FreeBSD Administration - Support #666

Hardening Nginx & PHP-FPM on FreeBSD

09/30/2015 04:18 PM - Daniel Curtis

Status:	Closed	**Start date:**	09/30/2015
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Web Server	**Estimated time:**	2.00 hours
Target version:	FreeBSD 9	**Spent time:**	2.50 hours

Description

These are a few tips for hardening nginx on FreeBSD.

Nginx

Disable nginx server_tokens

- Edit the main nginx config file:

```
vi /usr/local/etc/nginx/nginx.conf
```

  - And add the following line inside the http block to disable nginx server_tokens:

```
server_tokens off;
```

Configure an X-Frame-Options header

- Edit the main nginx config file:

```
vi /usr/local/etc/nginx/nginx.conf
```

  - And add the following line inside the http block to configure an X-Frame-Options header:

```
add_header X-Frame-Options "SAMEORIGIN";
```

Redirect to HTTPS

- Edit the nginx server block:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

  - And add the following inside the server block to redirect all regular HTTP requests to HTTPS:

```
# Redirect to HTTPS
if ($scheme = http) {
    return 301 https://$server_name$request_uri;
}
```

Disable unwanted HTTP methods

- Edit the nginx server block:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

- And add the following inside the server block to disable unwanted HTTP methods:

```
# Disable unwanted HTTP methods
if ($request_method !~ ^(GET|HEAD|POST)$ ) {
    return 444;
}
```

- (Optional) For websites that use WebDAV, like owncloud, additional requests methods can be included.:

```
# Disable unwanted HTTP methods
if ($request_method !~ ^(GET|HEAD|POST|PUT|DELETE|REPORT|PROPFIND)$ ) {
    return 444;
}
```

Limit the maximum upload file size

- Edit the nginx server block:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

- And add the following inside the server block to limit the maximum upload file size:

```
client_max_body_size 20m;
client_body_buffer_size 128k;
```

Deny access to hidden files

- Edit the nginx server block:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

- And add the following inside the server block to deny access to hidden files:

```
location ~ /\. {
    access_log off;
    log_not_found off;
    deny all;
}
```

PHP-FPM

- Edit the main php-fpm config file:

```
vi /usr/local/etc/php-fpm.conf
```

- And add the following:

```
include=/usr/local/etc/fpm.d/*.conf
```

- Create the php-fpm directory to store each individual site php-fpm configs:

```
mkdir /usr/local/etc/fpm.d
```

Define a pool for www.example.com

- Create the www.example.com website user:

```
pw add user -n wwwexamplecom -m -s /usr/sbin/nologin -c "www.example.com"
```

- Define a new pool for www.example.com:

```
vi /usr/local/etc/fpm.d/www.example.com.conf
```

  - And add the following

```
[www.example.com]
listen = /var/run/www.example.com-php-fpm.sock
listen.owner = wwwexamplecom
listen.group = www
listen.mode = 0660
user = wwwexamplecom
group = www
pm = dynamic
pm.max_children = 50
pm.start_servers = 20
pm.min_spare_servers = 5
pm.max_spare_servers = 35
```

- Edit the server config for www.example.com:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

  - And modify the PHP location handler:

```
server {
  location ~ \.php$ {
    try_files $uri =404;
    fastcgi_pass unix:/var/run/php5-fpm/www.example.com-php-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    fastcgi_param PATH_INFO $fastcgi_script_name;
    include /etc/nginx/fastcgi_params;
  }
}
```

Define a pool for mail.example.com

- Create the **mail.example.com** website user:

```
pw add user -n mailexamplecom -m -s /usr/sbin/nologin -c "mail.example.com"
```

- Define a new pool for **mail.example.com**:

```
vi /usr/local/etc/fpm.d/mail.example.com.conf
```

- And add the following

```
[mail.example.com]
listen = /var/run/mail.example.com-php-fpm.sock
listen.owner = mailexamplecom
listen.group = www
listen.mode = 0660
user = mailexamplecom
group = www
pm = dynamic
pm.max_children = 50
pm.start_servers = 20
pm.min_spare_servers = 5
pm.max_spare_servers = 35
```

- Edit the server config for **mail.example.com**:

```
vi /usr/local/etc/nginx/conf.d/mail.example.com.conf
```

- And modify the PHP location handler:

```
server {
  location ~ \.php$ {
    try_files $uri =404;
    fastcgi_pass unix:/var/run/php5-fpm/mail.example.com-php-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    fastcgi_param PATH_INFO $fastcgi_script_name;
    include /etc/nginx/fastcgi_params;
  }
}
```

Resources

- https://www.howtoforge.com/php-fpm-nginx-security-in-shared-hosting-environments-debian-ubuntu
- http://www.if-not-true-then-false.com/2011/nginx-and-php-fpm-configuration-and-optimizing-tips-and-tricks/
- https://www.acunetix.com/blog/articles/nginx-server-security-hardening-configuration-1/
- https://www.acunetix.com/blog/articles/nginx-security-hardening-configuration-2/
- http://sabre.io/dav/building-a-caldav-client/

History

#1 - 09/30/2015 05:32 PM - Daniel Curtis

- Description updated

- Status changed from New to In Progress

- % Done changed from 0 to 50

#2 - 09/30/2015 05:33 PM - Daniel Curtis

- Description updated

- % Done changed from 50 to 70

#3 - 10/04/2015 02:51 PM - Daniel Curtis

- Description updated

#4 - 10/04/2015 03:44 PM - Daniel Curtis

- Description updated

- % Done changed from 70 to 80

#5 - 10/04/2015 03:51 PM - Daniel Curtis

- Description updated

#6 - 10/04/2015 04:30 PM - Daniel Curtis

- Status changed from In Progress to Resolved

- % Done changed from 80 to 100

#7 - 11/27/2015 03:56 PM - Daniel Curtis

- Status changed from Resolved to Closed