Specifications for an Ansible LAMP tools for AGENCE 148

Summary

We have Wordpress website, Prestashop Website for client. In other words PHP MYSQL APACHE projects.
Today we install new machine manually and each time we need to update the machine (not the website) we do this manually.
The problem is that we have around 12 servers with different configuration and we would like to make it simplier.

We think that with a ansible script and a well documented procedure we could have a great solution to :

- Install a new machine
- Update a server

Constraints

We have some site that will need access to a git repository in order to deploy code.
We would like a high security mode.
We have to find a way to easely tweak apache vhost for each project
We have to find a way to make it simple to have a main base and a specific configuration for each server (vhosts, https, apaches modules enabled …)
It should work on Vagrant for Test

Suggested spécifications that need to be challenged

You will find bellow suggested spécification that can be challenged.
Please give us feedback to add more elements or suggest changes

Main part

Debian 8 jessie
English us_US
Timezone EUROPE/PARIS
Apache 2.4
Apache MPM event or MPM worker

- *It need to be tweak depending on server performance … we need a method and help for this. This should be in the documentation*

also check http://httpd.apache.org/docs/2.0/misc/perf-tuning.html

Apache specific modules

- Mod_evasive
  need to be tweeked

```
nano /etc/apache2/mods-available/mod-evasive.conf
## <IfModule mod_evasive20.c>
##     DOSHashTableSize    3097
##     DOSPageCount        2
##     DOSSiteCount        50
##     DOSPageInterval     1
##     DOSSiteInterval     1
##     DOSBlockingPeriod   10
##     DOSLogDir           "/var/lock/mod_evasive"
##     DOSEmailNotify      mathias@148.fr
## </IfModule>
```

- Auth : we need to place a simple .htpasswd when we need to
- Mod_security with rules : https://modsecurity.org/rules.html
- http2
- fast_cgi
- PageSpeed Module :
  https://developers.google.com/speed/pagespeed/module/download

Mysql

- Secure installation
- Change default port ?
- Optimise ?
- *Simple method to create database / user / rights / password*

php-fpm

- 5.6
  we need to be able to manage php.ini well documented in the procedure
  fpm need to be tweek for performance and prevent max process reached

- 7
  we need to be able to manage php.ini well documented in the procedure
  fpm need to be tweek for performance and prevent max process reached

Logs

- we should have a way to access or track log easely (php/mysql/apache)
- is there any tools ?
- we should have %D on log to see response time (is this a performance problem)

php composer

phpmyadmin

it need to be secured by https / by htaccess auth

let's encrypt : cerbot

it need to be customise to be simple to work with vhost configuration

sslmate

make server to be able to send emails

i need advice to best practice for that to avoid be in spam

i need a way to track sent message from the machine

rsnapshot or a backup strategy

we need backup of database on data

nagios client

it should work with our nagios server to track

- apache
- ping
- php
- mysql
- disk space / ram / cpu / inode
- backups

Security :
No root access from ssh (sudoer)
No ssh access with password
Change default ssh port
Use fail to ban
Create a deploy user that has www-data group access for /var/www folder were the web files will be
Change default firewall to more secure
Block all in/out authorise these :

- 80 in/out
- 443 in/out
- 25/587/2525/4065/25025 out for sending email ➔ need advice for this
- ssh new port in
- 9418 in/out ➔ git port
- nagios port ??

have a strong security policies on file right on htdocs :

- shall we git the wall repo to track changed files ?
- regarding Wordpress i did a setup that need to be challenged :

```
###   root
###   webmaster (sudo su ok)
###   backup (for rsnapshot only .. accept only rsync command)
###   publisher (owner of data)
###   www-data
```

```
###
###   GROUP
###   www-data
###   www-pub
###   admins

## https://blog.sucuri.net/2012/07/wordpress-and-server-hardening-taking-
security-to-another-level.html
## https://www.digitalocean.com/community/tutorials/how-to-configure-
secure-updates-and-installations-in-wordpress-on-ubuntu
## http://blog.johnpray.net/2013/02/wordpress-security-quickly-set-the-
proper-file-and-folder-permissions/
## http://serverfault.com/questions/6895/whats-the-best-way-of-handling-
permissions-for-apache2s-user-www-data-in-var

adduser webmaster
adduser publisher
groupadd www-pub

usermod -a -G www-pub webmaster
usermod -a -G www-pub publisher
usermod -a -G www-pub root
chown -R root:www-pub /var/www
mkdir /var/www/mysite.net/wp-content/uploads
chown -R www-data:www-data /var/www/mysite.net/wp-content/uploads
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} +
find /var/www -type f -exec chmod 0664 {} +

cd /var/www/
mkdir mysite.net
cd mysite.net/


---------------------------------------------------------------------
TMP - FOR UPDATES PROCEDURE
---------------------------------------------------------------------
echo "chown -R www-data:www-data /var/www/mysite.net" >> /root/unsecure-
wp.sh
echo "chmod 2775 /var/www/mysite.net" >> /root/unsecure-wp.sh
echo "find /var/www/mysite.net -type d -exec chmod 2775 {} +" >>
/root/unsecure-wp.sh
echo "find /var/www/mysite.net -type f -exec chmod 0664 {} +" >>
/root/unsecure-wp.sh

echo "chown -R root:www-pub /var/www/mysite.net" >> /root/secure-wp.sh
echo "chown -R www-data:www-data /var/www/mysite.net/wp-content/uploads" >>
/root/secure-wp.sh
echo "chmod 2775 /var/www/mysite.net" >> /root/secure-wp.sh
echo "find /var/www/mysite.net -type d -exec chmod 2775 {} +" >>
/root/secure-wp.sh
echo "find /var/www/mysite.net -type f -exec chmod 0664 {} +" >>
/root/secure-wp.sh


chmod 744 secure-wp.sh
chmod 744 unsecure-wp.sh
```

Others :
Filesystem : what filesystem should be used for best performance for webserver.
Use Nagios to check this :

- http://stackoverflow.com/questions/22906040/grep-whole-server-for-shell-hacks-malware

read and appy advices from : https://www.debian.org/doc/manuals/securing-debian-howto/index.en.html

sometime we will use VPS sometime VAGRANT sometime Real Server ➔ is there, shall we have a different filesystem ? Swap mode ? …

Ressources to read

https://www.debian.org/doc/manuals/securing-debian-howto/index.en.html
http://crunchbang.org/forums/viewtopic.php?id=24722
http://serverfault.com/questions/383526/how-do-i-select-which-apache-mpm-to-use
http://unix.stackexchange.com/questions/30879/what-user-should-apache-and-php-be-running-as-what-permissions-should-var-www
http://serverfault.com/questions/402186/is-it-secure-to-grant-apache-user-ownership-of-directories-files-for-wordpress
https://blog.sucuri.net/2012/07/wordpress-and-server-hardening-taking-security-to-another-level.html
http://blog.johnpray.net/2013/02/wordpress-security-quickly-set-the-proper-file-and-folder-permissions/
http://serverfault.com/questions/6895/whats-the-best-way-of-handling-permissions-for-apache2s-user-www-data-in-var