Setting up a VPS server for WordPress

Index

1. Introduction

In this guide we will see how to quickly and easily setup a webserver for running your WordPress website.

We will be setting up Nginx, MariyaDB and PHP 7 on a Ubuntu server, then we will setup LMD and ClamAV to reduce malware infection and configure fail2ban to block these attempts to infect the website. Finally, we will see how to quickly setup S3 based WordPress backup.

So, let’s gets started.

2. Setting up the Server - Nginx, MySQL and PHP7 & Redis

Let’s start by installing easyengine, it will help us setup rest of the things.

1. *wget -qO ee rt.cx/ee && sudo bash ee # install easyengine*
2. *ee stack install*

We prefer to use Maradb10.2 of we will install that

1. *ee stack remove –mysql*
2. *nano /etc/apt/sources.list.d/ee-repo.list* to edit the file and change the value from 10.1 to 10.2 for mariadb.
3. *ee stack install –mysql*
4. *mysql -V*
5. you can get the root password at /etc/mysql/conf.d/my.cnf

Now, setup the domain with PHP 7

1. *ee site create nxt.smartinstitute.net –wpfc –php7*
2. *nano /etc/nginx/common/wpfc-php7.conf* and add aw2_vsesssion in $http_cookie line.

Let’s setup composer on the server

```
php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');"php -r "if (hash_file('SHA384', 'composer-setup.php') === '93b54496392c062774670ac18b134c3b3a95e5a5e5c8f1a9f115f203b75bf9a129d5daa8ba6a13e2cc8a1da0806388a8') { echo 'Installer verified'; } else { echo 'Installer corrupt'; unlink('composer-setup.php'); } echo PHP_EOL;"php composer-setup.phpphp -r "unlink('composer-setup.php');"
```

`mv composer.phar /`usr/local/bin/composer

Let’s make sure PHPMyAdmin is properly setup

`cd /var/www/22222/htdocs/db/pmacomposer update --no-dev`

Now let’s setup Redis

1. *add-apt-repository ppa:chris-lea/redis-server*
2. *apt-get update*
3. *apt-get install redis-server php-redis*

phpRedisAdmin

1. *mkdir /var/www/22222/htdocs/cache/redis && cd /var/www/22222/htdocs/cache/redis*
2. *git clone https://github.com/ErikDubbelboer/phpRedisAdmin.git*
3. *cd phpRedisAdmin*

4*git clone https://github.com/nrk/predis.git vendor*

WordPress Object Cache

1. cd /var/www/example.com/htdocs/wp-content
2. wget https://raw.githubusercontent.com/alleyinteractive/wp-redis/master/object-cache.php
3. chown www-data: object-cache.php

Block XML-RPC

1. nano /var/www/yourdomain.ltd/conf/nginx/xmlrpc.conf
2. And to add the following content in this .conf file :

```
location = /xmlrpc.php { deny all; access_log off; log_no
t_found off;}
```

3. Enable SSL

Let’s enable SSL using letsencrypt

1. *ee site update nxt.smartinstitute.net –letsencrypt*
2. *which ee* #to find the exact path of ee
3. *crontab -e*
4. update cron line to *0 0 * * 0 /usr/local/bin/ee site update –le=renew –all 2>> /var/log/ee/renew.log # Renew all letsencrypt SSL cert. Set by EasyEngine*

4. Preventing Malware

We will be using *Maldetect* and *ClamAV* for virus and malware scaning to pervent infection on the server.

```
1 wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
2 tar -zxvf maldetect-current.tar.gz
3 cd maldetect-1.6.2/
4 ./install.sh
5 apt-get install apparmor-utils
6 apt-get install inotify-tools
7 apt-get install clamav
8 apt-get install clamav-daemon
9 aa-complain clamd
10 service clamav-daemon start
11 nano /usr/local/maldetect/conf.maldet
12 nano /usr/local/maldetect/monitor_paths
13 nano /usr/local/maldetect/ignore_file_ext
14 service maldet start
```

5. Secure Your Server using Fail2ban

We use Fail2ban to parse log files and block IP address of malicious requests, just set up the fail2ban.

```
apt-get install fail2ban
```

After that simply add the following lines to *jail.conf* file.

```
jail.conf--------------[wordpress]enabled  = trueport     = http,httpsfilter   = wordpress-authlogpath  = /var/log/nginx/access.log     /var/log/nginx/wpoets.com.access.log     maxretry = 2bantime  = 3600[wordpress-extras]enabled  = trueport     = http,httpsfilter   = wordpress-extraslogpath  = /var/log/nginx/access.log     /var/log/nginx/wpoets.com.access.log    maxretry = 1bantime  = 43200
```

you will need to adjust the *logpath* above to point to actual log path on your server. *maxretry* is used to define the number of attempts before banning and bantime is used to define the number of seconds to ban the IP address.

Now create wordpress-*auth.conf* and wordpress-*extras.conf* file within filter.d folder using code mentioned below, you can put your own regex pattern in failregex key.

```
wordpress-auth.conf--------------------[Definition]failregex = <HOST>.*POST.*(wp-login\.php|xmlrpc\.php).* 403            <HOST>.*POST.*\/wp-content\/.*\.phpignoreregex =
```

```
wordpress-extras.conf----------------------------[Definition]failregex = <HOST>.*POST.*\/wp-content\/.*\.php     <HOST>.*POST.*\/wp-includes\/js\/.*\.php     <HOST>.*GET.*\/Purchase-2017     <HOST>.*GET.*\/Holidays-Card     <HOST>.*GET.*\/Outstanding-INVOICE-VVX     <HOST>.*GET.*\/oboskej     <HOST>.*GET.*\/vlnoeiw     <HOST>.*GET.*\/vlaofr     <HOST>.*GET.*\/ljysix     <HOST>.*GET.*\/journal\/y5eh2\.php     <HOST>.*GET.*\/blnoitez     <HOST>.*GET.*\/updatecorex\/     <HOST>.*GET.*\/wp-caches\.php  <HOST>.*POST.*(wp-login\.php|xmlrpc\.php).* 499  <HOST>.*POST.*\/wp-includes\/images\/.*\.php  <HOST>.*POST.*\/wp-admin\/css\/colors\/.*\.php  <HOST>.*POST.*\/wp-includes\/rest-api\/fields\/.*\.php    ignoreregex =
```

Finally just restart fail2ban using

```
service fail2ban restart
```

In case you get an error while restarting, make sure you don’t have the jail.*local* file, in case it is present make it blank.

6. Setting Up Backup Strategy

7. Quickly Creating Development Environment