Nginx Tricks for PHP Developers

Ilia Alshanetsky
@iliaa
http://ilia.ws

- Core PHP Developer
- CTO @ Gubagoo Inc.
  (We are hiring!!)
- Security & Scalability aficionado ;-)

Brief History

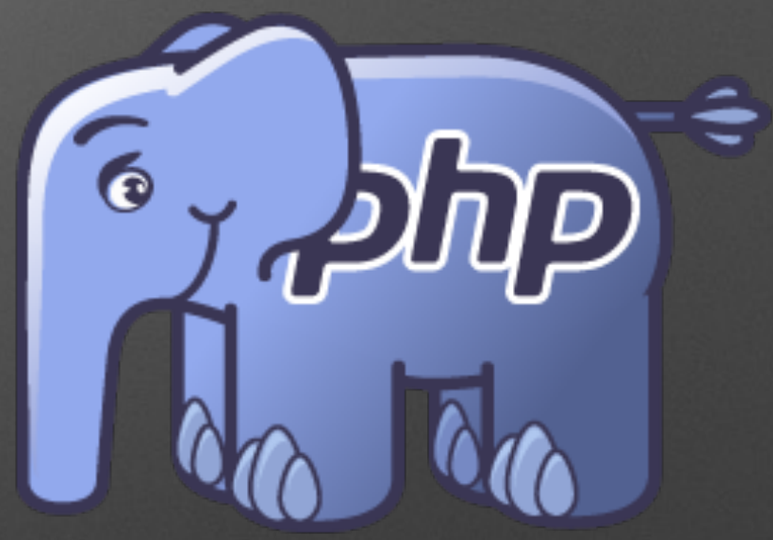
- Developed in 2002 at rambler.ru by Igor Sysoev to solve c10k problem
- First public release in the end of 2006
- In 2015 powers 15.5% of all sites, 23% of busiest sites

Party Tricks

- High Performance Event based HTTP Server
  - 10k+ connections with very low memory footprint
- Reverse Proxy with Caching
- Load Balancer
- Mail Proxy
- Any many many more…

The Basics

+



Base Config

```
location ~* \.php$ {

}
```

Initial File

```
location ~* \.php$ {
    fastcgi_index   index.php;



}
```

PHP-FPM Socket Location

```
location ~* \.php$ {
    fastcgi_index   index.php;
    fastcgi_pass    unix:/var/run/php5-fpm.sock;


}
```

Initialize $_SERVER Values

```
location ~* \.php$ {
    fastcgi_index   index.php;
    fastcgi_pass    unix:/var/run/php5-fpm.sock;
    include         fastcgi_params;
    fastcgi_param   SCRIPT_FILENAME $document_root$fastcgi_script_name;

}
```

Files to Try, then 404

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

Connection Pools

PHP-FPM Pools

```
upstream php_fpm_cluster {
  server 192.168.1.10:9000;
  server 192.168.1.11:9000;
  server 192.168.1.12:9000;
}
```

Cluster Name

```
location ~* \.php$ {
    fastcgi_index   index.php;
    fastcgi_pass    @php_fpm_cluster;
    include         fastcgi_params;
    fastcgi_param   SCRIPT_FILENAME $document_root$fastcgi_script_name;
    try_files       $uri =404;
}
```

Pool Connection Persistence

```
upstream php_fpm_cluster {
 ip_hash;
 server 192.168.1.10:9000;
 server 192.168.1.11:9000;
 server 192.168.1.12:9000;
}
```

Based on Client IP Address

```
upstream php_fpm_cluster {
 hash $request_uri consistent;
 server 192.168.1.10:9000;
 server 192.168.1.11:9000;
 server 192.168.1.12:9000;
}
```

Based on request URI with Ketama consistent hashing

```
upstream php_fpm_cluster {
 least_conn;
 server 192.168.1.10:9000;
 server 192.168.1.11:9000;
}
```

Least busy server based on connection count

Cookie Based Persistence

```
upstream php_fpm_cluster {
 server 192.168.1.10:9000;
 server 192.168.1.11:9000;
 server 192.168.1.12:9000;

 sticky cookie __server__ expires=1h domain=.ilia.ws httponly secure path=/;
}
```

Cookie Name

Expiry Time

Domain

Flags
(1.7.11+)

Path

Managing Pool Failures

```
upstream php_fpm_cluster {
 server 192.168.1.10:9000
     max_fails=10 fail_timeout=60s;

 server 192.168.1.11:9000
     max_fails=5; default 10s failure interval


 server 192.168.1.12:9000 backup;
}
```

Failure interval & hold

Maximum number of failures

Backup server in case primaries have failed

Managing Pool Failures

```
upstream php_fpm_cluster {
 server 192.168.1.10:9000
     max_fails=10 fail_timeout=60s;

 server 192.168.1.11:9000
     max_fails=5 slow_start=60s max_conns=150;

 server 192.168.1.12:9000 backup;
}
```

Recovery time after return to healthy state

Active connection limit

Managing Pool Priorities

```
upstream php_fpm_cluster {
 server 192.168.1.10:9000 weight=7;
 server 192.168.1.11:9000 weight=2;
 server 192.168.1.12:9000;
}
```

7 requests (70%)

2 requests (20%)

1 request (10%)

Default weight of 1

Connection Persistence

```
upstream php_fpm_cluster {
 server 192.168.1.10:9000 weight=7;
 server 192.168.1.11:9000 weight=2;
 server 192.168.1.12:9000;

 keepalive 25;
}

location ~* \.php$ {
    fastcgi_index   index.php;
    fastcgi_keep_conn on;
    fastcgi_pass    @php_fpm_cluster;
    include         fastcgi_params;
    fastcgi_param   SCRIPT_FILENAME $document_root$fastcgi_script_name;
    try_files       $uri =404;
}
```


NGINX
+
SSL

HTTP > HTTPs

```
server {
 listen 80;
 service_name domain.tld;
 rewrite ^ https://domain.tld$request_uri permanent;
}
```

And now without rewrite!

```
server {
 listen 80;
 service_name domain.tld;
 return 301 https://domain.tld$request_uri;
}
```

Basic SSL Config

```
server {
  listen 443 ssl spdy;
  service_name domain.tld;

  ssl_certificate /etc/nginx/ssl/domain.pem;
  ssl_certificate_key /etc/nginx/ssl/domain.key;

  add_header Alternate-Protocol 443:npn-spdy/3;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";
}
```

Necessary header to tell browsers about SPDY support

Tell browsers to only use HTTPs for this site

SSL Protocols & Ciphers

```
server {
  listen 443 ssl spdy;
  service_name domain.tld;

  ssl_certificate /etc/nginx/ssl/domain.pem;
  ssl_certificate_key /etc/nginx/ssl/domain.key;

  add_header Alternate-Protocol 443:npn-spdy/3;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";

  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_prefer_server_ciphers on;
  ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH
+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-
AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-
SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-
DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA';
}
```

SSL Session Management

```
server {
  listen 443 ssl spdy;
  service_name domain.tld;

  ssl_certificate /etc/nginx/ssl/domain.pem;
  ssl_certificate_key /etc/nginx/ssl/domain.key;

  add_header Alternate-Protocol 443:npn-spdy/3;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";

  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_prefer_server_ciphers on;
  ssl_ciphers …;

  ssl_session_timeout 30m;
  ssl_session_cache shared:SSL:50m;
}
```

Use your typical session length

~200,000 sessions

Forward Secrecy & Diffie Hellman Ephemeral Parameters

- A session specific secret key used to encrypt communication
- Session specific key is never part of client <> server communication, thus is secure from MITM attack
- Past communication cannot be decrypted even if server's private key is compromised

1 Alice and Bob agree to use a modulus $p = 23$ and base $g = 5$

2 Alice chooses a secret integer ***a*** = **6**, then sends Bob $A = g^a \bmod p$
- $A = 5^6 \bmod 23 = 8$

3 Bob chooses a secret integer ***b*** = **15**, then sends Alice $B = g^b \bmod p$
- $B = 5^{15} \bmod 23 = 19$

4 Alice computes ***s*** = $B^a \bmod p$
- ***s*** = $19^6 \bmod 23$ = **2**

5 Bob computes ***s*** = $A^b \bmod p$
- ***s*** = $8^{15} \bmod 23$ = **2**

6 Alice and Bob now share a secret (the number **2**).

https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

Forward Secrecy & Diffie Hellman Ephemeral Parameters

Step #1 - Generate strong DHE parameter

```
openssl dhparam -out /etc/nginx/ssl/dhparam.pem 2048
```

Step #2 - Add to SSL Config

```
server {
 # other ssl config options

 ssl_dhparam /etc/nginx/ssl/dhparam.pem;
}
```

Step #3 - Have a beer ;=)

OCSP Stapling

```
server {
 # other ssl config options
 ssl_stapling on;
 ssl_stapling_verify on;

 resolver 8.8.8.8 8.8.4.4 valid=300s;
 resolver_timeout 5s;
}
```

Enable & Verify

DNS settings for resolving your domains

Does it work?

```
openssl s_client -connect domain.tld:443 -tls1 -tlsextdebug -status
```

```
OCSP response:
======================================
OCSP Response Data:
    OCSP Response Status: successful (0x0)
   Response Type: Basic OCSP Response
   Version: 1 (0x0)
   Responder Id: 5168FF90AF0207753CCCD9656462A212B859723B
   Produced At: Oct  7 12:33:00 2015 GMT
   Responses:
   Certificate ID:
     Hash Algorithm: sha1
     Issuer Name Hash: CF26F518FAC97E8F8CB342E01C2F6A109E8E5F0A
     Issuer Key Hash: 5168FF90AF0207753CCCD9656462A212B859723B
     Serial Number: 0D08CDC290EBA038ED8B21E77B94E506
    Cert Status: good
   This Update: Oct  7 12:33:00 2015 GMT
   Next Update: Oct 14 11:48:00 2015 GMT
```

```
server {
  listen 443 ssl spdy;
  service_name domain.tld;

  ssl_certificate /etc/nginx/ssl/domain.pem;
  ssl_certificate_key /etc/nginx/ssl/domain.key;

  add_header Alternate-Protocol 443:npn-spdy/3;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";

  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_prefer_server_ciphers on;
  ssl_ciphers ‘…’;

  ssl_session_timeout 30m;
  ssl_session_cache shared:SSL:50m;

  ssl_dhparam /etc/nginx/ssl/dhparam.pem;

  ssl_stapling on;
  ssl_stapling_verify on;
  resolver 8.8.8.8 8.8.4.4 valid=300s;
  resolver_timeout 5s;
}
```

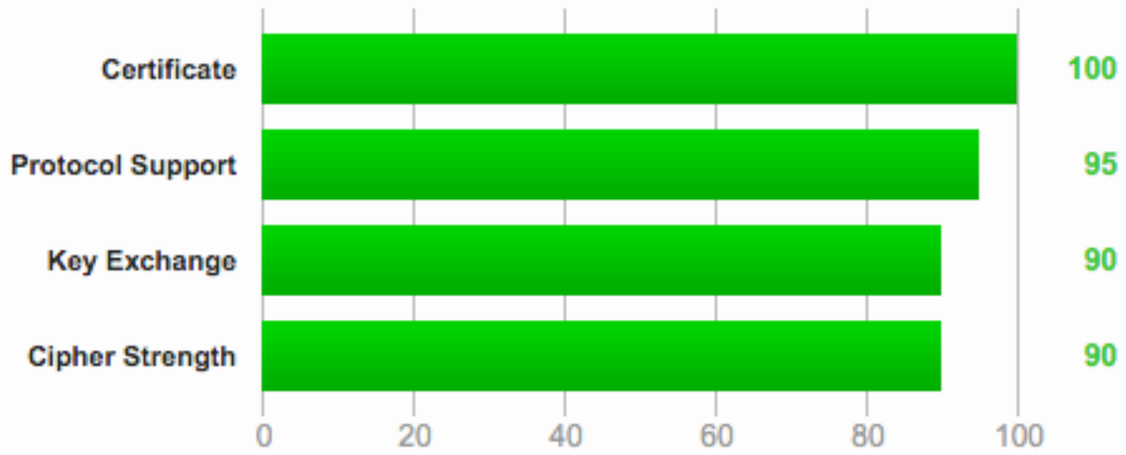
Final Config

Geek Cred!

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

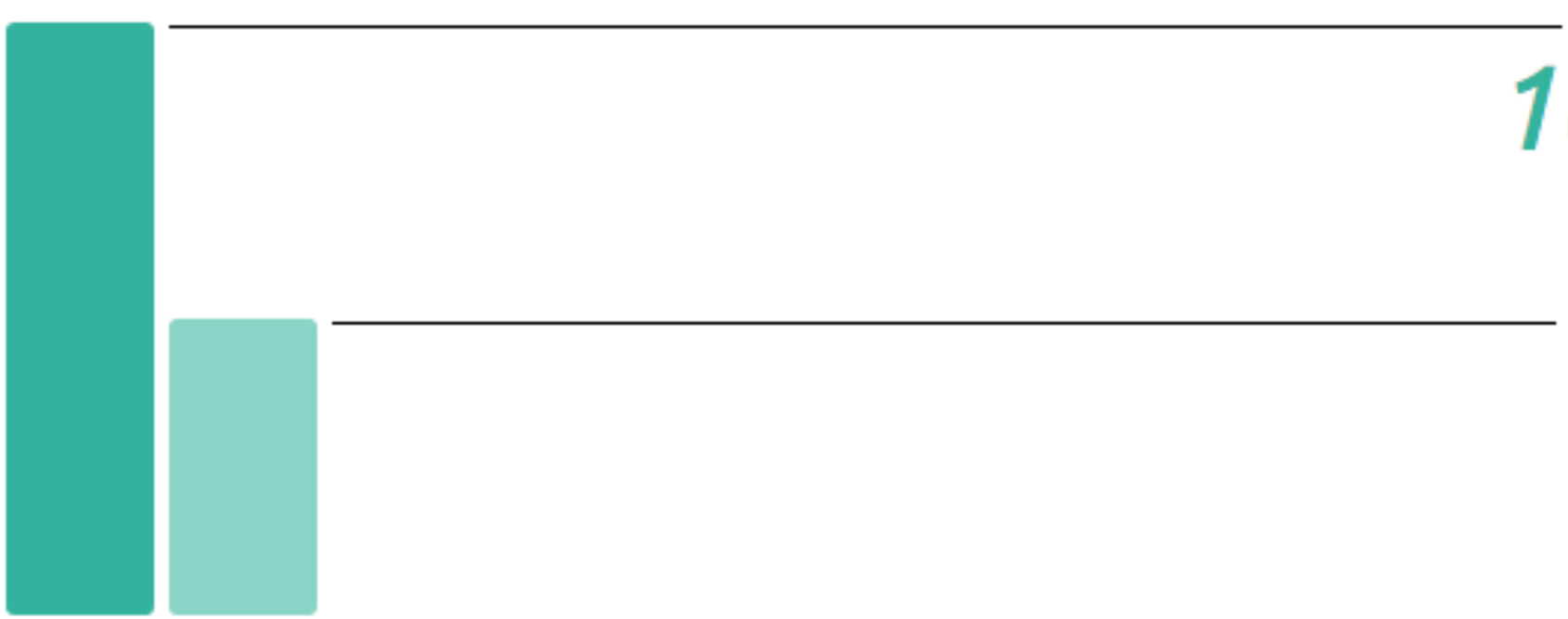
This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

ssllabs.com

You're blessed!

It's GZIP Enabled.

Was saved by compressing this page with GZIP.



Uncompressed size

106,589 bytes

Compressed size

9,550 bytes

http://checkgzipcompression.com/

Turning On

```
http {
  gzip on;
  gzip_vary on;
  gzip_proxied any;

  spdy_headers_comp 1;
}
```

enable header compression when using SPDY

Disabling Gzip

```
http {
  gzip on;
  gzip_vary on;
  gzip_disable “MSIE [4-6]\.(?!.*SV1)”;
}
```

Regex

```
http {
  gzip on;
  gzip_vary on;
  gzip_disable “msie6”;
}
```

Simpler & faster old
IE block

Disabling Gzip

```
http {
  gzip on;
  gzip_vary on;
  gzip_disable “msie6”;

  gzip_types text/plain text/css application/json
             application/javascript text/xml application/xml
             application/xml+rss text/javascript;

  gzip_http_version 1.1;
}
```

HTTP Version Controls

Mime Limits

Compression Performance

```
http {
 gzip on;
 gzip_disable “msie6”;
 gzip_vary on;
 gzip_types text/plain text/css application/json
            application/javascript text/xml application/xml
            application/xml+rss text/javascript;
 gzip_http_version 1.1;

 gzip_comp_level 1;
 gzip_min_length 1000;
 gzip_buffers 4 32k;
}
```

Don’t waste CPU time

Avoid Gzip overhead
for smaller pages

Buffer memory management

Serve Pre-Compressed Files

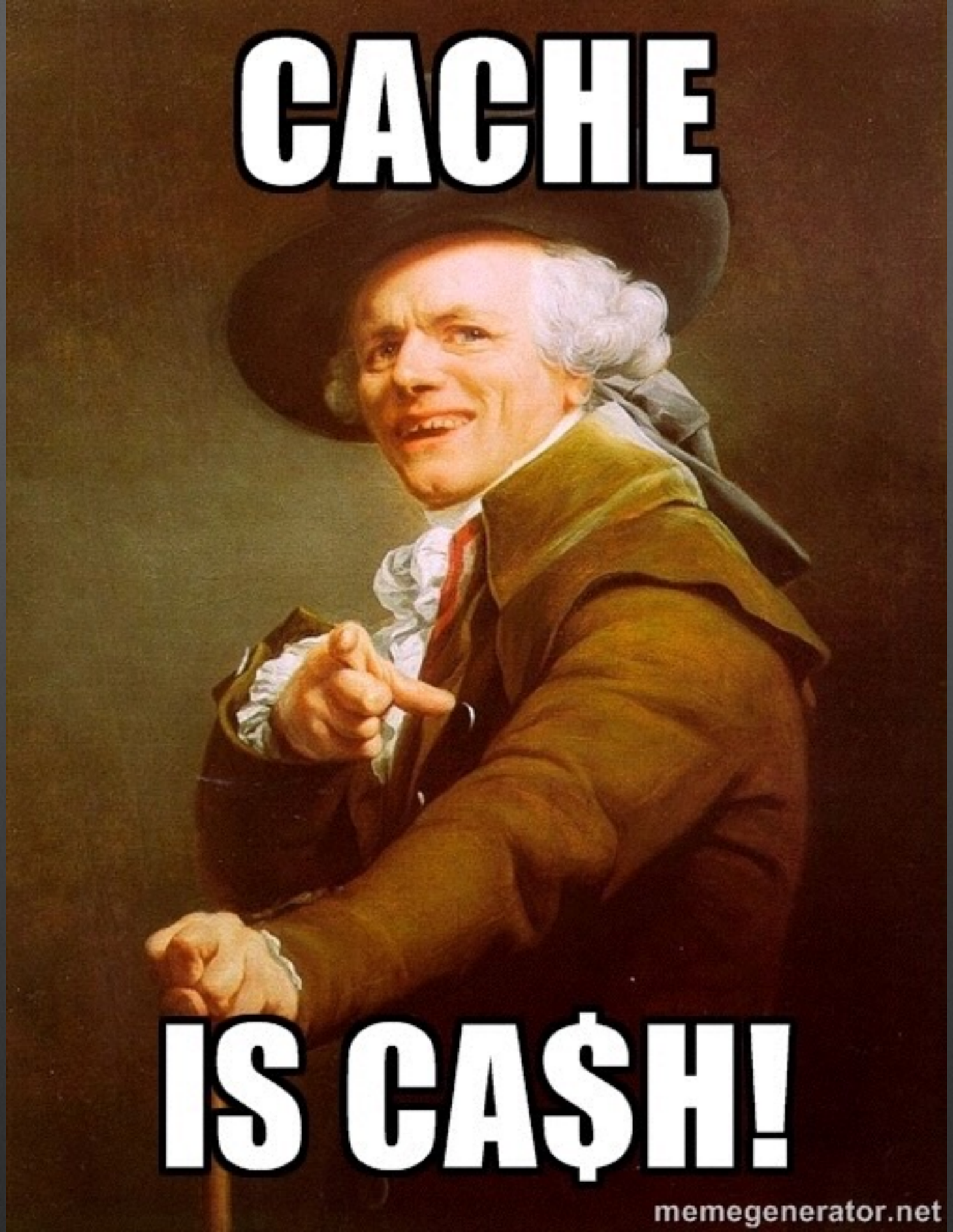
```
http {
  gzip on;
  gzip_disable “msie6”;
  gzip_vary on;
  gzip_types text/plain text/css application/json
             application/javascript text/xml application/xml
             application/xml+rss text/javascript;
  gzip_http_version 1.1;
  gzip_comp_level 1;
  gzip_min_length 1000;
  gzip_buffers 4 32k;

  gzip_static on;
}
```

If foo.js is requested and foo.js.gz is available, serve it**

Generate Compressed Cache

```
for file in
`find /web/root -name \*.css -o -name \*.js -o -name \*.html`;
   do gzip -9 -f -c $file > $file.gz;
done
```

** browser must support gzip compression


CACHE
IS CA$H!
memegenerator.net

Basic Static Cache

```
server {
 location ~* \.(jpg|jpeg|gif|png|css|js|ico|xml|html)$ {
  expires 365d;

  access_log off;

  log_not_found off;

  add_header Cache-Control "public";
 }
}
```

Disable static request logging

Dynamic Content Cache

/var/cache/phpfpmcache/67/2f/95b4fd079cff865abc1309f6dce02f67

```
http {
 fastcgi_cache_path /var/cache/phpfpmcache levels=2:2
        keys_zone=phpfpmcache:10m inactive=20m max_size=1000m;

 fastcgi_cache_key $scheme$host$request_uri;

 fastcgi_cache_lock on;

 fastcgi_cache_valid 200 302 20m;
 fastcgi_cache_valid any     60s;

 fastcgi_cache_use_stale error timeout invalid_header http_500;

 fastcgi_ignore_headers Cache-Control Expires Set-Cookie;
}
```

~80k keys

remove after 20m of idleness

Cache Size

Cache Key

One @ a time

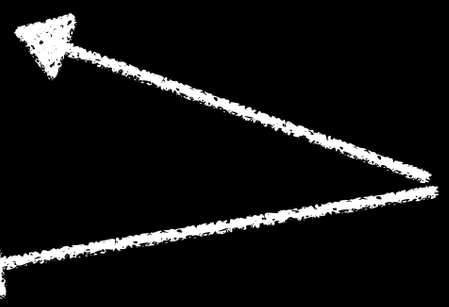
Cache duration by response code

Serve stale content on error

Ignore what PHP says ;-)

Dynamic Content Cache

```
http {
  [ … ]
  server {
    set $skip_cache 0;

    if ($request_method = POST) {
      set $skip_cache 1;
    }
    if ($request_uri ~* “(/admin/|/manage/|/secret/)”) {
      set $skip_cache 1;
    }
    if ($http_cookie ~ “app_logged_in_user”) {
      set $skip_cache 1;
    }
    if ($http_x_disable_cache) {
      set $skip_cache 1;
    }
    if ($http_x_force_cache) {
      set $skip_cache 0;
    }
  }
}
```



Allow PHP Cache Control
via
X-Disable-Cache
and
X-Force-Cache
headers

Dynamic Content Cache

```
http {
  [ … ]
  server {
    [ … ]

    location ~ "\.php$" {
      [ … ]

      add_header X-Cache-Status $upstream_cache_status;
      fastcgi_cache phpfpmcache;

      fastcgi_cache_bypass $skip_cache;
      fastcgi_no_cache $skip_cache;
    }
  }
}
```

Expose cache state

Cache pool reference

Disable cache when…

Performance Tuning

General Performance Settings

```
worker_processes 4; # one per CPU core (grep ^processor /proc/cpuinfo | wc -l)

worker_rlimit_nofile 40000; # max number of open files

pcre_jit on; # speed up regex expression processing

events {
 use epoll; # for BSD OSes use queue

 worker_connections 1024; # 4 * 1024 = 4096 connections

 multi_accept on; # accept as many connections as possible
}
```

General Performance Settings

```
http {
 sendfile            on;
 tcp_nopush          on;
 tcp_nodelay         on;


 keepalive_timeout   30;
 keepalive_requests  10000;
}
```

Use faster kernel mechanism to transmit files

KeepAlive limits to prevent resource exhaustion

Cache FD, and commonly used files

Max # of elements in cache,
that expire after 30s of inactivity

```
server {
 open_file_cache          max=10000 inactive=30s;

 open_file_cache_valid    2m;   <-- Cache “valid” duration

 open_file_cache_min_uses 2;    <-- Min uses to be considered “active”

 open_file_cache_errors   on;   <-- Cache Errors “file not found”
}
```

Buffers

```
server {
 client_body_buffer_size      16k;   # typical request body size
 client_header_buffer_size    2k;    # request header buffer
 client_max_body_size         10m;   # maximum request size
 large_client_header_buffers  3 4k; # big header buffers
}
```

```
location ~ .php$ {
   fastcgi_buffer_size          128k;    # ~ avg. PHP page size
   fastcgi_buffers              256 32k; # for larger pages
   fastcgi_busy_buffers_size    256k;    # client not ready buffer
   fastcgi_temp_file_write_size 256k;    # write to disk blocks
}
```

Timeouts

```
server {
  reset_timedout_connection on;

  client_body_timeout 10s;
  client_header_timeout 10s;

  send_timeout 5s;
}
```

Drop timeout connections

# of seconds before sending to 408 to client

# of seconds before considering client “gone” during output transmission

GIF Beacon

```
location = /beacon {
    empty_gif;
}
```

Serves a 1x1 transparent gif from memory

Information Logs

Error Logging

```
error_log /var/log/nginx/errors.log error
```


```
emerg:   Emergency situations where the system is in an unusable state
alert:   Severe situation where action is needed promptly
crit:    Important problems that need to be addressed
error:   An Error has occurred. Something was unsuccessful
warn:    Something out of the ordinary happened, but not a cause for concern
notice:  Something normal, but worth noting has happened
info:    An informational message that might be nice to know
debug:   Debugging information that can be useful to pinpoint where a problem is occurring
```

Access Logging

```
access_log /var/log/nginx/access.log verbose buffer=64k flush=5m
```

Could be stderr

Write in 64k chunks or every 5mins, which ever is sooner

Could be syslog

```
syslog:log.server,facility=local7,tag=nginx,severity=info
```

What to Log?

```
log_format  verbose  'your format string';
```

PARAMETER	WHAT & WHY
$remote_addr	IP Address of the User
$host	Host request *(one log file per server)*
$body_bytes_sent	Size of the response body w/o header
$bytes_sent	Total bytes sent
$time_local	Local time in the Common Log Format
$status	Response status
$request_length	Request length
$request_time	Request processing time
$http_referer	Referrer
$http_user_agent	User agent
$request	Full request line *(GET /index.php HTTP/1.1)*
$gzip_ratio	Gzip Compression Ratio

Live Monitoring

```
location /nginx_status {
  stub_status on;
  access_log off;
  allow your-ip;
  deny all;
}
```

```
Active connections: 291
server accepts   handled   requests
       16630948 16630948 31070465
Reading: 6 Writing: 179 Waiting: 106
```

KEEP
CALM
AND
START
DEBUGGING

Debugging

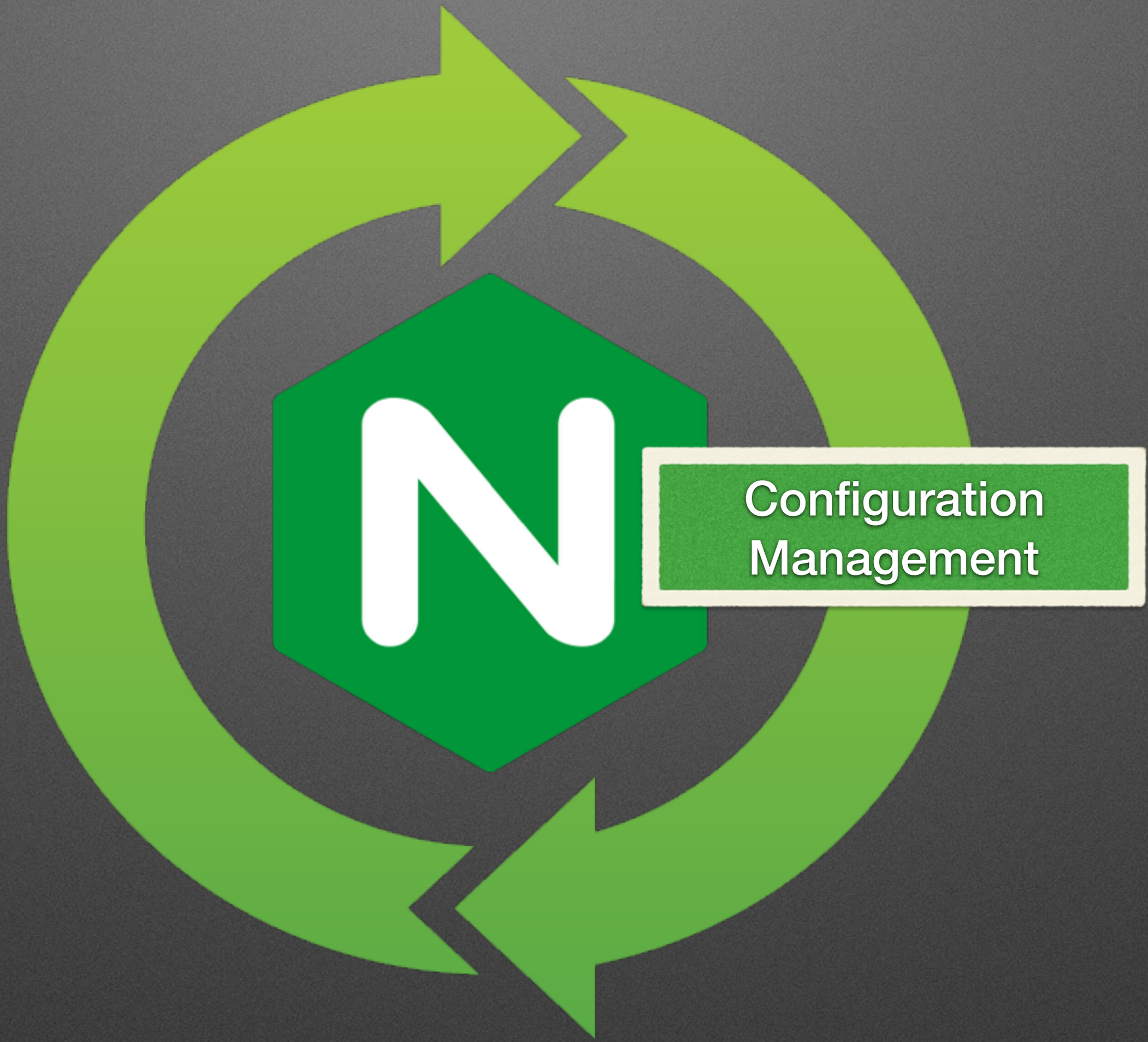
```
error_log /var/log/nginx/errors.log debug
```

requires
--with-debug

```
events {
  debug_connection 192.168.0.0/24;
  debug_connection 2001:0db8::/32;
}
```

```
server {
  rewrite_log on;
  error_log /var/log/nginx/errors.log notice;
}
```

Do configtest !


Configuration
Management

kill -HUP

- Configuration Reload
- Start new workers based on new config
- Allow old workers to complete work and gracefully exit

kill -USR1

- Rotate Log Files

kill -USR2

- No downtime executable upgrade

```
kill -USR2 `cat /var/run/nginx.pid`
```

```
/var/run/nginx.pid >> /var/run/nginx.pid.oldbin
```

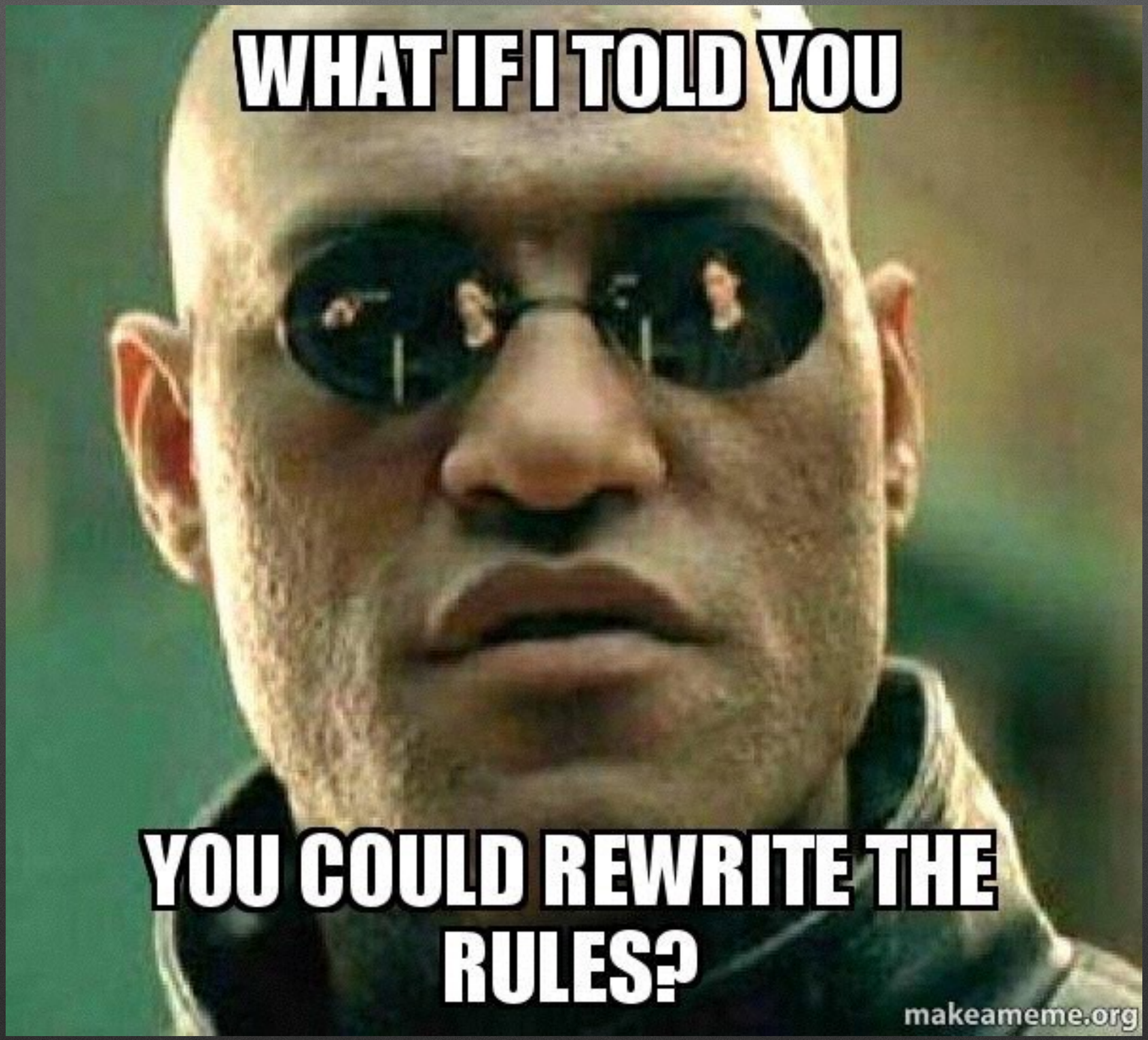
```
: PID   PPID USER     %CPU   VSZ WCHAN  COMMAND
33126      1 root      0.0  1164 pause  nginx: master process nginx
36264  33126 root      0.0  1148 pause  nginx: master process nginx
```

Failure

Success

```
kill -WINCH `cat /var/run/nginx.pid.oldbin`
```

```
kill -HUP  `cat /var/run/nginx.pid.oldbin`
kill -QUIT `cat /var/run/nginx.pid`
kill -TERM `cat /var/run/nginx.pid`
```


WHAT IF I TOLD YOU
YOU COULD REWRITE THE RULES?
makeameme.org

Rewrite Module

- PCRE based regular expression
- Basis of nearly all conditional expressions
- Access to virtually entire set of Nginx variables
- Allows creation of own variables via **set**

Rewrite in Practice

```
if ($request_filename ~* \.(htaccess|phps|inc)$) {
   return 401;
}
```

```
location ~ \.(htaccess|phps|inc)$ {
   return 401;
}
```

Faster

```
location /static/ {
   rewrite ^(/static/)[^/]+/(.*)$ $1/$2 break;
   return 403;
}
```

No other GET args

```
rewrite ^/users/([0-9]+)$ /user.php?id=$1? last;
```

Finish rewrite rules

Variables in Action

```
server {
   server_name ~ ^(?:www\.)?(?<domain>.+)$;

   location / {
      if ($domain !~ '\.\.') {
         root   /sites/$domain;
      }
   }
}
```

```
geo $slow {
  default     0;

  8.8.0.0/24 1;
}

if ($slow) {
    limit_rate 10k;
}
```

Map Directive

```
map $geoip_country_code $closest_server {

  default www.acme.co;

  CA      ca.acme.co;
  DE      de.acme.co;
  CN      cn.acme.co;
  AU      au.acme.co;
}
```

Securing Nginx

Mod Security

```
location ~* \.php$ {
    ModSecurityEnabled on;
    ModSecurityConfig  modsecurity.conf;
    proxy_read_timeout 180s;

    fastcgi_index   index.php;
    fastcgi_pass    unix:/var/run/php5-fpm.sock;
    include         fastcgi_params;
    fastcgi_param   SCRIPT_FILENAME $document_root$fastcgi_script_name;
    try_files       $uri =404;
}
```

Prior to ModSecurity 2.7.2, ModSecurityPass was needed

```
location ~* \.php$ {
    ModSecurityEnabled on;
    ModSecurityConfig  modsecurity.conf;
    ModSecurityPass    @backend;
}
location @backend {
    fastcgi_index   index.php;
    fastcgi_pass    unix:/var/run/php5-fpm.sock;
    include         fastcgi_params;
    fastcgi_param   SCRIPT_FILENAME $document_root$fastcgi_script_name;
    try_files       $uri =404;
}
```

NAXSI - Nginx Anti XSS & SQL Injection

```
http {
    include /etc/nginx/naxsi_core.rules;
}
```

```
server {
   location ~* \.php$ {
      include /etc/nginx/naxsi.rules;
   }

   location /RequestDenied {
      return 444;
   }
}
```

Special code that just drops connection

```
LearningMode; #Enables learning mode
SecRulesEnabled;

DeniedUrl "/RequestDenied";
## check rules
CheckRule "$SQL >= 8" BLOCK;
CheckRule "$RFI >= 8" BLOCK;
CheckRule "$TRAVERSAL >= 4" BLOCK;
CheckRule "$EVADE >= 4" BLOCK;
CheckRule "$XSS >= 8" BLOCK;
```

https://github.com/nbs-system/naxsi

DDOS Protection

- Most DDOS bots are pretty limited in function and can be identified by their lack of support for:
  - Cookies
  - Redirect Support
  - JavaScript Capability
- The test_cookie module can detect this and block access based on lack of fundamental features

https://github.com/kyprizel/testcookie-nginx-module

Throttle Down Offenders

```
http {
   limit_conn_zone $binary_remote_addr zone=slow1:10m;
   limit_req_zone  $binary_remote_addr zone=slow2:10m rate=1r/s;

   server {
      location /login/ {
         limit_conn slow1 1;
      }

      location /search/ {
         limit_req zone=slow2 burst=5;
      }
   }
}
```

General Security Settings

```
disable_symlinks if_not_owner;


server_tokens off;


if ($request_method !~ ^(GET|HEAD|POST)$) {
   return 444;
}

add_header X-Frame-Options "SAMEORIGIN";

add_header X-XSS-Protection "1; mode=block";

add_header X-Content-Type-Options "nosniff";
```

Prevent clickjacking

Enable XSS filer protection in browser

Don't guess mime-type

https://www.owasp.org/index.php/List_of_useful_HTTP_headers

THANK YOU FOR LISTENING

Ilia Alshanetsky

http://ilia.ws

@iliaa