Инструкция по установке (Linux)

Версия 4.5

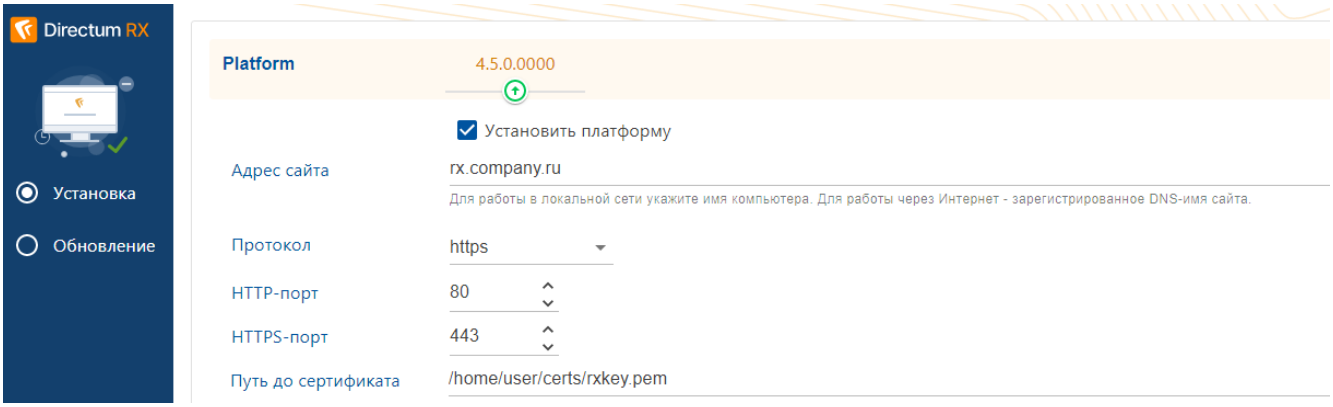
Содержание

Введение

Для установки, обновления и настройки системы используется кроссплатформенный инструмент **Directum Launcher**.

Directum Launcher поставляется в виде архива, который нужно распаковать. В распакованной папке хранится дистрибутив системы. Туда же при установке системы копируются файлы веб-сервера и сервисов Directum RX. Для корректной работы системы папку удалять нельзя.

При запуске Directum Launcher открывается страница в браузере:



Режим **Установка**, **Обновление** или **Настройка** выбирается автоматически в зависимости от того, была ли развернута система ранее. При необходимости положение переключателя можно изменить вручную.

Все параметры установки задаются в одном окне. Чтобы установить компоненты системы, необходимо в корень папки Directum Launcher добавить их архивы. Например, для установки серверной части Directum RX нужно добавить архив Platform.tar.gz, а для установки стандартной прикладной разработки – DirectumRX. tar.gz. Таким образом на странице появляются доступные параметры. При этом для компонента отображается номер версии и значок: – если версия доступна для установки, – если версия установлена.

По кнопке **Установить** генерируется конфигурационный файл config.yml и проверяются заполненные поля. Если проверка проходит без ошибок, запускается установка.

На странице выводятся результаты установки по каждому этапу и отображаются сообщения из лог-файла. Если возникли ошибки, их можно устранить и по кнопке **Повторить** выполнить повторную установку. По кнопке **Вернуться к настройкам** можно изменить ранее заданные настройки и также повторить установку. Когда установка завершится, на странице появляется ссылка для входа в веб-клиент.

После установки системы для повышения ее безопасности можно зашифровать значения заданных параметров: строки подключения к базе данных и другие конфиденциальные данные. Подробнее см. в руководстве администратора (Linux), раздел «Шифрование параметров».

Порядок установки системы

1. Ознакомьтесь с типовыми требованиями. Подробнее см. в документе «Directum RX 4.5. Типовые требования к аппаратному и программному обеспечению», входит в комплект поставки.
2. Выполните подготовительные действия.

3. Установите систему с помощью Directum Launcher. Также возможна установка с помощью командной строки.
4. Установите сервер NOMAD, если планируется использовать мобильные приложения Directum Solo и Directum Jazz.
5. Выполните дополнительные действия, если нужно перенести сервисы на выделенный сервер или настроить Directum RX в отказоустойчивом кластере. Подробнее см. руководство администратора, раздел «Расширенная установка».
6. Запросите и активируйте ключ лицензии. Если ключ лицензии не активирован, то работать в системе Directum RX одновременно смогут не более трех сотрудников. Подробнее см. руководство администратора, разделы «Запрос ключа лицензии» и «Активация ключа лицензии», входит в комплект поставки.
7. Настройте систему. Подробнее см. руководство администратора, входит в комплект поставки.

Подготовка к установке

Перед установкой системы:

1. Если планируется работа в Directum RX через Интернет, то приобретите у текущего интернет-провайдера внешний постоянный IP-адрес. Это необходимо, чтобы настроить на маршрутизаторе перенаправление необходимых портов с IP-адреса к серверу Directum RX. Также можно использовать существующий IP-адрес.
2. У регистратора доменных имен приобретите доменное имя, которое будет использоваться при установке Directum RX. Также можно использовать существующее доменное имя, если с ним не связаны другие сервисы, используемые в компании.

   ВАЖНО. После установки Directum RX изменять доменное имя не рекомендуется, так как для корректной работы необходимо будет полностью переустановить систему.
3. Создайте публичную DNS-запись, с помощью которой будет проходить перенаправление с доменного имени на внешний IP-адрес. Это необходимо для маршрутизации запросов на сервер Directum RX.
4. Приобретите SSL-сертификат с проверкой домена для работы по защищенному протоколу HTTPS. Он необходим для настройки доступа к системе Directum RX через Интернет.

   ПРИМЕЧАНИЕ. Доступ к системе по протоколу HTTPS также необходим для работы сервисов предпросмотра.
5. Установите SSL-сертификат на компьютер, где будут развернуты сервисы Directum RX.
6. Запросите в службе поддержки Directum RX код системы, который используется сервисами Directum RX, в штрихкодах документов, чтобы различать штрихкоды разных систем и т.д.

   ВАЖНО. Если приобретена лицензия на работу со средой разработки, запросите в службе поддержки Directum RX код компании, который будет использоваться в именах решений, модулей, сборок, пространств имен.
7. Установите сервер базы данных PostgreSQL или Postgres Pro, если его еще нет. Подробнее см. на сайте Postgres Pro статью «Документация PostgreSQL и Postgres Pro».

   ПРИМЕЧАНИЕ. Помимо пакета postgresql-server также установите postgresql-contrib.
8. Установите поисковую систему Elasticsearch и необходимые программные продукты, если в Directum RX планируется искать документы, задачи и задания по их содержимому.
9. Установите Docker Engine на сервере, на котором планируется развертывание серверных и сторонних компонентов Directum RX.
10. Если на сервере отсутствует доступ к сети Интернет или к репозиторию с базовыми образами, то загрузите базовые образы из локального архива.
11. Установите MongoDB – систему управления базами данных, которая используется для хранения данных сервисов Directum RX.
12. Установите брокер сообщений RabbitMQ. Брокер используется для обеспечения взаимодействия серверных компонентов Directum RX посредством сообщений. Если RabbitMQ уже установлен, убедитесь, что созданы необходимые учетные записи.

13. Если Directum RX устанавливается на компьютер с операционной системой Ubuntu 22.04 LTS, то установите на нем библиотеки libicu70 и libssl1.1. Они необходимы для корректного подключения к базе данных. Для этого последовательно выполните команды:

```
sudo apt update && sudo apt -y install libicu70

echo "deb http://old-releases.ubuntu.com/ubuntu impish-security main" | sudo tee /etc/apt/sources.list.d/impish-security.list

sudo apt update && sudo apt -y install libssl1.1
```

ПРИМЕЧАНИЕ. Среда разработки устанавливается только на компьютер с операционной системой Microsoft Windows. Подробнее см. инструкцию по установке, раздел «Среда разработки».

Создание SSL-сертификата

Для работы с системой можно использовать протокол HTTP или HTTPS. Протокол выбирается на этапе установки сервера.

Вариант работы по протоколу HTTP не рекомендуется использовать для удаленного доступа к системе Directum RX. Допускается только для работы в локальной сети, например, для тестирования системы. В этом случае данные от клиентских приложений передаются к серверу по сети в открытом виде.

Чтобы предоставить доступ к системе Directum RX через Интернет, необходимо использовать защищенный протокол HTTPS. В этом случае данные передаются в зашифрованном виде по технологии SSL. HTTPS-соединение устанавливается при успешной проверке валидности SSL-сертификата.

В главе рассматриваются способы получения SSL-сертификата:

- в официальном удостоверяющем центре (рекомендуемый);
- в удостоверяющем центре предприятия с помощью службы сертификации Active Directory.

Если используются мобильные приложения Directum Solo и Directum Jazz, для безопасной работы с данными установите сертификат, выданный удостоверяющим центром предприятия, на мобильные устройства сотрудников. Подробнее см. разделы по установке мобильных приложений:

- Directum Solo для iOS
- Directum Solo для Android
- Directum Jazz для iOS
- Directum Jazz для Android

Если для работы по протоколу HTTPS используется сертификат, выданный официальным удостоверяющим центром, дополнительная настройка на мобильном устройстве не требуется.

В официальном удостоверяющем центре

Удостоверяющий центр – это организация, которая выпускает сертификаты ключей электронной подписи. SSL-сертификаты рекомендуется приобретать в любом официальном удостоверяющем центре, у партнеров удостоверяющих центров либо на сайте регистратора доменных имен. Такие сертификаты создаются с использование криптографических средств, подтвержденных ФСБ РФ, и состоят из сложной цепочки сертификатов, которую сложно подделать.

Чтобы получить SSL-сертификат:

1. Сформируйте запрос, например, на сайте удостоверяющего центра, и укажите в запросе:
   - **доменное имя**, которое планируется использовать в адресе сайта для доступа к Directum RX;
   - **тип сертификата** – «SSL-сертификат с проверкой домена (Domain Validation)»;
   - **вариант приобретения сертификата**. Можно указать один из вариантов:

     «На один домен». SSL-сертификат подтверждает достоверность только конкретного домена.

     «На группу доменов (Wildcard-сертификат)». SSL-сертификат подтверждает достоверность конкретного домена и всех его поддоменов. Например, если сертификат приобретен для домена mycompany.ru, то SSL-сертификат будет защищать все поддомены вида *.mycompany.ru: rx.mycompany.ru, rabbitmq.mycompany.ru, office.mycompany.ru и другие.

     ПРИМЕЧАНИЕ. Если Wildcard-сертификат уже используется в организации, то новый сертификат приобретать не требуется. Достаточно зарегистрировать для существующего защищенного домена необходимый поддомен.
   - **адрес администратора домена**, если планируется подтверждать владение доменом через электронную почту. Возможные значения: admin@, administrator@, hostmaster@, postmaster@, webmaster@ в рамках домена, для которого запрашивается SSL-сертификат;
   - **дополнительную информацию**, например, о компании, на имя которой запрашивается сертификат.
2. Подтвердите владение доменом одним из способов, предложенных удостоверяющим центром, например:
   - **через электронную почту** (DCV Email). Удостоверяющий центр высылает верификационное письмо на электронную почту, указанную в запросе. В письме перейдите по ссылке для подтверждения владением домена;
   - **с помощью DNS-записи** (DNS CNAME). Если в компании настроен почтовый сервер, и для почты настроена приватная регистрация, то подтвердить владение доменом можно с помощью DNS-записи. В этом случае нужно создать специальную запись в DNS-сервере, удостоверяющий центр автоматически ее проверит;

- **с помощью хеш-файла** (HTTP CSR Hash). Удостоверяющий центр может предоставить специальный .txt файл, который необходимо загрузить на сервер компании. Удостоверяющий центр проверяет наличие файла и подтверждает владение доменом.

В результате удостоверяющий центр выдает комплект файлов, который состоит из открытого ключа, сертификата и файла, содержащего цепочку сертификатов, которые подписывают сертификат.

В удостоверяющем центре предприятия

SSL-сертификаты также можно создавать без обращения в официальный удостоверяющий центр, но такие сертификаты менее надежны. Их можно использовать, например, в рамках сети предприятия. В этом случае необходимо установить и настроить службу сертификации Active Directory для центра сертификации предприятия и сгенерировать сертификат.

Служба сертификации Active Directory – это служба для создания сертификатов открытых ключей и их управления, которые используются в системах безопасности программного обеспечения, где применяются технологии открытого ключа.

Чтобы получить SSL-сертификат:

1. Установите и настройте службу сертификации Active Directory на используемую ОС Microsoft Windows Server 2012/2012R2/2016. Подробнее см. в документации Microsoft статью Install the Certification Authority.

   ПРИМЕЧАНИЕ. Настраивайте службу сертификации Active Directory и ее компоненты с учетом специфики политики безопасности предприятия.
2. Настройте действие по умолчанию при получении запроса на сертификат. Для этого откройте оснастку **Центр сертификации** и в дереве консоли выберите ваш центр сертификации. В меню **Действие** выберите **Свойства**. Затем на вкладке **Модуль политики** выберите **Свойства** и выберите нужный параметр:
   - **Присвоить запросу состояние ожидания**, чтобы администратор центра сертификации мог просматривать каждый запрос на сертификат перед выдачей сертификата;
   - **Следовать параметрам, установленным в шаблоне сертификата, если они применимы, иначе автоматически выдавать сертификат**, чтобы центр сертификации мог выдавать сертификаты на основе конфигурации шаблона сертификата.

   После этого остановите и перезапустите центр сертификации.

   Подробнее см. в документации Microsoft статью Set the Default Action Upon Receipt of a Certificate Request.
3. Установите сертификат центра сертификации на компьютерах с клиентскими приложениями Directum RX.
4. При необходимости создайте и разверните шаблоны сертификатов.
5. Создайте SSL-сертификат.

Требования к оборудованию и программному обеспечению для установки службы сертификации Active Directory см. в документации Microsoft статью AD CS Migration: Preparing to Migrate.

После окончания срока действия центра сертификации все сертификаты нужно выдавать заново.

Для обеспечения контроля доверия к сертификату, который используется для подписания в системе Directum RX, необходимо иметь актуальный список отозванных сертификатов (CRL), установленный на локальный компьютер. Подробнее см. в документации Microsoft статью Configuring Certificate Revocation.

Установка сертификата центра сертификации

Для создания доверия к сертификатам пользователей, выданных центром сертификации, необходимо зарегистрировать сертификат центра сертификации на компьютерах пользователей системы.

Чтобы установить сертификат центра сертификации:

1. В сетевом окружении обратитесь к ресурсу \\<Сервер>\CertEnroll, где <Сервер> – это имя компьютера, на котором установлен центр сертификации.
2. Дважды щелкните мышью на файле с расширением *.crt, например, «study1.domain1.comp.npo_NameCA.crt».
3. В окне «Сертификат» на закладке «Общие» нажмите на кнопку **Установить сертификат...**.
4. В окне «Мастер импорта сертификатов»:
   - нажмите на кнопку **Далее>**;
   - установите переключатель **Поместить все сертификаты в следующее хранилище**;
   - нажмите на кнопку **Обзор** и выберите хранилище сертификатов **Доверенные корневые центры сертификации**;
   - нажмите на кнопку **Далее>**;
   - нажмите на кнопку **Готово**;
   - нажмите на кнопку **ОК**;
   - в окне «Сертификат» нажмите на кнопку **ОК**.

Для удобства рекомендуется устанавливать сертификаты на компьютеры пользователей через групповые политики Active Directory.

Шаблоны сертификатов центра сертификации

Использование шаблонов сертификатов производится с учетом специфики политики безопасности вашего предприятия. Настройка шаблонов не является обязательной.

Шаблон сертификата

Образец сертификата с заранее заданными настройками по умолчанию. Используется для создания новых сертификатов.

Шаблоны сертификатов упрощают задачу администрирования центра сертификации, позволяя администраторам выдавать сертификаты, предварительно настроенные для выбранных задач. Оснастка «Шаблоны сертификатов» устанавливается при установке центра сертификации и позволяет администратору выполнять задачи:

- просматривать свойства каждого шаблона сертификата;
- копировать и изменять шаблоны сертификатов;
- указывать пользователей и компьютеры, которые могут считывать шаблоны и регистрировать сертификаты;
- выполнять другие задачи администрирования, относящиеся к шаблонам сертификатов.

Примечание

Сертификаты, основанные на шаблонах сертификатов, могут выдаваться только центрами сертификации с типом «Предприятие».

Чтобы создать шаблон сертификатов:

1. В меню **Пуск** последовательно выберите пункты **Администрирование**, **Центр сертификации**.
2. В окне «Центр сертификации» выберите созданный центр сертификации в папке **Шаблоны сертификатов**. Выберите пункт контекстного меню **Управление**.
3. В окне «Консоль шаблонов сертификатов» выберите пункт контекстного меню **Скопировать шаблон** для шаблона «Компьютер».
4. В окне «Свойства нового шаблона» на закладке «Совместимость»:
   - в поле **Центр сертификации** укажите значение **Windows Server 2003**;
   - в поле **Сертификат получателя** укажите значение **Windows XP / Server 2003**;
   - нажмите на кнопку **ОК**.
5. На закладке «Общие»:
   - заполните поле **Отображаемое имя шаблона**. Отображается в оснастке **Шаблоны сертификатов**, а также во всех других компонентах, используемых для выдачи сертификатов;
   - заполните поле **Имя шаблона**. Отображается только в свойствах самого сертификата;
   - задайте период действия шаблона в поле **Период действия**;
   - задайте период обновления шаблона сертификата в поле **Период обновления**;
   - установите флажок **Опубликовать в Active Directory**.
6. На закладке «Обработка запроса»:
   - в выпадающем списке **Цель сертификата** выберите значение **Подпись и шифрование**;
   - установите флажок **Включить симметричные алгоритмы, разрешенные субъектом**;
   - установите флажок **Разрешить экспортировать закрытый ключ**;

- в поле **Минимальный размер ключа** укажите:
  a) **1024** или выше для модулей расширения Standard Encryption;
  b) **512** для модуля расширения GOST Encryption.
- установите переключатель **Подавать заявку для субъекта, не требуя ввода данных**.

7. На закладке «Имя субъекта» установите переключатель **Предоставляется в запросе**.
8. На закладке «Безопасность»:
   - для группы пользователей «Прошедшие проверки» установите флажок **Чтение**;
   - для группы пользователей «Administrator» установите флажки **Чтение**, **Запись**, **Заявка**;
   - для группы пользователей «Domain Admins» установите флажки **Чтение**, **Запись**, **Заявка**;
   - для группы пользователей «Domain Users» установите флажок **Заявка**;
   - для группы пользователей «Enterprise Admins» установите флажки **Чтение**, **Запись**, **Заявка**.
9. Нажмите на кнопку **ОК**.

Администратор может:

- добавить шаблон сертификата в центр сертификации. Подробнее см. в документации Microsoft статью Add a Certificate Template to a Certification Authority;
- настроить автоматическую подачу заявок на сертификаты. Подробнее см. в документации Microsoft статью Set Up Automatic Certificate Enrollment.

Создание SSL-сертификата из оснастки

Чтобы создать SSL-сертификат из оснастки:

1. Запросите сертификат через мастер создания запроса;
2. Экспортируйте сертификат в PFX-файл.

Запрос и получение SSL-сертификата

1. Откройте окно консоли MMC и добавьте оснастку «Сертификаты» для учетной записи локального компьютера.
2. В контекстном меню узла **Личное** последовательно выберите пункты **Все задачи**, **Запросить новый сертификат**.
3. Откроется окно мастера «Регистрация сертификатов». Нажмите в окне два раза на кнопку **Далее**, чтобы получить доступ к запросу сертификатов.
4. Выберите ранее созданный шаблон сертификата.
5. Перейдите по ссылке **Требуется больше данных для подачи заявки на сертификат. Щелкните здесь для настройки параметров...**.
6. На вкладке «Субъект» в группе **Имя субъекта** в поле **Тип** выберите значение **Общее имя**.
7. Введите доменное имя сервиса, для которого будет подготовлен SSL-сертификат, например, «directumrx.mycompany.com» и нажмите на кнопку **Добавить**.

8. Перейдите на вкладку «Закрытый ключ».
9. В группе **Параметры ключа** установите флажок **Сделать закрытый ключ экспортируемым** и нажмите на кнопку **ОК**.
10. В окне мастера «Запрос сертификатов» установите флажок рядом с нужным шаблоном и нажмите на кнопку **Заявка**.
11. После генерации сертификат будет помещен в личное хранилище сертификатов локального компьютера.

Экспорт SSL-сертификата в PFX-файл

1. Откройте окно консоли MMC и добавьте оснастку «Сертификаты» для учетной записи локального компьютера.
2. Откройте узел с сертификатами **Личное** > **Сертификаты**.
3. Выберите сертификат, наименование которого соответствует DNS-имени сервиса, для которого создавался SSL-сертификат.
4. Щелкните два раза левой кнопкой мыши по сертификату.
5. В окне «Сертификат» перейдите на вкладку «Состав» и нажмите на кнопку **Копировать в файл**.
6. Откроется окно мастера экспорта сертификатов. Нажмите в нем на кнопку **Далее**.
7. Установите переключатель в положение **Да**, экспортировать закрытый ключ и нажмите на кнопку **Далее**.
8. Установите флажки **Включить по возможности все сертификаты в путь сертификации**, **Экспортировать все расширенные свойства** и нажмите на кнопку **Далее**.
9. Задайте пароль для сертификата и нажмите на кнопку **Далее**.
10. Выберите расположение и имя экспортируемого файла, нажмите на кнопку **Далее**.
11. Нажмите на кнопку **Готово**. Будет экспортирован SSL-сертификат в формате **PFX**.

Установка SSL-сертификата

1. На сервере Directum RX добавьте корневой сертификат удостоверяющего центра сертификации в список доверия. Порядок установки зависит от используемого дистрибутива Linux.

   Альт Сервер

   Выполните команду:

   ```
   sudo trust anchor --store <Путь до корневого сертификата>
   ```

   Astra Linux

   Скопируйте сертификат *.crt в папку /usr/local/share/ca-certificates и выполните команду:

   ```
   update-ca-certificates
   ```
2. Перейдите в распакованный архив с Directum Launcher и в папку etc скопируйте закрытый ключ в формате PFX в папку etc.

3. Сконвертируйте закрытый PFX-ключ в формат PEM. Для этого выполните команду:

   ```
   ./do.sh convert_pfx_to_pem <Путь к сертификату *.pfx> <пароль от сертификата>
   ```

   Пример:

   ```
   ./do.sh convert_pfx_to_pem /srv/rxscripts/etc/rxkey.pfx "Password"
   ```

Загрузка базовых образов

Базовые образы включают в себя сторонние компоненты и образы для последующего развертывания системы, например SDK для .NET. Базовые образы автоматически скачиваются из репозитория во время установки системы. Если на сервере отсутствует доступ к сети Интернет или к репозиторию, то загрузите базовые образы из локального архива. Для этого:

1. Архив с Directum Launcher распакуйте в локальную папку на сервере с помощью команды:

   ```
   tar -xvf <Имя архива> -C <Имя папки>
   ```

   ВАЖНО. Для корректной установки общий путь к файлам должен быть не более 256 символов. Также он не должен содержать пробелы, символы кириллицы, запятые и спецсимволы. Поэтому используйте, например, папку /srv/DirectumLauncher.

2. Загрузите базовые образы из архива images.tar.gz в среду Docker с помощью команды:

   ```
   ./do.sh images load --path="<Путь к архиву с образами>"
   ```

   Пример:

   ```
   ./do.sh images load --path="srv/images.tar.gz"
   ```

Установка поисковой системы Elasticsearch

В разделе рассмотрены варианты установки поисковой системы Elasticsearch:

- ручная установка
- установка готовой виртуальной машины

Вариант с виртуальной машиной используется для быстрой установки поисковой системы. Образ виртуальной машины можно получить бесплатно по запросу в службе поддержки Directum RX.

Ручная установка Elasticsearch

В разделе рассмотрена установка поисковой системы в Linux на примере Альт Сервер 9.1.

В службе поддержки Directum RX запросите архив с поисковой системой Elasticsearch, панелью управления Kibana и дополнительными файлами для настройки. Дистрибутивы предоставляются бесплатно, дополнительную лицензию приобретать не нужно.

ВАЖНО. Для ручной установки в Linux необходимо использовать Elasticsearch 7.16.3. Работа с другими версиями не гарантируется.

На сервере, который планируется использовать для поисковой системы:

1. Установите Elasticsearch 7.16.3. Для этого выполните команду:

   ```
   sudo rpm --install <Путь к пакету>/elasticsearch-7.16.3-x86_64.rpm
   ```

   Пример:

   ```
   sudo rpm --install /srv/elasticsearch-7.16.3-x86_64.rpm
   ```

2. Запустите службу Elasticsearch с помощью команд:

   ```
   sudo systemctl daemon-reload
   sudo systemctl enable elasticsearch
   sudo systemctl start elasticsearch
   ```

3. Проверьте состояние службы с помощью команды:

   ```
   sudo systemctl status elasticsearch
   ```

   Если служба запущена, то в командной строке отобразится состояние **active (running)**:

```
operator_vm@ubu-es:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2019-11-19 14:23:25 +05; 34s ago
     Docs: http://www.elastic.co
 Main PID: 2745 (java)
    Tasks: 43 (limit: 2197)
   CGroup: /system.slice/elasticsearch.service
           └─2745 /usr/share/elasticsearch/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSIni

Nov 19 14:23:08 ubu-es systemd[1]: Starting Elasticsearch...
Nov 19 14:23:10 ubu-es elasticsearch[2745]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC
Nov 19 14:23:25 ubu-es systemd[1]: Started Elasticsearch.
```

4. Установите плагин ingest-attachment, который входит в состав дистрибутива Elasticsearch. Для этого выполните команду:

   ```
   sudo /usr/share/elasticsearch/bin/elasticsearch-plugin install file:<Путь к архиву>/ingest-attachment-7.16.3.zip
   ```

   Пример:

   ```
   sudo /usr/share/elasticsearch/bin/elasticsearch-plugin install file:/srv/ingest-attachment-7.16.3.zip
   ```

5. Установите плагин analysis-morphology. Для этого из архива скопируйте файл analysis-morphology-7.16.3.zip в локальную папку и выполните команду:

   ```
   /usr/share/elasticsearch/bin/elasticsearch-plugin install file:<Путь к архиву>/analysis-morphology-7.16.3.zip
   ```

   Пример:

   ```
   /usr/share/elasticsearch/bin/elasticsearch-plugin install file:/srv/analysis-morphology-7.16.3.zip
   ```

6. Из архива скопируйте словарь синонимов synonyms.txt в папку /etc/elasticsearch.
7. Настройте прокси-сервер nginx для безопасного подключения к Elasticsearch.
8. Установите панель управления Kibana 7.16.3. Панель используется для настройки словаря синонимов и мониторинга работы полнотекстового поиска. Чтобы установить службу Kibana, выполните команду:

   ```
   sudo rpm --install <Путь к пакету>/kibana-7.16.3-x86_64.rpm
   ```

   Пример:

   ```
   sudo rpm --install /srv/kibana-7.16.3-x86_64.rpm
   ```

9. Запустите службу Kibana с помощью команд:

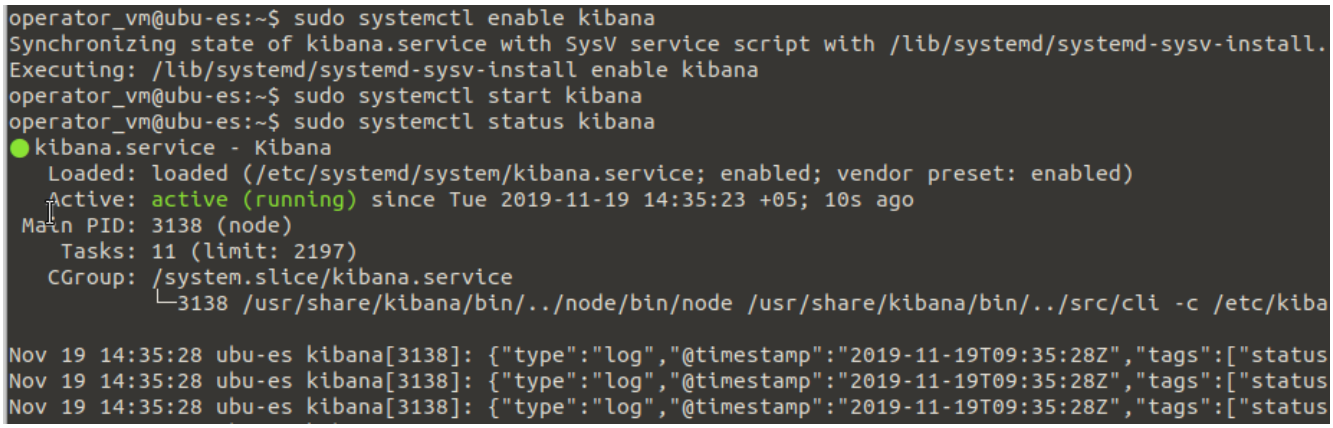
   ```
   sudo systemctl enable kibana
   ```

```
sudo systemctl start kibana
```

10. Проверьте состояние службы с помощью команды:

    ```
    sudo systemctl status kibana
    ```

    Если служба запущена, то в командной строке отобразится состояние **active (running)**:



Настройка nginx

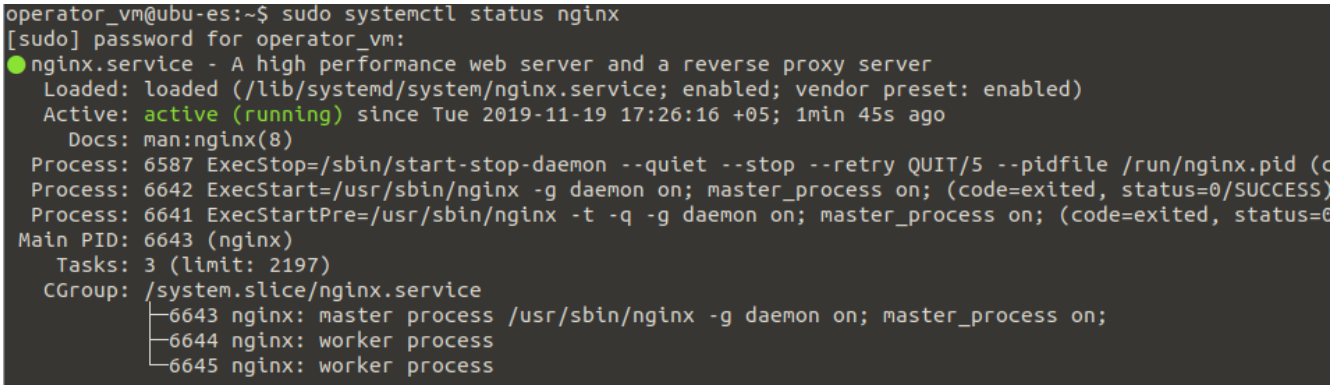
1. Скачайте и установите прокси-сервер nginx с помощью команд:

   ```
   sudo apt-get update
   sudo apt-get install nginx
   ```

2. Проверьте состояние прокси-сервера с помощью команды:

   ```
   sudo systemctl status nginx
   ```

   Если прокси-сервер запущен, то в командной строке отобразится состояние **active (running)**:



3. В конфигурационном файле /etc/nginx/nginx.conf в качестве максимального размера запроса укажите 100 МБ. Для этого в секции **http** в параметре **client_max_body_size** задайте значение **100M**.

   Пример настройки:

   ```
   http {
       ...
       client_max_body_size 100M;
       ...
   }
   ```

4. Из архива, полученного в службе поддержки, скопируйте конфигурационный файл nginx default.conf в папку /etc/nginx/sites-enabled.d.
5. Задайте настройки доступа к Elasticsearch и Kibana в конфигурационном файле nginx – /etc/nginx/sites-enabled.d/default.conf. Для этого выполните аналогичные действия из раздела «Настройка nginx». В параметре **listen** укажите IP-адрес компьютера с установленным прокси-сервером.

Установка виртуальной машины с Elasticsearch

На виртуальной машине развернуты:

- операционная система Ubuntu 18.04;
- поисковая система Elasticsearch 7.16.3 и ее плагины;
- панель управления Kibana 7.16.3;
- прокси-сервер nginx 1.14.0.

Чтобы установить виртуальную машину в Microsoft Windows:

1. Распакуйте архив с образом виртуального жесткого диска на локальный компьютер.
2. Запустите **Диспетчер Hyper-V**.
3. В меню **Действие** выберите пункт **Создать**, в открывшемся списке выберите пункт **Виртуальная машина**. Запустится **Мастер создания виртуальной машины**.
4. На странице «Укажите имя и расположение» укажите **Имя** виртуальной машины и нажмите на кнопку **Далее**.
5. На странице «Поколение» установите переключатель **Поколение 1** и нажмите на кнопку **Далее**.
6. На странице «Выделить память» в поле **Память** укажите объем ОЗУ в соответствии с системными требованиями. Подробнее см. документ «Directum RX 4.5. Типовые требования к аппаратному и программному обеспечению», входит в комплект поставки. Нажмите на кнопку **Далее**.
7. На странице «Настройка сетевых подключений» выберите имя внутренней виртуальной сети и нажмите на кнопку **Далее**.
8. На странице «Подключить виртуальный жесткий диск» установите переключатель **Использовать имеющийся виртуальный жесткий диск**, нажмите на кнопку **Обзор** и выберите файл виртуального диска. Затем нажмите на кнопку **Далее**.
9. На странице «Сводка» нажмите на кнопку **Готово**.
10. В списке виртуальных машин выберите созданную виртуальную машину и в ее контекстном меню выберите пункт **Параметры**.
11. В открывшемся окне выделите пункт **Процессор** и укажите количество процессоров в соответствии с системными требованиями. Подробнее см. документ «Directum RX 4.5. Типовые требования к аппаратному и программному обеспечению», входит в комплект поставки.
12. Настройте сетевой доступ к виртуальной машине. Для этого в конфигурационном файле /etc/netplan/50-cloud-init.yaml в параметре **addresses** укажите IP-адрес виртуальной машины. При необходимости в IP-адресе виртуальной машины можно указать адрес подсети в формате CIDR.

    Затем в группе **nameservers** в параметре **addresses** укажите IP-адреса DNS-серверов.

Пример:

```
network:
    renderer: networkd
    ethernets:
        eth0:
            dhcp4: no
            dhcp6: no
            #   IP-адрес виртуальной машины
            addresses: [192.168.4.252/18]
            nameservers:
            #   IP-адреса предпочитаемого DNS-сервера и альтернативного
                addresses: [192.168.4.1,192.168.4.2]
    version: 2
```

13. Настройте прокси-сервер nginx, чтобы разрешить доступ к Elasticsearch и Kibana только с серверов, на которых развернут сервис индексирования и веб-сервер.

Подробнее о создании виртуальной машины см. в документации Microsoft, в статье «Создание виртуальной машины с помощью Hyper-V в Windows10».

Виртуальную машину можно развернуть в другой операционной системе. Например, в Linux можно использовать эмулятор QEMU. В этом случае используйте документацию на соответствующий программный продукт.

Настройка nginx

1. На виртуальной машине в конфигурационном файле /etc/nginx/sites-enabled/default укажите настройки доступа:
   - к Elasticsearch – с компьютеров, на которых установлены веб-сервер и сервис индексирования;
   - к Kibana – с компьютера администратора.

   Пример настройки:

```
# Настройка доступа к Elasticsearch
server {
  listen 192.168.4.252:9200;

  location / {
    allow 192.168.47.37;
    deny all;
    proxy_pass http://127.0.0.1:9200;
  }
}

# Настройка доступа к Kibana
server {
  listen 192.168.4.252:5601;

  location / {
    allow 192.168.45.35;
    deny all;
    proxy_pass http://127.0.0.1:5601;
  }
}
```

Где:

- **server** – секция настроек проксируемого сервера, с установленными Elasticsearch и Kibana;
- **listen** – имя и порт проксируемого сервера. Значение, указанное по умолчанию, замените на IP-адрес виртуальной машины;
- **allow** – список IP-адресов, с которых разрешено подключение;
- **deny** – список IP-адресов, с которых запрещено подключение. Чтобы запретить доступ со всех адресов кроме разрешенных, укажите значение **all**.

  ПРИМЕЧАНИЕ. Настройки, указанные в секции **allow**, имеют больший приоритет, чем в секции **deny**. Если IP-адрес указан в секции **allow**, то настройки из секции **deny** не применяются к нему;
- **proxy_pass** – проксируемый IP-адрес. Для Elasticsearch укажите **http://127.0.0.1:9200**, для Kibana – **http://127.0.0.1:5601**.

Подробнее о настройке конфигурационного файла см. в документации nginx, в статье «Структура конфигурационного файла».

2. Перезапустите службу nginx, чтобы применить заданные настройки. Для этого выполните команду:

   ```
   sudo systemctl restart nginx
   ```

3. Убедитесь, что поисковая система Elasticsearch доступна с компьютеров, на которых установлены веб-сервер и сервис индексирования. Для этого в браузере перейдите по адресу <Адрес сервера с поисковой системой Elasticsearch>:9200. Если настройки выполнены верно, откроется страница с параметрами Elasticsearch.
4. Убедитесь, что панель Kibana доступна с компьютера администратора. Для этого в браузере перейдите по адресу <Адрес сервера с панелью Kibana>:5601. Если настройки выполнены верно, откроется стартовая страница Kibana.

Установка Docker Engine

Порядок установки компонентов Docker Engine отличается в зависимости от используемого дистрибутива Linux. Подробнее см. в документации Docker Engine статью Install Docker Engine. Далее приведены примеры установки в Альт Сервер 9.1, Astra Linux Common Edition 2.12.29 (Орел) и РЕД ОС 7.3.

Альт Сервер 9.1

1. Получите список обновлений и установите Docker Engine. Для этого выполните команды:

   ```
   sudo apt-get update
   sudo apt-get install docker-ce
   ```

2. Настройте запуск сервиса docker без использования команды **sudo**. Для этого в группу docker добавьте пользователя, в сеансе которого запускается сервис:

   ```
   sudo usermod -aG docker $USER
   ```

3. Чтобы применить настройки группы, перезайдите в операционную систему под текущим пользователем:

   ```
   logout
   ```

4. Запустите сервис docker:

```
sudo systemctl enable --now docker
```

5. Проверьте, что сервис запущен корректно:

```
docker -v
```

```
docker ps -a
```

Если установка выполнена успешно, первая команда выведет версию Docker Engine, вторая – пустой список контейнеров.

Astra Linux Common Edition 2.12.29 (Орел)

1. Подключите репозиторий и установите Docker Engine. Для этого последовательно выполните команды:

```
apt update && apt upgrade
```

```
sudo apt-get install apt-transport-https ca-certificates curl gnupg2
```

```
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -
```

```
echo "deb [arch=amd64] https://download.docker.com/linux/debian stretch
stable" | sudo tee -a /etc/apt/sources.list
```

```
sudo apt update
```

```
sudo apt install docker-ce
```

2. Проверьте, что сервис запущен корректно:

```
sudo systemctl status docker
```

Если сервис запущен, команда выведет статус сервиса «Active: active (running)». Нажмите клавиши CTRL+C, чтобы завершить выполнение команды.

3. Проверьте установленную версию Docker Engine с помощью команды:

```
docker --version
```

4. Настройте запуск сервиса docker без использования команды **sudo**. Для этого в группу docker добавьте пользователя, в сеансе которого запускается сервис:

```
sudo usermod -aG docker $USER
```

5. Чтобы применить настройки группы, перезайдите в операционную систему под текущим пользователем:

```
logout
```

6. Установите Docker Compose. Для этого последовательно выполните команды:

```
sudo curl -L
https://github.com/docker/compose/releases/download/1.23.2/docker-compose-
Linux-x86_64 -o /usr/local/bin/docker-compose
```

```
sudo chmod +x /usr/local/bin/docker-compose
```

7. Проверьте, что Docker Compose установлен:

```
docker-compose --version
```

Если установка выполнена успешно, команда выведет версию Docker Compose.

РЕД ОС 7.3

1. Установите Docker Engine. Для этого выполните команду:

   ```
   dnf install docker-ce
   ```

2. Запустите Docker Engine:

   ```
   systemctl start docker
   ```

3. Настройте запуск сервиса docker без использования команды **sudo**. Для этого в группу docker добавьте пользователя, в сеансе которого запускается сервис:

   ```
   sudo usermod -aG docker $USER
   ```

4. Чтобы применить настройки группы, перезайдите в операционную систему под текущим пользователем:

   ```
   logout
   ```

5. Проверьте, что сервис docker запущен корректно:

   ```
   docker -v
   ```

   ```
   docker ps -a
   ```

   Если установка выполнена успешно, первая команда выведет версию Docker Engine, вторая – пустой список контейнеров.

Подробнее см. в документации РЕД ОС статью «Установка и настройка docker».

Установка MongoDB

MongoDB можно установить вместе с веб-сервером либо на отдельный сервер.

Чтобы установить MongoDB:

1. Распакуйте архив с Directum Launcher в локальную папку на сервере, если это не было сделано ранее. Для этого выполните команду:

   ```
   tar -xvf <Имя архива> -C <Имя папки>
   ```

   Пример команды:

   ```
   tar -xvf DirectumLauncher.tar.gz -C /srv/DirectumLauncher
   ```

2. Установите Docker Engine, если это не сделано ранее.
3. Если отсутствует доступ к сети Интернет либо к репозиторию базовых образов, загрузите базовые образы из локального архива. Если они загружены ранее, пропустите пункт.
4. Если конфигурационный файл config.yml ранее не был создан, создайте конфигурационный файл config.yml на основе файла DirectumLauncher/etc/config.yml.example, который входит в комплект поставки. Для этого выполните команду:

   ```
   cp /srv/DirectumLauncher/etc/config.yml.example /srv/DirectumLauncher/etc/config.yml
   ```

5. Создайте локальную папку, например /srv/rxdata, и укажите путь к ней в секции **variables** в переменной **home_path**. В созданной папке появятся подпапки для хранения содержимого документов, файлов предпросмотра, лог-файлов системы и других данных. Если часть данных нужно хранить в отдельных папках, после установки измените путь в соответствующей настройке конфигурационного файла.

6. В созданном конфигурационном файле добавьте секцию **SungeroMongodb** и заполните параметры:

   mongodb_data_path – папка для хранения данных MongoDB;

   user, **password** – имя и пароль пользователя для подключения к MongoDB. Укажите свои значения;

   port – порт, по которому MongoDB взаимодействует с сервисами Directum RX. Если параметр не заполнен, используется порт **27017**.

   ВАЖНО. В пароле нельзя использовать спецсимвол @. С помощью @ в строке подключения отделяется пароль от адреса сервера. Если пароль содержит @, то его часть не будет обрабатываться, при подключении к MongoDB возникнет ошибка.

   Указанные параметры будут использоваться для создания базы данных MongoDB и пользователя для подключения к ней.

   Пример настройки:

```
SungeroMongodb:
  mongodb_data_path: '{{ home_path }}/mongodb_data'
  user: admin
  password: 11111
  port: 27017
```

7. Разверните контейнер MongoDB. Для этого в командной строке перейдите в папку с Directum Launcher и выполните команду:

```
./do.sh mongodb up
```

Установка RabbitMQ

Установите и затем настройте RabbitMQ. Установить можно вместе с веб-сервером или на отдельный сервер.

Установка RabbitMQ

1. Распакуйте архив с Directum Launcher в локальную папку на сервере, если это не было сделано ранее. Для этого выполните команду:

```
tar -xvf <Имя архива> -C <Имя папки>
```

   Пример команды:

```
tar -xvf DirectumLauncher.tar.gz -C /srv/DirectumLauncher
```

2. Установите Docker Engine, если это не сделано ранее.
3. Если отсутствует доступ к сети Интернет либо к репозиторию базовых образов, загрузите базовые образы из локального архива. Если они загружены ранее, пропустите пункт.
4. Если конфигурационный файл config.yml ранее не был создан, создайте конфигурационный файл config.yml на основе файла DirectumLauncher/etc/config.yml.example, который входит в комплект поставки. Для этого выполните команду:

```
cp /srv/DirectumLauncher/etc/config.yml.example /srv/DirectumLauncher/etc/config.yml
```

5. В секции **variables** в переменной **home_path** укажите путь до папки с данными, например /srv/rxdata.

6. В конфигурационном файле config.yml добавьте секцию **SungeroRabbitMQ**. В параметре **rabbitmq_data_path** укажите папку для хранения данных RabbitMQ.

   Пример настройки:

   ```
   SungeroRabbitMQ:
       rabbitmq_data_path: '{{ home_path }}/rabbitmq_data'
   ```

7. Разверните контейнер RabbitMQ. Для этого в командной строке перейдите в папку с Directum Launcher и выполните команду:

   ```
   ./do.sh rabbitmq up
   ```

8. Настройте RabbitMQ.

Настройка RabbitMQ

ВАЖНО. Для значений параметров RabbitMQ учитывается регистр символов.

Чтобы настроить RabbitMQ:

1. Откройте страницу администрирования RabbitMQ. Для этого перейдите по ссылке **https://<IP-адрес или имя компьютера с RabbitMQ>/rabbitmq/**. В открывшемся окне заполните поля: **login** – guest, **password** – guest.
2. На открывшейся странице создайте пользователя с правами администратора. Для этого перейдите на вкладку **Admin** и в разделе «Add a user» заполните поля **Username**, **Password** – логин и пароль администратора RabbitMQ. Права администратора в дальнейшем нужны для создания пользователя, от имени которого система Directum RX будет подключаться к RabbitMQ.
3. В поле **Tags** выберите значение «Admin» и нажмите на кнопку **Add user**.
4. Повторно перейдите на страницу администрирования и в открывшемся окне укажите логин и пароль созданного пользователя.
5. Удалите пользователя guest. Для этого выберите в списке пользователя guest и в разделе «Delete this user» нажмите на кнопку **Delete**.
6. Создайте виртуальный хост RabbitMQ для работы с Directum RX. Для этого на вкладке **Admin** на панели справа перейдите в группу **Virtual Hosts** и в разделе «Add a new virtual host» в поле **Name** заполните название хоста, например, rxhost. Затем нажмите на кнопку **Add virtual host**.
7. На панели справа перейдите в группу **Users**.
8. Создайте пользователя, от имени которого система Directum RX сможет подключаться к RabbitMQ. Для этого на вкладке **Admin** в разделе «Add a user» заполните поля **Username**, **Password** – логин и пароль пользователя. Затем в поле **Tags** выберите значение «None» и нажмите на кнопку **Add user**.
9. Выберите созданного пользователя в списке, затем в разделе **Permissions** в поле **Virtual Host** выберите созданный виртуальный хост и нажмите на кнопку **Set permission**.
10. В разделе «Topic permissions» в поле **Virtual Host** выберите созданный виртуальный хост и нажмите на кнопку **Set topic permission**.

Подробнее об установке RabbitMQ см. в документации на сайте продукта, статья Documentation: Table of Contents.

Установка системы (Directum Launcher)

1. Архив с Directum Launcher распакуйте в локальную папку на сервере. В корень папки скопируйте архивы:
   - Platform.tar.gz – веб-сервер и сервисы Directum RX;
   - DirectumRX.tar.gz – стандартная прикладная разработка Directum RX, а также утилиты RxCmd и DrxUtil;
   - WebHelp.zip – справка и слайдер.

   ВАЖНО. Для корректной установки общий путь к файлам должен быть не более 256 символов. Также он не должен содержать пробелы, символы кириллицы, запятые и спецсимволы. Поэтому используйте, например, папку /srv/DirectumLauncher. В зависимости от настроек операционной системы для дальнейших действий могут потребоваться права суперпользователя.
2. Увеличьте максимально допустимое количество наблюдателей за файлами на текущем компьютере – системный параметр /proc/sys/fs/inotify/max_user_instances. Для этого в командной строке перейдите в созданную папку и с привилегиями суперпользователя выполните команду:

   ```
   ./do.sh set_inotify_instances_limit
   ```
3. Если в компании не используется DNS-сервер, создайте конфигурационный файл config.yml на основе файла DirectumLauncher/etc/config.yml.example. В созданном файле в секции **extra_hosts** укажите соответствие IP-адреса текущего сервера и доменного имени, по которому доступна система Directum RX.

   Пример настройки:

   ```
   extra_hosts:
       company-rx.directum.ru: '192.168.0.42'
   ```

   Во время установки указанное соответствие запишется в файл hosts docker-контейнеров. Это необходимо для корректного импорта шаблонов документов и пакетов разработки.

   ПРИМЕЧАНИЕ. Настройка секции **extra_hosts** также может потребоваться, если используемый дистрибутив Linux не поддерживает работу docker-контейнеров с DNS.
4. Запустите Directum Launcher. Способ запуска зависит от используемого дистрибутива Linux.

   Linux с графической оболочкой:

   ```
   ./DirectumLauncher
   ```

   В командной строке запустится сервис для работы с Directum Launcher, в браузере откроется страница с параметрами установки и обновления. Окно командной строки не закрывайте до окончания установки.

   Страницу установки можно открыть вручную по ссылке **http://127.0.0.1:5000/**, где **5000** – порт по умолчанию. Порт можно изменить, добавив к команде ключ **--port=<номер порта>**.

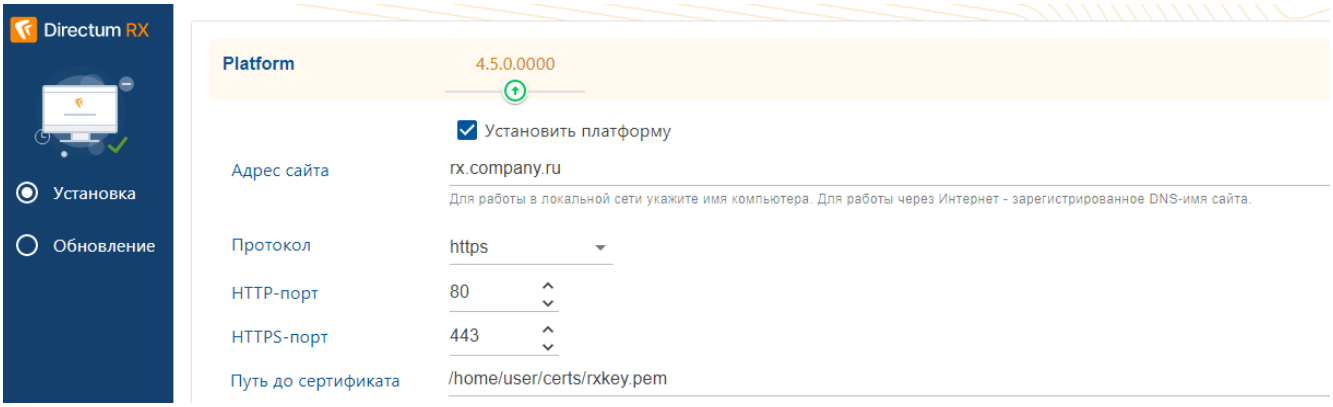
   Linux без графической оболочки:

   ```
   ./DirectumLauncher --host=0.0.0.0
   ```

   При выполнении команды с ключом **--host** выведется адрес страницы с параметрами установки и обновления. Страницу откройте в браузере на компьютере с графической оболочкой, дальнейшие действия выполняйте там.

ПРИМЕЧАНИЕ. С помощью ключей запуска можно подключиться к Directum Launcher с другого компьютера, настроить аутентификацию для входа и использовать защищенный протокол HTTPS. Также можно сменить локализацию на английскую. Подробнее см. раздел «Дополнительные параметры запуска Directum Launcher».

5. На открывшейся странице убедитесь, что выбран режим **Установка**, и укажите настройки веб-сервера:



Установить платформу. Убедитесь, что флажок установлен. Если флажок не установлен, то поля с настройками веб-сервера и сервисов Directum RX недоступны.

Адрес сайта. Имя компьютера, на котором будет установлен веб-сервер Directum RX. По умолчанию заполняется полным доменным именем текущего компьютера. Для работы через Интернет необходимо указать внешнее зарегистрированное DNS-имя сайта, например rx.company.ru.

ВАЖНО. После установки системы изменять адрес сайта не рекомендуется.

Протокол, который будет использоваться для работы с системой. Возможные значения: **https**, **http**. Значение по умолчанию **https**. Для работы с системой рекомендуется использовать защищенный протокол HTTPS.

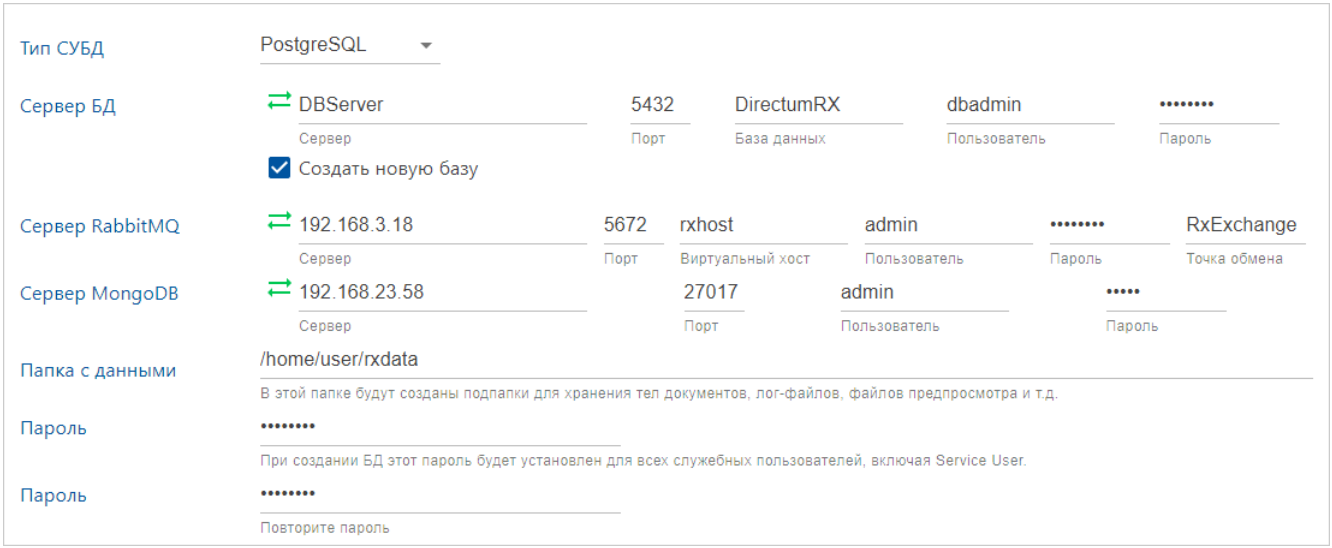
Протокол HTTP не рекомендуется использовать для удаленного доступа к системе Directum RX. Допускается только при работе в локальной сети компании для тестирования системы. В этом случае данные от клиентского приложения к веб-серверу передаются по сети в открытом виде.

HTTP-порт. Порт для работы с системой по протоколу HTTP. Значение по умолчанию **80**.

HTTPS-порт. Порт для работы с системой по протоколу HTTPS. Значение по умолчанию **443**. Поле активно, если в поле **Протокол** указано значение **https**.

Путь до сертификата, расположенного на сервере, в формате PEM. Сертификат должен подходить для указанного имени сайта и содержать цепочку сертификатов. Подробнее см. раздел «Установка SSL-сертификата». Поле активно, если в поле **Протокол** указано значение **https**.

6. Укажите настройки базы данных и сервисов:



Тип СУБД, которая используется для хранения данных системы Directum RX. Возможные значения: **PostrgreSQL** – PostgreSQL/Postgres Pro, **Microsoft SQL** – Microsoft SQL Server. При установке системы в Linux рекомендуется использовать PostgreSQL.

Выберите вариант развертывания базы данных:

- если БД была создана ранее, снимите флажок **Создать новую базу**. По умолчанию флажок установлен;
- если нужно создать новую БД, оставьте флажок **Создать новую базу** установленным.

В поле **Сервер БД** укажите параметры подключения к новой базе данных PostgeSQL:

- **Сервер**. Имя экземпляра СУБД, на котором будет развернута база данных системы Directum RX;
- **Порт** для работы с PostgreSQL. Параметр задается, если в поле **Тип СУБД** выбрано значение **PostgreSQL**;
- **База данных** системы Directum RX;
- **Пользователь** сервера БД, обладающий правами администратора. Права нужны для создания базы данных во время установки системы. Права администратора есть у пользователей, которые на сервере БД включены в роль superuser. Для повышения информационной безопасности не рекомендуется указывать стандартного пользователя admin;
- **Пароль** пользователя сервера БД. Использование пустого пароля не допускается.

ПРИМЕЧАНИЕ. Параметры подключения к базе данных Microsoft SQL Server см. в инструкции по установке системы в Microsoft Windows.

Сервер RabbitMQ. Заполните параметры подключения:

- **Сервер**. IP-адрес сервера, на котором установлен RabbitMQ;
- **Порт**, по которому RabbitMQ взаимодействует с веб-сервером, например **5672**;
- **Виртуальный хост** RabbitMQ, например rxhost. По умолчанию **/**;
- **Пользователь**, **Пароль**. Имя и пароль пользователя для подключения к RabbitMQ. Пользователь создается на этапе установки RabbitMQ;
- **Точка обмена**, к которой привязываются очереди сообщений веб-сервера. Также используется для наименования очередей сообщений. Укажите произвольное имя для новой точки обмена, например **RxExchange**. Она создастся во время установки системы.

  ВАЖНО. Необходимо задать новую точку обмена. Если указать точку обмена, которая по умолчанию уже есть в RabbitMQ, при установке системы может возникнуть ошибка.

Сервер MongoDB. В строке подключения задаются:

- **Сервер**. IP-адрес сервера, на котором установлена СУБД MongoDB;
- **Порт**, по которому MongoDB взаимодействует с сервисами Directum RX. Значение по умолчанию **27017**;
- **Пользователь**, **Пароль**. Имя и пароль пользователя для подключения к MongoDB. Пользователь создается на этапе установки MongoDB.

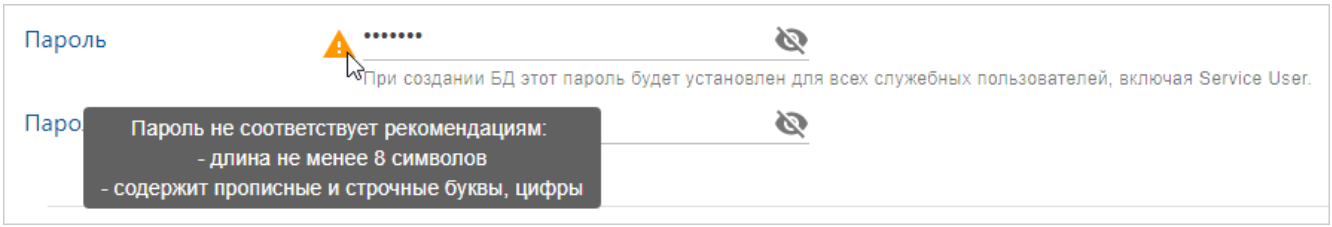
ВАЖНО. Для значений параметров MongoDB учитывается регистр символов.

При заполнении полей **Сервер БД**, **Сервер RabbitMQ** и **Сервер MongoDB** по кнопке ⇄ можно переключиться на настройку параметров в виде строки подключения. Подробнее см. в руководстве администратора, раздел «Минимальные настройки».

Папка с данными. В указанной папке будут созданы подпапки для хранения содержимого документов, файлов предпросмотра, лог-файлов системы и других данных.

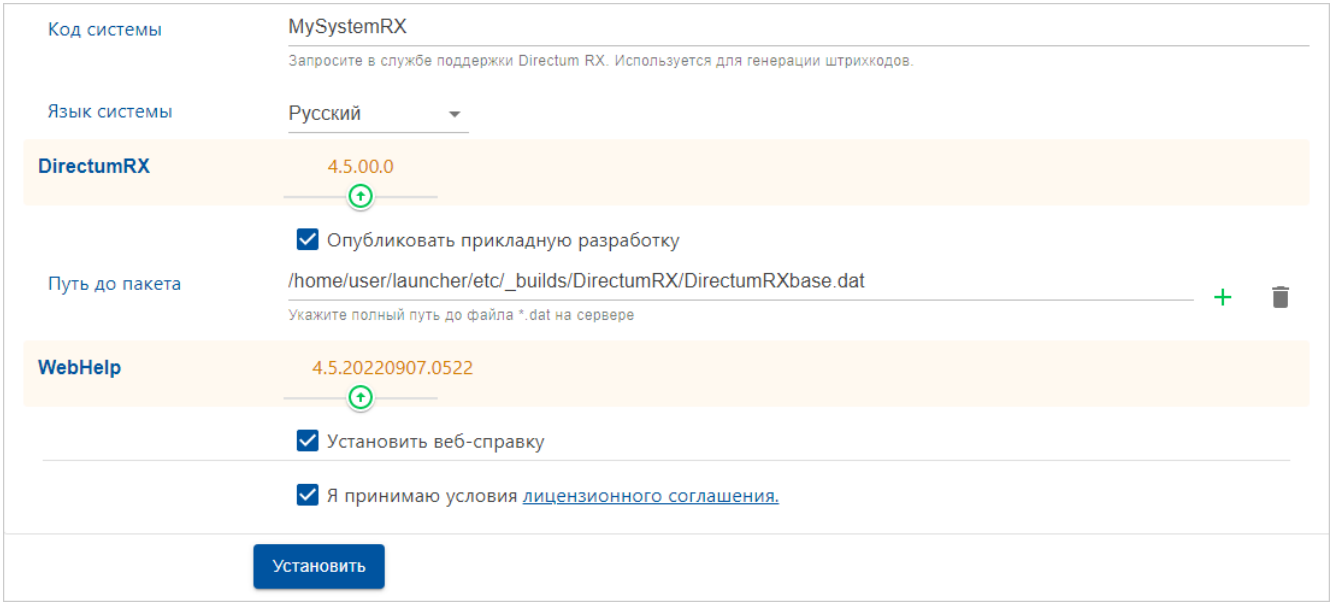
Пароль, который будет задан для служебных пользователей: Administrator, Service User, Integration Service и Adviser. В поле ниже повторите пароль.

СОВЕТ. Рекомендуется использовать пароль, который состоит из 8 и более символов, содержит строчные и прописные буквы, а также цифры. Это повышает стойкость пароля ко взлому. Если пароль не соответствует рекомендациям, появляется значок предупреждения. При наведении курсора на него отображается подсказка:



С помощью значка можно показать пароль.

7. Укажите дополнительные настройки:



Код системы, который используется в работе сервисов Directum RX и в штрихкодах документов, чтобы различать штрихкоды разных систем. Параметр должен быть уникальным для каждой новой установленной системы Directum RX. Для продуктивной системы запросите код в службе поддержки Directum RX.

Язык системы. Возможные значения: **Русский**, **Английский**. На выбранном языке будут отображаться наименования шаблонов и видов документов, тексты задач и заданий по умолчанию, а также другие автоматически создаваемые данные.

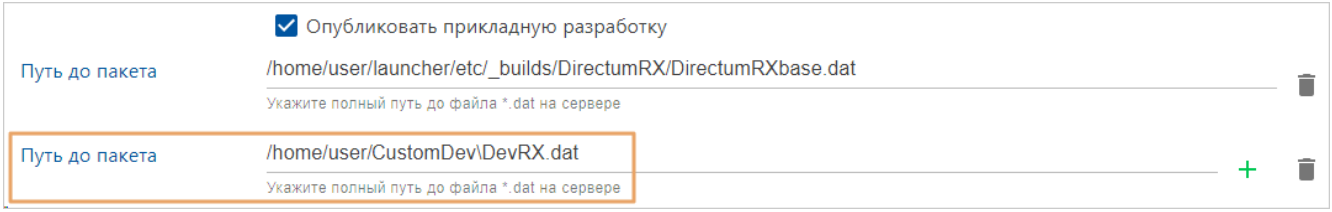
При этом язык интерфейса веб-клиента Directum RX по умолчанию будет таким же, как и в операционной системе. Пользователи могут изменить язык интерфейса в проводнике Directum RX.

Данные в системе отображаются на том языке, на котором их занесли в систему. Их можно заносить на любом языке и любыми символами, независимо от основного языка системы. Все данные хранятся в кодировке Unicode.

ВАЖНО. Язык системы можно задать только во время установки Directum RX, в дальнейшем его изменять нельзя.

8. При первой установке системы убедитесь, что установлен флажок **Опубликовать прикладную разработку** и заполнено поле **Путь до пакета**. Флажок и поле доступны, если в корне локальной папки с Directum Launcher есть архив DirectumRX.tar.gz.

   Если разработка состоит из нескольких пакетов или нужно опубликовать пакет другого решения, то нажмите на кнопку + и в появившемся поле укажите путь до пакета:



   Таким же образом добавьте все необходимые пакеты. Они должны включать в себя исходные коды. Если нужно удалить поле с пакетом, нажмите на кнопку .

   ПРИМЕЧАНИЕ. Если в строке подключения указана существующая база данных Directum RX с прикладной разработкой, то снимите флажок **Опубликовать прикладную разработку**.

9. Для установки справки убедитесь, что стоит флажок **Установить веб-справку**. Флажок можно снять, например, если система устанавливается для тестирования и нужно сэкономить место на диске.
10. Ознакомьтесь с текстом лицензионного соглашения и установите флажок **Я принимаю условия лицензионного соглашения**.
11. Нажмите на кнопку **Установить**. При этом сгенерируется конфигурационный файл config.yml, выполнится проверка подключения к СУБД, RabbitMQ и MongoDB. Неверно заполненные поля подсветятся красным цветом.
12. Дождитесь окончания установки. На странице выводятся этапы установки. В раскрывающейся области с названием этапа отображаются сообщения из лог-файла установки.

    Если при выполнении этапа возникает ошибка, с помощью сообщения из лог-файла проанализируйте и устраните ее, затем нажмите на кнопку **Повторить**.

    Если нужно изменить ранее заданные настройки, нажмите на кнопку **Вернуться к настройкам**. В результате откроется страница с исходными параметрами. Укажите новые значения параметров и повторно нажмите на кнопку **Установить**.

    Когда установка завершится, на странице появится ссылка для входа в веб-клиент.

Справочная информация

Во время установки в папке DirectumLauncher/etc автоматически создается конфигурационный файл config.yml с заполненными параметрами. Соответствие полей в Directum Launcher и параметров конфигурационного файла:

Параметр установки	Секция config.yml	Параметр config.yml
Адрес сайта	variables	host_fqdn
Протокол	variables	protocol
HTTP-порт	variables	http_port
HTTPS-порт	variables	https_port
Папка с данными	variables	home_path
Тип СУБД	common_config	DATABASE_ENGINE
Сервер БД	common_config	CONNECTION_STRING
Сервер RabbitMQ	common_config	QUEUE_CONNECTION_STRING
Сервер MongoDB	common_config	MONGODB_CONNECTION_STRING
Пароль администратора	common_config	AUTHENTICATION_PASSWORD
Код системы	common_config	PRIMARY_TENANT
Язык системы	common_config	LANGUAGE
Путь до сертификата	common_config	DATA_PROTECTION_CERTIFICATE_FILE

Установка с помощью командной строки

Серверные компоненты Directum RX в операционной системе на базе Linux развертываются с использованием docker-контейнеров. Каждому серверному компоненту соответствует отдельный контейнер.

Параметры развертывания задаются в конфигурационном файле config.yml. На компьютере развертываются сервисы, указанные в секции **services_config**. Брокер сообщений RabbitMQ и MongoDB можно развернуть вместе с системой Directum RX или на отдельный компьютер.

Порядок развертывания

1. Архив с Directum Launcher распакуйте в локальную папку на сервере с помощью команды:

   ```
   tar -xvf <Имя архива> -C <Имя папки>
   ```

   ВАЖНО. Для корректной установки общий путь к файлам должен быть не более 256 символов, поэтому используйте, например, папку /srv/DirectumLauncher.

2. В папку с Directum Launcher скопируйте архив Platform.tar.gz. Затем выполните команду:

   ```
   ./do.sh components add platform
   ```

3. Создайте конфигурационный файл config.yml на основе файла DirectumLauncher/etc/config.yml.example. Сгенерируйте минимально необходимые настройки с помощью команды:

   ```
   ./do.sh platform generate_config_yaml
   ```

4. Если планируется работа Directum RX только в локальной сети и для настройки используется самоподписанный (self-signed) сертификат, то в созданном файле в секции **extra_hosts** укажите соответствие IP-адреса текущего сервера и доменного имени, по которому доступна система Directum RX.

   Пример настройки:

   ```
   extra_hosts:
       company-rx.directum.ru: '192.168.0.42'
   ```

   Во время установки указанное соответствие запишется в файл hosts docker-контейнеров. Это необходимо для корректного импорта шаблонов документов и пакетов разработки.

5. Настройте и установите RabbitMQ, MongoDB.

6. Откройте на редактирование конфигурационный файл config.yml и заполните минимальные настройки.

7. Настройте утилиту DeploymentToolCore.

8. Установите и настройте справку и слайдер. Для этого в локальную папку скопируйте архив со справкой WebHelp.zip и затем последовательно выполните команды:

   ```
   ./do.sh components add_package --package="<Путь до папки со справкой>"
   ./do.sh webhelp install
   ```

   В результате установки в конфигурационном файле автоматически заполнятся:

   - в секции **SungeroWebClient** параметр **help_path** – путь до папки с файлами справки;
   - в секции **SungeroWebServer** параметры:

     HELP_URI – URI-адрес веб-справки;

     RELEASE_NOTES_SLIDER_FILE_PATH – путь к файлу с настройками слайдера;

     PRODUCT_NOTES_SLIDER_FILE_PATH – путь к файлу с настройками слайдера о базовых возможностях системы, который отображается при первой авторизации сотрудника в системе.

9. Сгенерируйте сертификат с настройками, указанными в параметрах **DATA_PROTECTION_CERTIFICATE_FILE**, **DATA_PROTECTION_CERTIFICATE_FILE_PASSWORD**. Для этого выполните команду:

   ```
   ./do.sh generate_data_protection_cert_from_config
   ```

   Если в папке уже есть сертификат с указанным именем, он заменится на новый.
10. Установите платформу, включающую в себя веб-сервер и сервисы:

    ```
    ./do.sh platform install
    ```
11. Разверните базу данных Directum RX с помощью команды:

    ```
    ./do.sh db up
    ```

    В результате создается база данных с именем, указанным в параметре **CONNECTION_STRING**.
12. Разверните компоненты Directum RX. Для этого выполните команду:

    ```
    ./do.sh directumrx install
    ```
13. Проверьте, что компоненты системы запустились. Для этого выполните команду:

    ```
    docker ps -a
    ```

    Отобразится список запущенных контейнеров. Сравните список с компонентами в секции **services_config** конфигурационного файла config.yml.
14. Добавьте компонент с прикладной разработкой и утилитами RxCmd, DrxUtil. Для этого выполните команду:

    ```
    ./do.sh components add --name=DirectumRX
    ```
15. Опубликуйте стандартную прикладную разработку. Для этого выполните команду:

    ```
    ./do.sh rx install
    ```

    Если нужно опубликовать заказную разработку, то в параметре **--package** укажите путь к пакету:

    ```
    ./do.sh dt deploy --package="<Путь к пакету разработки>" --init
    ```

    Пример:

    ```
    ./do.sh dt deploy --
    package="/srv/rx/etc/_builds/DirectumRX/4.5.17.0/DirectumRX.dat" --init
    ```
16. Импортируйте шаблоны документов. Для этого выполните команду:

    ```
    ./do.sh rxcmd import_templates
    ```

    Если нужно импортировать свои шаблоны, в параметре **--templates_dir_path** укажите папку с ними:

    ```
    ./do.sh rxcmd import_templates --templates_dir_path="<Путь к шаблонам>"
    ```

    Пример:

    ```
    ./do.sh rxcmd import_templates --templates_dir_path="/srv/rxdata/templates/"
    ```
17. Чтобы зайти в веб-клиент системы, воспользуйтесь ссылкой: http или https://<адрес сайта>:<порт>/<имя приложения, по умолчанию client>. Для удобства рекомендуется сохранить ссылку для работы в веб-клиенте, например добавить в закладки браузера, и отправить ее пользователям.

В результате развертывания:

- собираются docker-образы;
- запускаются контейнеры с сервисами Directum RX.

Установка сервера NOMAD

Сервер NOMAD устанавливается как отдельный компонент вместе с системой Directum RX с помощью кроссплатформенного инструмента **Directum Launcher**.

NOMAD поставляется в виде архива, который нужно скопировать в корневую папку **Directum Launcher** вместе с архивами платформы, стандартной разработки, веб-справки и других устанавливаемых компонентов. Подробнее см. раздел «Установка системы (Directum Launcher)».

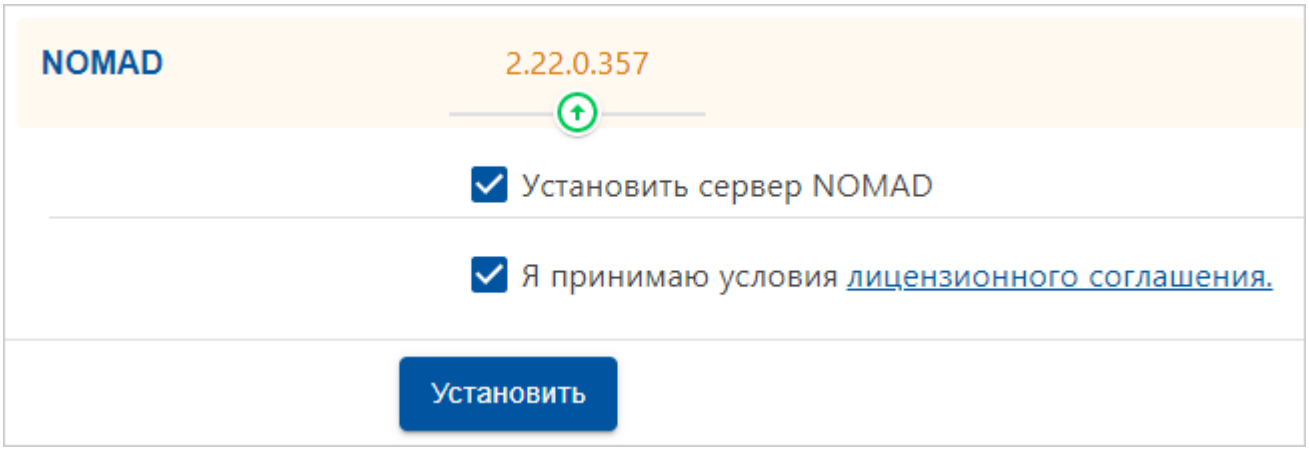
Перед началом установки ознакомьтесь с типовыми требованиями и убедитесь, что ваше аппаратное и программное обеспечение подходит для установки сервера NOMAD.

Выполните дополнительные действия, если нужно перенести NOMAD на выделенный сервер или настроить NOMAD в ферме серверов.

Порядок установки

1. В корень локальной папки с Directum Launcher скопируйте архив Nomad.tar.gz.

   ВАЖНО. Для корректной установки общий путь к файлам должен быть не более 256 символов. Также он не должен содержать пробелы, символы кириллицы, запятые и спецсимволы. Поэтому используйте, например, папку /srv/DirectumLauncher. В зависимости от настроек операционной системы для дальнейших действий могут потребоваться права суперпользователя.
2. Запустите Directum Launcher. Способ запуска зависит от используемого дистрибутива Linux. На открывшейся странице установки заполните поля. Подробнее см. раздел «Установка системы (Directum Launcher)».
3. Убедитесь, что установлен флажок **Установить сервер NOMAD**:



4. Продолжите установку согласно инструкции по установке Directum RX.

Также сервер NOMAD можно развернуть с помощью командной строки. Для этого:

1. В корень локальной папки с Directum Launcher скопируйте архив Nomad.tar.gz.
2. В папке с Directum Launcher последовательно выполните команды:

```
./do.sh components add_package --package="<Путь до папки с архивом NOMAD>"
./do.sh nomad_component install
```

3. Продолжите установку согласно инструкции по установке Directum RX. Подробнее см. раздел «Установка с помощью командной строки».

В результате установки генерируется конфигурационный файл config.yml. На основе этого файла создается XML-файл с настройками для сервера NOMAD при его развертывании.

Завершающие работы

После завершения установки:

1. Настройте доступ к приложению Directum Solo, если в организации приобретены лицензии на его использование. Для этого добавьте сотрудников, которые будут работать с мобильным приложением, в предопределенную роль «Пользователи Solo». Подробнее см. разделы «Предопределенные роли» и «Роли».
2. Чтобы сотрудники начали работу в Directum Solo и Directum Jazz, сообщите им адрес для подключения к NOMAD. Формат адреса зависит от настройки сервера, по умолчанию: https://<адрес сайта>:<порт>/nomad.
3. Настройте сервер NOMAD.

Дополнительные параметры запуска Directum Launcher

Directum Launcher можно запускать из командной строки и с помощью ключей указывать дополнительные параметры, чтобы настроить:

- подключение к Directum Launcher с другого компьютера
- аутентификацию при входе
- подключение по протоколу HTTPS
- запуск с английской локализацией

Параметры можно использовать вместе или отдельно друг от друга.

Подключение к Directum Launcher с другого компьютера

Страницу Directum Launcher можно открыть с другого компьютера. Например, когда Directum Launcher постоянно запущен на сервере, администратор в любой момент может открыть страницу со своего рабочего места и изменить настройки системы.

Чтобы подключиться к Directum Launcher с другого компьютера:

1. На сервере запустите командную строку от имени администратора.
2. В командной строке перейдите в папку с Directum Launcher и запустите исполняемый файл с ключом **--host**. Значение ключа зависит от того, подключение будет по IP-адресу или по доменному имени компьютера.

   Подключение по IP-адресу:

   ```
   ./DirectumLauncher --host=0.0.0.0
   ```

   Подключение по доменному имени:

   ```
   ./DirectumLauncher --host=<Доменное имя сервера>
   ```

   Пример команды:

   ```
   ./DirectumLauncher --host= rxserver.domain.comp
   ```

В командной строке появится адрес страницы Directum Launcher.

3. Скопируйте адрес страницы и откройте ее в браузере на другом компьютере. Дальнейшие действия выполняйте там.

   ПРИМЕЧАНИЕ. Для подключения может потребоваться настройка сетевого доступа.

Для безопасного подключения к странице Directum Launcher рекомендуется настроить аутентификацию при входе и использование протокола HTTPS.

Настройка аутентификации при входе

Если страницу Directum Launcher планируется открывать с другого компьютера, рекомендуется настроить аутентификацию. В этом случае войти на страницу сможет только зарегистрированный пользователь.

Чтобы настроить аутентификацию:

1. На сервере запустите командную строку от имени администратора и перейдите в ней в папку с Directum Launcher.
2. Запустите исполняемый файл с ключами **--host** и **--auth**.

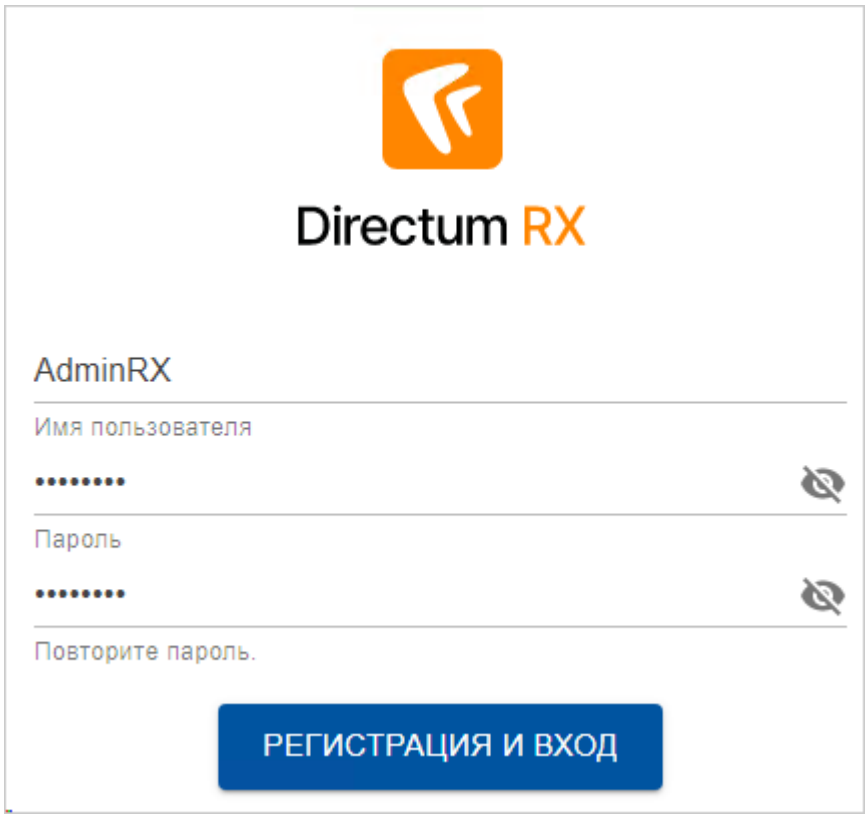
   Примеры команды:

   ```
   ./DirectumLauncher --host=0.0.0.0 --auth
   ./DirectumLauncher --host= rxserver.domain.comp --auth
   ```

   В командной строке появится адрес страницы Directum Launcher.
3. Скопируйте адрес страницы и откройте ее в браузере.

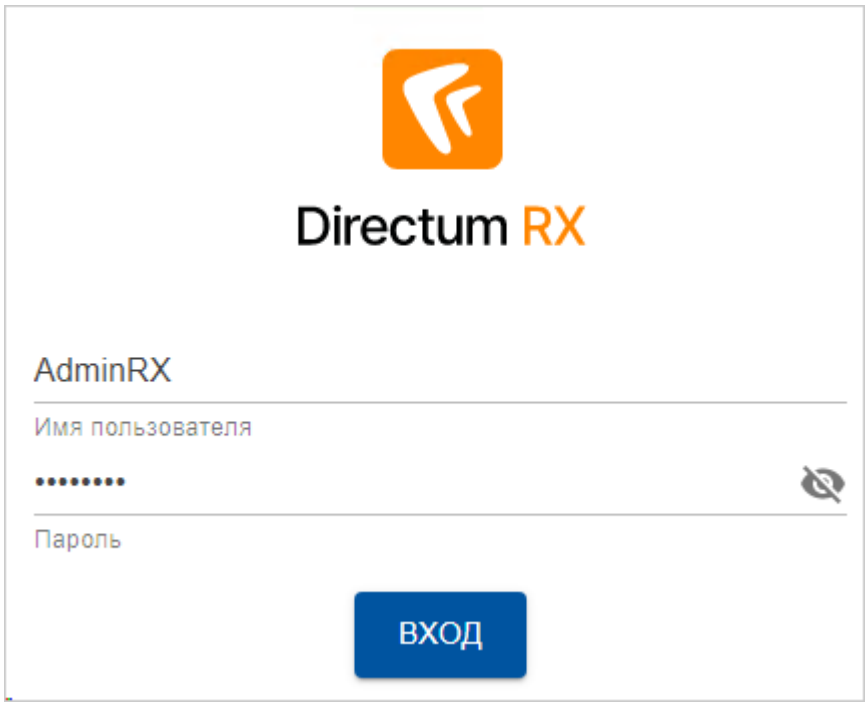
   ПРИМЕЧАНИЕ. В зависимости от настроек браузера и операционной системы страница может открыться автоматически.

4. На открывшейся странице заполните имя и пароль пользователя, повторите пароль. Затем нажмите на кнопку **Регистрация и вход**:



В результате зарегистрируется пользователь и откроется страница Directum Launcher. Можно зарегистрировать только одного пользователя.

При последующих запусках с ключом **--auth** с текущего или другого компьютера нужно проходить аутентификацию. Также она потребуется, если закрыть браузер и затем повторно открыть страницу. Чтобы войти в Directum Launcher, укажите имя и пароль зарегистрированного пользователя и нажмите на кнопку **Вход**:



Учетные данные знает только администратор, а запустить Directum Launcher без аутентификации можно только локально на сервере, куда доступ ограничен. В результате посторонний не сможет открыть страницу, даже если получит ссылку для подключения.

При регистрации пользователя заполняется секция **launcher** в конфигурационном файле config.yml. Если нужно создать другого пользователя или сбросить пароль, очистите в этой секции параметр **username** и обновите страницу Directum Launcher. В результате откроется страница регистрации, создайте на ней нового пользователя.

Для дополнительной безопасности рекомендуется настроить подключение к Directum Launcher по защищенному протоколу HTTPS.

Настройка подключения по протоколу HTTPS

Если страницу Directum Launcher планируется открывать с другого компьютера, для защищенного обмена данными рекомендуется настроить подключение по протоколу HTTPS. Для этого:

1. На сервере запустите командную строку от имени администратора и перейдите в ней в папку с Directum Launcher.
2. Запустите исполняемый файл с ключами **--host** и **--https**.

   Примеры команд:

   ```
   ./DirectumLauncher --host=0.0.0.0 --https
   ./DirectumLauncher --host=rxserver.domain.comp --https
   ```

   В результате сгенерируется PEM-сертификат, который будет использоваться для шифрования передаваемых данных. В командной строке появится адрес страницы Directum Launcher, при этом в качестве протокола будет указан HTTPS.

3. Скопируйте адрес страницы и откройте ее в браузере на другом компьютере. Дальнейшие действия выполняйте там.

   ПРИМЕЧАНИЕ. В зависимости от настроек операционной системы и антивирусного программного обеспечения может потребоваться настройка безопасности в браузере.

В дальнейшей работе для подключения по HTTPS можно использовать сертификат, выданный в официальном удостоверяющем центре. Для этого:

1. Из папки DirectumLauncher/etc/ui_cert удалите сертификат https-cert.pem и скопируйте туда сертификат, выданный в удостоверяющем центре. Необходимо использовать сертификат в формате PEM.

   Если вам выдан PFX-сертификат, его нужно сконвертировать в формат PEM. Для этого в командной строке перейдите в папку с Directum Launcher и выполните команду:

   ```
   ./do.sh convert_pfx_to_pem "<Путь к сертификату *.pfx>" "<Пароль от сертификата>"
   ```

   Пример команды:

   ```
   ./do.sh convert_pfx_to_pem "/srv/DirectumLauncher/etc/ui_cert/rxkey.pfx" "password"
   ```

2. Запустите Directum Launcher и перейдите на его страницу, как описано выше. При этом в ключе **--host** рекомендуется указывать доменное имя сервера, на которое выдан сертификат, чтобы страница открылась в браузере без дополнительных настроек безопасности.

Для дополнительной безопасности рекомендуется настроить аутентификацию при входе.

Запуск с английской локализацией

По умолчанию Directum Launcher запускается с русской локализацией. Чтобы использовать английскую локализацию, запустите Directum Launcher через командную строку с ключом **--locale** и укажите для него значение **en**:

```
./DirectumLauncher --locale=en
```

В результате откроется страница Directum Launcher со строками на английском языке.

Устранение неисправностей

Сообщения об ошибках текущей установки фиксируются в лог-файл DirectumLauncher/log/current.log. Сообщения предыдущих установок автоматически переносятся в лог-файл all.log в этой же папке.

Ситуации

- **Контейнер не запускается**

  Если контейнер не запускается или постоянно перезапускается, причиной может быть ошибка в настройке параметров серверного компонента Directum RX.

  Решение: проверьте соответствующий лог-файл. Путь к лог-файлам задается в конфигурационном файле config.yml в параметре **LOGS_PATH**.

- **При запуске установки возникает ошибка «Couldn't find a valid ICU package ...»**

  Решение: в операционной системе включите настройку System.Globalization.Invariant. Для этого выполните команду:

  ```
  export DOTNET_SYSTEM_GLOBALIZATION_INVARIANT=1
  ```

- **При подключении по имени к СУБД, MongoDB или RabbitMQ возникает ошибка**

  Решение: в конфигурационный файл config.yml добавьте секцию extra_hosts и укажите в ней соответствие DNS-имен и IP-адресов.

  ВАЖНО. В доменном имени используйте только строчные буквы.

  Пример настройки:

  ```
  extra_hosts:
      rx.company.ru: '192.168.5.42'
  ```

  Настроенный список добавляется в файл /etc/hosts каждого контейнера.

- **При установке системы на этапе публикации прикладной разработки возникает ошибка с кодом 503**

  Возможная причина: из сети docker-контейнеров, в которых разворачиваются сервисы Directum RX, нет доступа к СУБД PostgreSQL/Postgres Pro.

  Решение: настройте доступ к СУБД с адресов docker-контейнеров. По умолчанию в сети docker-контейнеров используются адреса 172.18.0.X. Чтобы настроить с них доступ, в конфигурационном файле pg_hba.conf добавьте строку:

  ```
  host all all 172.18.0.0/0 md5
  ```

Удаление системы

1. В дальнейшем может потребоваться установка системы с такими же параметрами, поэтому рекомендуется сохранить ранее заданные настройки. Для этого в отдельную папку скопируйте:
   - конфигурационный config.yml;
   - конфигурационный файл HAProxy;
   - папки с данными, в том числе конфигурационные файлы MongoDB и RabbitMQ;
   - сертификаты.
2. Остановите компоненты Directum RX, RabbitMQ и MongoDB с удалением контейнеров. Для этого выполните команды:

   ```
   ./do.sh all down
   ./do.sh rabbitmq down
   ./do.sh mongodb down
   ```
3. Средствами Docker удалите образы, чтобы они не занимали дисковое пространство на сервере. Подробнее см. в документации Docker статью docker rmi.
4. Убедитесь, что в папке со скриптами развертывания не осталось нужных данных. После этого удалите папки со скриптами и справкой.