# *Nginx modsecurity*

Este documento faz a compilação do Nginx, ModSecurity.

**Autor:** Gustavo Soares <slot.mg@gmail.com>

## Instalando dependências.

```
root@debian:~# apt-get install git build-essential libpcre3 libpcre3-dev libssl-dev libtool  autoconf
apache2-prefork-dev libxml2-dev libcurl4-openssl-dev
```

## Download e compilação do ModSecurity.

```
root@debian:~# cd /usr/src
root@debian:/usr/src# git clone https://github.com/SpiderLabs/ModSecurity.git modsecurity
root@debian:/usr/src# cd modsecurity/
root@debian:/usr/src/modsecurity# ./autogen.sh
root@debian:/usr/src/modsecurity# ./configure --enable-standalone-module --disable-mlogc
root@debian:/usr/src/modsecurity# make
```

## Download e compilação do Nginx.

```
root@debian:/usr/src/modsecurity# cd /usr/src
root@debian:/usr/src# wget http://nginx.org/download/nginx-1.8.0.tar.gz
root@debian:/usr/src# tar zxf nginx-1.8.0.tar.gz
root@debian:/usr/src# cd nginx-1.8.0
root@debian:/usr/src/nginx-1.8.0# ./configure \
--prefix=/etc/nginx \
--sbin-path=/usr/sbin/nginx \
--conf-path=/etc/nginx/nginx.conf \
--error-log-path=/var/log/nginx/error.log \
--http-log-path=/var/log/nginx/access.log \
--pid-path=/var/run/nginx.pid \
--lock-path=/var/run/nginx.lock \
--http-client-body-temp-path=/var/cache/nginx/client_temp \
--http-proxy-temp-path=/var/cache/nginx/proxy_temp \
--http-fastcgi-temp-path=/var/cache/nginx/fastcgi_temp \
--http-uwsgi-temp-path=/var/cache/nginx/uwsgi_temp \
--http-scgi-temp-path=/var/cache/nginx/scgi_temp \
--user=nginx \
--group=nginx \
--with-http_ssl_module \
--with-http_realip_module \
--with-http_addition_module \
--with-http_sub_module \
--with-http_dav_module \
--with-http_flv_module \
--with-http_mp4_module \
--with-http_gunzip_module \
--with-http_gzip_static_module \
--with-http_random_index_module \
--with-http_secure_link_module \
--with-http_stub_status_module \
--with-http_auth_request_module \
--with-mail \
--with-mail_ssl_module \
--with-file-aio \
--with-http_spdy_module \
--with-ipv6 \
--with-cc-opt="-g -O2 -fstack-protector-strong -Wformat -Werror=format-security" \
--with-ld-opt="-Wl,-z,relro" \
--add-module=/usr/src/modsecurity/nginx/modsecurity

root@debian:/usr/src/nginx-1.8.0# make -j2
root@debian:/usr/src/nginx-1.8.0# make -j2 install
root@debian:/usr/src/nginx-1.8.0# mkdir -p /var/cache/nginx/client_temp
root@debian:/usr/src/nginx-1.8.0# addgroup --system nginx
root@debian:/usr/src/nginx-1.8.0# adduser --system --disabled-login --ingroup nginx --no-create-home --
home /nonexistent --gecos "nginx user" --shell /bin/false nginx
root@debian:/usr/src/nginx-1.8.0# chown -R nginx /var/cache/nginx
```

# Configurando o Nginx.

Edite o arquivo */etc/nginx/nginx.conf* e acerte o usuário do nginx na variável *user* para *www-data* e crie os arquivos abaixo com o respectivo conteúdo.

## /etc/logrotate.d/nginx

```
/var/log/nginx/*.log {
        daily
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 nginx adm
        sharedscripts
        postrotate
                [ -f /var/run/nginx.pid ] && kill -USR1 `cat /var/run/nginx.pid`
        endscript
}
```

## /etc/init.d/nginx

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          nginx
# Required-Start:    $network $remote_fs $local_fs
# Required-Stop:     $network $remote_fs $local_fs
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Stop/start nginx
### END INIT INFO

# Author: Sergey Budnevitch <sb@nginx.com>

PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC=nginx
NAME=nginx
CONFFILE=/etc/nginx/nginx.conf
DAEMON=/usr/sbin/nginx
PIDFILE=/var/run/$NAME.pid
SCRIPTNAME=/etc/init.d/$NAME
SLEEPSEC=1
UPGRADEWAITLOOPS=5

[ -x $DAEMON ] || exit 0

[ -r /etc/default/$NAME ] && . /etc/default/$NAME

DAEMON_ARGS="-c $CONFFILE $DAEMON_ARGS"

. /lib/init/vars.sh

. /lib/lsb/init-functions

do_start()
{
    start-stop-daemon --start --quiet --pidfile $PIDFILE --exec $DAEMON -- \
        $DAEMON_ARGS
    RETVAL="$?"
    return "$RETVAL"
}

do_stop()
{

    # Return
    #   0 if daemon has been stopped
    #   1 if daemon was already stopped
    #   2 if daemon could not be stopped
    #   other if a failure occurred
    start-stop-daemon --stop --quiet --oknodo --retry=TERM/30/KILL/5 --pidfile $PIDFILE
    RETVAL="$?"
    rm -f $PIDFILE
    return "$RETVAL"
}

do_reload() {
    #
    start-stop-daemon --stop --signal HUP --quiet --pidfile $PIDFILE
    RETVAL="$?"
    return "$RETVAL"
}

do_configtest() {
    if [ "$#" -ne 0 ]; then
        case "$1" in
            -q)
                FLAG=$1
                ;;
            *)
                ;;
        esac
        shift
    fi
    $DAEMON -t $FLAG -c $CONFFILE
    RETVAL="$?"
```

```
    return $RETVAL
}

do_upgrade() {
    OLDBINPIDFILE=$PIDFILE.oldbin

    do_configtest -q || return 6
    start-stop-daemon --stop --signal USR2 --quiet --pidfile $PIDFILE
    RETVAL="$?"

    for i in `/usr/bin/seq  $UPGRADEWAITLOOPS`; do
        sleep $SLEEPSEC
        if [ -f $OLDBINPIDFILE -a -f $PIDFILE ]; then
            start-stop-daemon --stop --signal QUIT --quiet --pidfile $OLDBINPIDFILE
            RETVAL="$?"
            return
        fi
    done

    echo $"Upgrade failed!"
    RETVAL=1
    return $RETVAL
}

case "$1" in
    start)
        [ "$VERBOSE" != no ] && log_daemon_msg "Starting $DESC " "$NAME"
        do_start
        case "$?" in
            0|1) [ "$VERBOSE" != no ] && log_end_msg 0 ;;
            2) [ "$VERBOSE" != no ] && log_end_msg 1 ;;
        esac
        ;;
    stop)
        [ "$VERBOSE" != no ] && log_daemon_msg "Stopping $DESC" "$NAME"
        do_stop
        case "$?" in
            0|1) [ "$VERBOSE" != no ] && log_end_msg 0 ;;
            2) [ "$VERBOSE" != no ] && log_end_msg 1 ;;
        esac
        ;;
  status)
        status_of_proc -p "$PIDFILE" "$DAEMON" "$NAME" && exit 0 || exit $?
        ;;
  configtest)
        do_configtest
        ;;
  upgrade)
        do_upgrade
        ;;
  reload|force-reload)
        log_daemon_msg "Reloading $DESC" "$NAME"
        do_reload
        log_end_msg $?
        ;;
  restart|force-reload)
        log_daemon_msg "Restarting $DESC" "$NAME"
        do_configtest -q || exit $RETVAL
        do_stop
        case "$?" in
            0|1)
                do_start
                case "$?" in
                    0) log_end_msg 0 ;;
                    1) log_end_msg 1 ;; # Old process is still running
                    *) log_end_msg 1 ;; # Failed to start
                esac
                ;;
            *)
                # Failed to stop
                log_end_msg 1
                ;;
        esac
        ;;
```

```
    *)
        echo "Usage: $SCRIPTNAME {start|stop|status|restart|reload|force-reload|upgrade|configtest}"
>&2
        exit 3
        ;;
esac

exit $RETVAL
```

## Ativando o start do Nginx

```
root@debian:~# cd /etc/init.d/
root@debian:/etc/init.d# chmod +x nginx
root@debian:/etc/init.d# insserv nginx
root@debian:/etc/init.d# update-rc.d nginx defaults
```

# Configurando o ModSecurity.

```
root@debian:/etc/init.d# cd /etc/nginx
root@debian:/etc/nginx# cp /usr/src/modsecurity/modsecurity.conf-recommended modsecurity.conf
root@debian:/etc/nginx# cp /usr/src/modsecurity/unicode.mapping .
```

## Altere o arquivo /etc/nginx/modsecurity.conf

SecRuleEngine On
SecRequestBodyLimit 100000000
SecAuditLogType Concurrent

# Configurando OWASP.

```
root@debian:/etc/nginx# cd /usr/src/
root@debian:/usr/src# git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
root@debian:/usr/src# cd owasp-modsecurity-crs
root@debian:/usr/src/owasp-modsecurity-crs# cp -R base_rules/ /etc/nginx
root@debian:/usr/src# cd /etc/nginx
root@debian:/etc/nginx# vi modsecurity.conf
```

## Adicione ao final do arquivo /etc/nginx/modsecurity.conf

```
SecDefaultAction "log,deny,phase:1"
Include base_rules/*.conf
SecRuleRemoveById 981172 981173 960032 960034 960017 960010 950117 981004 960015
```

## Ativando o modsecurity no /etc/nginx/nginx.conf

Adicione as linhas ModSecurity* no arquivo, conforme o pedaço da configuração abaixo:

```
[.....]
    server {
        listen       80;
        server_name  localhost;

        ModSecurityEnabled on;
        ModSecurityConfig modsecurity.conf;
[.....]
```

# Referências:

https://www.modsecurity.org/documentation.html
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual