LAMP Centos 7 на AWS Lightsail

```
# yum install update
```

- Timezone Centos 7

```
# yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
# yum -y install https://rpms.remirepo.net/enterprise/remi-release-7.rpm

# yum -y install yum-utils
# yum-config-manager --enable remi-php72
# yum update
# yum install wget zip unzip
# yum install httpd
```

MariaDB

```
# yum install mariadb-server mariadb
# mysql_secure_installation
```

And answer to questions in wizard:

- Switch to unix_socket authentication [Y/n] **Y**
- Change the root password? [Y/n] **Y**
- New password: ******
- Re-enter new password: ******
- Remove anonymous users? [Y/n] **Y**
- Disallow root login remotely? [Y/n] **Y**
- Remove test database and access to it? [Y/n] **Y**
- Reload privilege tables now? [Y/n] **Y**

PhP

```
# yum install php php-common php-mcrypt php-cli php-gd php-curl php-mysql
```

```
php-xml php-mbstring php-sodium php-pecl-mysql

# yum install gcc php-devel php-pear
# yum install ImageMagick ImageMagick-devel
# pecl install imagick

You should add "extension=imagick.so" to php.ini или создать файлик в
# vi /etc/php.d/imagick.so
extension=imagick.so
```

ProFTP

```
https://tst-amo.net.ua/blog/?p=2937
# yum install proftpd

mount -o bind /var/www/html /home/aws/html
```

Apache

```
# httpd -M
# yum install mod_ssl openssh
# apachectl restart
# httpd -t
# systemctl status httpd

# cat httpd.conf | egrep "^[^#]"
ServerRoot "/etc/httpd"
ServerTokens ProductOnly
  ServerSignature Off
  Listen 0.0.0.0:80
  Include conf.modules.d/*.conf
  User apache
  Group apache
  ServerAdmin root@localhost
  ServerName aws.tst-amo.net.ua:80
<Directory />
  AllowOverride none
  Require all denied
</Directory>
  DocumentRoot "/var/www/"

# Relax access to content within /var/www
```

```
<Directory "/var/www">
  AllowOverride All
  #Allow open access:
  Require all granted
  #Require all denied
</Directory>

# Further relax access to the default document root
<Directory "/var/www/html">
  Options -Indexes +FollowSymLinks
  AllowOverride All
  Require all granted
</Directory>

<Directory "/var/www/cgi-bin">
  AllowOverride None
  Options None
  Require all granted
</Directory>

<IfModule mime_module>
  TypesConfig /etc/mime.types
  AddType application/x-compress .Z
  AddType application/x-gzip .gz .tgz
  AddType text/html .shtml
  AddOutputFilter INCLUDES .shtml
</IfModule>

<IfModule dir_module>
  DirectoryIndex index.php index.html index.htm index.shtml
</IfModule>

<Files ".ht*">
  Require all denied
</Files>

ErrorLog "logs/error_log"
LogLevel warn

<IfModule log_config_module>
   LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
```

```
\"%{User-Agent}i\"" combined
  LogFormat "%h %l %u %t \"%r\" %>s %b" common

  <IfModule logio_module>
  # You need to enable mod_logio.c to use %I and %O
   LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\" %I %O" combinedio
  </IfModule>

  CustomLog "logs/access_log" combined
</IfModule>

<IfModule alias_module>
  ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
</IfModule>

<IfModule mime_magic_module>
  MIMEMagicFile conf/magic
</IfModule>

EnableSendfile on
IncludeOptional conf.d/*.conf
```

Запускаем сайт на протоколе http

```
# vi /etc/httpd/conf.d/aws.conf

<VirtualHost 0.0.0.0:80>
  ServerName aws.tst-amo.net.ua
  ServerAlias www.aws.tst-amo.net.ua
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ErrorLog /var/log/httpd/error.log
  CustomLog /var/log/httpd/access.log combined
  Redirect permanent / https://aws.tst-amo.net.ua/
</VirtualHost>
```

PhpMyAdmin

```
#                                                    wget
https://files.phpmyadmin.net/phpMyAdmin/4.9.11/phpMyAdmin-4.9.
11-all-languages.zip
```

Правим конфиг:

```
# cp config.sample.inc.php config.inc.php
# vi config.inc.php
$cfg['blowfish_secret'] = '12345678901234273190123456789012'
/**
* Directories for saving/loading files from server
*/
$cfg['TempDir'] = '/tmp';
```

Certbot

```
# yum install certbot
# certbot certonly -n --standalone -m user@gmail.com --agree-tos -d aws.tst-amo.net.ua
# ss -tlpn | grep -E ":(80|443)"
# systemctl stop httpd
# certbot certonly -n --standalone -m user@gmail.com --agree-tos -d aws.tst-amo.net.ua
# systemctl start httpd
```

Продление сертификатов:

```
# vi /etc/cron.daily/certbot-renew

#!/bin/sh
if certbot renew > /var/log/letsencrypt/renew.log 2>&1 ; then
          /usr/sbin/service    httpd    reload    >> /var/log/letsencrypt/renew.log
fi

exit
```

```
# crontab -e
07 02,18 * * * /etc/cron.daily/certbot-renew
```

Apache HTTPS

Подключим SSL в apache, создаем конф файл

```
# vi /etc/httpd/conf.d/aws-ssl.conf

<VirtualHost 0.0.0.0:443>
  ServerName aws.tst-amo.net.ua
```

```
  ServerAlias www.aws.tst-amo.net.ua
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ErrorLog /var/log/httpd/error.log
  CustomLog /var/log/httpd/access.log combined
  SSLEngine on
  SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL
  SSLHonorCipherOrder on
  SSLCompression off
    Header always set Strict-Transport-Security "max-
age=15552000; includeSubDomains; preload"

     SSLCertificateFile /etc/letsencrypt/live/aws.tst-
amo.net.ua/cert.pem
    SSLCertificateChainFile /etc/letsencrypt/live/aws.tst-
amo.net.ua/chain.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/aws.tst-
amo.net.ua/privkey.pem
</VirtualHost>
```

Проверяем на сайте ssllabs.com и радуемся рейтингу A+.

Postfix

Доустановим немобходимый механизм и консольный почтовик для проверки:

```
# yum install cyrus-sasl-plain
# yum install mailx
```

Postfix будет настроен как релей, используя google учетку:

```
# vi /etc/postfix/main.cf

relayhost = [smtp.gmail.com]:587

# Enables SASL authentication for postfix
smtp_sasl_auth_enable = yes
#  Disallow methods that allow anonymous authentication
smtp_sasl_security_options
```

```
= noanonymous
# Location of sasl_passwd we saved
smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
# Enable STARTTLS encryption for SMTP
smtp_tls_security_level = encrypt
# Location of CA certificates for TLS
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_sasl_security_options = noanonymous

# TLS parameters
smtpd_tls_cert_file=/etc/letsencrypt/live/aws.tst-amo.net.ua/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/aws.tst-amo.net.ua/privkey.pem
smtp_use_tls=yes
#smtpd_tls_mandatory_protocols=!SSLv2, !SSLv3
smtpd_tls_session_cache_database                    =
btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database                     =
btree:${data_directory}/smtp_scache

# vi /etc/postfix/master.cf
submission inet n - n - - smtpd

# vi /etc/postfix/aliases
postmaster: postmaster@aws.tst-amo.net.ua
root: no_reply_dataverse@aws.tst-amo.net.ua

# postmap aliases

# vi /etc/aliases
# Basic system aliases -- these MUST be present.
mailer-daemon: postmaster
postmaster: root
root: user@gmail.com

# newaliases

# vi /etc/postfix/sasl/sasl_passwd
[smtp.gmail.com]:587 user@mail.com:your_password

# postmap /etc/postfix/sasl/sasl_passwd
#   chown   root:root   /etc/postfix/sasl/sasl_passwd
/etc/postfix/sasl/sasl_passwd.db
```

```
#     chmod     600     /etc/postfix/sasl/sasl_passwd
/etc/postfix/sasl/sasl_passwd.db

# yum install ca-certificates
# systemctl restart postfix
```

Проверка:

```
# echo "Test Postfix Gmail https://example.com" | mail -s
"Postfix Gmail" to_user@domen.ua
```