# 1 Centos 7 установка Nginx

1. Установить репозиторий EPEL:

yum install epel-release

1. Устанавливаем Nginx

yum install nginx

1. Добавляем правила для фаервола:

firewall-cmd --zone=public --permanent --add-service=http

firewall-cmd --zone=public --permanent --add-service=https

1. Перезагружаем фаервол:

firewall-cmd –reload

1. Запускаем Nginx (80 порт должен быть свободный):

systemctl start nginx

1. Проверяем работу Nginx. Если все было сделано правильно, то, открыв адрес сервера (в данном случае 176.254.47.3), на который вы устанавливали Nginx, вы увидите страницу по умолчанию:



1. Добавить nginx в автозапуск

systemctl enable nginx

# 2 Настройки Nginx

Конфигурация Nginx храниться в файле *nginx.conf* в папке Nginx по умолчанию *(/etc/nginx),* дополнительные конфигурации в папке *conf.d*.

Файл примера c комментариями: <https://github.com/aleksandrov-ivan/domino_nginx>

ВАЖНО: Certbot для Centos 7 не поддерживает парсинг комментариев на русском.

# 3 Настройка Let’s Encrypt для Nginx CentOS 7

1. Устанавливаем упал пакет

yum install <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>

1. Устанавливаем сербот

yum install certbot python2-certbot-nginx

1. Создаем сертификаты они автоматические попадут в настройки nginx. (Nginx должен работать)

ИЛИ

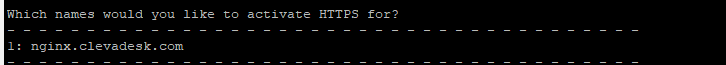
certbot --nginx

ИЛИ

Если нет необходимости восстанавливать сертификаты без доступа к данной машине:

certbot --nginx --register-unsafely-without-email

После покажет список найденных доменов в настройках nginx



Если серверов несколько пишем через пробел, в примере сервер 1.

После в настройках nginx будут автоматически добавлены созданные сертификаты:

listen 443 ssl; # managed by Certbot

ssl\_certificate /etc/letsencrypt/live/nginx.clevadesk.com/fullchain.pem; # managed by Certbot

ssl\_certificate\_key /etc/letsencrypt/live/nginx.clevadesk.com/privkey.pem; # managed by Certbot

include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot

ssl\_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

и перенаправление с 80 на 443 порт

server {

if ($host = nginx.clevadesk.com) {

return 301 https://$host$request\_uri;

} # managed by Certbot

server\_name nginx.clevadesk.com;

listen 80;

return 404; # managed by Certbot  
}

1. Для включения http/2 изменить строку:

listen 443 ssl; # managed by Certbot

на

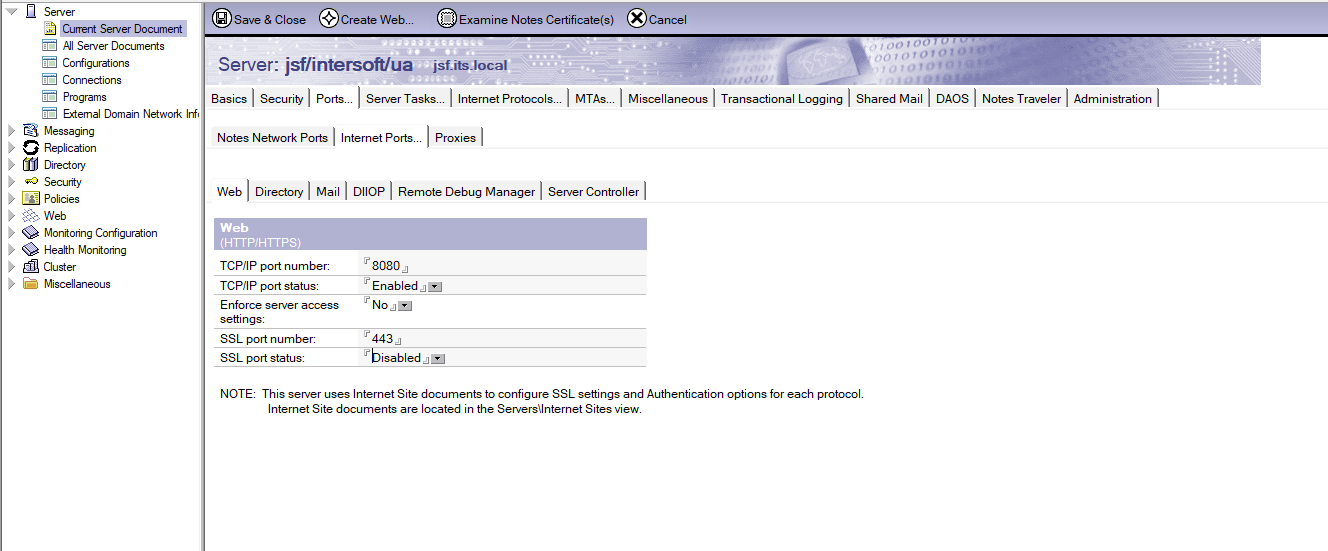
listen 443 ssl http2; # managed by Certbot

1. Автоматическое продление (каждую субботу проверяем, если < 30 дней осталось продлевает и выполнять мягкую перезагрузку веб-сервера):

echo "00 00 \* \* 6 certbot renew --post-hook 'service nginx reload' >> /var/log/le-renew.log" | sudo tee -a /etc/crontab > /dev/null

# 4 Настройки Domino

1. Разрешаем использование заголовков notes.ini => HTTPEnableConnectorHeaders=1
2. Переносим работу http на порт 8080



1. Перезагрузить домино.