Р7-ОФИС

Инструкция по установке reverse proxy на базе nginx для архитектуры middle

Содержание

1. Архитектура

В данной инструкции рассмотрим установку **reverse proxy** для программного продукта Р7 Сервер Базовый в архитектуре **Middle**.

Ниже представлена схема архитектуры **Middle** с **reverse proxy** (**nginx**)

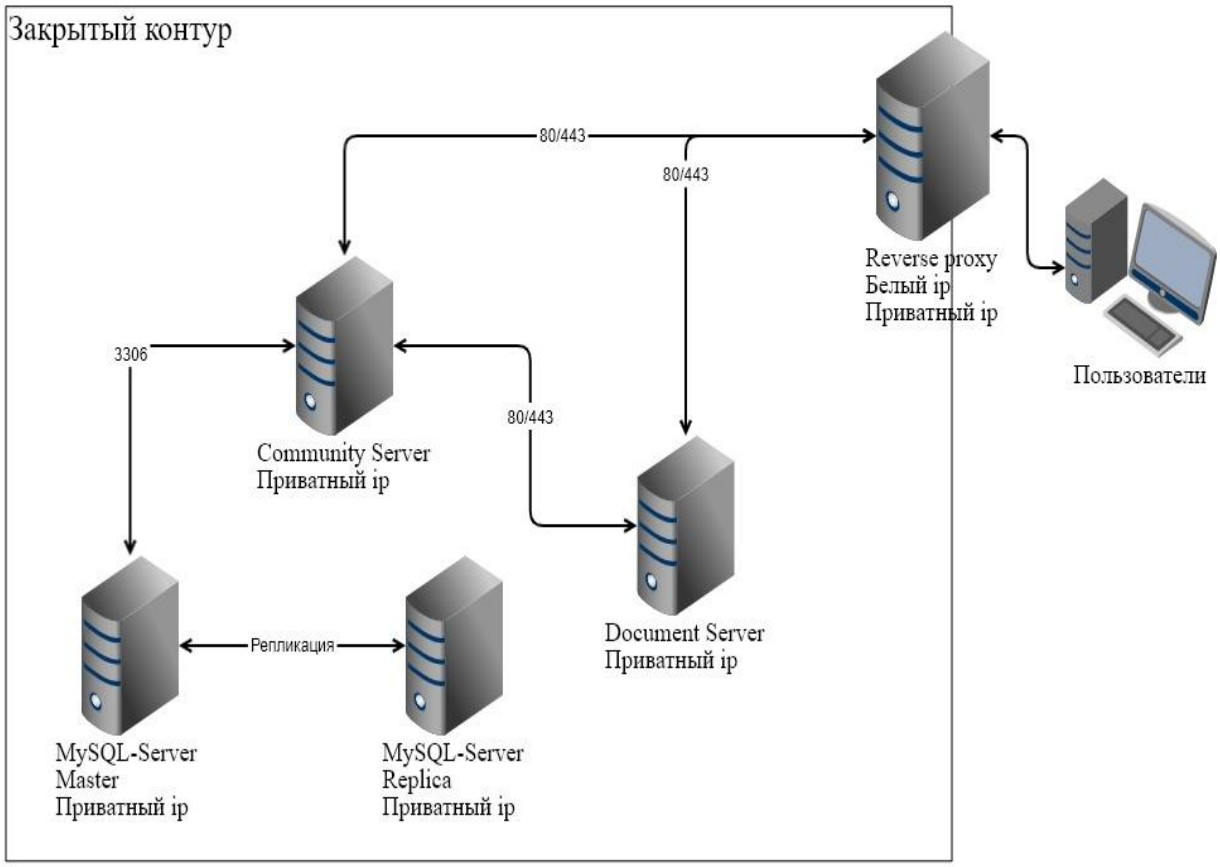


схема middle архитекруры за reverse proxy

Преимущества данной архитектуры заключаются в повышении отказоустойчивости системы в целом и закрытия доступа к серверам из вне.

1.1 Front-end / back-end приложения

Как в случае с **Microsoft Windows**, так и в случае с **Linux** версией продукта, **front-end** и **back-end** приложения размещается на одном сервере. Нагрузка на сервер приложений снижается за счёт размещения функциональных модулей на отдельных серверах.

1.2 Система Управления Базами Данных

База данных является неотъемлемой частью Продукта, обеспечивает хранение и управление следующими данными (укрупнённо):

- информация о пользователях системы;
- содержится мета информация для документов и писем;
- пользовательские данные по рабочим модулям Продукта.

Для устранения факторов, влияющих на деградацию производительности Программного комплекса в целом, в архитектурном решении **Middle**, система управления базами данных устанавливается на отдельные сервера для исключения воздействия сторонних систем, которые могут привести, в том числе, и к увеличению времени ожидания диска, что является одним из критических показателей для информационных систем.

1.3 Документ сервер

Система документ сервера в данном варианте инсталляции предусматривает размещение на отдельных серверах как в версии **Docker** контейнера так и с применением обычной установки.

Функционирование документ сервера возможно как на базе операционных систем типа **Microsoft Windows** так и **Linux** подобных системах.

1.4 Reverse proxy

Установленный **nginx** на отдельном сервере, для осуществления ретрансляции запросов клиентов из внешней сети на один, при однонодовой инсталляции, или несколько серверов, в архитектуре **middle**, как в данном случае (Связь через **reverse proxy** происходит с **CS** и **DS**).

2. Установка nginx

Примечание: Можно воспользоваться инструкцией на официальном сайте для установки свежей версии nginx. Также можно использовать ту, что в официальном репозитории для Вашей ОС, т.е. сразу выполнить установку.

В данном примере рассмотрим установку **nginx** для Astra Linux Common Edition 2.12.45 с установленными последними пакетами из репозитория.

2.1 Добавление репозитория

Добавьте в файл **/etc/apt/sources.list.d/nginx.list** данные записи:

```
deb https://nginx.org/packages/debian/ stretch nginx
deb-src https://nginx.org/packages/debian/ stretch nginx
```

Выполните далее команду:

```
apt update
```

Если возникает ошибка

```
Следующие подписи не могут быть проверены, так как недоступен открытый ключ:
NO_PUBKEY $KEY
```

То выполните команду:

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys $KEY
```

Где,

```
$KEY – значение, которое необходимо подставить из уведомления во время
обновления репозитория.
```

2.2 Установка пакета

2.2.1 Изменить значение в файле orel

Измените значение в файле **/etc/apt/preferences.d/orel** с 900 на 500, пример:

```
Package: *
Pin: release n=orel
Pin-Priority: 500
```

2.2.2 Установить nginx

Выполните команды:

```
apt update
apt install nginx
```

2.2.3 Запускаем и добавляем в автозагрузку

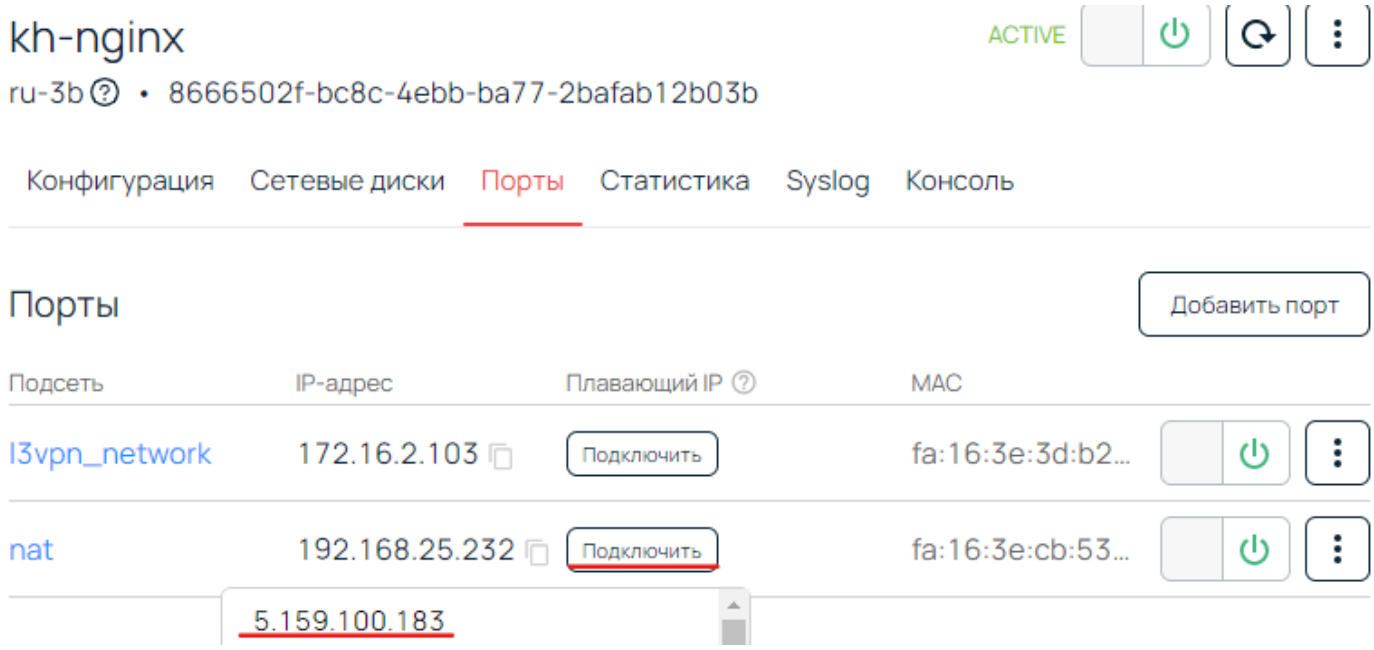
Выполните команды:

```
systemctl start nginx
systemctl enable nginx
```

3. Создаём записи в DNS

3.1 Добавляем на ВМ белый ip

Добавляем **ip**, в нашем случае, на площадке **Selectel** мы добавили к **nat** интерфейсу белый **ip**.



3.2 Создаём **A**-записи

Создаём **A**-запись, в нашем случае, на площадке **Selectel**. Создаём для **CS** и для **DS**, т.е. 2 **A**-записи.

3.3 Записи в hosts

3.3.1 Запись для CS

Делаем запись в **/etc/hosts** на **CS**:

```
<приватный ip reverse proxy> <dns_name for DS reverse proxy>
Пример:
172.19.3.120 ds.r7.ru
```

Где,

```
<приватный ip reverse proxy> – ip reverse proxy из закрытой сети;
<dns_name for DS reverse proxy> – A-запись reverse proxy для Документсервера.
```

3.3.2 Запись для DS

Делаем запись в **/etc/hosts** на **DS**:

```
<приватный ip reverse proxy>   <dns_name for CS reverse proxy>
Пример:
172.19.3.120 cs.r7.ru
```

Где,

```
<приватный ip reverse proxy> – ip reverse proxy из закрытой сети;
<dns_name for CS reverse proxy> – A-запись reverse proxy для Сервера Совместной
Работы.
```

4. Настраиваем nginx

4.1 Убираем конфиг по умолчанию

Удалите конфигурационный файл по умолчанию:

```
/etc/nginx/conf.d/default.conf
```

Также очистите каталог от файлов/ссылок, если такой есть:

```
/etc/nginx/sites-available/
```

4.2 Создаём файл конфигурации общий

Создайте конфигурационный файл:

```
mcedit /etc/nginx/conf.d/r7-proxy.conf
```

И добавьте записи (пример для **https reverse proxy** и **http** сервиса **CS**):

```
upstream ds {
  server <IP_DS>;
}

upstream cs {
  server <IP_CS>;
}

map $http_host $this_host {
    "" $host;
    default $http_host;
}

map $http_x_forwarded_proto $the_scheme {
     default $http_x_forwarded_proto;
     "" $scheme;
}

map $http_x_forwarded_host $the_host {
    default $http_x_forwarded_host;
    "" $this_host;
}

map $http_upgrade $proxy_connection {
  default upgrade;
  "" close;
}
```

Где,

```
<IP_CS> - приватный ip адрес Community Server
<IP_DS> - приватный ip адрес Document Server
```

4.3 Добавляем конфигурационный файл для CS

Создайте конфигурационный файл:

```
mcedit /etc/nginx/conf.d/r7-cs.conf
```

И добавьте записи (пример для **https reverse proxy** и **http** сервиса **CS**):

```
server {
    listen 80;
    server_name <DNS_CS>;
    server_tokens off;

    ## Redirects all traffic to the HTTPS host
    return 301 https://$server_name$request_uri;
}
server {
    listen  443 ssl http2;
    server_name <DNS_CS>;

# пути до сертификатов
    ssl_certificate     <SSL_CERTIFICATE_PATH>;
    ssl_certificate_key <SSL_KEY_PATH>;
    ssl_protocols TLSv1.1 TLSv1.2;
    ssl_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";
    ssl_prefer_server_ciphers on;
    large_client_header_buffers 4 64k;
    client_max_body_size 50m;

    location / {  # Контекст описывающий проксирование сервера приложения
        proxy_pass          http://cs;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $proxy_connection;
        proxy_set_header X-Forwarded-Host $the_host;
        proxy_set_header X-Forwarded-Proto $the_scheme;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header Host $the_host;
        proxy_connect_timeout 7d;
        proxy_send_timeout 7d;
        proxy_read_timeout 7d;
        proxy_redirect off;

    }
}
```

Где,

```
<DNS_CS> - имя для сервиса CS, например cs.r7-office.ru
<SSL_CERTIFICATE_PATH> - путь до ssl сертификата
<SSL_KEY_PATH> - путь до приватного ключа сертификата
```

4.4 Добавляем конфигурационный файл для DS

Создайте конфигурационный файл:

```
mcedit /etc/nginx/conf.d/r7-ds.conf
```

И добавьте записи (пример для **https reverse proxy** и **http** сервиса **DS**):

```
server {
  listen 80;
  server_name <DNS_DS>;
  server_tokens off;
  ## Redirects all traffic to the HTTPS host
  return 301 https://$server_name$request_uri;
}

server {
  listen 443 ssl http2;
  server_name <DNS_DS>;
  server_tokens off;
  root /usr/share/nginx/html;

  ssl_certificate     <SSL_CERTIFICATE_PATH>;
  ssl_certificate_key <SSL_KEY_PATH>;
  ssl_verify_client off;
  ssl_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";

  ssl_protocols  TLSv1.1 TLSv1.2 TLSv1.3;
  ssl_session_cache  builtin:1000  shared:SSL:10m;

  ssl_prefer_server_ciphers   on;

  add_header X-Content-Type-Options nosniff;

  location / {
    proxy_pass http://ds;
    proxy_http_version 1.1;

    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection $proxy_connection;
    proxy_set_header X-Forwarded-Host $the_host;
    proxy_set_header X-Forwarded-Proto $the_scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  }
}
```

Где,

```
<DNS_DS> – имя для сервиса DS, например ds.r7-office.ru
<SSL_CERTIFICATE_PATH> – путь до ssl сертификата
<SSL_KEY_PATH> – путь до приватного ключа сертификата
```

4.5 Выписываем ssl сертификаты

4.5.1 Устанавливаем letsencrypt

4.5.1.1 Добавляем репозиторий

Выполните команду:

```
mcedit /etc/apt/sources.list.d/debian.list
```

Добавляем строку:

```
deb https://mirror.yandex.ru/debian/ stretch main contrib non-free
```

4.5.1.2 Устанавливаем пакет

Выполните команды:

```
apt update
apt install letsencrypt python3-certbot-nginx
```

4.5.2 Редактируем конфигурационные файлы

Временно комментируем строки в двух файлах конфигурационных, нами созданных:

```
# ssl_certificate     /etc/nginx/ssl/domain.crt;
# ssl_certificate_key /etc/nginx/ssl/domain.key;
```

Преобразуем строку

```
listen 443 ssl http2;
```

В строку вида

```
listen 443 http2;
```

Перезапускаем nginx с проверкой конфигов перед этим:

```
nginx -t
systemctl restart nginx
```

4.5.3 Выписываем сертификат

Выполните команду:

```
letsencrypt certonly --nginx -d kh-ds.r7-office.ru -d kh-cs.r7-office.ru
```

Где,

```
kh-ds.r7-office.ru – A запись для DS;
kh-cs.r7-office.ru – A запись для CS.
```

Во время инсталляции подготовки сертификатов будут задаваться вопросы, примеры ответов ниже.

4.5.3.1 Указывать почту

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): kharitonov.vadim@r7-office.ru
```

4.5.3.2 Отвечаете A

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017-w-v1.3-notice.pdf.
You must agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A
```

4.5.4.3 На своё усмотрение отвечаете

```
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
```

4.5.4.4 Используем сертификаты

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for kh-cs.r7-office.ru
http-01 challenge for kh-ds.r7-office.ru
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/kh-ds.r7-office.ru/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/kh-ds.r7-office.ru/privkey.pem
   Your cert will expire on 2022-12-20. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Сертификаты для обоих имён созданы тут:

```
/etc/letsencrypt/live/kh-ds.r7-office.ru/
```

Где,

```
kh-ds.r7-office.ru – первый указанный домен в команде
```

4.5.4.4.1 Создаём каталог:

```
mkdir /etc/nginx/ssl
```

4.5.4.4.2 Создаём ссылки:

```
ln              -rs              /etc/letsencrypt/live/kh-ds.r7-office.ru/fullchain.pem
/etc/nginx/ssl/domain.crt
ln -rs /etc/letsencrypt/live/kh-ds.r7-office.ru/privkey.pem /etc/nginx/ssl/domain.key
```

4.5.4.4.2 Редактируем конфигурационные файлы

Раскомментируем строки в двух файлах, которые мы создали в п.4.2 и п.4.3:

```
ssl_certificate     /etc/nginx/ssl/domain.crt;
ssl_certificate_key /etc/nginx/ssl/domain.key;
```

Преобразуем строку

```
listen 443 http2;
```

В строку вида

```
listen 443 ssl http2;
```

4.6 Проверяем и перезапускаем

4.6.1 Проверяем корректность настроек

Выполните команду

```
nginx -t
```

Если всё хорошо, то идём дальше, если получаем ошибки, то необходимо их исправить.

4.6.2 Перезапускаем nginx

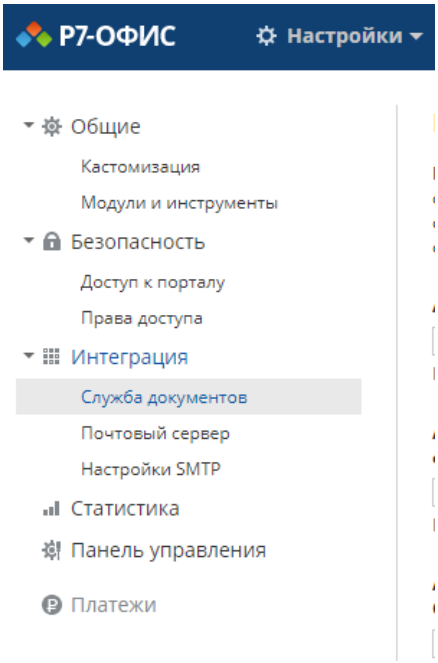
Выполните команду для перезагрузки и добавления в автозагрузку:

```
systemctl restart nginx
```

5. Донастраиваем портал для работы

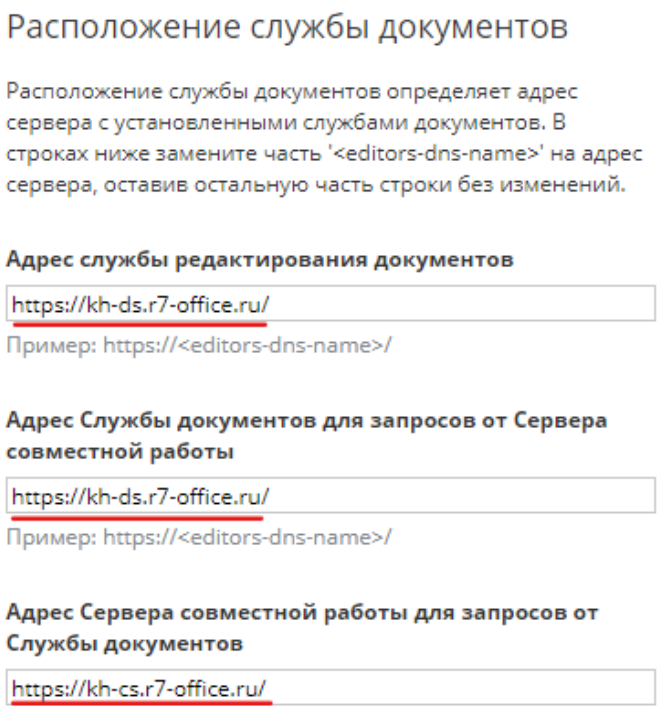
5.1 Переходим в настройки

Переходим в "Настройки"—>"Интеграция"—>"Служба документов" уже по созданной DNS записи



5.2 Изменяем настройки

Приводим к виду:



Где,

```
kh-ds-r7-office.ru – A-запись для Document Server
kh-cs.r7-office.ru – A-запись для Community Server
```

5.3 Проверяем работу

Заходим в модуль документы и проверяем его работу, открывая документы и т.п.