

Matomo是一个开源的网站分析平台

<https://builds.matomo.org>

下载

```
wget https://builds.matomo.org/matomo.zip
unzip matomo.zip
mv ./matomo /var/www/
chown -R www-data:www-data /var/www/matomo
```

配置依赖

```
apt install php php-curl php-gd php-cli mysql-server php-mysql php-xml php-mbstring
```

数据库设置

```
#连接到您的 MySQL 数据库
mysql -u root -p
输入密码,后enter
#为 Matomo 创建数据库:
CREATE DATABASE matomo_db;
#显示数据库
SHOW DATABASES;
#权限
#创建其他用户
CREATE USER admin IDENTIFIED BY "*****";
#WordPress权限授权给admin用户
GRANT ALL PRIVILEGES ON matomo_db.* TO admin;
#系统会重新加载权限表, 确保使用的是最新的权限设置。
FLUSH PRIVILEGES;
#退出mysql数据库
EXIT;
```

服务器配置

[matomo.conf](#)

```
server {
    listen [::]:80; # remove this if you don't want Matomo to be
    reachable from IPv6
    listen 80;
    server_name matomo.example.com;
    # Redirect all HTTP requests to HTTPS with a 301 Moved Permanently
    response.
    location / {
        return 301 https://$host$request_uri;
    }
}
server {
    listen [::]:443 ssl http2; # remove this if you don't want Matomo
```

```
to be reachable from IPv6
    listen 443 ssl http2;
    server_name matomo.example.com; # list all domains Matomo should be
    reachable from
    access_log /var/log/nginx/matomo.access.log;
    error_log /var/log/nginx/matomo.error.log;

    ## uncomment if you want to enable HSTS with 6 months cache
    ## ATTENTION: Be sure you know the implications of this change (you
    won't be able to disable HTTPS anymore)
    #add_header Strict-Transport-Security max-age=15768000 always;

    ## replace with your SSL certificate
    ssl_certificate
    /etc/letsencrypt/live/matomo.example.com/fullchain.pem;
    ssl_certificate_key
    /etc/letsencrypt/live/matomo.example.com/privkey.pem;

    include ssl.conf; # if you want to support older browsers, please
    read through this file

    add_header Referrer-Policy origin always; # make sure outgoing
    links don't show the URL to the Matomo instance
    add_header X-Content-Type-Options "nosniff" always;
    add_header X-XSS-Protection "1; mode=block" always;

    root /var/www/matomo/; # replace with path to your matomo instance

    index index.php;

    ## only allow accessing the following php files
    location ~
    ^/(index|matomo|piwik|js/index|plugins/HeatmapSessionRecording/configs)
    \.php$ {
        include snippets/fastcgi-php.conf; # if your Nginx setup
        doesn't come with a default fastcgi-php config, you can fetch it from
        https://github.com/nginx/nginx/blob/master/conf/fastcgi.conf
        try_files $fastcgi_script_name =404; # protects against
        CVE-2019-11043. If this line is already included in your
        snippets/fastcgi-php.conf you can comment it here.
        fastcgi_param HTTP_PROXY ""; # prohibit httpoxy:
        https://httpoxy.org/
        fastcgi_pass unix:/var/run/php/php7.2-fpm.sock; #replace with
        the path to your PHP socket file
        #fastcgi_pass 127.0.0.1:9000; # uncomment if you are using PHP
        via TCP sockets (e.g. Docker container)
    }

    ## deny access to all other .php files
    location ~* ^.+\.php$ {
        deny all;
```

```
        return 403;
    }

    ## serve all other files normally
    location / {
        try_files $uri $uri/ =404;
    }

    ## disable all access to the following directories
    location ~ ^/(config|tmp|core|lang) {
        deny all;
        return 403; # replace with 404 to not show these directories
exist
    }

    location ~ /\.ht {
        deny all;
        return 403;
    }

    location ~ js/container.*_preview\.js$ {
        expires off;
        add_header Cache-Control 'private, no-cache, no-store';
    }

    location ~
\.(gif|ico|jpg|png|svg|js|css|htm|html|mp3|mp4|wav|ogg|avi|ttf|eot|woff
|woff2)$ {
        allow all;
        ## Cache images,CSS,JS and webfonts for an hour
        ## Increasing the duration may improve the load-time, but may
cause old files to show after an Matomo upgrade
        expires 1h;
        add_header Pragma public;
        add_header Cache-Control "public";
    }

    location ~ ^/(libs|vendor|plugins|misc|node_modules) {
        deny all;
        return 403;
    }

    ## properly display textfiles in root directory
    location ~/(.*\.md|LEGALNOTICE|LICENSE) {
        default_type text/plain;
    }
}
# vim: filetype=nginx
```

ssl.conf

```
##
## Modern profile created with the Mozilla SSL Configuration Generator
## Oldest compatible clients: Firefox 27, Chrome 30, IE 11 on Windows
## 7, Edge, Opera 17, Safari 9, Android 5.0, and Java 8
## If you need to support older clients, create your own config here
## https://mozilla.github.io/server-side-tls/ssl-config-generator/

ssl_session_timeout 1d;
ssl_session_cache shared:SSL:50m;
ssl_session_tickets off;

# modern configuration. tweak to your needs.
ssl_protocols TLSv1.2;
ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256';
ssl_prefer_server_ciphers on;

# OCSP Stapling ---
# fetch OCSP records from URL in ssl_certificate and cache them
ssl_stapling on;
ssl_stapling_verify on;

# vim: filetype=nginx
```

修改

```
Nginx
cd /etc/nginx/conf.d/

#查看nginx的配置文件路径，记录nginx.conf路径
nginx -t
sudo systemctl restart nginx
chown -R www-data:www-data /var/www/matomo
```

将 zip 文件解压缩到硬盘驱动器上的文件夹中。这将创建一个包含文件和目录的“matomo”文件夹。

打开您的 FTP 客户端并将 Matomo 文件以“二进制模式”上传到 Web 服务器上的所需位置。例如，使用 Filezilla FTP 客户端，您可以在顶部菜单中启用二进制模式传输 传输 > 传输类型 > 二进制）。所有文件都可以上传到公共 www 文件夹中的“分析”子目录，例如 <http://yourdomain.org/analytics/>，或者您可以在自己的子域中设置 Matomo 并在 <http://analytics.example.org/> 上传所有文件

欢迎屏幕

是时候开始点击式安装了！单击下一步 »

安装 JavaScript 跟踪标记

在您要分析的每个页面上安装 Matomo 生成的 JavaScript 跟踪标签。我们建议将此代码放在结束标记之前或包含在所有页面顶部的共享头文件中</head>

From:

<https://sujj.wiki/> - 落月思君归

Permanent link:

<https://sujj.wiki/doku.php?id=%E8%BD%AF%E4%BB%B6:matomo&rev=1759692770>

Last update: **2026/01/02 02:07**

