToken	Токен, который дает службам неограниченные привилегии	—
ConsulRpcPort	RPC-порт сервера Consul	8330
ConsulSecret	32-битный ключ шифрования стандарта Base64 для обмена данными между агентами Consul	—
ConsulUI	Интерфейс пользователя Consul включен (флажок установлен) или выключен (флажок снят)	Флажок установлен
ConsulWanPort	WAN-порт сервера Consul	8332
CoreAddress	IP-адрес или FQDN сервера с установленной ролью Core	https://localhost:443
DefaultLocale	Язык интерфейса MaxPatrol 360: русский (ru-RU) или английский (en-US)	ru-RU
DefaultTenantName	Название тенанта, которое отображается в интерфейсе до добавления тенантов пользователем	DefaultTenant
DisableTenantLocator	Возможность бесшовного перехода между тенантами в веб-интерфейсе MaxPatrol 360 включена (флажок снят) или выключена (флажок установлен)	Флажок установлен
DisplayName	Название приложения Central Management Console в веб-интерфейсе MaxPatrol 360	Central Management Console
DockerRegistry	Номер порта для доступа к локальному реестру Docker-образов	localhost:5000

Параметр	Описание	Значение по умолчанию
EnableIncidentManagementIntegration	Возможность интеграции с приложением Incident Management включена (флажок установлен) или выключена (флажок снят)	Флажок снят
HostAddress	IP-адрес или FQDN сервера с установленной ролью Central Management Console	localhost
IncidentManagementBaseAddress	IP-адрес или FQDN, а также порт сервера с установленной службой IncidentManagement	https://im-apigateway.im-application:8898
IncidentManagementScope	Доступ по токenu к API приложения Incident Management	pt.im.api
MaxRequestBodySize	Максимальный размер HTTP-запроса, который может обработать приложение Central Management Console (в байтах)	524288000
MCAddress	IP-адрес или FQDN сервера PT MC	https://localhost:3334
Network	Название виртуальной сети Docker роли Central Management Console	cmc-network
NetworkDriver	Тип виртуальной сети Docker роли Central Management Console	bridge
NginxLogRotateCount	Максимальное количество файлов журналов для сервера nginx	14
NginxLogRotateSize	Максимальный размер файла в журнале сервера nginx (G для гигабайтов, M для мегабайтов, K для килобайтов)	50M
PlatformRegistrationRequestId	Идентификатор запроса на регистрацию MaxPatrol 360 в PT MC	00000000-0000-0000-0000-000000000000
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт для доступа к СУБД PostgreSQL	5432
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PtkbAddress, PtkbFrontendAddress	IP-адрес или FQDN сервера компонента Knowledge Base	https://localhost:8091

Параметр	Описание	Значение по умолчанию
PtkbApiScope	Доступ по токену к API приложения Knowledge Base	ptkb.api
ReverseProxyPort	Порт для доступа к компоненту ReverseProxy	4302
RMQSSLCertificateFile	Имя файла пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.crt
RMQSSLKeyFile	Имя файла закрытого ключа пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.key
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key
TenantLocatorCertFileName	Имя файла пользовательского доверенного wildcard-сертификата для домена *.<Доменное имя сервера с ролью Central Management Console>, который используется для перехода между тенантами	Locator.crt
TenantLocatorKeyFileName	Имя файла закрытого ключа сертификата	Locator.key
TimeZone	Часовой пояс Docker-контейнера	Europe/Moscow
ValidationServiceAddress	IP-адрес или FQDN сервера компонента Knowledge Base	https://localhost:8091

Роль Incident Management

Таблица 13. Параметры конфигурации роли Incident Management

Параметр	Описание	Значение по умолчанию
CACertificateFileName	Имя корневого сертификата	rootCA.crt
ClientId	Идентификатор приложения MaxPatrol 10	pt.im
ClientSecret	Ключ доступа к приложению MaxPatrol 10	—

Параметр	Описание	Значение по умолчанию
CollectorAgentHttpPort	Порт доступа к коллектору OpenTelemetry для роли Incident Management по протоколу HTTP	4319
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
ConnectorsMpxIsSynchronizeIncidentStatusesEnabled	Отправка изменения статуса инцидента из MaxPatrol 360 в MaxPatrol 10 включена (флажок установлен) или выключена (флажок снят)	Флажок установлен
ConsulAgentToken	Токен, который службы используют для доступа к серверу Consul. Создается автоматически при первом запуске Consul	—
ConsulDatacenter	Идентификатор центра обработки данных Consul	IM-dc
ConsulDnsPort	DNS-порт сервера Consul	8631
ConsulHttpPort	HTTP-порт сервера Consul	8531
ConsulLanPort	Ethernet-порт сервера Consul	8331
ConsulMasterToken	Токен, который дает службам неограниченные привилегии	—
ConsulRpcPort	RPC-порт сервера Consul	8330
ConsulSecret	32-битный ключ шифрования стандарта Base64 для обмена данными между агентами Consul	—
ConsulUI	Интерфейс пользователя Consul включен (флажок установлен) или выключен (флажок снят)	Флажок установлен
ConsulWanPort	WAN-порт сервера Consul	8332
CoreAddress	IP-адрес или FQDN сервера с установленной ролью Core	—
DefaultLocale	Язык интерфейса MaxPatrol 360: русский (ru-RU) или английский (en-US)	ru-RU
DeploymentConfigurationPort	Порт, используемый для подключения к службе конфигурации развертывания	9740

Параметр	Описание	Значение по умолчанию
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Номер порта для доступа к локальному реестру Docker-образов	5000
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (флажок установлен) или выключена (флажок снят)	Флажок снят
HostAddress	IP-адрес или FQDN сервера с установленной ролью Incident Management	—
IncidentManagementConnectorsGossopkaEnabled	Возможность подключения к системе ГосСОПКА включена (флажок установлен) или выключена (флажок снят)	Флажок установлен
IncidentManagementConnectorsGossopkaPort	Порт, используемый для подключения к системе ГосСОПКА	8891
IncidentManagementConnectorsMaxPatrolPort	Порт, используемый для подключения к MaxPatrol 10	8890
IncidentManagementConnectorsTelegramChatId	Идентификатор телеграм-канала (ChatID) для отправки уведомлений об инцидентах	—
IncidentManagementConnectorsTelegramEnabled	Служба incidentmanagement.connectors.telegram, используемая для отправки уведомлений об инцидентах в Telegram, включена (флажок установлен) или выключена (флажок снят)	Флажок установлен
IncidentManagementConnectorsTelegramToken	Токен телеграм-бота, используемый для отправки уведомлений об инцидентах	—
IncidentManagementCoreReadModelPort	Порт, используемый службой incidentmanagement.core.readmodel	8889
IncidentManagementCoreWriteModelPort	Порт, используемый службой incidentmanagement.core.writemodel	8888

Параметр	Описание	Значение по умолчанию
IncidentManagementFileStoragePort	Порт, используемый службой incidentmanagement.filestorage	8892
IncidentManagementPortalPort	Порт, используемый службой incidentmanagement.portal	8893
IncidentManagementUIPort	Порт для доступа к пользовательскому интерфейсу MaxPatrol 360	8887
MCAddress	IP-адрес или FQDN сервера PT MC	—
Network	Название виртуальной сети Docker роли Incident Management	core-network.core-1
NetworkDriver	Тип виртуальной сети Docker роли Incident Management	bridge
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	—
PostgrePassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт для доступа к СУБД PostgreSQL	5432
PostgreUserName	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
ReverseProxyPort	Порт для доступа к компоненту ReverseProxy	8091
RMQSslCertificateFile	Имя файла пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.crt
RMQSslKeyFile	Имя файла закрытого ключа пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.key
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key
SaltMasterHost	Адрес сервера Salt Master	—
TimeZone	Часовой пояс Docker-контейнера	Europe/Moscow

Роль Playbooks

Таблица 14. Параметры конфигурации роли Playbooks

Параметр	Описание	Значение по умолчанию
NginxLogRotateCount	Максимальное количество файлов журналов для сервера nginx	14
NginxLogRotateSize	Максимальный размер файла в журнале сервера nginx (G для гигабайтов, M для мегабайтов, K для килобайтов)	50M
PlaybooksUiPort	Порт для доступа к службе Playbooks	8886
RMQSSLCertificateFile	Имя файла пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.crt
RMQSSLKeyFile	Имя файла закрытого ключа пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.key

Роль Requests

Таблица 15. Параметры конфигурации роли Requests

Параметр	Описание	Значение по умолчанию
NginxLogRotateCount	Максимальное количество файлов журналов для сервера nginx	14
NginxLogRotateSize	Максимальный размер файла в журнале сервера nginx (G для гигабайтов, M для мегабайтов, K для килобайтов)	50M
RequestsPortalPort	Порт, используемый службой requests.portal	8884
RequestsUiPort	Порт для доступа к службе Requests	8883
RMQSSLCertificateFile	Имя файла пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.crt
RMQSSLKeyFile	Имя файла закрытого ключа пользовательского сертификата для службы RabbitMQ	RMQ_Core_Client.key

Глоссарий

актив

Информация или оборудование, имеющие ценность для организации и подлежащие защите от киберугроз.

активность

Связанные события ИБ, объединенные в последовательность согласно правилам, установленным экспертами Positive Technologies.

инцидент ИБ

Событие (группа событий) информационной безопасности, которое может привести к нарушению функционирования ИТ-инфраструктуры или возникновению угроз безопасности обрабатываемой в ней информации.

кибератака

Целенаправленное воздействие программных и (или) программно-аппаратных средств на ИТ-инфраструктуру и ее компоненты с целью нарушения (прекращения) ее функционирования или создания угрозы безопасности обрабатываемой в ней информации. Целями кибератаки могут быть, например, несанкционированный перевод денежных средств, нарушение или блокировка работы системы, получение несанкционированного доступа к инфраструктуре или хищение персональных данных.

корреляционное событие

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

корреляция событий

Процесс обнаружения нарушений ИБ на основе анализа потока событий от источников. Виды и сочетания событий, характерные для различных видов нарушений, указываются в заранее созданных правилах. Для обнаруженных нарушений регистрируются события ИБ (корреляционные события) и инциденты.

паттерн атаки

Последовательность действий злоумышленника, каждому из которых сопоставлена техника из матрицы MITRE ATT&CK.

ресурс

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

событие ИБ

Отклонение от нормального или ожидаемого состояния и поведения системы, сервиса или сети, которое может иметь отношение к информационной безопасности.



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.