Акционерное общество «Р7»

Экз. № ____

СЕРВЕР ДОКУМЕНТОВ

РУКОВОДСТВО ПО ИНТЕГРАЦИИ

RU.48324255.СД-РА.001-ИУ-В1.0

Листов 30

2025

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. №	

Аннотация

Настоящее руководство по интеграции содержит инструкции по подключению **Сервера документов** к сторонним системам. Рассмотрена интеграция с Directum RX, включая установку компонентов (Docker, RabbitMQ), настройку Directum RX и сервера коллаборации. Также описана интеграция с CommuniGate Pro. Документ предназначен для системных администраторов и специалистов, осуществляющих развертывание и сопровождение указанных систем.

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение документа

Руководство описывает процесс интеграции сервера документов Р7-Офис с системами:

Directum RX;

CommuniGate Pro.

Интеграция обеспечивает возможность совместного редактирования офисных документов в веб-интерфейсе указанных систем.

1.2 Наименование программы

Полное название: «Р7-Офис. Профессиональный. Сервер документов» или Программный комплекс «Сервер документов».

Сокращенное наименование: ПК СД.

Номер документа: RU.48324255.СД-РИ-В1.0.

Программа «Р7-Офис. Сервер документов» предназначена для организации совместной работы с документами, обеспечения их просмотра и редактирования в онлайн-режиме. Интеграция с внешними системами позволяет использовать эти возможности непосредственно в интерфейсе сторонних продуктов, обеспечивая единое информационное пространство.

1.3 Требования к программному обеспечению

- Операционная система: Debian 11 или совместимая;
- Docker: версии от 19.3 до 25;
- Docker Compose;
- RabbitMQ версии 3.12.13;
- PostgreSQL с расширением citext;
- SSL-сертификаты в формате .pem.

1.4 Требования к техническим средствам

Серверы с характеристиками, удовлетворяющими требованиям:

- Directum RX;
- RabbitMQ;
- R7-Офис;

Настроенные DNS A-записи или альтернативный механизм разрешения имен.

Сетевые порты:

- 15672 (RabbitMQ management);
- 5000 (Directum Launcher);
- 8090 (сервер коллаборации)

  Требуется наличие SSL-сертификата и ключа в формате .pem на сервере с Directum RX.

Для сервера БД PostgreSQL необходимо:

- Разрешить подключения с сервера Directum RX в файле pg_hba.conf;
- Установить расширение postgresql-contrib;
- Активировать расширение citext в БД: CREATE EXTENSION IF NOT EXISTS citext;

Необходимо увеличить максимальное количество наблюдателей inotify:

```
./do.sh set_inotify_instances_limit
```

2. ПОДГОТОВКА К ИНТЕГРАЦИИ

2.1 Настройка DNS

Перед инсталляцией рекомендуется внести необходимые записи в глобальный dns, для возможности работы приложения, после всех указанных ниже действий.

Необходимо задать две A записи: для Directum RX и Сервера документов (если предполагается использование сервера документов на отдельном сервере).

Примечание:
на сервере с Directum RX: Установка производилась на ОС Debian 11

Если DNS-сервер не используется:

– добавьте соответствие в `/etc/hosts` на всех серверах;

– в конфигурационный файл `etc/config.yml` добавьте секцию:

`extra_hosts`:

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

2.2 Установка Docker и Docker Compose

Установите из стандартных репозиториев ОС. Выполните команду:

```
apt update && apt install docker.io docker-compose
```

Проверьте установку командой:

```
docker -v && docker-compose -v
```

При работе с реджистри директума, необходимо добавить реджистри в доверенные для докер. Для этого, откройте на редактирование файл `/etc/docker/daemon.json`.

В файл добавьте адрес реджистри:

```
{
 "insecure-registries": [ "ciaregistry.directum.ru" ]
}
```

Сохраните файл и перезапустите службу докер:

```
systemctl restart docker
```

2.3 Подготовка дистрибутивов

Скачайте дистрибутив Directum RX по ссылке (пример для версии 4.10.48):

```
wget https://download.r7-office.ru/directum/directum_rx_4.10.48.0x.zip
```

Распакуйте архив дистрибутива:

```
unzip directum_rx_4.10.48.0x.zip
```

Создайте каталог для установщика и распакуйте архив:

```
mkdir /launcher
tar -xvzf DirectumLauncher.tar.gz -C /launcher
cd /launcher
```

Для дальнейшей загрузки образов Docker выполните одно из действий:

– авторизацию в docker registry Directum;

– импорт образов из поставки DockerImages.tar.gz;

В каталог с распакованным установщиком перенесем архивы, необходимые для минимальной установки DirectumRX.tar.gz Platform.tar.gz WebHelp.zip:

```
mv /root/DirectumRX.tar.gz /root/Platform.tar.gz /root/WebHelp.zip
/launcher
```

3. УСТАНОВКА И НАСТРОЙКА RABBITMQ

3.1 Установка сервиса

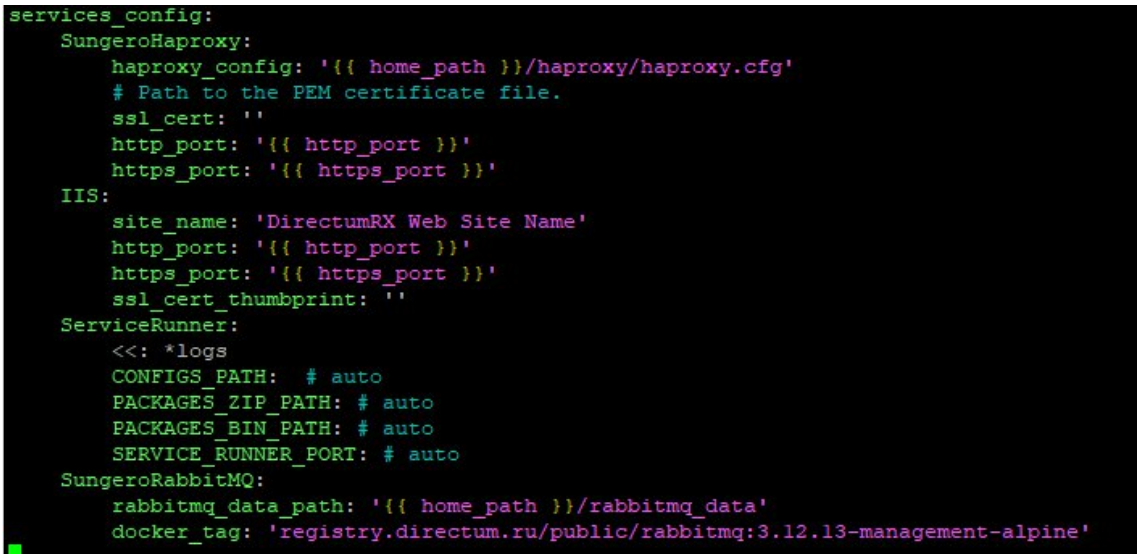
Скопируйте файл конфигурации:

```
cp ./etc/config.yml.example ./etc/config.yml
nano ./etc/config.yml
```

В файле в секции variables в переменной `home_path` укажите путь до папки с данными, например `/home/directum`:

В секции `services_config` добавьте секцию `SungeroRabbitMQ` с данными образа и каталогом хранения данных:

```
SungeroRabbitMQ:
  rabbitmq_data_path: '{{ home_path }}/rabbitmq_data'
  docker_tag:   'registry.directum.ru/public/rabbitmq:3.12.13-management-
alpine'
```



После сохранения конфигурации запустите rabbitmq:

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

По окончании появится сообщение «Container ‘sungerorabbitmq’ has status ‘running’», а также, будет доступна веб страница rabbitmq на порту 15672 сервера.

3.2 Базовая настройка

1. Откройте страницу в браузере `http://ip_адрес_сервера:15672`
2. Введите «guest/guest» логин и пароль.
3. 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 потребуются для создания пользователя, от имени которого система **Directum RX** будет подключаться к **RabbitMQ**.
4. В поле «Tags» выберите значение «Admin» и нажмите на кнопку «Add user».
5. 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».
6. На панели справа перейдите в группу Users.
7. 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».
8. Выберите созданного пользователя в списке, затем в разделе «Permissions» в поле «Virtual Host» выберите созданный виртуальный хост и нажмите на кнопку «Set permission».

В разделе «Topic permissions» в поле «Virtual Host» выберите созданный виртуальный хост и нажмите на кнопку «Set topic permission».

Меры безопасности

После завершения настройки, из соображений безопасности,отключите страницу администрирования RabbitMQ. Для этого в Directum Launcher перейдите в режим «Настройка». Затем в конфигураторе в секции RabbitMQ добавьте параметр `management_panel_disabled` и установите для него флажок.

Во избежание проблем с сертификатами установите сертификат на локальную машину:

```
sudo cp your-cert.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

4. ИНТЕГРАЦИЯ С DIRECTUM RX

4.1 Установка и настройка Directum RX

Предварительные требования

Перед установкой **Directum RX** необходимо выполнить следующие предварительные настройки:

- **Операционная система**: установка производится на ОС Debian 11;
- **Сертификаты**: на сервере должны быть расположены сертификат и ключ в формате **.pem**;
- **База данных**: если БД расположена на выделенном сервере, необходимо:
  - разрешить подключение с сервера **Directum RX** в файле `pg_hba.conf`;
  - установить расширение `postgresql-contrib: apt install postgresql-contrib`;
  - активировать расширение citext в БД: CREATE EXTENSION IF NOT EXISTS citext;
  - увеличить 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
```

Запуск веб-установщика

1. Запустите установщик командой:

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

2. Перейдите по адресу сервера, указав порт 5000, например, `http://192.168.26.160:5000/`
3. Заполните обязательные параметры (Рисунок 1):
   - **Адрес сайта**: имя сервера, например, `directum.ubuntu.s7-office.site`.

- **Путь до сертификата**: укажите путь до сертификата в формате **.pem** на сервере.
- **Строка подключения к БД, порт, имя БД, УЗ для подключения**. Если БД не создана, то установите флаг и укажите УЗ админа БД для создания.
- **Строка подключения к rabbitMQ, порт, виртуальный хост, созданный ранее, УЗ и точка обмена** (можно указать произвольное значение).
- **Папка с данными**: каталог, где будут храниться данные директум.
- **Пароль**: пароль для УЗ администратора, сервисной УЗ директум.
- **Код системы**: для тестового контура можно указать произвольное значение.

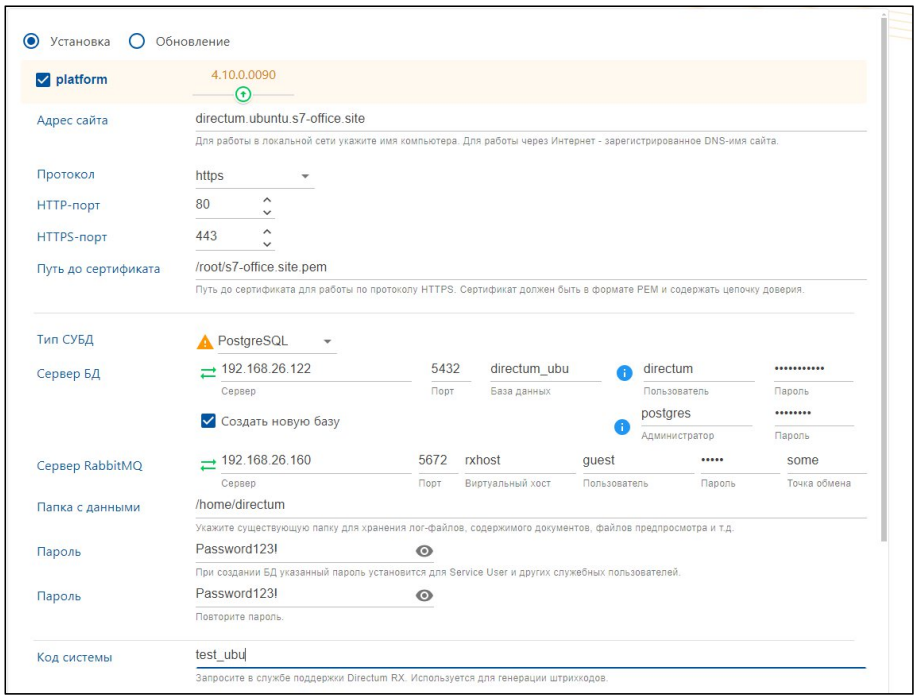


Рисунок 1 – Заполнение обязательных параметров

После заполнения строк нажмите «Установить».

Решение проблем установки

Если не проходит проверка работоспособности сервисов, проверяем состояние докер контейнеров на сервере.

При постоянном рестарте контейнера sungerohaproxy выполните:

```
docker cp s7-office.site.key.pem sungerohaproxy:/usr/local/etc/ssl.pem.key && docker restart sungerohaproxy
```

Далее нажмите кнопку «Повторить» на веб странице.

После прохождения всех шагов директум будет доступен по ссылке внизу страницы установщика.

4.2 Настройка онлайн-редактирования в Directum RX

Включение онлайн-редактирования

1. Откройте веб-страницу **Directum RX** (Рисунок 2) и включите онлайн-редактирование в настройках системы.

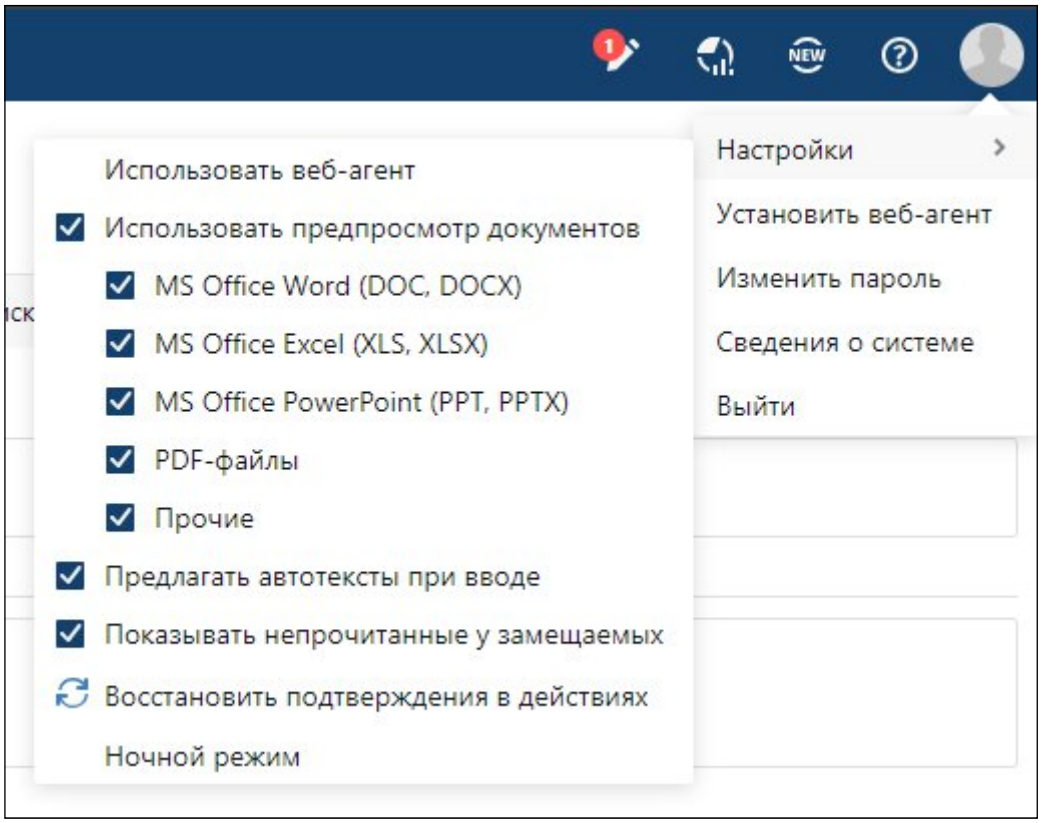


Рисунок 2 – Веб-страница Directum

2. Перейдите на страницу установщика (порт 5000) и на вкладке «Настройки сервисов» добавьте переменные (Рисунок 3):

– ENABLE_COLLABORATIVE_EDITING;
– ENABLED_WEB_EDITORS.

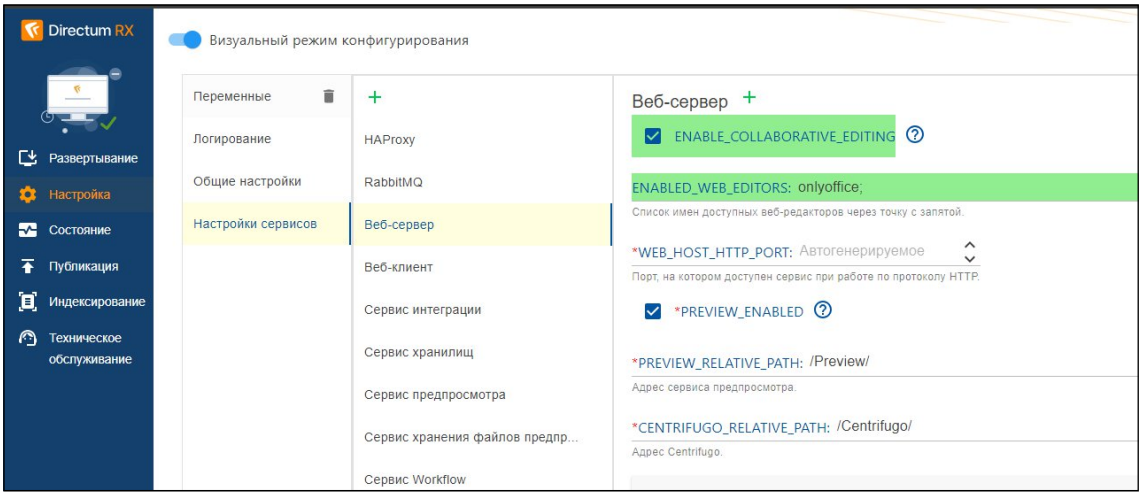


Рисунок 3 – Страница установщика

3. Нажмите кнопку «Применить настройки» и дождитесь перезапуска сервисов.

Конфигурация веб-сервера

После успешного перезапуска отключите визуальный режим конфигурирования и добавьте в блок SungeroWebServer следующий YAML-конфигурацию (Рисунок 4):

```
WEB_EDITORS:
   r7-office:
   -   '@name': 'r7-office'
       '@url': '/collaboration'
       '@extensions':
'doc;docx;dotx;xlsx;xltx;xls;pptx;potx;ppt;odt;ott;ods;ots;odp;otp;txt;html;rtf;csv;pdf;
epub;xps;djvu;'
       '@supportEncrypted': 'false'
       '@supportStrictAccess': 'false'
```

Рисунок 4 – Конфигурация веб-сервиса

Примените настройки и ждите перезапуска сервисов.

После выполненных действий в веб клиенте должна быть доступна кнопка настройки онлайн редактирование (Рисунок 5).

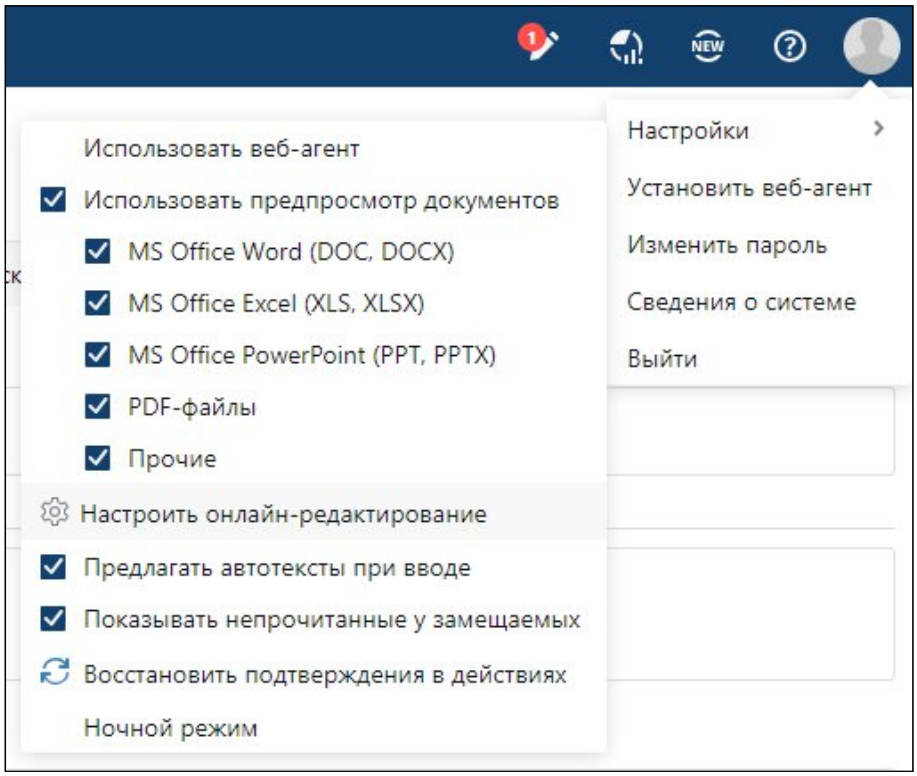


Рисунок 5 – Окно выбора кнопки «Настроить онлайн-редактирование»

Добавьте строки в конфигурационный файл `HAProxy` для перенаправления на онлайн редактор.

Конфигурационный файл расположен в директории, указанной при установке в строке «Папка с данными», в примере `/home/directum`

Откройте файл на редактирование:

```
nano /home/directum/haproxy/haproxy.cfg
```

Добавьте строку в секцию frontend directumrx после строк в формате use_backend:

```
use_backend collaboration-backend if { path_beg -i /collaboration/ /editor/ }
```

```
resolvers docker_resolver
    nameserver dns 127.0.0.11:53


frontend directumrx
    bind 0.0.0.0:80
    http-request set-header X-Forwarded-Host %[req.hdr(host)]
    http-request redirect code 301 prefix / drop-query append-slash if { path -i /Centrifugo }
    use_backend sungerocentrifugo_backend if { path_beg -i /Centrifugo }
    http-request redirect location https://%[req.hdr(host)]/Client/redirect.html?%[query] if { path_end -i /Sungero }
    use_backend sungerowebclient_backend if { path_beg -i /Client } !{ path_beg -i /Client/api }
    use_backend storageservice_backend if { path_beg -i /Storage }
    use_backend previewstorage_backend if { path_beg -i /Preview }
    use_backend integrationservice_backend if { path_beg -i /Integration }
    use_backend collaboration-backend if { path_beg -i /collaboration/ /editor/ }
    http-request redirect scheme https code 307 if !{ ssl_fc } { path_beg -i /Integration }
    use_backend logservice_backend if { path_beg -i /Log }
    bind 0.0.0.0:443 ssl crt /usr/local/etc/ssl.pem
    redirect scheme https if !{ ssl_fc }
    http-request set-header X-Forwarded-Proto https
    use_backend sungerowebserver_backend if { path_beg -i /Client/api } !{ path_beg -i /Client/api/public/ }
    http-request redirect code 301 prefix / drop-query append-slash if { path -i /Client }
    http-request redirect code 301 prefix /Client if { path / }


backend sungerocentrifugo_backend
    http-request set-path "%[path,regsub(^/Centrifugo/,/,i)]"
    server sungerocentrifugo_server sungerocentrifugo:15672
```

После секций вида backend <…> добавьте секцию решения:

```
backend collaboration-backend
   mode http
   http-request set-header Host directum-ubuntu.s7-office.site
   http-request set-header X-Forwarded-Host "directum-ubuntu.s7-office.site/editor" if { path_beg -i /editor/ }
   http-request set-header X-Forwarded-Host "directum-ubuntu.s7-office.site/collaboration" if { path_beg -i /collaboration/ }
   http-request set-header X-Forwarded-Proto https
   http-request set-header X-Real-Ip %[src]
   http-request set-header X-Original-Url %[path]
```

Где:

– **directum-ubuntu.s7-office.**site – имя сервера с директум.

– **192.168.27.227:8090** – адрес и порт сервера с онлайн редактором

После сохранения изменений в конфигурационном файле перезапустите хапрокси:

```
docker restart sungerohaproxy
```

4.3 Настройки коллаборации редактора

Подготовка файлов интеграции

Скачайте архив с файлами интеграции онлайн-редактора по ссылке. Перенесите архив на сервер и выполните следующие действия:

```
mkdir /collab
unzip integration_r7_ofis_Directum.zip -d /collab/
cd /collab/collab-build-v1.5.0
```

Настройка переменных окружения

Откройте файл с переменными `./settings/tenant1.env` окружения для редактирования и поменяйте значение переменных:

```
CLIENT_HOST=directum-ubuntu.s7-office.site

CLIENT_PATH=/Client
EDITOR_PATH=/editor
SELF_PATH=/collaboration

CLIENT_USERNAME=Service User
CLIENT_PASSWORD=Password123!

GOOGLE_ANALYTICS_ID=GA_ID
```

Где:

- CLIENT_HOST – имя, по которому доступен сервис Directum RX;
- CLIENT_PATH – параметр WEB_HOST_PATH_BASE из общих настроек установщика;
- CLIENT_PASSWORD – пароль, заданный при установке системы;

Настройка JWT-безопасности

В подпапке **settings** откройте конфигурационный файл: `settings.share.env`.

Раскомментируйте параметр **JWT_SECRET** и укажите строку для генерации JWT-токенов длиной не менее 20 символов.

Рекомендуется использовать специализированный сервис генерации безопасных случайных паролей.

Конфигурация Docker Compose

Откройте файл `docker-compose.yml` для редактирования:

```
nano docker-compose.yml
```

Измените образ документ-сервера на актуальную версию Р7:

```
documentserver:
  image: downloads.r7-office.ru:9010/r7office/documentserver-ee:2024.3.2.622
  depends_on:
    - postgres
    - redis
    - rabbit
    - saver
  volumes:
    - ./oo_data:/var/lib/r7-office/documentserver/App_Data
    - ./oo_logs:/var/log/r7-office
    - ./fonts:/usr/share/fonts
  env_file:
    - settings/system/oo.env
    - settings/settings.share.env
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "5"
  hostname: documentserver
  container_name: meta_documentserver
  restart: on-failure
```

Добавьте следующие блоки в конец файла:

```
collaboration_tenant1:
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "5"
  image: ${DOCKER_REGISTRY}/collaboration/backend:${VERSION_TAG}
  env_file:
    - settings/system/collaboration.env
    - settings/tenant1.env
    - settings/settings.share.env
  environment:
    - CALLBACK_URL=http://collaboration_tenant1:3333/callback
    - INTERNAL_HAPROXY_URL=http://haproxy_tenant1/
  volumes:
    - ./db_tenant1/:/db/
  hostname: collaboration_tenant1
  restart: on-failure
  container_name: collaboration_tenant1
  depends_on:
    - saver

haproxy_tenant1:
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "5"
  image: ${DOCKER_REGISTRY}/collaboration/haproxy:${VERSION_TAG}
  hostname: haproxy
  environment:
    - COLLABORATION_SERVICE_ADDRESS=collaboration_tenant1:3333
  ports:
```

```
  - "8090:80"
restart: on-failure
container_name: haproxy_tenant1
depends_on:
  - documentserver
  - collaboration_tenant1
  - staticfiles
```

Итоговый файл `docker-compose.yml` должен выглядеть так: https://download.r7-office.ru/directum/docker-compose.yml

Запуск сервиса коллаборации

Выполните авторизацию в корпоративном Docker registry Р7:

```
docker login -u admin -p jgbHw224teWqf https://downloads.r7-office.ru:9010
```

Запустите сервис коллаборации:

```
docker-compose up -d
```

Проверка работы интеграции

После успешного запуска всех контейнеров откройте настройки онлайн-редактирования в Directum RX (Рисунок 6).

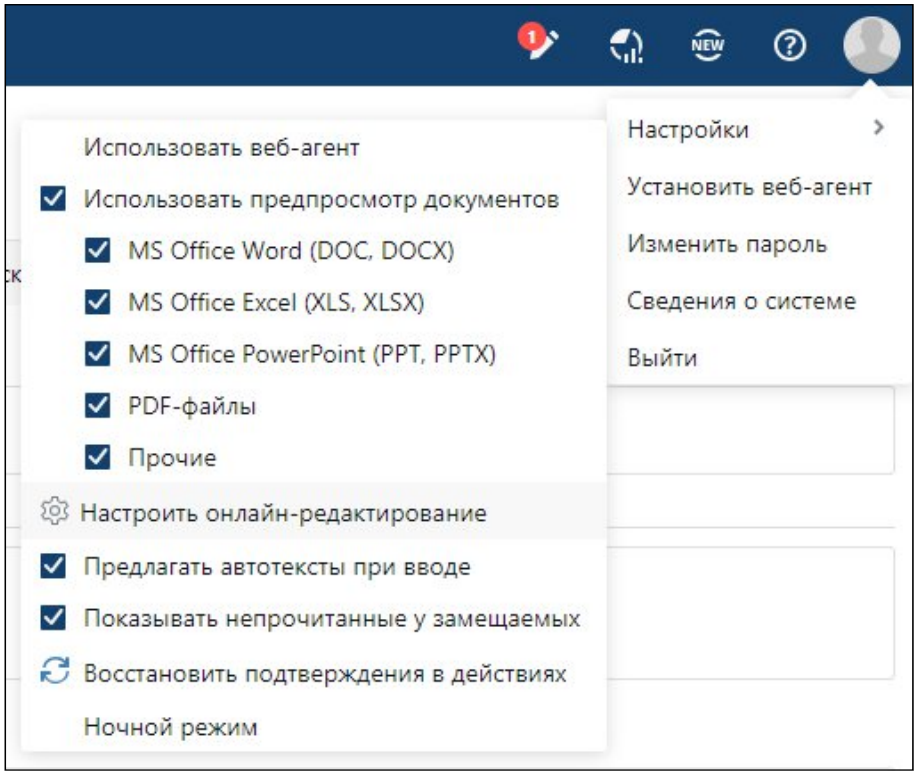


Рисунок 6 – Настройки онлайн-редактирования

При корректной настройке отобразится страница настроек редактора (Рисунок 7).

Рисунок 7 – Окно настроек редактора

Далее можно выполнить тестирование редактора. Для тестирования функциональности выполните следующие действия:

1. Создайте документ (выберите «Прочее» → «Простой документ»).
2. Заполните обязательные поля карточки документа.
3. Импортируйте существующий или создайте новый документ.
4. Откройте документ на редактирование.

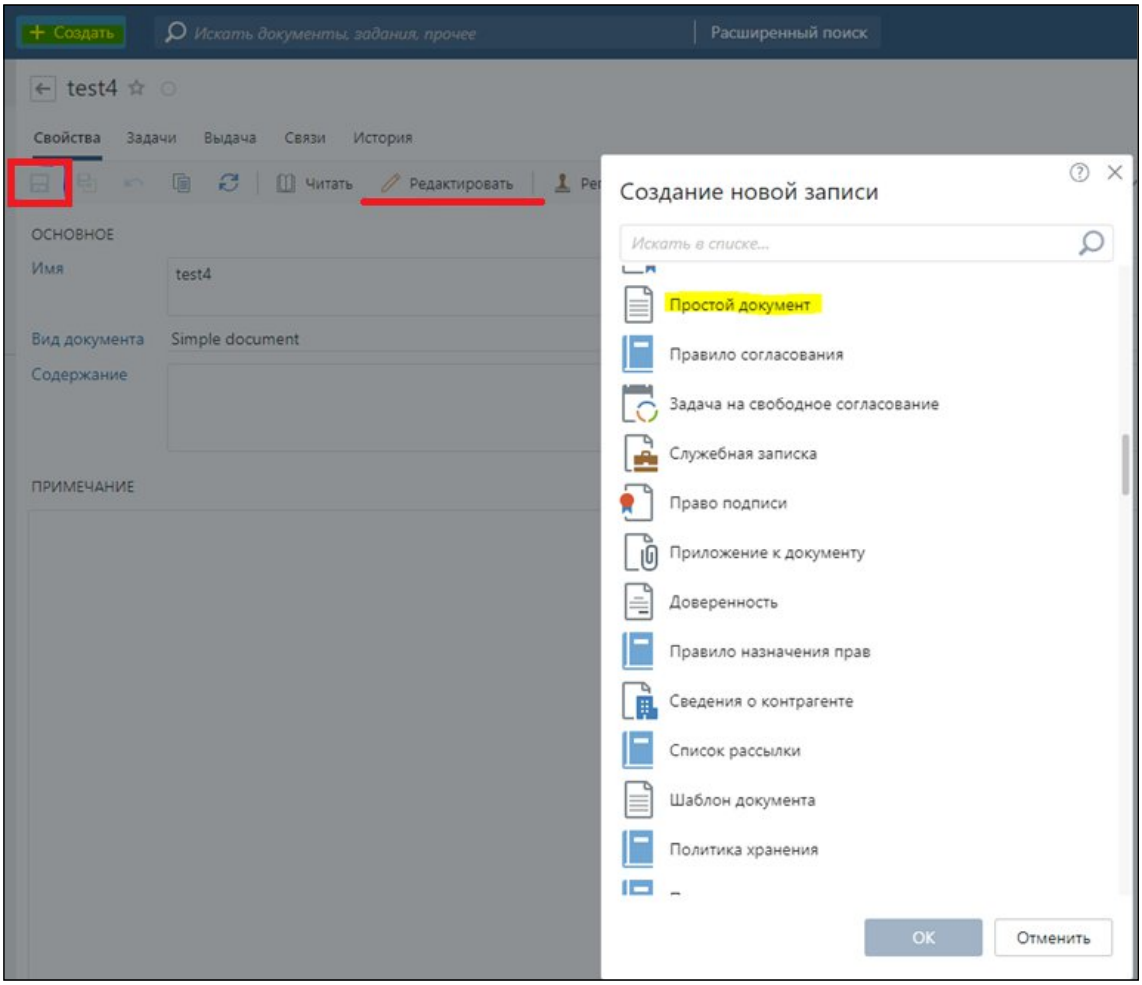


Рисунок 8 – Создание новой записи

5. Убедитесь, что документ открывается в онлайн-редакторе Р7-Офис.

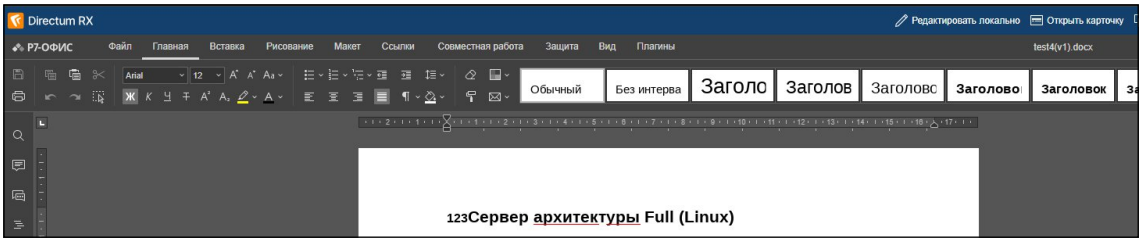


Рисунок 9 – Редактор Р7-Офис

Вынос онлайн редактора на другой сервер

Для подключения внешнего редактора из контейнера HAProxy необходимо извлечь файл конфигурации и выполнить его внешнее монтирование. Выполните следующие команды:

```
docker cp haproxy_tenant1:/usr/local/etc/haproxy/haproxy.cfg ./tenant_haproxy.cfg
```

Добавьте монтирование файла конфигурации и дополнительные переменные в файл `docker-compose.yml`:

```
haproxy_tenant1:
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "5"
  image: ${DOCKER_REGISTRY}/collaboration/haproxy:${VERSION_TAG}
  hostname: haproxy
  environment:
    - COLLABORATION_SERVICE_ADDRESS=collaboration_tenant1:3333
    - DOCUMENTSERVER_ADDRESS=ds.test4.s7-office.site # здесь указываем доменное имя или ip ДС
    - DOCUMENTSERVER_PORT=443 # указываем порт ДС
  ports:
    - "8090:80"
    - "8095:8095" # вынос порта для просмотра статистики хапрокси (по дефолту УЗ и пароль - пустые строки)
  volumes:
    - ./tenant_haproxy.cfg:/usr/local/etc/haproxy/haproxy.cfg # файл конфига хапрокси
  restart: on-failure
  container_name: haproxy_tenant1
  depends_on:
    - documentserver
    - collaboration_tenant1
    - staticfiles
```

В файле конфигурации HAProxy добавьте дополнительный DNS-сервер:

```
resolvers docker_dns
  nameserver dns1 127.0.0.11:53
  nameserver dns2 8.8.8.8:53
  accepted_payload_size 8192
```

Настройка HTTPS-подключения

Если документ-сервер доступен по протоколу HTTPS, добавьте параметр отключения проверки сертификата:

```
server-template docserver 20 ${DOCUMENTSERVER_ADDRESS}:${DOCUMENTSERVER_PORT} check port ${DOCUMENTSERVER_PORT} resolvers docker_dns init-addr none check ssl verify none
```

Проверка доступности

Убедитесь, что документ-сервер доступен для HAProxy через страницу статистики (порт 8095). Для проверки состояния подключения используйте команды:

```
docker logs haproxy_tenant
```

5. ИНТЕГРАЦИЯ С COMMUNIGATE PRO

5.1 Особенности интеграции с CommuniGate Pro

Интеграция Сервера документов Р7-Офис с платформой CommuniGate Pro реализована технологическими партнерами CommuniGate Pro. Интеграция позволяет организовать работу с документами в веб-интерфейсе Samoware CommuniGate Pro.

5.2 Настройка отключения JWT-токенов

Интеграция с CommuniGate Pro не поддерживает использование шифрования JWT-токенами. Для корректной работы необходимо отключить поддержку JWT-токенов на сервере редактора документов.

Для сервера документов R7-Офис:

Откройте файл конфигурации `local.json`:

– Для Linux: `/etc/r7-office/documentserver/local.json`;

– Для Windows: `%ProgramFiles%\R7OFFICE\DocumentServer\config\local.json`.

Приведите параметры токенов к следующему виду:

```
"token": {
"enable": {
"request": {
"inbox": false,
"outbox": false
},
"browser": false
},
"inbox": {
"header": "Authorization"
},
"outbox": {
"header": "Authorization"
}
},
"secret": {
"inbox": {
"string": "secret"
},
"outbox": {
"string": "secret"
},
"session": {
"string": "secret"
```

Для корпоративного сервера Р7-Офис:

Откройте файлы конфигурации:

– Для Linux: `/var/www/r7office/WebStudio/web.appsettings.config` и `/var/www/r7office/Services/TeamLabSvc/TeamLabSvc.exe.config`;

– Для Windows: `%ProgramFiles%\R7-OFFICE\CommunityServer\WebStudio\web.appsettings.config` и `%ProgramFiles%\R7-`

OFFICE\CommunityServer\Services\TeamLabSvc\TeamLabSvc.exe.config;

Установите следующие значения:

```
<add key="files.docservice.secret" value="" />
<add key="files.docservice.secret.header" value="" />
```

Перезапустите сервисы редактора документов

– Для версий ниже 7.3.3:

```
supervisorctl restart all
```

– Для версий 7.3.3 и выше:

```
sudo systemctl restart ds-docservice.service ds-converter.service ds-metrics.service
```

– Для Windows: перезапустите службы через оснастку «Службы».

5.3 Конфигурация параметров в Samoware

Добавьте в параметр `strings.files.data` интерфейса Samoware CommuniGatePro:

```
{
 "P7OfficeEditorUrl": "scheme://documentserver:_port_/web-apps/apps/api/documents/api.js",
 "P7OfficeEditorCustomPort_http": "80",
 "P7OfficeEditorCustomPort_https": "443"
}
```

– Замените **documentserver** на DNS-имя или IP-адрес сервера R7-Офис;

– Параметр **_port_** является переменной и не должен изменяться;

При подключении к корпоративному серверу:

Измените адрес в файле `strings.files.data`:

```
{
 "P7OfficeEditorUrl": "scheme://example.com:_port_/ds-vpath/OfficeWeb/apps/api/documents/api.js",
 "P7OfficeEditorCustomPort_http": "80",
 "P7OfficeEditorCustomPort_https": "443"
}
```

– Используйте префикс `/ds-vpath/` при обращении к корпоративному серверу;

– Замените `example.com` на адрес вашего корпоративного сервера.

5.4 Настройка адреса редактора документов

Настройка NGINX для корпоративного сервера

Для корректной работы интеграции с корпоративным сервером необходимо настроить NGINX:

1. Откройте файл конфигурации NGINX:
   - Для RedHat-производных: `/etc/nginx/conf.d/r7-office.conf`;
   - Для Debian-производных: `/etc/nginx/sites-enabled/r7-office.conf` и `/etc/nginx/sites-available/r7-office.conf`.
2. Добавьте значение `ds-vpath` в секцию:

```
map $request_uri $header_x_frame_options {
 ~*^/(ds-vpath|favicon\.ico|products\/files\/share\.aspx|products\/files\/saveas\.aspx|products\/files\/filechoice\.aspx|products\/files\/doceditor\.aspx|thirdparty\/plugin) "";
 default "SAMEORIGIN";
}
```

3. Сохраните файл и перезапустите NGINX.

Дополнительные настройки

1. Проверьте настройки прослушивания портов в веб-интерфейсе администрирования CommuniGatePro:
   - Перейдите в раздел «Установки => Услуги => HTTPU»;
   - Нажмите на ссылку «Приемник»;

2. Убедитесь, что сервер слушает порт 443. Переведите работу корпоративного сервера на HTTPS.
3. Добавьте правила в файрволл при необходимости:

```
firewall-cmd --permanent --add-port=80/tcp --add-port=443/tcp
```

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
изм	измененных	замененных	новых	аннулированных					