Encuesta Productos Mexicanos

1. En DigitalOcean crear un DropLet de Ubuntu 18.04.3 LTS con plan standard de $5 dlls al mes ($0.007/hora) 1GB/1CPU, 25 GB SSD disk, 1000GB transfer.
2. Hostname: ubuntuWebsite (64.225.125.18)
3. Sudo apt-get update
4. sudo apt-get upgrade -y
5. date
   1. timedatectl status
   2. timedatectl list-timezones
   3. sudo timedatectl set-timezone America/Tijuana
6. sudo apt-get install apache2 -y
7. Copiar con sftp [root@64.225.125.18](mailto:root@64.225.125.18); cd /var/www/backend-productosmexicanos/server-https.js
8. Para instalar nodejs
   1. Sudo apt-get install nodejs -y
   2. Sudo apt-get install npm -y
   3. Nodejs -v
   4. Npm -v
9. Npm install express
10. Npm install pg
11. Adduser eugalde
    1. Usermod -aG sudo eugalde
    2. Su – eugalde
12. SSL Certificate
    1. <https://letsencrypt.org/>
    2. <https://certbot.eff.org/>
13. sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
    1. Los certificados fueron creados en /etc/ssl
    2. While we are using OpenSSL, we should also create a strong Diffie-Hellman group, which is used in negotiating [Perfect Forward Secrecy](https://en.wikipedia.org/wiki/Forward_secrecy) with clients.
    3. sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
14. sudo wget https://dl.eff.org/certbot-auto -O /usr/sbin/certbot-auto
15. sudo chmod a+x /usr/sbin/certbot-auto
16. sudo certbot-auto certonly --standalone -d quieroproductosdemexico.com -d www.quieroproductosdemexico.com
17. Digital Ocean SSL Certificate
    1. sudo apt-get install python3-certbot-apache -y
    2. Letsencrypt –apache -d quieroproductosdemexico.com
       1. IMPORTANTE:El dominio ya tiene que haber replicado en los servidores DNS (ping quieroproductosdemexico.com)
18. Sudo apt-get install postgresql postgresql-contrib -y
    1. Passwd postgres
19. Dentro de postgres psql crear el usuario eugalde:
    1. create user myuser with encrypted password 'mypass';
    2. GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO eugalde;
    3. create table productosmexicanos(fecha date DEFAULT CURRENT\_DATE, fechahora timestamp without time zone DEFAULT CURRENT\_TIMESTAMP, pais varchar, productos varchar, ip varchar,xciudad varchar, xpais varchar);
20. SSL
    1. <https://timonweb.com/posts/running-expressjs-server-over-https/>
    2. <https://hostadvice.com/how-to/how-to-install-a-self-signed-ssl-certificate-for-apache-on-ubuntu-18-04-server/>
    3. sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/my.key -out /etc/ssl/certs/my.crt
    4. State or Province: e.g. CENTRAL
    5. Locality Name:  Name of City e.g. NAIROBI
    6. Organisation Name: e.g. MY SAMPLE COMPANY
    7. Organizational Unit Name (eg, section) []: e.g. IT DEPARTMENT
    8. Common Name (e.g. server FQDN or YOUR name) []: The exact domain name or public IP address e.g. [www.example.com](http://www.example.com)
    9. Email Address: e.g. info@example.com
    10. After answering the questions above, the private and crt files will be placed on the path that you specified on the OpenSSL command. For instance, in our case, the private key will be placed in /etc/ssl/private/my.key while the CRT will be placed in /etc/ssl/certs/my.crt
    11. Enable port
        1. Sudo ufw enable
        2. Sudo ufw status
        3. Sudo ufw allow 443 o sudo ufw allow https
        4. Sudo ufw allow 80
        5. Sudo ufw allow 22
        6. Sudo ufw allow <port>
21. Node server-https.js
22. Para crear un ssl comprado en NOIP.COM:
    1. Lo compré en noip.com a 20 dlls.
    2. Me pidió correr el siguiente comando para craer un csr
       1. openssl req -new -nodes -keyout myserver.key -out server.csr
       2. Es NECESARIO no poner password en las preguntas que hace. Eso me marcaba error cuando me pedía que lo abriera y lo copiara para crear el ssl.
       3. Levanté un ticket para ver cómo funciona el APPROVAL Email
       4. Esta página ayuda a validar el CSR (CSR Decoder) (La busqué en google así “csr checker”: <https://www.sslshopper.com/csr-decoder.html>
       5. También se puede validar con esta línea de comando: openssl req -in mycsr.csr -noout -text
23. Para validar la configuración de apache: apachectl configtest
    1. Restart Apache2:
       1. Service apache2 restart
       2. /etc/init.d/apache2 restart
24. En /etc/apache2/sites-enabled/000-default.conf
    1. Comentariar todas las lineas iniciales que están en la sección de <VirtualHost \*:80> </VirtualHost>
    2. <VirtualHost \*:443>

ServerAdmin admin@quieroproductosdemexico.com

DocumentRoot /var/www/html

ServerName quieroproductosdemexico.com

SSLEngine on

SSLCertificateFile /etc/ssl/certs/myserver.cert

SSLCertificateKeyFile /etc/ssl/certs/myserver.key

SSLCertificateChainFile /etc/ssl/certs/myserver.ca

<Directory /var/www/html>

AllowOverride All

Options FollowSymlinks

</Directory>

</VirtualHost>

<VirtualHost \*:80>

Servername quieroproductosdemexico.com

Redirect permanent / https://quieroproductosdemexico.com

</VirtualHost>

1. Para poder dejar corriendo el servicio de backend como servicio:
   1. Instalar pm2:
      1. Npm install -g pm2
   2. Correr el backend como servicio:
      1. pm2 start server\_https.js
      2. pm2 status
   3. Para ver los commandos que se pueden correr con pm2:
      1. Pm2 examples
      2. Ejemplos:
         1. Pm2 status
         2. Pm2 monitor
         3. Pm2 startup
         4. http://pm2.io