

Bài thực hành

Cài đặt và cấu hình Apache Web Server

I. Cài đặt và khởi tạo dịch vụ Apache Web Server

Bước 1. Cấu hình card mạng máy ảo Linux với địa chỉ 192.168.1.1/24, kết nối đến máy ảo Windows có địa chỉ 192.168.1.100/24 qua mạng ảo NAT. Tắt firewall trên máy ảo Linux.

```
[root@CentOS]# ifconfig eth0 192.168.1.1/24 up
[root@CentOS]# service iptables stop
```

Bước 2. Cấu hình DNS cho phép máy thật Windows truy cập vào máy ảo Linux qua Domain Name **web.ipmac.lab** (xem lại bài thực hành cấu hình DNS-BIND)

(Trong trường hợp không có máy chủ DNS có thể chỉnh sửa file

C:\Windows\System32\drivers\etc\hosts trên máy Windows và thêm vào dòng sau:

```
192.168.1.1      web.ipmac.lab
)
```

Bước 3. Kiểm tra package **httpd** đã được cài đặt hay chưa. Nếu chưa cần tiến hành cài đặt package này qua **yum** hoặc **rpm**

```
[root@CentOS]# rpm -qa | grep httpd
httpd-2.2.3-43.el5.centos
```

Bước 4. Mở file cấu hình tổng thể của **httpd** (/etc/httpd/conf/httpd.conf) và xem các thông tin cấu hình chính

```
[root@CentOS]# less /etc/httpd/conf/httpd.conf
...
ServerRoot "/etc/httpd"          #Thư mục chứa các file cấu hình
...
Listen 80                        #Cổng mặc định khi khởi tạo dịch vụ
...
Include conf.d/*.conf            #Các file cấu hình bổ sung cho httpd
...
User apache                      #Account sử dụng để chạy dịch vụ httpd
Group apache
...
ServerAdmin root@localhost       #Địa chỉ email của Web Admin
...
DocumentRoot "/var/www/html"     #Thư mục gốc chứa các Website
...
<Directory ...>
...
</Directory>                    #Phân quyền cho từng thư mục trên Website
...
DirectoryIndex index.html ...    #Tên trang chủ mặc định cho từng thư mục
...
### Section 3 : Virtual Hosts    #Phần cấu hình cho từng Virtual Hosts
...
```

Bước 5. Tạo trang web thử nghiệm bên trong thư mục **/var/www/html** và khởi động dịch vụ **httpd**

```
[root@CentOS]# cd /var/www/html
[root@CentOS]# vi index.html
```

```
<html>
<body>
    Welcome to my Website
</body>
</html>
[root@CentOS]# service httpd start
Starting httpd: [ OK ]
```

Bước 6. Trên máy thật Windows, mở Web Browser và truy cập vào website **web.ipmac.lab** để xem trang web thử nghiệm

II. Cài đặt module hỗ trợ php cho Apache

Bước 7. Kiểm tra package **php** đã được cài đặt hay chưa. Nếu chưa tiến hành cài đặt package này thông qua **yum** hoặc **rpm**

```
[root@CentOS]# rpm -qa | grep php
[root@CentOS]# yum install php
[root@CentOS]# rpm -qa | grep php
php-cli-5.1.6-27.el5
php-5.1.6-27.el5
php-common-5.1.6-27.el5
```

Bước 8. Xem file cấu hình module php cho dịch vụ web

```
[root@CentOS]# cd /etc/httpd/conf.d
[root@CentOS]# less php.conf
```

Bước 9. Tạo thư mục **php** bên trong **/var/www/html** và tạo trang web php thử nghiệm bên trong thư mục này

```
[root@CentOS]# mkdir /var/www/html/php
[root@CentOS]# vi index.php
<html>
<body>
    <?phpinfo() ?>
</body>
</html>
```

Bước 10. Khởi động lại dịch vụ **httpd**

```
[root@CentOS]# service httpd restart
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
```

Bước 11. Trên máy thật Windows, mở Web Browser và truy cập vào website **web.ipmac.lab/php** để xem trang web thử nghiệm viết bằng php

III. Giới hạn truy cập và bảo mật cho các thư mục

Bước 12. Tạo thư mục con tên **safe** bên trong **/var/www/html** và tạo một số file&folder bên trong thư mục này. Tạo thêm một symlink bên trong thư mục **safe** để trỏ đến thư mục gốc (/) của hệ thống

```
[root@CentOS]# mkdir /var/www/html/safe
[root@CentOS]# cd /var/www/html/safe
```

```
[root@CentOS]# mkdir test1 test2
[root@CentOS]# touch test3.txt
[root@CentOS]# ln -s / link-to-root
```

Bước 13. Trên máy thật Windows, mở Web Browser và truy cập vào website **web.ipmac.lab/safe** để xem danh mục các file/folder bên trong thư mục **safe**. Click vào đường dẫn **link-to-root** để thấy toàn bộ nội dung thư mục / của hệ thống đã bị liệt kê ra.

Cấu hình không cho phép sử dụng Symbolic Link trong thư mục

Bước 14. Backup file cấu hình **httpd.conf**.

```
[root@CentOS]# cd /etc/httpd/conf
[root@CentOS]# cp httpd.conf httpd.conf.bk
```

Bước 15. Chỉnh sửa file **httpd.conf** và chèn thêm nội dung như bên dưới (phần không in nghiêng) để không cho phép sử dụng symlink bên trong thư mục **safe**. Sau khi chỉnh sửa xong, restart lại dịch vụ **httpd**

```
[root@CentOS]# vi /etc/httpd/conf/httpd.conf
...
<Directory "/var/www/html">      #Đây là nội dung có sẵn trong httpd.conf
...
</Directory>                    #Chèn nội dung xuống bên dưới phần này

<Directory "/var/www/html/safe">
    Options -FollowSymLinks
</Directory>
...
[root@CentOS]# service httpd restart
```

Bước 16. Trên máy thật Windows, refresh lại trang **web.ipmac.lab/safe** để thấy đường dẫn **link-to-root** đã mất

Cấu hình không cho phép liệt kê nội dung thư mục

Bước 17. Chỉnh sửa file **httpd.conf** và chèn thêm nội dung như bên dưới (phần không in nghiêng) để không cho phép liệt kê danh sách các file/folder bên trong thư mục **safe**. Sau khi chỉnh sửa xong, restart lại dịch vụ **httpd**

```
[root@CentOS]# vi /etc/httpd/conf/httpd.conf
...
<Directory "/var/www/html/safe">
    Options -FollowSymLinks -Indexes
</Directory>
...
[root@CentOS]# service httpd restart
```

Bước 18. Trên máy thật Windows, refresh lại trang **web.ipmac.lab/safe** để thấy việc truy cập vào nội dung trang này đã bị chặn lại

Bước 19. Tạo trang **index.html** bên trong thư mục **safe**

```
[root@CentOS]# vi /var/www/html/safe/index.html
<html>
<body>
```

```
Welcome to the safe site
</body>
</html>
```

Bước 20. Trên máy thật Windows, refresh lại trang **web.ipmac.lab/safe** để thấy nội dung của **index.html** đã được hiển thị

Cấu hình yêu cầu xác thực người dùng khi truy cập

Bước 21. Tạo cơ sở dữ liệu người dùng để xác thực truy cập, trong cơ sở dữ liệu này sẽ chứa thông tin về người dùng có tên là **ipmac**. Nhập thông tin về password cho người dùng này.

```
[root@CentOS]# htpasswd -c /etc/httpd/conf/safe.htpasswd ipmac
New password:
Re-type new password:
Adding password for user ipmac
```

Bước 22. Chỉnh sửa file **httpd.conf** và chèn thêm nội dung như bên dưới (phần không in nghiêng) để yêu cầu người dùng phải xác thực khi truy cập vào thư mục **safe**. Sau khi chỉnh sửa xong, restart dịch vụ **httpd**.

```
[root@CentOS]# vi /etc/httpd/conf/httpd.conf
...
<Directory "/var/www/html/safe">
    Options -FollowSymLinks -Indexes
    AuthType basic
    AuthName "This is a protected site"
    AuthUserFile /etc/httpd/conf/safe.htpasswd
    Require user ipmac
</Directory>
...
[root@CentOS]# service httpd restart
```

Bước 23. Trên máy thật Windows, refresh lại trang **web.ipmac.lab/safe** để thấy việc truy cập vào trang web này đã yêu cầu phải xác thực người dùng.

IV. Cấu hình Virtual Host

Cấu hình IP-Based Virtual Host

Bước 24. Bổ sung thêm Virtual IP với địa chỉ 192.168.1.2 cho interface **eth0** của máy ảo Linux

```
[root@CentOS]# ifconfig eth0:1 192.168.1.2/24
```

Bước 25. Cấu hình lại dịch vụ DNS và tạo các bản ghi cho **web1.ipmac.lab** và **web2.ipmac.lab**

```
web1    IN A    192.168.1.1
```

```
web2    IN A    192.168.1.2
```

(Trong trường hợp không có máy chủ DNS có thể chỉnh sửa file

C:\Windows\System32\drivers\etc\hosts trên máy Windows và chỉnh sửa thêm như sau:

```
192.168.1.1    web1.ipmac.lab
```

```
192.168.1.2    web2.ipmac.lab
```

)

Bước 26. Tạo các thư mục **vhost1** và **vhost2** bên trong **/var/www/html** và các trang **index.html** bên trong các thư mục này

```
[root@CentOS]# cd /var/www/html
[root@CentOS]# mkdir vhost1 vhost2
[root@CentOS]# echo "This is Virtual Host 1" > vhost1/index.html
[root@CentOS]# echo "This is Virtual Host 2" > vhost2/index.html
```

Bước 27. Khôi phục lại file **httpd.conf** gốc (đã được backup ở **Bước 14**)

```
[root@CentOS]# cd /etc/httpd/conf
[root@CentOS]# rm httpd.conf
[root@CentOS]# cp httpd.conf.bk httpd.conf
```

Bước 28. Chỉnh sửa file **httpd.conf** và chèn thêm nội dung như bên dưới vào cuối file để mô tả các Virtual Host dựa trên địa chỉ IP. Sau khi chỉnh sửa xong, restart dịch vụ **httpd**.

```
[root@CentOS]# vi /etc/httpd/conf/httpd.conf
...
<VirtualHost 192.168.1.1>
    DocumentRoot /var/www/html/vhost1/
</VirtualHost>

<VirtualHost 192.168.1.2>
    DocumentRoot /var/www/html/vhost2/
</VirtualHost>
[root@CentOS]# service httpd restart
```

Bước 29. Trên máy thật Windows, lần lượt truy cập vào các trang **web1.ipmac.lab** và **web2.ipmac.lab** để xem các nội dung trên từng Virtual Host.

Cấu hình Name-Based Virtual Host

Bước 30. Gỡ bỏ Virtual IP trên interface eth0 của máy ảo Linux

```
[root@CentOS]# ifconfig eth0:1 down
```

Bước 31. Cấu hình lại dịch vụ DNS và sửa lại các bản ghi cho **web1.ipmac.lab** và **web2.ipmac.lab**

```
web1    IN A      192.168.1.1
web2    IN CNAME  web1
```

(Trong trường hợp không có máy chủ DNS có thể chỉnh sửa file

C:\Windows\System32\drivers\etc\hosts trên máy Windows và chỉnh sửa như sau:

```
192.168.1.1    web1.ipmac.lab  web2.ipmac.lab
)
```

Bước 32. Khôi phục lại file **httpd.conf** gốc (đã được backup ở **Bước 14**)

```
[root@CentOS]# cd /etc/httpd/conf
[root@CentOS]# rm httpd.conf
[root@CentOS]# cp httpd.conf.bk httpd.conf
```

Bước 33. Chỉnh sửa file **httpd.conf** và chèn thêm nội dung như bên dưới vào cuối file để mô tả các Virtual Host dựa trên domain name. Sau khi chỉnh sửa xong, restart dịch vụ **httpd**.

```
[root@CentOS]# vi /etc/httpd/conf/httpd.conf
...
NameVirtualHost 192.168.1.1
```

```
<VirtualHost 192.168.1.1>
    DocumentRoot /var/www/html/vhost1/
    ServerName    web1.ipmac.lab
</VirtualHost>

<VirtualHost 192.168.1.1>
    DocumentRoot /var/www/html/vhost2/
    ServerName    web2.ipmac.lab
</VirtualHost>
[root@CentOS]# service httpd restart
```

Bước 34. Trên máy thật Windows, lần lượt truy cập vào các trang **web1.ipmac.lab** và **web2.ipmac.lab** để xem các nội dung trên từng Virtual Host.