**SETUP WEBSITE SERVER ẢO(Apache)**

**1. Cài đặt Apache**

Khi user sudo không phải root được cấu hình trong yêu cầu , hãy cài đặt gói Apache:

* sudo dnf install httpd

Nếu bạn cũng cấu hình Apache để cho truy cập qua HTTPS, bạn cũng cần mở cổng 443 bằng cách bật dịch vụ https :

* sudo firewall-cmd --permanent --add-service=https

Cập nhật firewall để các luật mới này có hiệu lực:

* sudo firewall-cmd --reload

Kiểm tra Server Web của bạn

* sudo systemctl start httpd

Xác minh dịch vụ đang chạy bằng lệnh sau:

* sudo systemctl status httpd

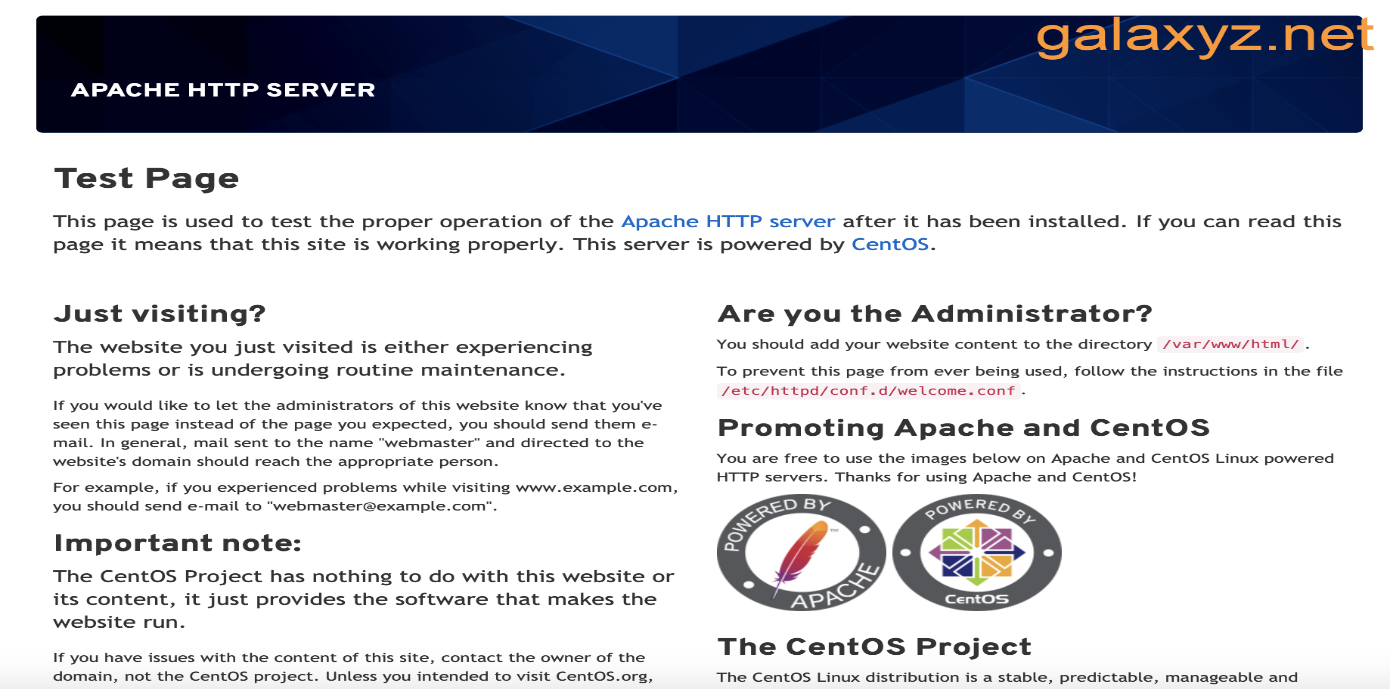
Gõ q để quay lại dấu nhắc lệnh, sau đó gõ:

* hostname -I

Khi bạn có địa chỉ IP của server , hãy nhập địa chỉ đó vào thanh địa chỉ của trình duyệt:

* http://your\_server\_ip

Màn hình Apache hiển thị ra -> **Cài đặt thành công** !



**Quản lý tiến trình Apache:**

Để dừng web server của bạn, hãy nhập:

* sudo systemctl stop httpd

Để khởi động web server khi nó bị dừng, hãy nhập:

* sudo systemctl start httpd

Để dừng và sau đó bắt đầu lại dịch vụ, hãy nhập:

* sudo systemctl restart httpd

Nếu bạn chỉ đơn giản là thực hiện thay đổi cấu hình, Apache có thể reload mà không làm mất kết nối . Để thực hiện việc này, hãy sử dụng lệnh sau:

* sudo systemctl reload httpd

Theo mặc định, Apache được cấu hình để khởi động tự động khi server khởi động. Nếu bạn không muốn vậy , hãy tắt hành vi này bằng lệnh :

* sudo systemctl disable httpd

Để bật lại dịch vụ khởi động khi server khởi động , hãy nhập:

* sudo systemctl enable httpd

Apache bây giờ sẽ tự động khởi động khi server khởi động lại.

Cấu hình mặc định cho Apache sẽ cho phép server của bạn lưu trữ một trang web duy nhất. Nếu bạn định lưu trữ nhiều domain trên server của bạn , bạn cần phải cấu hình các server ảo trên web server Apache của bạn .

**2. Cài đặt PHP**

Cài đặt trên CentOS8

sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm  
sudo dnf -y install https://rpms.remirepo.net/enterprise/remi-release-8.rpm  
sudo dnf -y install yum-utils  
sudo dnf module reset php  
sudo dnf module install php:remi-8.0 -y  
sudo dnf install php -y  
sudo dnf -y install php-{cli,fpm,mysqlnd,zip,devel,gd,mbstring,curl,xml,pear,bcmath,json}

Cài đặt trên CentOS7

sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm  
sudo yum -y install https://rpms.remirepo.net/enterprise/remi-release-7.rpm  
sudo yum -y install yum-utils  
sudo yum-config-manager --disable 'remi-php\*'  
sudo yum-config-manager --enable remi-php80  
sudo yum -y install php php-{cli,fpm,mysqlnd,zip,devel,gd,mbstring,curl,xml,pear,bcmath,json}

Cài đặt các package php khác

sudo yum install php-xxx

Check version php sau khi cài đặt xong

php --version  
PHP 8.0.0 (cli) (built: Nov 24 2020 17:04:03) ( NTS gcc x86\_64 )  
Copyright (c) The PHP Group  
Zend Engine v4.0.0-dev, Copyright (c) Zend Technologies  
    with Zend OPcache v8.0.0, Copyright (c), by Zend Technologies

**3. Cài đặt Mariadb & phpMyAdmin**

**3.1 MariaDB**

Đầu tiên, sử dụng **dnf** để cài đặt gói [MariaDB](https://mariadb.org/):

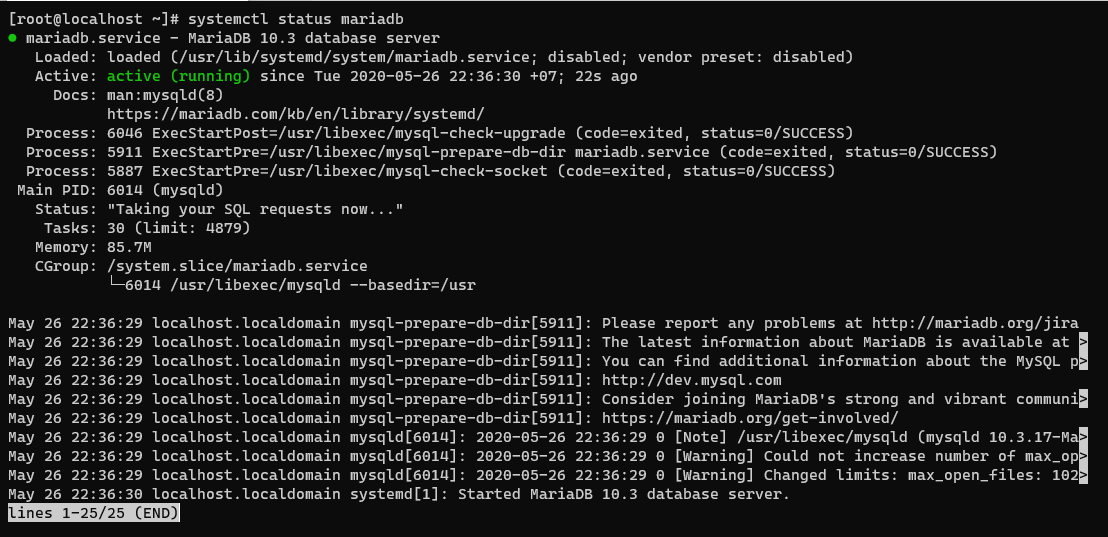
dnf install mariadb-server -y

Sau khi cài đặt hoàn tất, hãy khởi động dịch vụ với **systemctl**:

systemctl start mariadb

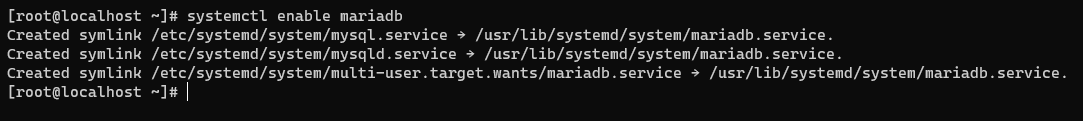
Sau đó kiểm tra trạng thái của dịch vụ:

systemctl status mariadb



Tiếp theo, hãy kích hoạt MariaDB khởi động cùng hệ thống với lệnh **enable systemctl**:

systemctl enable mariadb



Bây giờ MariaDB dã chạy và được cấu hình khởi động cùng hệ thống. Tiếp theo, hãy tiến hành cấu hình bảo mật cho MariaDB

**Bảo mật MariaDB Server**

MariaDB bao gồm một tập lệnh bảo mật để thay đổi một số tùy chọn mặc định kém an toàn như **Remote Connect** và user **test**. Sử dụng lệnh sau để chạy tập lệnh bảo mật:

mysql\_secure\_installation

Bước đầu tiên yêu cầu mật khẩu root, bạn nhấn ENTER để đến bước sau. Tiếp theo, bạn sẽ được nhắc đặt mật khẩu root. Hãy nhớ rằng đây là dành cho người dùng root của MariaDB, không phải người dùng root của CentOS.

Gõ **Y** rồi **ENTER** để nhập mật khẩu cho user root. Sau khi đặt mật khẩu, các bạn tiến hành làm theo hướng dẫn từng bước như dưới đây

Enter current password for root (enter for none): **Nhấn Enter**  
Set root password? [Y/n]: **y**  
New password: **Nhập mật khẩu root MariaDB bạn muốn đặt**  
Re-enter new password: **Nhập lại mật khẩu**  
Remove anonymous users? [Y/n]: **y**  
Disallow root login remotely? [Y/n]: **y**  
Remove test database and access to it? [Y/n]:**y**  
Reload privilege tables now? [Y/n]: **y**

**3.2 phpMyAdmin**

Đầu tiên, bạn sẽ cần cài đặt Apache, MariaDB, PHP và các thư viện PHP khác vào máy chủ của mình. Bạn có thể cài đặt tất cả chúng bằng lệnh sau:

*dnf install httpd mariadb-server php php-pdo php-pecl-zip php-json php-common php-fpm php-mbstring php-cli php-mysqlnd php-json php-mbstring wget unzip*

**Ở đây chúng ta đã cài đặt Apache, MariaDB, PHP rồi, ta chỉ cần cài thêm các thư viện khác của PHP vào là được:**

*dnf install php php-pdo php-pecl-zip php-json php-common php-fpm php-mbstring php-cli php-mysqlnd php-json php-mbstring wget unzip*

Khi tất cả các gói được cài đặt, hãy khởi động dịch vụ Apache và MariaDB và cho phép chúng khởi động sau khi hệ thống khởi động lại bằng lệnh sau:

*systemctl start httpd  
 systemctl start mariadb  
 systemctl enable httpd  
 systemctl enable mariadb*

**3.2.1 Cài đặt phpMyAdmin**

Theo mặc định, phpMyAdmin không có sẵn trong kho lưu trữ mặc định của CentOS 8. Vì vậy, bạn sẽ cần tải xuống phiên bản phpMyAdmin mới nhất từ ​​trang web chính thức của họ. Bạn có thể tải xuống bằng lệnh sau:

*wget https://files.phpmyadmin.net/phpMyAdmin/4.9.2/phpMyAdmin-4.9.2-all-languages.zip*

Sau khi tải xuống, hãy giải nén tệp đã tải xuống bằng lệnh sau:

*unzip phpMyAdmin-4.9.2-all-languages.zip*

Tiếp theo, di chuyển nội dung đã trích xuất vào thư mục / usr / share như hình dưới đây:

*mv phpMyAdmin-4.9.2-all-languages /usr/share/phpmyadmin*

Tiếp theo, thay đổi thư mục thành / usr / share / phpmyadmin và đổi tên tệp config.sample.inc.php:

*cd /usr/share/phpmyadmin  
 mv config.sample.inc.php config.inc.php*

Next, open the file with your favorite text editor as shown below:

*nano config.inc.php*

Thay đổi dòng sau:

$cfg['blowfish\_secret'] = 'your-secret-password';

Lưu và đóng tệp khi bạn hoàn tất. Sau đó, nhập create\_tables.sql bằng lệnh sau:

**Chúng ta có thể không tạo ở đây và sẽ tạo cơ sở dữ liệu khi cài đặt xong.**

*mysql < /usr/share/phpmyadmin/sql/create\_tables.sql -u root -p*

Tiếp theo, tạo một thư mục tmp cho phpmyadmin và cấp quyền thích hợp:

*mkdir /usr/share/phpmyadmin/tmp  
 chown -R apache:apache /usr/share/phpmyadmin  
 chmod 777 /usr/share/phpmyadmin/tmp*

**3.2.2 Cấu hình Apache cho phpMyAdmin**

Tạo tệp cấu hình máy chủ ảo Apache cho phpMyAdmin. Bạn có thể tạo nó bằng lệnh sau:

*nano /etc/httpd/conf.d/phpmyadmin.conf*

Thêm các dòng sau:

Alias /phpmyadmin /usr/share/phpmyadmin

<Directory /usr/share/phpmyadmin/>

AddDefaultCharset UTF-8

<IfModule mod\_authz\_core.c>

# Apache 2.4

<RequireAny>

Require all granted

</RequireAny>

</IfModule>

<IfModule !mod\_authz\_core.c>

# Apache 2.2

Order Deny,Allow

Deny from All

Allow from 127.0.0.1

Allow from ::1

</IfModule>

</Directory>

<Directory /usr/share/phpmyadmin/setup/>

<IfModule mod\_authz\_core.c>

# Apache 2.4

<RequireAny>

Require all granted

</RequireAny>

</IfModule>

<IfModule !mod\_authz\_core.c>

# Apache 2.2

Order Deny,Allow

Deny from All

Allow from 127.0.0.1

Allow from ::1

</IfModule>

</Directory>

Lưu và đóng tệp khi bạn hoàn tất. Sau đó, khởi động lại dịch vụ Apache bằng lệnh sau:

*systemctl restart httpd*

Kiểm tra trạng thái của Apache bằng lệnh sau:

*systemctl status httpd*

You should see the following output:

? httpd.service - The Apache HTTP Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)

Drop-In: /usr/lib/systemd/system/httpd.service.d

??php-fpm.conf

Active: active (running) since Wed 2019-12-18 01:07:52 EST; 6s ago

Docs: man:httpd.service(8)

Main PID: 5636 (httpd)

Status: "Started, listening on: port 80"

Tasks: 213 (limit: 25044)

Memory: 28.7M

CGroup: /system.slice/httpd.service

??5636 /usr/sbin/httpd -DFOREGROUND

??5639 /usr/sbin/httpd -DFOREGROUND

??5640 /usr/sbin/httpd -DFOREGROUND

??5641 /usr/sbin/httpd -DFOREGROUND

??5642 /usr/sbin/httpd -DFOREGROUND

Dec 18 01:07:52 centos8 systemd[1]: Stopped The Apache HTTP Server.

Dec 18 01:07:52 centos8 systemd[1]: Starting The Apache HTTP Server...

Dec 18 01:07:52 centos8 httpd[5636]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::200:d0>

Dec 18 01:07:52 centos8 httpd[5636]: Server configured, listening on: port 80

Dec 18 01:07:52 centos8 systemd[1]: Started The Apache HTTP Server.

**3.2.3 Cấu hình SELinux và Tường lửa**

Mặc định, SELinux được bật trong CentOS 8. Vì vậy, bạn sẽ cần phải cấu hình SELinux cho phpMyAdmin để hoạt động chính xác.

Đầu tiên, cài đặt gói Policycoreutils-python-utils để quản lý môi trường SELinux bằng lệnh sau:

*dnf install policycoreutils-python-utils*

Tiếp theo, cho phép truy cập vào thư mục / usr / share / phpmyadmin bằng lệnh sau:

*semanage fcontext -a -t httpd\_sys\_rw\_content\_t '/usr/share/phpmyadmin/'  
 semanage fcontext -a -t httpd\_sys\_rw\_content\_t "/usr/share/phpmyadmin/tmp(/.\*)?"*

Bây giờ đệ quy lại tất cả các tệp trong thư mục phpmyadmin của bạn bằng cách chạy lệnh sau:

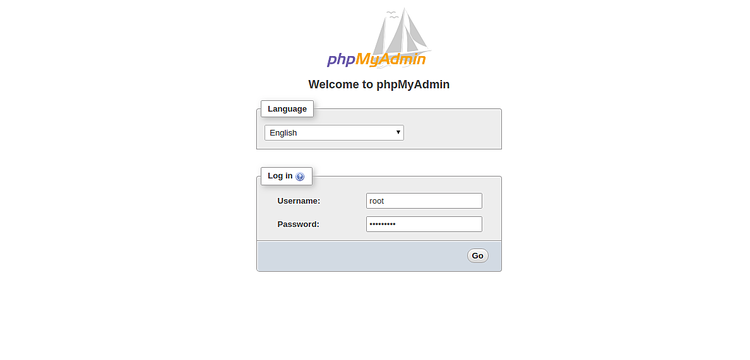
*restorecon -Rv '/usr/share/phpmyadmin/'*

Tiếp theo, bạn sẽ cần tạo quy tắc tường lửa để cho phép dịch vụ HTTP từ các mạng bên ngoài. Bạn có thể cho phép nó bằng lệnh sau:

*firewall-cmd --permanent --add-service=http  
 firewall-cmd --reload*

phpMyAdmin hiện đã được cài đặt và cấu hình. Bây giờ là lúc để kiểm tra xem nó có hoạt động hay không.

Mở trình duyệt web của bạn và nhập URL http: // your-server-ip / phpmyadmin. Bạn sẽ được chuyển hướng đến trang sau:



**3.2.4 Bảo mật phpMyAdmin**

Tại thời điểm này, phiên bản phpMyAdmin đang hoạt động bình thường. Tuy nhiên, việc bảo vệ phiên bản phpMyAdmin của bạn khỏi thế giới bên ngoài là một nhiệm vụ quan trọng đối với bạn. Trong phần này, chúng tôi sẽ chỉ cho bạn cách bảo mật phiên bản phpMyAdmin của bạn.

Cho phép phpMyAdmin từ IP cụ thể:

Trước tiên, bạn sẽ cần phải định cấu hình phpMyAdmin của mình để chỉ có thể truy cập từ địa chỉ IP của kết nối gia đình của bạn.

Bạn có thể định cấu hình nó bằng cách chỉnh sửa tệp /etc/httpd/conf.d/phpmyadmin.conf:

*nano /etc/httpd/conf.d/phpmyadmin.conf*

Tìm các dòng sau:

<RequireAny>

Require all granted

</RequireAny>

Và thay thế chúng bằng những thứ sau:

<RequireAny>

Require ip your-home--connection-ip-address

Require ip ::1

</RequireAny>

Lưu và đóng tệp khi bạn hoàn tất.

Cấu hình lớp xác thực bổ sung

Bạn nên mật khẩu bảo vệ thư mục phpmyadmin của mình bằng cách thiết lập xác thực cơ bản.

Để làm như vậy, hãy tạo một tệp xác thực mới bằng công cụ htpasswd như hình dưới đây:

*mkdir /etc/phpmyadmin  
 htpasswd -c /etc/phpmyadmin/.htpasswd admin*

Bạn sẽ được yêu cầu cung cấp mật khẩu quản trị của mình như hình dưới đây:

New password:

Re-type new password:

Adding password for user admin

Tiếp theo, bạn sẽ cần cấu hình Apache để sử dụng tệp .htpasswd. Bạn có thể thực hiện việc này bằng cách chỉnh sửa tệp /etc/httpd/conf.d/phpmyadmin.conf.

*nano /etc/httpd/conf.d/phpmyadmin.conf*

Thêm các dòng sau vào bên dưới dòng "AddDefaultCharset UTF-8":

Options +FollowSymLinks +Multiviews +Indexes

AllowOverride None

AuthType basic

AuthName "Authentication Required"

AuthUserFile /etc/phpmyadmin/.htpasswd

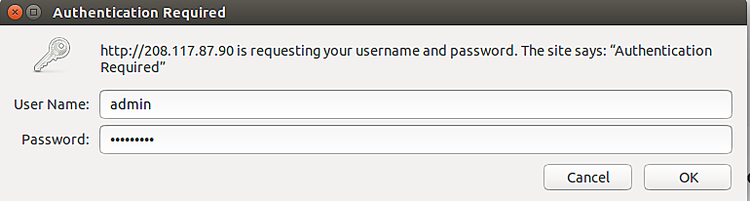
Require valid-user

Lưu tệp và khởi động lại dịch vụ Apache để các thay đổi có hiệu lực:

*systemctl restart httpd*

Truy cập phpMyAdmin

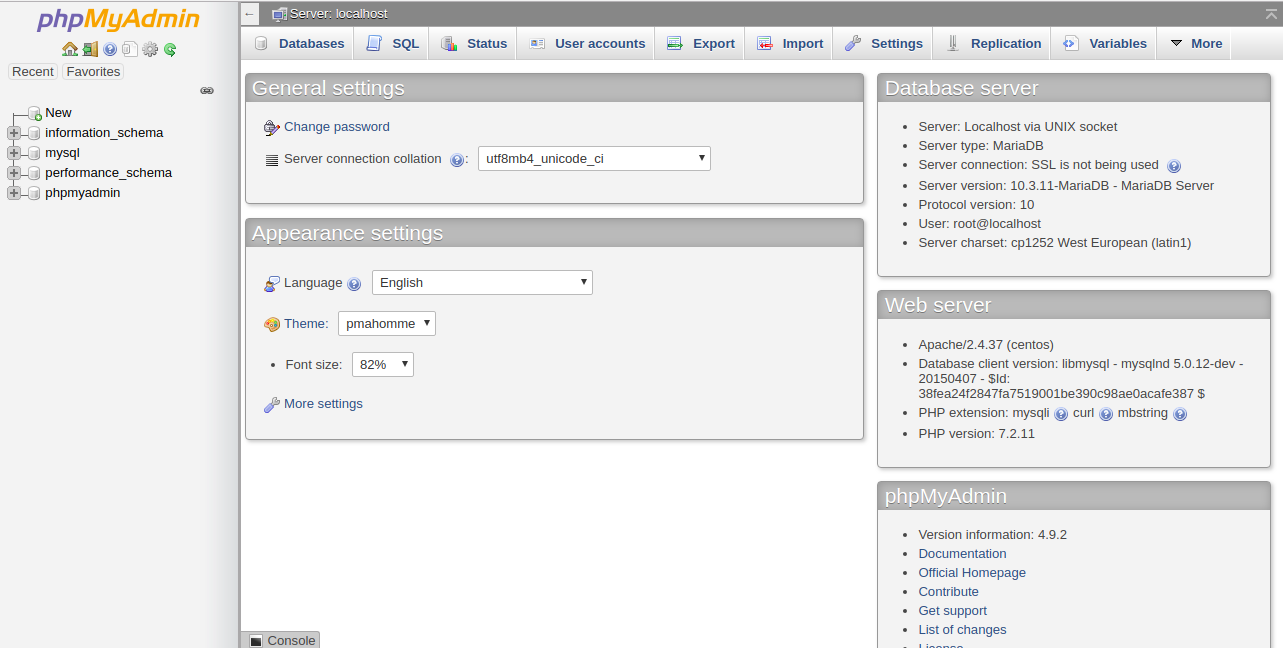
Bây giờ, phiên bản phpMyAdmin của bạn đã được bảo mật bằng một lớp bảo mật bổ sung. Mở trình duyệt web của bạn và nhập URL http: // your-server-ip / phpmyadmin. Bạn sẽ được yêu cầu nhập thông tin đăng nhập của người dùng mà bạn đã tạo trước đó như hình dưới đây:



Cung cấp tên người dùng và mật khẩu quản trị viên của bạn, sau đó nhấp vào nút OK. Bạn sẽ được chuyển hướng đến trang đăng nhập phpMyAdmin:



Bây giờ, cung cấp thông tin đăng nhập người dùng quản trị MySQL của bạn và nhấp vào nút Bắt đầu. Bạn sẽ thấy trang sau:



*Bạn đã cài đặt và bảo mật thành công phpMyAdmin trên máy chủ CentOS 8.*

**4. Cài đặt Vitual host – Chạy nhiều web trên một server**

Khi sử dụng web server Apache, bạn có thể sử dụng các server ảo (nếu bạn quen thuộc hơn với Nginx, chúng tương tự như các khối server ) để đóng gói các chi tiết cấu hình và lưu trữ nhiều domain từ một server duy nhất. Trong bước này, bạn sẽ cài đặt một domain có tên là example.com , nhưng bạn nên thay thế domain này bằng domain của bạn . Nếu bạn đang cài đặt domain với DigitalOcean, vui lòng tham khảo [Tài liệu về mạng](https://galaxyz.net/truoc-khi-ban-co-the-lam-dieu-do-de-hoan-thanh-hanh-dong-nay-hay-dang-nhap-vao-tai-khoan-cong-dong-cua-ban-hoac-tao-mot-tai-khoan-moi.3510.anews) của ta .

Apache trên CentOS 8 có một server ảo được kích hoạt theo mặc định được cấu hình để cung cấp tài liệu từ folder /var/www/html . Mặc dù điều này hoạt động tốt cho một trang web, nhưng nó có thể trở nên khó sử dụng nếu bạn đang lưu trữ nhiều trang web. Thay vì sửa đổi /var/www/html , bạn sẽ tạo cấu trúc folder bên trong /var/www cho trang web example.com , giữ nguyên /var/www/html làm folder mặc định được phục vụ nếu khách hàng không yêu cầu ' không phù hợp với bất kỳ trang web nào khác.

Tạo folder html cho example.com như sau, sử dụng cờ -p để tạo bất kỳ folder mẹ nào cần thiết:

* sudo mkdir -p /var/www/example.com/html

Tạo một folder bổ sung để lưu trữ các file log cho trang web:

* sudo mkdir -p /var/www/example.com/log

Tiếp theo, chỉ định quyền sở hữu folder html với biến môi trường $USER :

* sudo chown -R $USER:$USER /var/www/example.com/html

Đảm bảo rằng root web của bạn có các quyền mặc định được đặt:

* sudo chmod -R 755 /var/www

Tiếp theo, tạo một trang index.html mẫu bằng vi hoặc trình soạn thảo yêu thích của bạn:

* sudo vi /var/www/example.com/html/index.html

Nhấn i để chuyển sang chế độ INSERT và thêm HTML mẫu sau vào file :

**/var/www/example.com/html/index.html**

<html>

<head>

<title>Welcome to Example.com!</title>

</head>

<body>

<h1>Success! The example.com virtual host is working!</h1>

</body>

</html>

Lưu file bằng cách nhấn ESC , nhập :wq và nhấn ENTER .

Với folder trang web và file index mẫu của bạn tại chỗ, bạn gần như đã sẵn sàng để tạo file server ảo. Các file server ảo chỉ cấu hình của các trang web riêng biệt của bạn và cho web server Apache biết cách phản hồi các yêu cầu domain khác nhau.

Trước khi tạo server ảo, bạn cần tạo một folder sites-available để lưu trữ chúng. Bạn cũng cần tạo folder sites-enabled báo cho Apache rằng server ảo đã sẵn sàng phục vụ khách truy cập. Thư mục sites-enabled sẽ chứa các softlink đến các server ảo mà ta muốn xuất bản. Tạo cả hai folder bằng lệnh sau:

* sudo mkdir /etc/httpd/sites-available /etc/httpd/sites-enabled

Tiếp theo, bạn sẽ yêu cầu Apache tìm kiếm các server ảo trong folder sites-enabled . Để thực hiện điều này, hãy chỉnh sửa file cấu hình chính của Apache bằng vi hoặc editor yêu thích của bạn và thêm một dòng khai báo folder tùy chọn cho các file cấu hình bổ sung:

* sudo vi /etc/httpd/conf/httpd.conf

Nhấn viết hoa G để chuyển về cuối file . Sau đó nhấn i để chuyển sang chế độ INSERT và thêm dòng sau vào cuối file :

**/etc/httpd/conf/httpd.conf**

... # Supplemental configuration # # Load config files in the "/etc/httpd/conf.d" directory, if any. IncludeOptional conf.d/\*.conf IncludeOptional sites-enabled/\*.conf

Lưu file khi bạn hoàn tất việc thêm dòng đó. Đến đây bạn đã có các folder server ảo của bạn , bạn sẽ tạo file server ảo của bạn .

Bắt đầu bằng cách tạo một file mới trong folder sites-available trên sites-available :

* sudo vi /etc/httpd/sites-available/example.com.conf

Thêm đoạn cấu hình sau và thay đổi domain example.com domain của bạn:

**/etc/httpd/sites-available/example.com.conf**

<VirtualHost \*:80>

ServerName www.example.com

ServerAlias example.com

DocumentRoot /var/www/example.com/html

ErrorLog /var/www/example.com/log/error.log

CustomLog /var/www/example.com/log/requests.log combined

</VirtualHost>

Điều này sẽ cho Apache biết nơi để tìm trực tiếp root chứa các tài liệu web có thể truy cập . Nó cũng cho Apache biết nơi lưu trữ lỗi và yêu cầu log cho trang web cụ thể này.

Lưu file khi bạn hoàn tất.

Đến đây bạn đã tạo các file server ảo, bạn sẽ kích hoạt chúng để Apache biết để phục vụ chúng cho khách truy cập. Để thực hiện việc này, hãy tạo một softlink cho từng server ảo trong folder sites-enabled :

* sudo ln -s /etc/httpd/sites-available/example.com.conf /etc/httpd/sites-enabled/example.com.conf

Server ảo của bạn hiện đã được cấu hình và sẵn sàng cung cấp nội dung. Trước khi khởi động lại dịch vụ Apache, hãy đảm bảo SELinux có các policy phù hợp cho các server ảo của bạn.

**Điều chỉnh quyền SELinux cho Server ảo (Được khuyến nghị)**

[SELinux](https://galaxyz.net/.3045.anews) là một module bảo mật nhân Linux mang lại khả năng bảo mật cao hơn cho các hệ thống Linux. CentOS 8 được trang bị SELinux được cấu hình để hoạt động với cấu hình Apache mặc định. Vì bạn đã thay đổi cấu hình mặc định bằng cách cài đặt folder log tùy chỉnh trong file cấu hình server ảo, bạn sẽ gặp lỗi nếu cố khởi động dịch vụ Apache. Để giải quyết vấn đề này, bạn cần cập nhật các policy của SELinux để cho phép Apache ghi vào các file cần thiết.

Có nhiều cách khác nhau để đặt policy dựa trên nhu cầu của môi trường vì SELinux cho phép bạn tùy chỉnh mức độ bảo mật của bạn . Bước này sẽ bao gồm hai phương pháp điều chỉnh các policy của Apache: phổ biến và trên một folder cụ thể. Điều chỉnh các policy trên folder an toàn hơn và do đó là cách tiếp cận được khuyến khích .

**Điều chỉnh policy Apache phổ biến**

Việc đặt policy Apache trên phạm vi global sẽ yêu cầu SELinux xử lý tất cả các tiến trình Apache giống nhau bằng cách sử dụng httpd\_unified Boolean. Mặc dù cách tiếp cận này thuận tiện hơn, nhưng nó sẽ không cung cấp cho bạn mức độ kiểm soát giống như cách tiếp cận tập trung vào policy file hoặc folder .

Chạy lệnh sau để đặt một policy Apache chung:

* sudo setsebool -P httpd\_unified 1

Lệnh setsebool thay đổi các giá trị SELinux Boolean. Cờ -P sẽ cập nhật giá trị thời gian khởi động, làm cho thay đổi này vẫn tồn tại qua các lần khởi động lại. httpd\_unified là Boolean sẽ yêu cầu SELinux xử lý tất cả các tiến trình Apache là cùng một loại, vì vậy bạn đã bật nó với giá trị 1 .

### **Điều chỉnh policy Apache trên một folder**

Việc đặt riêng các quyền SELinux cho folder /var/www/ example.com /log sẽ giúp bạn kiểm soát nhiều hơn các policy Apache của bạn , nhưng cũng có thể yêu cầu bảo trì nhiều hơn. Vì tùy chọn này không phải là policy cài đặt trên phạm vi global , bạn cần phải đặt loại ngữ cảnh theo cách thủ công cho bất kỳ folder log mới nào được chỉ định trong cấu hình server ảo của bạn.

Đầu tiên, hãy kiểm tra kiểu ngữ cảnh mà SELinux đã cung cấp cho folder /var/www/ example.com /log :

* sudo ls -dlZ /var/www/example.com/log/

Lệnh này liệt kê và đưa ra ngữ cảnh SELinux của folder . Bạn sẽ nhận được kết quả tương tự như sau:

Output

drwxr-xr-x. 2 root root unconfined\_u:object\_r:httpd\_sys\_content\_t:s0 6 Apr 23 23:51 /var/www/example.com/log/

Bối cảnh hiện tại là httpd\_sys\_content\_t , cho SELinux biết rằng tiến trình Apache chỉ có thể đọc các file được tạo trong folder này. Trong hướng dẫn này, bạn sẽ thay đổi kiểu ngữ cảnh của folder /var/www/ example.com /log thành httpd\_log\_t . Loại này sẽ cho phép Apache tạo và nối vào các file log ứng dụng web:

* sudo semanage fcontext -a -t httpd\_log\_t "/var/www/example.com/log(/.\*)?"

Tiếp theo, sử dụng lệnh restorecon để áp dụng những thay đổi này và để chúng tồn tại qua các lần khởi động lại:

* sudo restorecon -R -v /var/www/example.com/log

Cờ -R chạy lệnh này một cách đệ quy, nghĩa là nó sẽ cập nhật mọi file hiện có để sử dụng ngữ cảnh mới. Cờ -v sẽ in ra các thay đổi ngữ cảnh mà lệnh được thực hiện. Bạn sẽ nhận được kết quả sau xác nhận các thay đổi:

Output

Relabeled /var/www/example.com/log from unconfined\_u:object\_r:httpd\_sys\_content\_t:s0 to unconfined\_u:object\_r:httpd\_log\_t:s0

Bạn có thể liệt kê các bối cảnh để xem các thay đổi:

* sudo ls -dlZ /var/www/example.com/log/

Đầu ra phản ánh loại ngữ cảnh được cập nhật:

Output

drwxr-xr-x. 2 root root unconfined\_u:object\_r:httpd\_log\_t:s0 6 Apr 23 23:51 /var/www/example.com/log/

Bây giờ, folder /var/www/ example.com /log đang sử dụng kiểu httpd\_log\_t , bạn đã sẵn sàng để kiểm tra cấu hình server ảo của bạn .

**Kiểm tra Server ảo (Được khuyến nghị)**

Khi ngữ cảnh SELinux đã được cập nhật bằng một trong hai phương pháp, Apache sẽ có thể ghi vào folder /var/www/ example.com /log . Đến đây bạn có thể khởi động lại thành công dịch vụ Apache:

* sudo systemctl restart httpd

Liệt kê nội dung của folder /var/www/ example.com /log để xem Apache có tạo các file log hay không:

* ls -lZ /var/www/example.com/log

Bạn sẽ nhận được xác nhận Apache đã có thể tạo ra các error.log và requests.log file quy định trong cấu hình server ảo:

Output

-rw-r--r--. 1 root root system\_u:object\_r:httpd\_log\_t:s0 0 Apr 24 00:06 error.log -rw-r--r--. 1 root root system\_u:object\_r:httpd\_log\_t:s0 0 Apr 24 00:06 requests.log

Sự thành công!  Server  ảo example.com đang hoạt động!Đến đây bạn đã cài đặt server ảo của bạn và cập nhật các quyền SELinux, Apache bây giờ sẽ phân phát domain của bạn. Bạn có thể kiểm tra bằng cách chuyển đến http:// example.com , nơi bạn sẽ thấy thông tin như sau:

Điều này xác nhận server ảo của bạn đã được cấu hình thành công và cung cấp nội dung. Lặp lại các bước 4 và 5 để tạo các server ảo mới với quyền SELinux cho các domain bổ sung.

***Nguồn tham khảo:***

[***https://galaxyz.net/cach-cai-dat-web-server-apache-tren-centos-8.428.anews***](https://galaxyz.net/cach-cai-dat-web-server-apache-tren-centos-8.428.anews)

[***https://www.itcweb.net/huong-dan-cai-dat-php8-tren-centos***](https://www.itcweb.net/huong-dan-cai-dat-php8-tren-centos)

[***https://www.howtoforge.com/install-and-secure-phpmyadmin-on-centos-8/***](https://www.howtoforge.com/install-and-secure-phpmyadmin-on-centos-8/)

[***https://blog.hostvn.net/chia-se/huong-dan-cai-dat-mariadb-tren-centos-8.html***](https://blog.hostvn.net/chia-se/huong-dan-cai-dat-mariadb-tren-centos-8.html)