Table of Contents

odoo with HTTPS and NGINX

Install nginx:

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

In /etc/odoo.conf set:

```
http_interface = 127.0.0.1
proxy_mode = True
```

In /etc/nginx/sites-available/odoo.conf set:

```
#odoo server
upstream odoo {
 server 127.0.0.1:8069;
}
upstream odoochat {
 server 127.0.0.1:8072;
}

# http -> https
server {
   listen 80;
   server_name odoo13.sempai.space;
   rewrite ^(.*) https://$host$1 permanent;
}

server {
 listen 443;
 server_name odoo13.sempai.space;
 proxy_read_timeout 720s;
 proxy_connect_timeout 720s;
 proxy_send_timeout 720s;

 # Add Headers for odoo proxy mode
 proxy_set_header X-Forwarded-Host $host;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 proxy_set_header X-Forwarded-Proto $scheme;
 proxy_set_header X-Real-IP $remote_addr;

 # SSL parameters
 ssl on;
 ssl_certificate /etc/ssl/nginx/odoo.crt;
 ssl_certificate_key /etc/ssl/nginx/odoo.key;
 ssl_session_timeout 30m;
 ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
 ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-
```

```
AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-
SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-
SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-
AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-
SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-
SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-
SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA';
 ssl_prefer_server_ciphers on;

 # log
 access_log /var/log/nginx/odoo.access.log;
 error_log /var/log/nginx/odoo.error.log;

 # Redirect longpoll requests to odoo longpolling port
 location /longpolling {
 proxy_pass http://odoochat;
 }

 # Redirect requests to odoo backend server
 location / {
   proxy_redirect off;
   proxy_pass http://odoo;
 }

 # common gzip
 gzip_types text/css text/scss text/plain text/xml application/xml
application/json application/javascript;
 gzip on;
}
```

Restart nginx:

```
ln -s /etc/nginx/sites-available/odoo.conf /etc/nginx/sites-enabled/
mkdir /etc/ssl/nginx/
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/nginx/odoo.key -out /etc/ssl/nginx/odoo.crt
systemctl restart nginx
```

To create multiple sites:

```
sed 's/odoo/angellomonge/' odoo.conf > angellomonge.conf
```

Cerbot

```
sudo apt-get install certbot python-certbot-nginx
sudo certbot certonly --nginx
```

Replace ssl paths, for example:

```
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/mallvirtual.sempai.space/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/mallvirtual.sempai.space/privkey.pem
  Your cert will expire on 2020-07-08. 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"
```

References

- https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-nginx-in-ubuntu-18-04
- https://www.odoo.com/documentation/12.0/setup/deploy.html
- https://certbot.eff.org/lets-encrypt/debianbuster-nginx
- https://www.digitalocean.com/community/tutorials/how-to-set-up-nginx-server-blocks-virtual-hosts-on-ubuntu-16-04