IBM QRadar Security Intelligence Platform

Версия 7.2.6

Руководство Быстрый старт

Это руководство поможет вам приступить к работе с использованием стандартной установки.

Версия на национальном языке: Чтобы получить руководство Быстрый старт на других языках, напечатайте файл PDF на нужном языке с носителя установки.

Обзор продукта

Продукты IBM® QRadar Security Intelligence Platform обеспечивают унифицированную архитектуру для интеграции информации о защите и управлении событиями (security information and event management, SIEM), управления журналами, выявления аномалий, экспертизы инцидентов и управления конфигурацией и уязвимостями. В этом руководстве Быстрый старт представлена информация об установке устройств IBM Security QRadar.

1 Шаг 1: Получите доступ к программе и документации

Прочтите замечания по выпуску для компонента QRadar, который вы хотите установить.

Загрузите ISO для нужного компонента QRadar с веб-сайта IBM FIX Central.

2 Шаг 2: Ознакомьтесь с компонентами передней и задней панелей

Прочтите информацию о компонентах передней и задней панелей для устройств, чтобы обеспечить правильное соединение и функционирование.

Более подробную информацию о компонентах передней и задней панелей для устройств смотрите в документе функции внешней и внутренней панелей.

На задней панели устройства каждого типа можно управлять последовательным разъемом и разъемами Ethernet с помощью модуля интегрированного управления. Более подробную информацию о модуле интегрированного управления смотрите в публикации *Модуль интегрированного управления: Руководство пользователя*.

3 Шаг 3: Требования при установке

Убедитесь, что выполняются следующие требования:

- Установлено необходимое оборудование.
- В случае устройств QRadar ноутбук соединяется с последовательным портом на задней панели устройства, или к устройству подключаются клавиатура и монитор.
- Вы вошли в систему как пользователь root.
- Вам доступен ключ активации.

Чтобы обеспечить успешную установку IBM® Security QRadar® на вашем собственном устройстве, нужно установить операционную систему Red Hat Enterprise Linux. Убедитесь, что ваше устройство отвечает требованиям к системе для внедрений QRadar. Более подробную информацию смотрите в публикации *QRadar: Руководство по аппаратному обеспечению*.

4 Шаг 4: Установка QRadar SIEM на вашем собственном устройстве

Учтите, что для продуктов Менеджер рисков QRadar и Экспертиза инцидентов QRadar требуются свои собственные лицензии, и они должны быть установлены на отдельных устройствах. Продукт QRadar Risk Manager должен быть установлен на управляемом хосте. Менеджер уязвмостей QRadar можно установить на одном компьютере с консолью в виде консоли 'все в одном'.

1. Если вы используете свое собственное устройство, смонтируйте образ QRadar ISO:
   a. Создайте каталог /media/cdrom, введя следующую команду:

      ```
      mkdir /media/cdrom
      ```

   b. Смонтируйте образ QRadar ISO, введя следующую команду:

      ```
      mount -o loop <путь QRadar ISO> /media/cdrom
      ```

   c. Чтобы начать установку, введите следующую команду:

      ```
      /media/cdrom/setup
      ```

2. Когда вас попросят ввести ключ активации, введите 24-значную алфавитно-цифровую строку из 4 частей, которую вы получили от IBM. Буква I и число 1 (один) обрабатываются одинаково. Буква O и число 0 (ноль) также обрабатываются одинаково.
3. В качестве типа установки выберите **Обычная**.
4. Выберите тип IP-адреса.
5. В мастере введите полное имя домена в поле **Имя хоста**.
6. В поле **IP адрес** введите статический IP-адрес или используйте IP-адрес, назначенный DHCP.

   Информацию о том, как задать первичный или вторичный хост IPv6, смотрите в публикации *IBM Security QRadar: Руководство по высокой доступности*.
7. Если у вас нет сервера электронной почты, введите значение `localhost` в поле **Имя сервера электронной почты**.
8. Нажмите **Готово**.
9. Создайте пароль в поле **Пароль root**. Пароли должны содержать не менее 5 символов, они не должны содержать пробелов и могут содержать следующие специальные символы: @, #, ^ и *.
10. Завершите установку, следуя инструкциям в мастере установки. Процесс установки может занять несколько минут.

5 Шаг 5: Примените свой лицензионный ключ

1. Войдите в систему QRadar:

   ```
   https://IP_адрес_QRadar
   ```

   По умолчанию, **Имя пользователя** - это `admin`. Значение **Пароль** - это пароль учетной записи пользователя root.
2. Откройте вкладку **Администрирование**.
3. В панели навигации выберите **Конфигурация системы**.
4. Щелкните по значку **Управление системой и лицензиями**.
5. В списке **Вид** выберите **Лицензии** и выгрузите ваш лицензионный ключ.
6. Выберите невыделенную лицензию и нажмите на **Выделить систему для лицензии**.
7. Выберите лицензию в списке лицензий и нажмите на **Выделить лицензию для системы**.

6 Шаг 6: Приступите к работе

Более подробную информацию о том, как начать использовать компоненты QRadar, смотрите в следующих источниках:

- Начинаем работу с IBM Security QRadar SIEM
- Начинаем работу с Менеджер рисков IBM Security QRadar
- Начинаем работу с Менеджер уязвмостей IBM Security QRadar
- Начинаем работу с Экспертиза инцидентов IBM Security QRadar
- Начинаем работу с Захват пакетов IBM Security QRadar.

Дополнительная информация

Чтобы получить полную документацию по продукту, посетите центр знаний IBM QRadar Security Intelligence Platform или загрузите документацию.

Код изделия: CN6J5ML

Printed in Ireland