

**BAN CƠ YẾU CHÍNH PHỦ  
HỌC VIỆN KỸ THUẬT MẬT MÃ**

**Module thực hành  
THIẾT LẬP AN TOÀN CHO DỊCH VỤ  
VÀ HỆ ĐIỀU HÀNH MẠNG**

**ThS. Cao Minh Tuấn**

**HÀ NỘI, 2017**

## MỤC LỤC

MỤC LỤC.....	1
BÀI 1. THỰC HÀNH THIẾT LẬP KIỂM SOÁT TRUY CẬP TỚI TÀI NGUYÊN TRÊN LINUX, WINDOWS, TÀI NGUYÊN CHIA SẺ.....	3
<b>1.1    Thiết lập kiểm soát truy cập tới tài nguyên lưu trữ .....</b>	<b>3</b>
1.1.1    Thiết lập kiểm soát truy cập tới tài nguyên lưu trữ trên Windows.	3
1.1.2    Thiết lập kiểm soát truy cập tới tài nguyên lưu trữ trên Linux ....	24
<b>1.2    Thiết lập kiểm soát truy cập tới tài nguyên chia sẻ .....</b>	<b>32</b>
1.2.1    Phân quyền tới tài nguyên chia sẻ trên Windows Server 2012 ....	32
1.2.2    Phân quyền tới tài nguyên chia sẻ trên Linux CentOS 6.5.....	42
BÀI 2. THỰC HÀNH THIẾT LẬP MẬT KHẨU AN TOÀN .....	43
<b>2.1    Thực hành thiết lập mật khẩu an toàn .....</b>	<b>43</b>
2.1.1    Thiết lập mật khẩu an toàn Windows Server 2012.....	43
2.1.2    Thiết lập mật khẩu an toàn trên hệ điều hành Windows 7.....	48
2.1.3    Thiết lập mật khẩu an toàn trên hệ điều hành Linux CentOS 6.5	52
BÀI 3. THỰC HÀNH THIẾT LẬP SỬ DỤNG SSL ĐỂ MÃ HÓA CHO DỊCH VỤ WEB, MAIL.....	60
<b>3.1    Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ web.....</b>	<b>60</b>
3.1.1    Cài đặt DNS trên máy chủ Windows Server 2012.....	60
3.1.2    Cài đặt dịch vụ web IIS 8 trên máy chủ Windows Server 2012 ...	67
3.1.3    Cài đặt dịch vụ Certification Authority (CA).....	71
3.1.4    Cấu hình SSL cho dịch vụ Web.....	73
<b>3.2    Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ Mail.....</b>	<b>78</b>
3.2.1    Tạo bản ghi MX trong DNS, tắt tường lửa của Server 2012 .....	79
3.2.2    Cài đặt phần mềm Mdaemon, tạo tài khoản mail client .....	81
3.2.3    Cài đặt phần mềm Mail Client để gửi và nhận mail .....	83

3.2.4	<i>Cấp chứng thư số cho người dùng user1 và user2.....</i>	85
3.2.5	<i>Gửi thư có mã hóa và ký số.....</i>	91
	Tài liệu tham khảo.....	93

# **BÀI 1. THỰC HÀNH THIẾT LẬP KIỂM SOÁT TRUY CẬP TỚI TÀI NGUYÊN TRÊN LINUX, WINDOWS, TÀI NGUYÊN CHIA SẺ**

## **1.1 Thiết lập kiểm soát truy cập tới tài nguyên lưu trữ**

### *1.1.1 Thiết lập kiểm soát truy cập tới tài nguyên lưu trữ trên Windows*

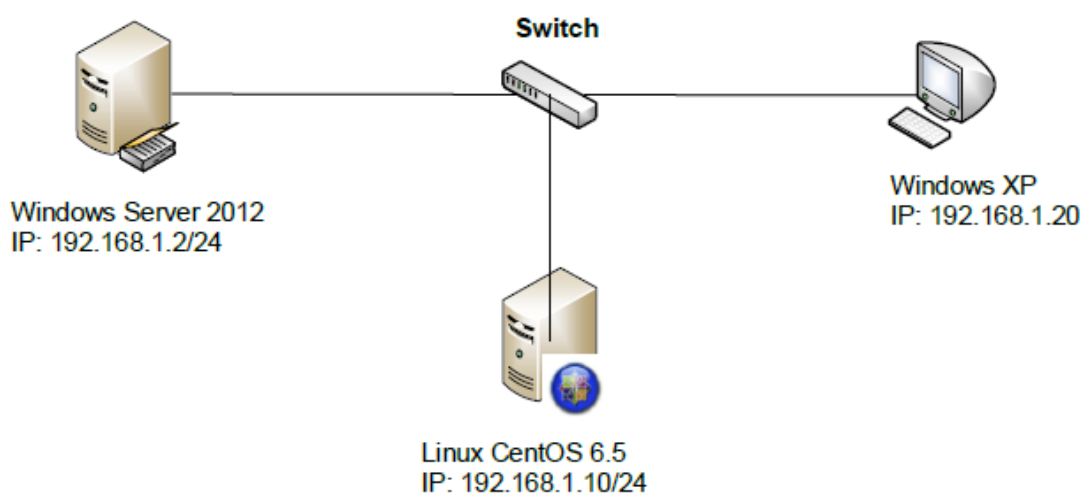
#### **Mục đích bài thực hành:**

Bài thực hành hướng dẫn sinh viên phân quyền truy cập tới các tài nguyên lưu trữ trên hệ điều hành Windows Server 2012, hệ điều hành Linux CentOS 6.5. Nhằm mục đích bảo vệ dữ liệu tương ứng cho người dùng. Bài thực hành cũng hướng dẫn phân quyền tới tài nguyên chia sẻ.

#### **Yêu cầu hệ thống:**

- Máy chủ chạy hệ điều hành Windows Server 2012
- Máy chủ chạy hệ điều hành Linux CentOS 6.5
- Máy trạm chạy hệ điều hành Windows XP

#### **Mô hình cài đặt:**

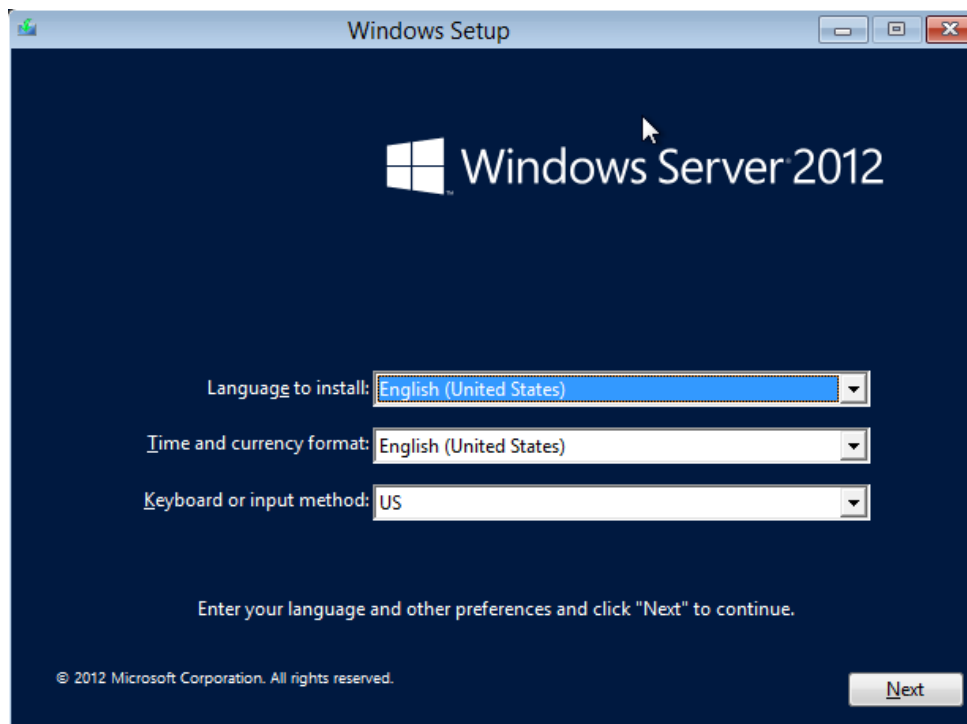


#### **Các bước triển khai:**

Triển khai trên hệ điều hành máy chủ Windows Server 2012

#### **Bước 1: Cài đặt hệ điều hành**

Cho đĩa cài đặt hoặc USB có năng boot chứa hệ điều hành Windows Server 2012 vào máy chủ. Màn hình đầu tiên xuất hiện như sau:

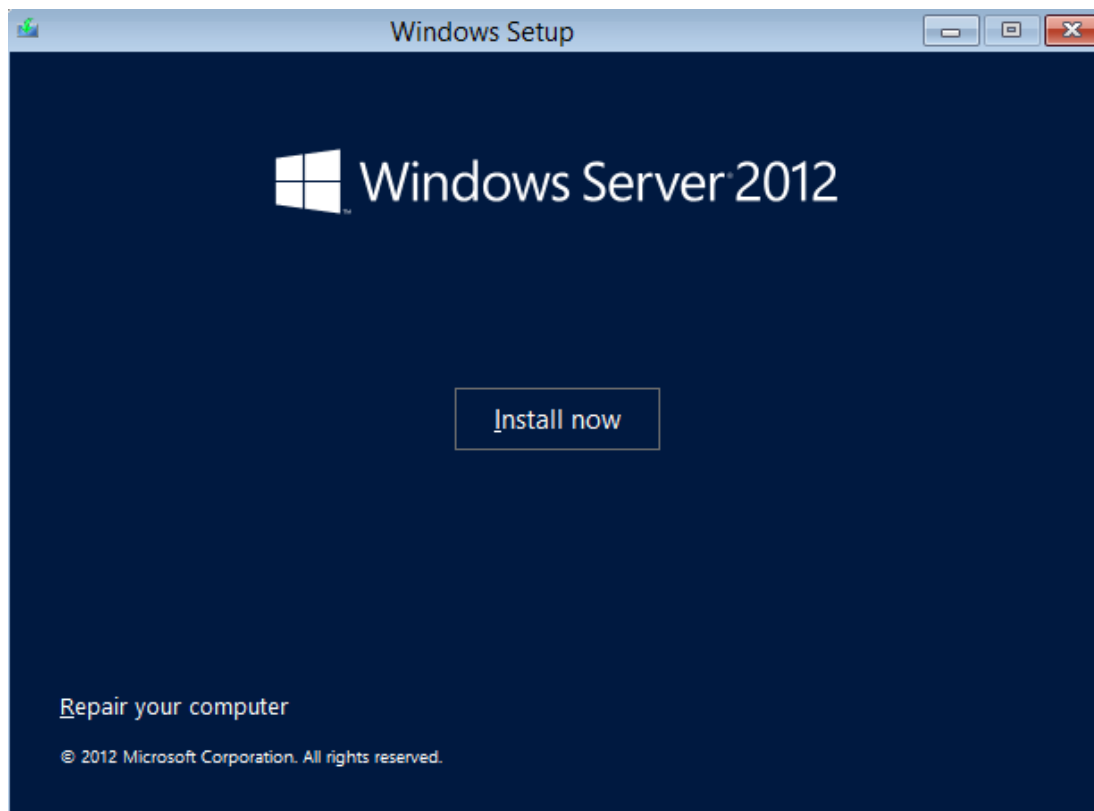


Lựa chọn ngôn ngữ mặc định là: English (United States)

Lựa chọn thời gian và định dạng mặc định: English (United States), không phải là múi giờ.

Lựa chọn chế độ bàn phím mặc định: US

Nhấn Next để tiếp tục cài đặt.



Ở bước này hệ điều hành cho 2 tùy chọn:

- Tùy chọn cài đặt mới (Install now): Cài đặt hệ điều hành này là bản cài đặt mới.
- Tùy chọn sửa chữa hệ điều hành đã có sẵn (Repair your computer): Sử dụng trong trường hợp đã cài hệ điều hành Windows Server 2012 trước đó và trong quá trình sử dụng gặp sự cố xảy ra do phần mềm. Thì sử dụng tùy chọn này để sửa chữa lại hệ điều hành.

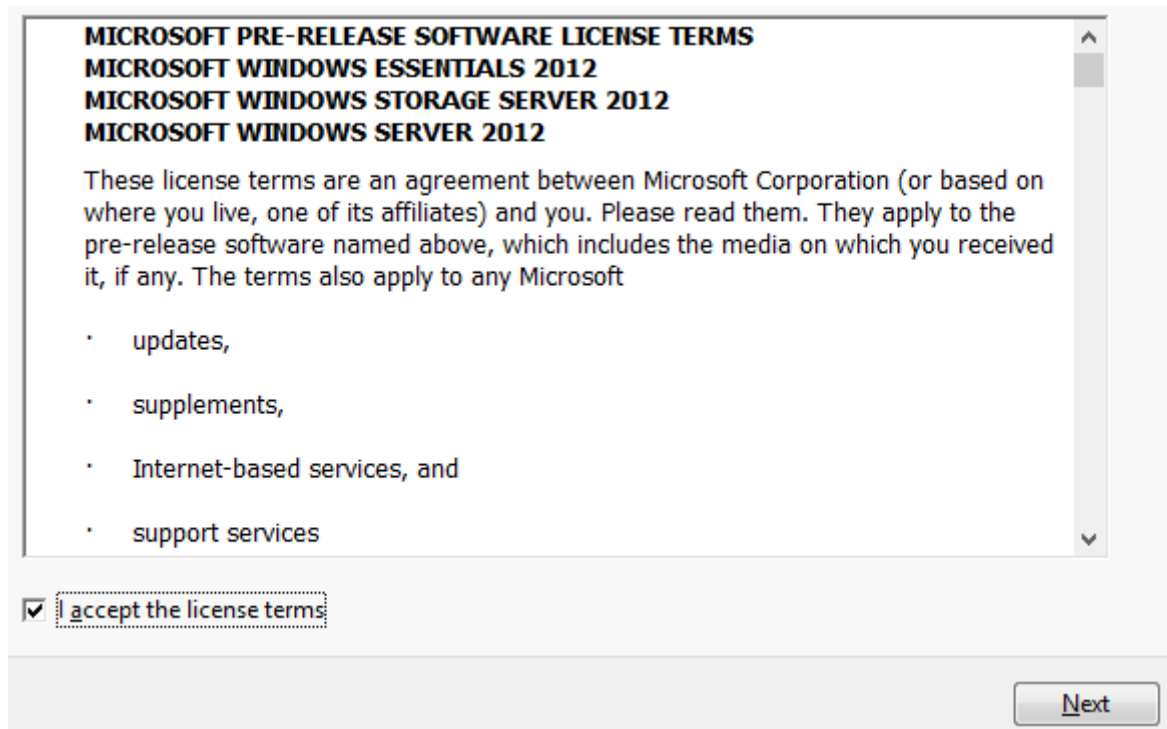
Trong bài thực hành này thực hiện cài mới nên chọn Install now.

Trong màn hình tiếp theo có 2 tùy chọn như sau:

Operating system	Architecture	D
Windows Server 2012 Release Candidate Datacenter (Server Core Installation)	x64	5/
Windows Server 2012 Release Candidate Datacenter (Server with a GUI)	x64	5/

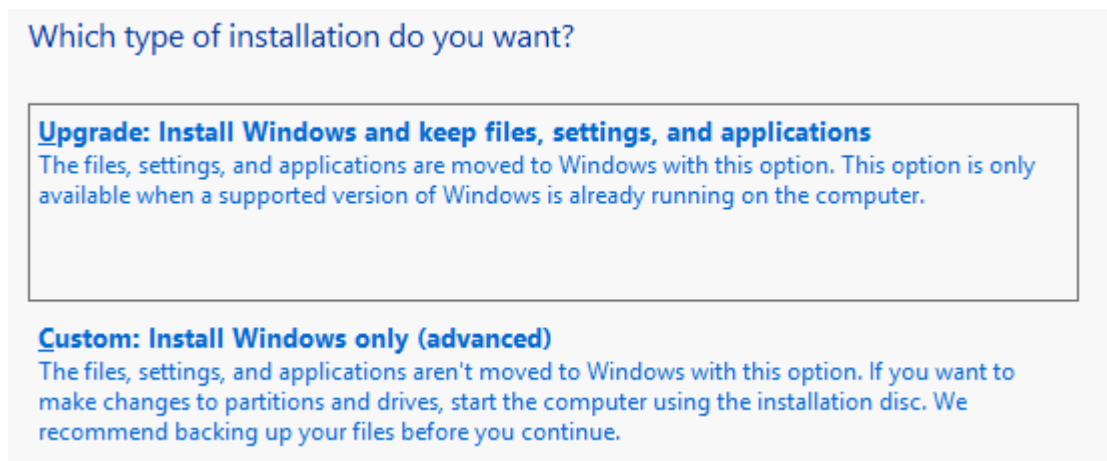
- Tùy chọn thứ nhất cài đặt hệ điều hành với chức năng tối giản (Server Core), cài đặt tùy chọn này hệ điều hành sẽ hạn chế cài đặt nhiều chức năng giúp đảm bảo an toàn cho hệ điều hành, chỉ sử dụng dòng lệnh để quản trị.
- Tùy chọn thứ hai cài đặt hệ điều hành với chế độ đồ họa.

Chọn tùy chọn thứ hai để tiếp tục quá trình cài đặt.



Tích vào tùy chọn chấp nhận giấy phép, chọn Next để tiếp tục.

Màn hình tiếp theo xuất hiện với 2 tùy chọn cài đặt:

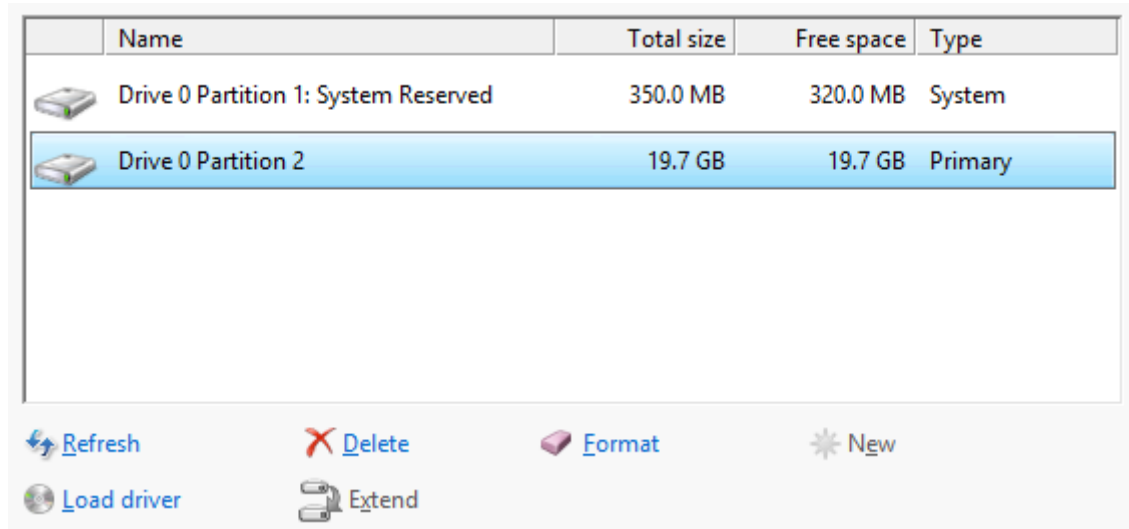


Hai tùy chọn này có ý nghĩa như sau:

- Upgrade: Cài đặt hệ điều hành mà trên máy chủ đã có sẵn hệ điều hành: Windows Server 2012, Windows Server 2008, Windows Server 2003...Sau khi cài đặt xong vẫn giữ lại hệ điều hành cũ.
- Custom: sử dụng tùy chọn này khi cài đặt mới hoặc muốn định dạng lại phân vùng lưu trữ.

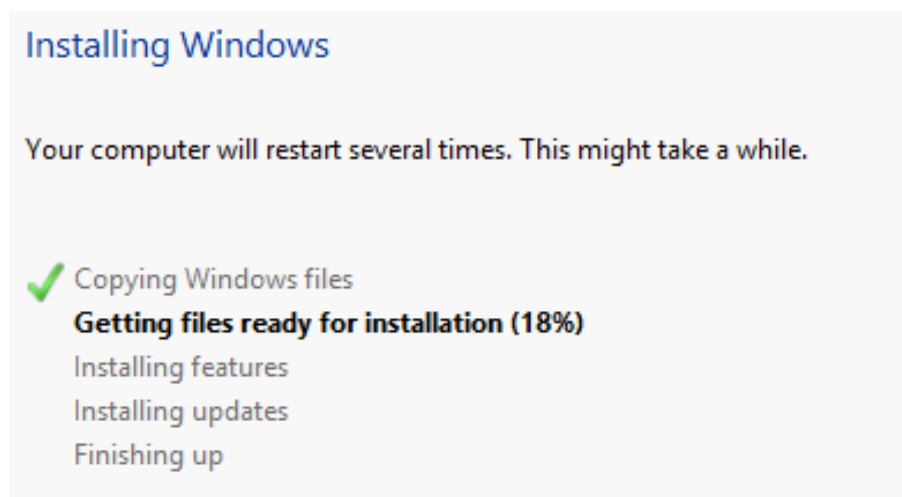
Trong bài thực hành này sử dụng tùy chọn thứ 2.

Màn hình tiếp tục tạo mới và định dạng phân vùng lưu trữ:



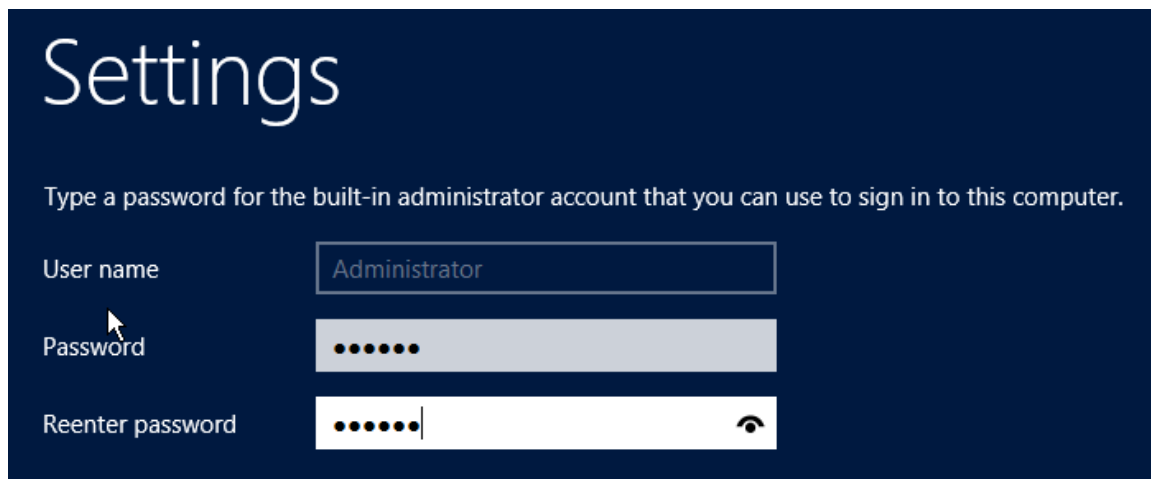
Chọn phân vùng Primary và chọn Next.

Quá trình cài đặt hệ điều hành tự động thực hiện:



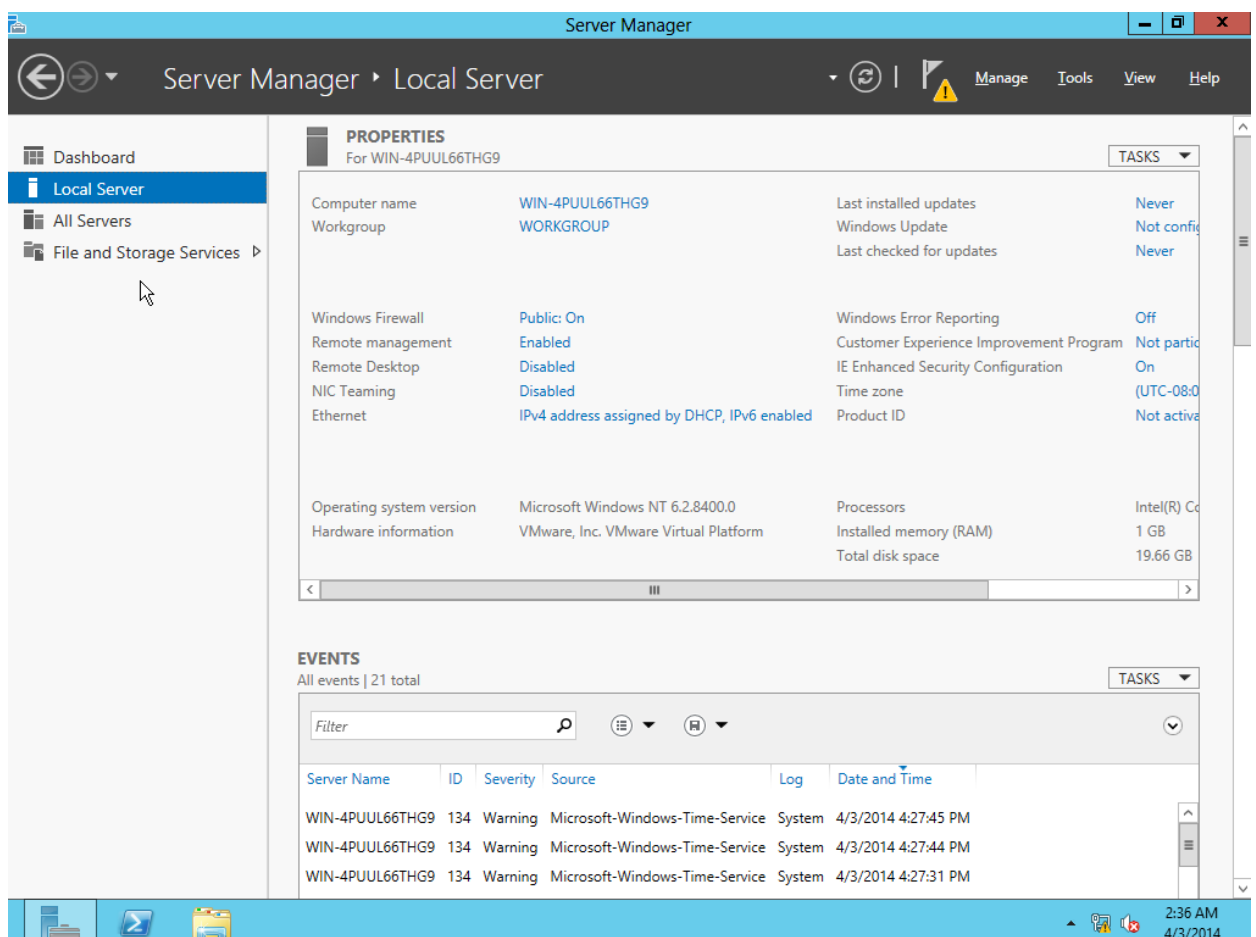
Quá trình sau khi cài đặt kết thúc, cài đặt mật khẩu cho tài khoản quản trị Administrator:





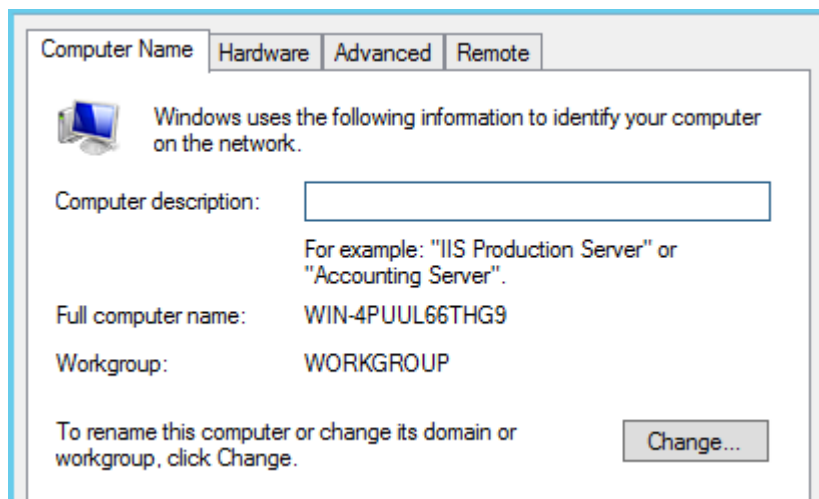
Kết thúc quá trình cài đặt.

Màn hình sau khi đăng nhập vào Windows Server 2012:

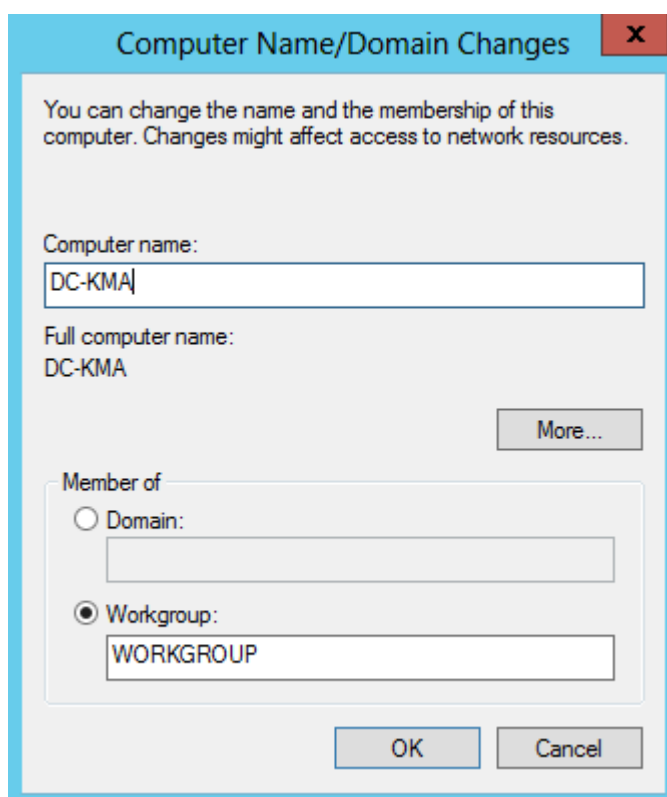


Thực hiện đổi tên mặc định của máy chủ:

Vào Local Server → Computer name → kích chuột vào tên mặc định.



Tab Computer Name chọn Change.

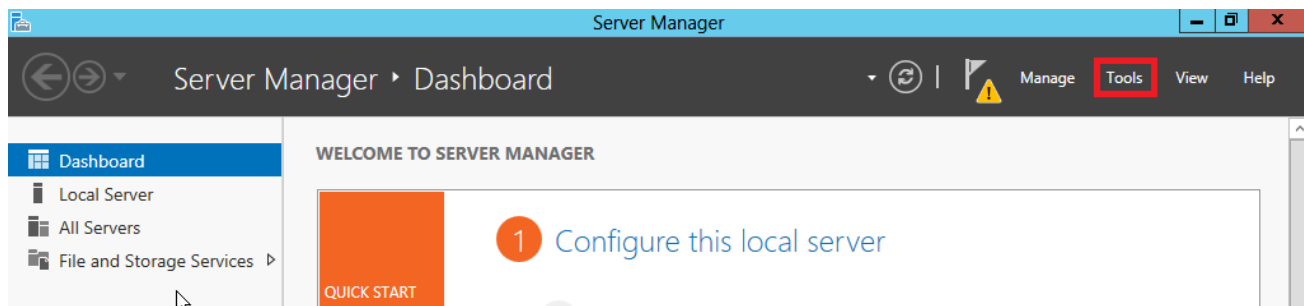


Nhập tên máy chủ cần thay đổi, ví dụ: DC-KMA.

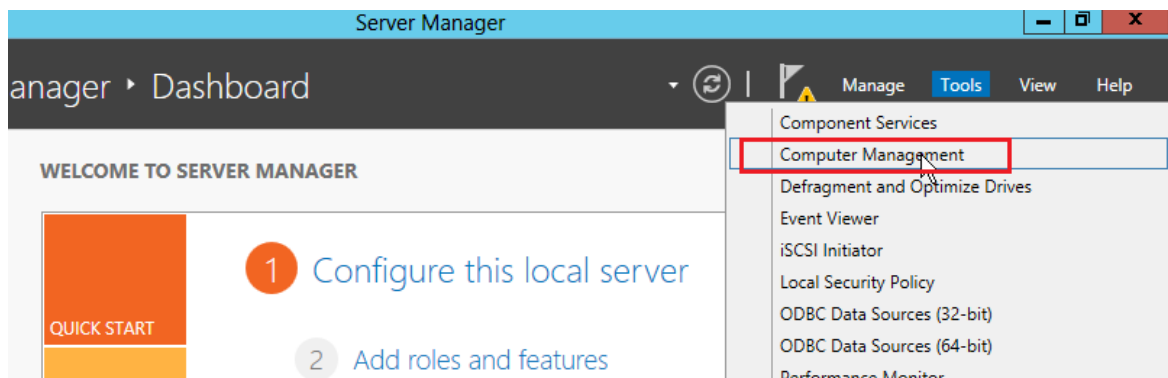
Chọn OK và khởi động lại máy.

**Bước 2: Tạo người dùng và nhóm người dùng để phân quyền truy cập**

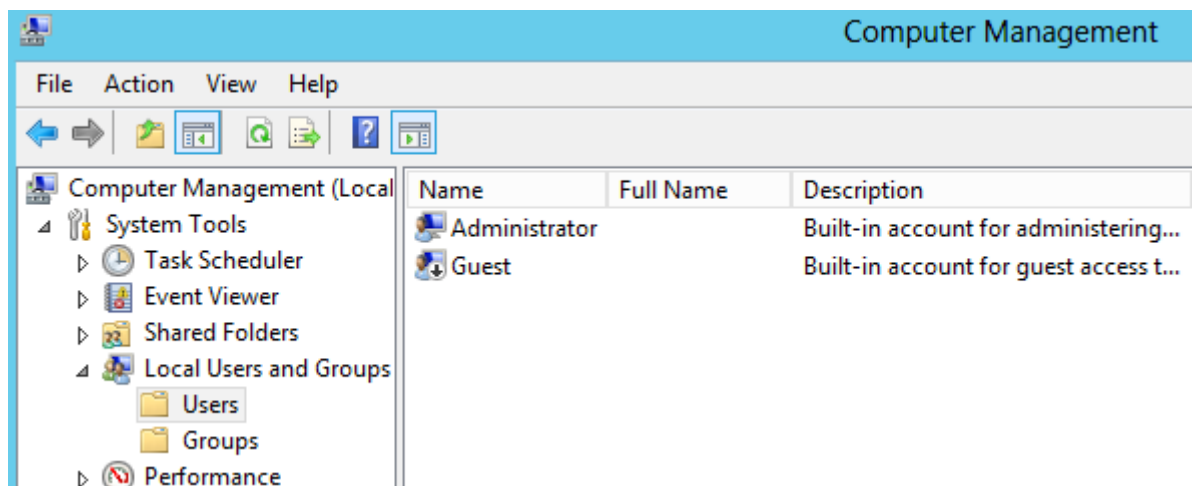
Bật Server Manager, chọn công cụ Tools ở góc bên phải phía trên.



Trong danh sách thả xuống chọn Computer Management:



Cửa sổ mới xuất hiện và chọn chức năng Local User and Groups như hình dưới đây:



Trong mục Users lần lượt tạo các người dùng: giaovien1, giaovien2, sinhvien1, sinhvien2. Thực hiện như sau:

Chuột phải vào Users → New User

Thực hiện tương tự cho giaovien2, sinhvien1, sinhvien2

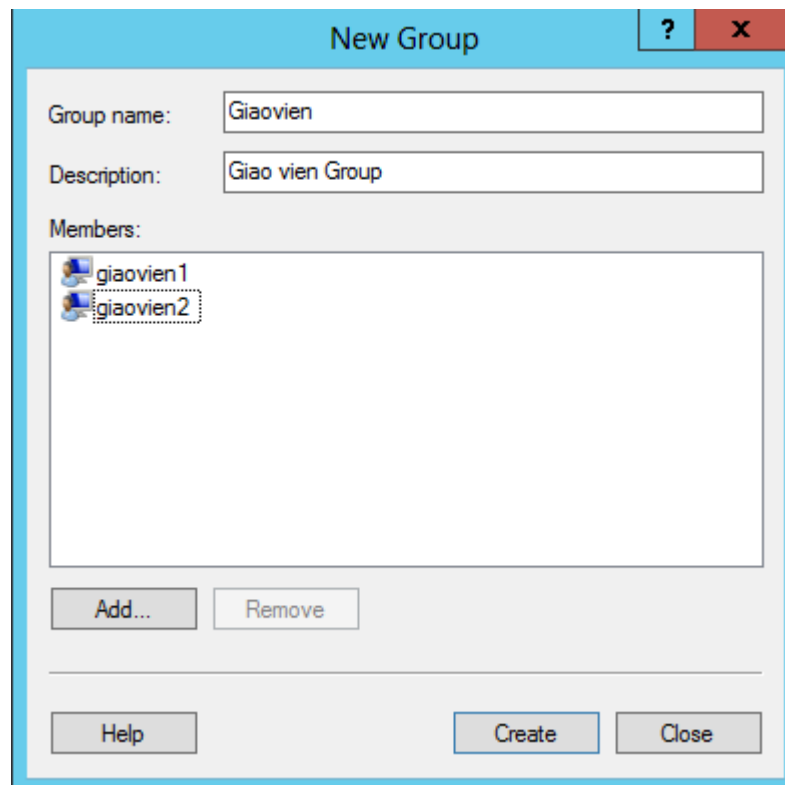
Hình ảnh sau khi tạo xong 4 tài khoản trên:

Name	Full Name	Description
Administrator		Built-in account for administering...
giaovien1	Giao vien 1	Tai khoan giao vien 1
giaovien2	Giao vien 2	Tai khoan giao vien 2
Guest		Built-in account for guest access t...
sinhvien1	Sinh vien 1	Tai khoan sinh vien 1
sinhvien2	Sinh vien 2	Tai khoan sinh vien 2

Tiếp tục trong mục Groups lần lượt tạo 2 nhóm đối tượng là: GiaoVien, SinhVien.

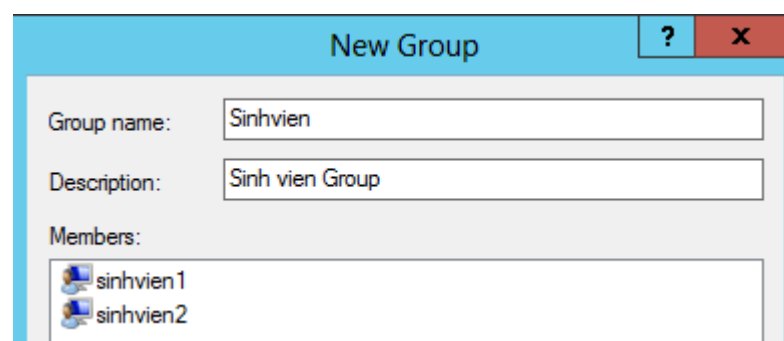
Chuột phải vào Groups → New Group

Nhập tên của nhóm là Giao Vien

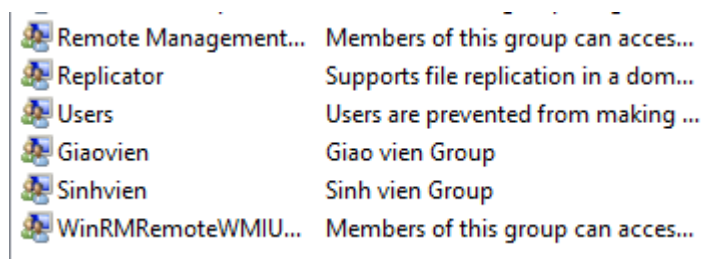


Trong mục Members trở đến 2 người dùng giaovien1 và giaovien2.  
Nhấn Create để tạo nhóm.

Tương tự tạo nhóm SinhVien.

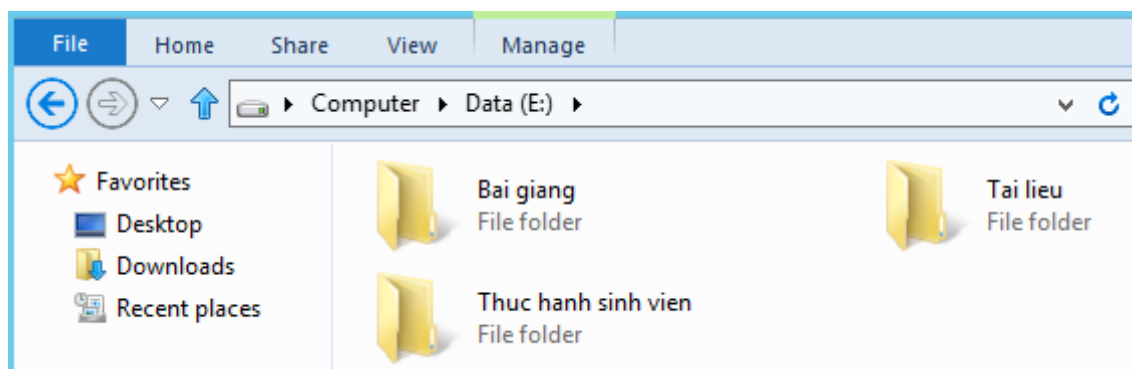


Kết quả sau khi tạo xong 2 nhóm đối tượng: Giao Vien, Sinh Vien.



**Bước 3:** Tạo dữ liệu lưu trữ để phân quyền truy cập

Thêm phân vùng ổ D và tạo thư mục cho mỗi nhóm như sau:



Thư mục Bài giảng chứa bài giảng của mỗi giáo viên. Thư mục này chỉ có thành viên trong nhóm Giáo viên mới được truy cập vào. Còn thành viên trong nhóm sinh viên không được phép truy cập vào thư mục này. Trong thư mục Bài giảng cũng tạo các thư mục con tương ứng cho mỗi giáo viên, và mỗi giáo viên chỉ được phép truy cập vào thư mục tương ứng của mình. Tài khoản quản trị Administrator có toàn quyền.

Thư mục Tài liệu dùng chung cho cả giáo viên và sinh viên. Trong thư mục này tất cả các thành viên của 2 nhóm đều được phép truy cập vào. Nhưng chỉ thành viên trong nhóm Giáo viên mới có quyền tạo, xóa, chỉnh sửa, sao chép còn thành viên trong nhóm sinh viên chỉ được phép đọc, sao chép.

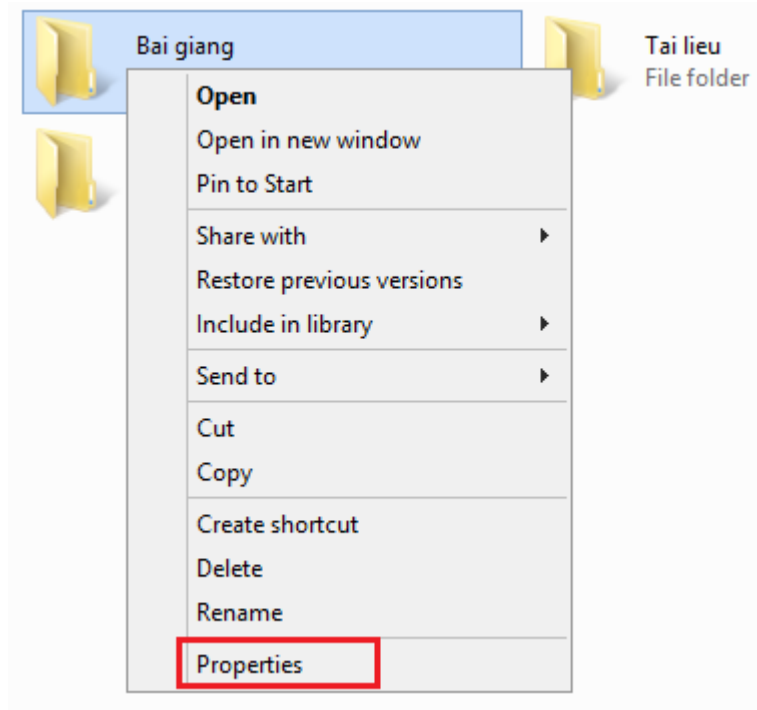
Thư mục Thực hành sinh viên chứa bài thực hành cho sinh viên. Thư mục này chứa các bài thực hành của sinh viên mà nhóm giáo viên có quyền tạo, xóa, chỉnh sửa, sao chép và sinh viên quyền tạo, sao chép, đọc.

**Bước 4:** Phân quyền để kiểm soát truy cập tới tài nguyên lưu trữ đã tạo ở trên

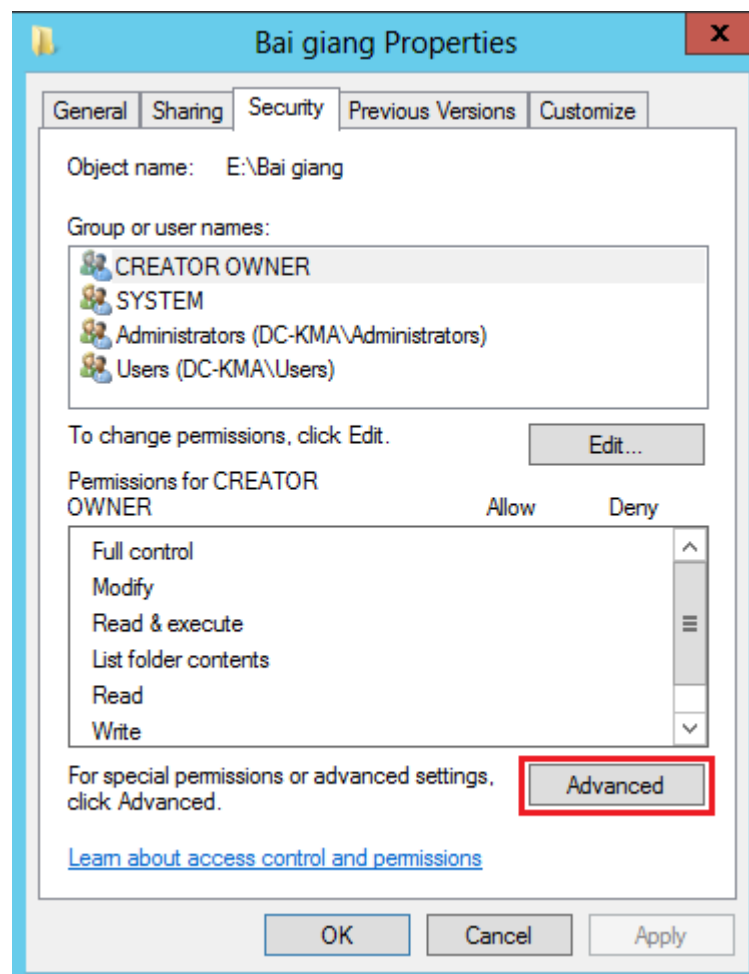
Để thực hiện được các yêu cầu ở bước 3, thực hiện phân quyền lần lượt với mỗi thư mục như sau:

- Thư mục Bài giảng:

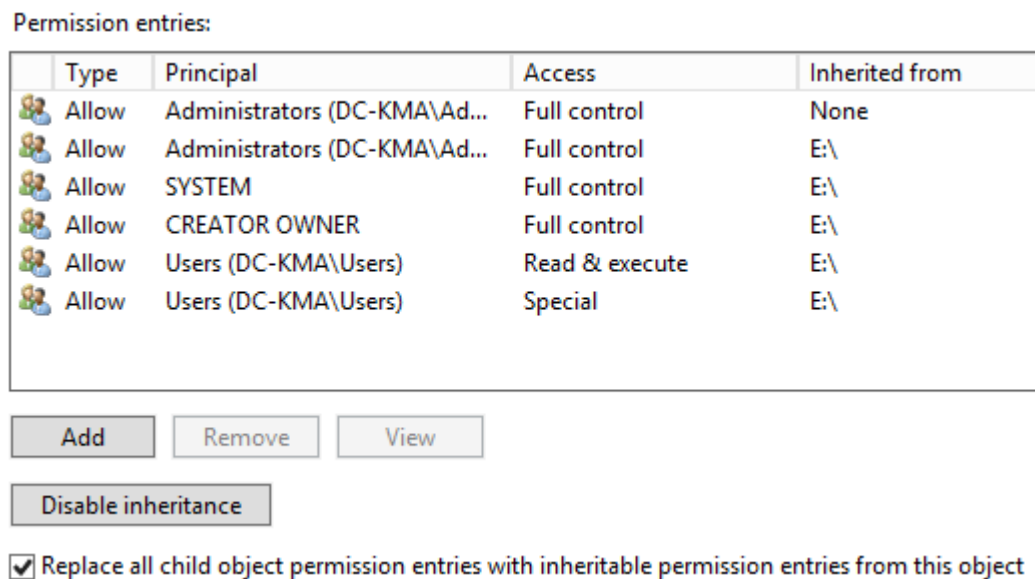
Chuột phải vào thư mục → Properties



Chọn tab Security → chọn Advanced:

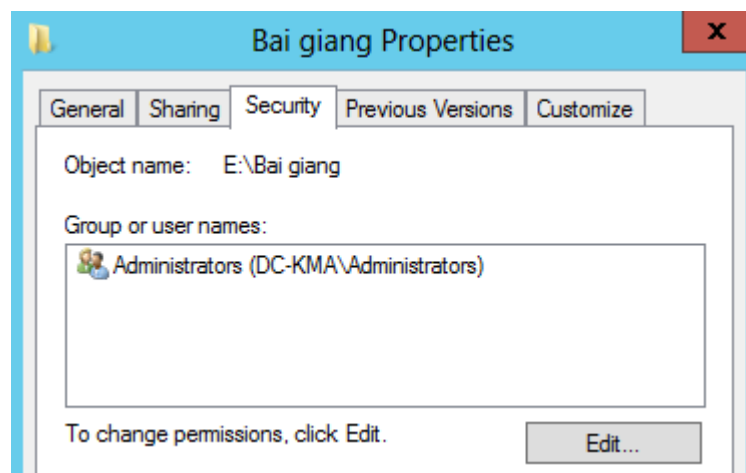


Tích vào tùy chọn Replace all child object permission entries... Và kích vào tùy chọn Disable inheritance để gỡ bỏ toàn bộ quyền đã có sẵn đối với thư mục này:



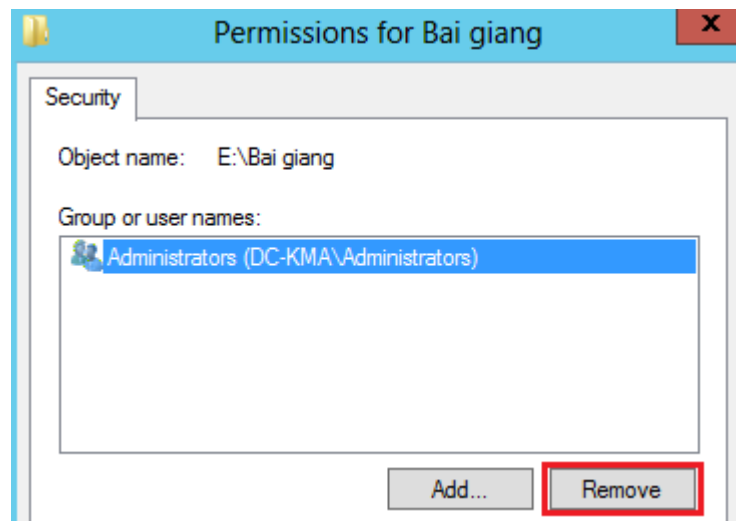
Apply → OK

Tiếp tục quay trở lại tab Security chọn Edit:



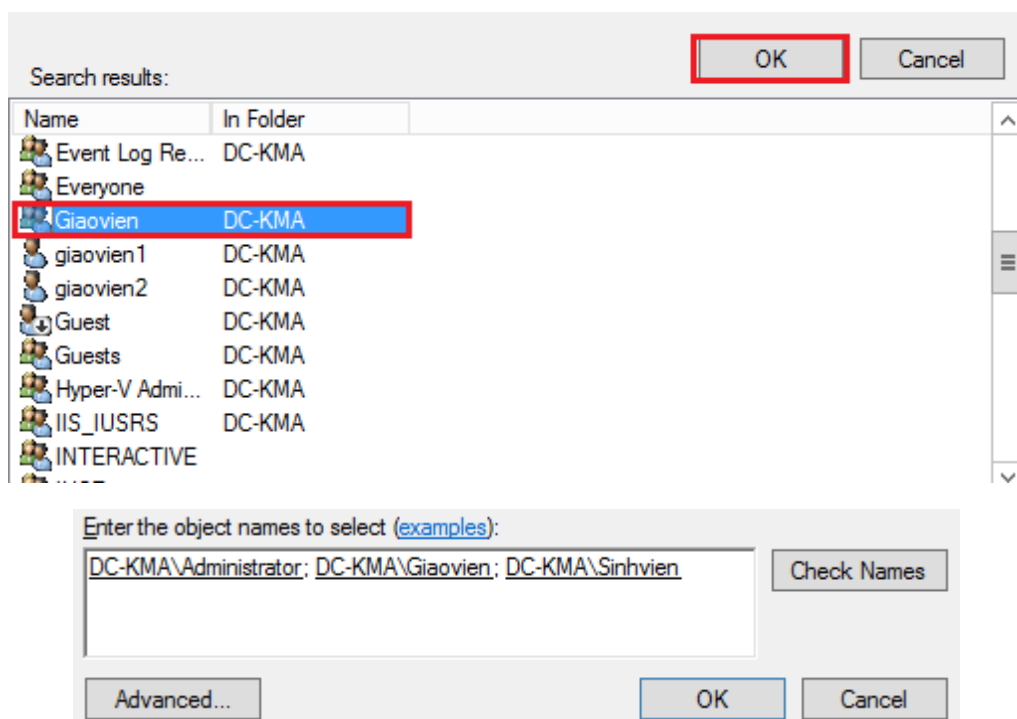
Chọn nhóm Administrators → chọn Remove nhằm gỡ bỏ tất cả những thành viên trong nhóm Administrators.





Tiếp tục chọn Add để thêm những người dùng cần phân quyền:

Add → Advanced → Find now, lần lượt chọn các đối tượng: Administrator, group giáo viên, group sinh viên:



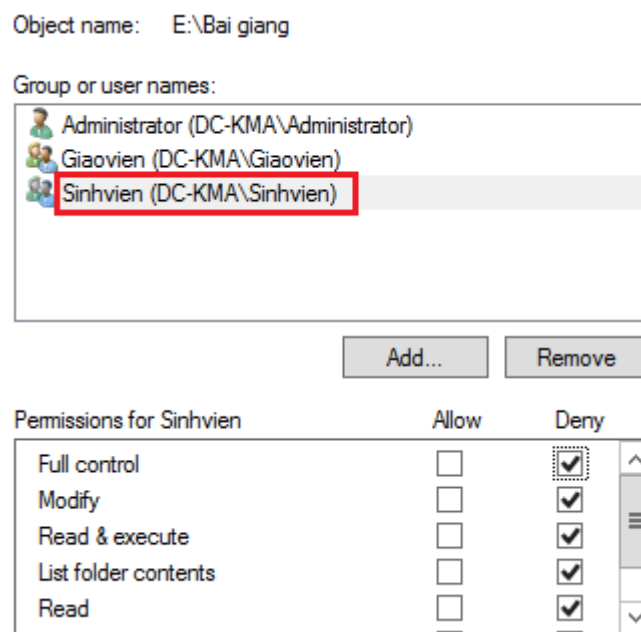
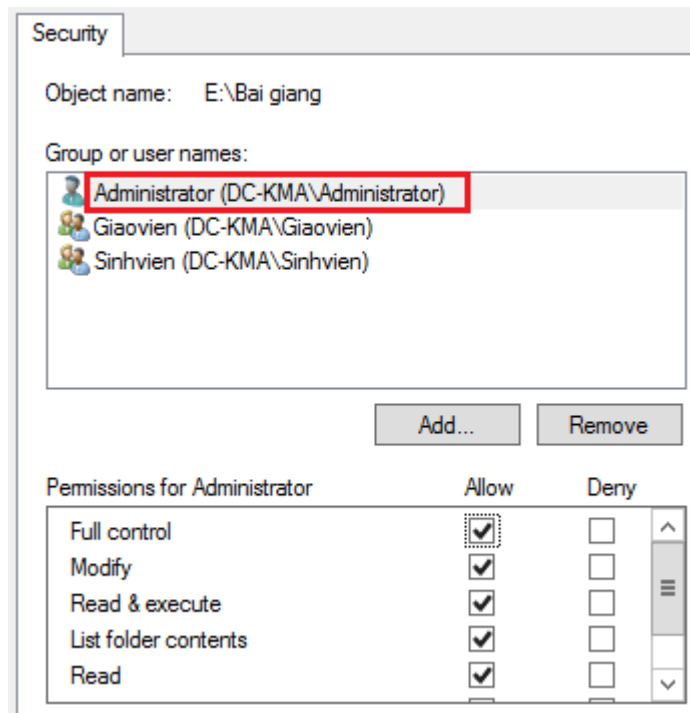
Nhấn OK để tiếp tục

Lần lượt chọn từng đối tượng để chọn quyền tương ứng:

Với tài khoản Administrator tích vào tùy chọn Full control.

Giaovien tích vào tùy chọn Full control.

Sinhvien tích vào tùy chọn Deny all.

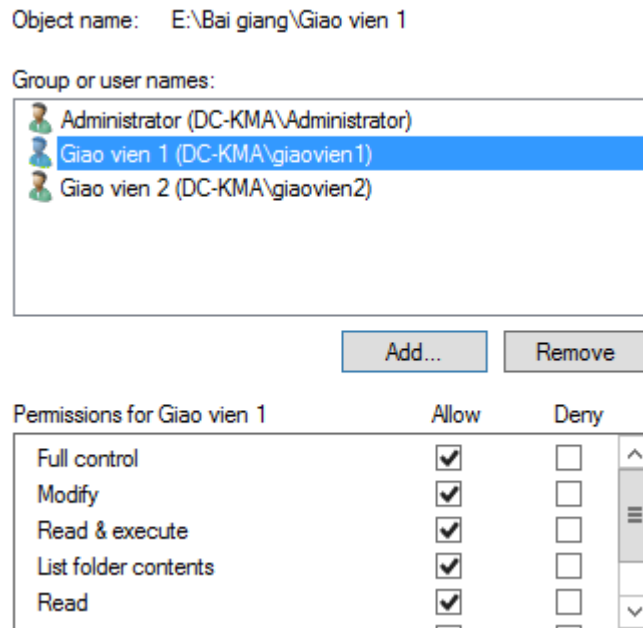


Apply → OK

Truy cập vào trong thư mục Bài giảng để phân quyền tiếp cho thư mục cho mỗi giáo viên tương ứng:

Thực hiện tương tự như thư mục Bài giảng, gỡ bỏ quyền thừa kế từ thư mục cha, và lần lượt thêm người dùng: administrot, giaovien1, giaovien2

Với thư mục của giáo viên 1 phân quyền như sau:



Đối với tài khoản Administrator tích vào Full control, giáo viên 2 tích vào Deny all → Apply → OK.

Đối với thư mục giáo viên 2 phân quyền cũng tương tự giáo viên 1, nhưng tài khoản giáo viên 2 là Full control và giáo viên 1 là Deny all.

Đến đây đã phân quyền xong cho thư mục Bài giảng

- Thư mục Tài liệu:

Tương tự thư mục Bài giảng đầu tiên gỡ bỏ quyền thừa kế. Sau đó tiếp tục thêm các đối tượng Administrator, group giáo viên, group sinh viên.

Với tài khoản Administrator tích vào tùy chọn Full control.

Group giáo viên với các quyền: Modify, Read & execute, List folder contents, Read, Write.

Object name: E:\Tai lieu

Group or user names:

Administrator (DC-KMA\Administrator)
<b>Giao vien (DC-KMA\Giao vien)</b>
Sinh vien (DC-KMA\Sinh vien)

Add... Remove

Permissions for Giao vien

	Allow	Deny	
Full control	<input type="checkbox"/>	<input type="checkbox"/>	^
Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>	≡
Read & execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
List folder contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	v

Group sinh viên với các quyền: Read & execute, List folder contents, Read

Object name: E:\Tai lieu

Group or user names:

Giao vien (DC-KMA\Giao vien)
<b>Sinh vien (DC-KMA\Sinh vien)</b>
Administrator (DC-KMA\Administrator)

Add... Remove

Permissions for Sinh vien

	Allow	Deny	
Modify	<input type="checkbox"/>	<input type="checkbox"/>	^
Read & execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>	≡
List folder contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Write	<input type="checkbox"/>	<input type="checkbox"/>	v

Apply - OK

Đến đây kết thúc phân quyền cho thư mục Tài liệu.

- Thư mục Thực hành sinh viên:

Tương tự như đối với hai thư mục trên, đầu tiên phải gỡ bỏ quyền thừa kế. Sau tiếp tục thêm các đối tượng: Administrator, group giáo viên, group sinh viên.

Lần lượt phân quyền tương ứng với các đối tượng:

Tài khoản Administrator tích vào tùy chọn Full control

Group giáo viên có các quyền: Modify, Read & execute, List folder contents, Read, Write.

Object name: E:\Thuc hanh sinh vien

Group or user names:

- Giaovien (DC-KMA\Giaovien)
- Sinhvien (DC-KMA\Sinhvien)
- Administrator (DC-KMA\Administrator)

Add... Remove

Permissions for Giaovien

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read & execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
List folder contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Group sinh viên có các quyền: Read & execute, List folder contents, Read, Write.

Object name: E:\Thuc hanh sinh vien

Group or user names:

- Giaovien (DC-KMA\Giaovien)
- Sinhvien (DC-KMA\Sinhvien)
- Administrator (DC-KMA\Administrator)

Add... Remove

Permissions for Sinhvien

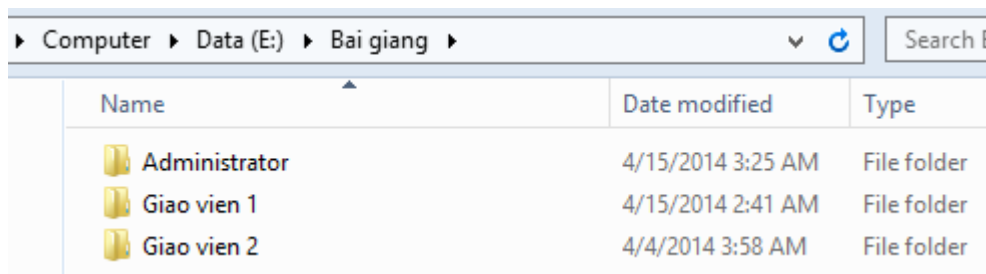
	Allow	Deny
Modify	<input type="checkbox"/>	<input type="checkbox"/>
Read & execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
List folder contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input type="checkbox"/>	<input type="checkbox"/>

Apply – OK

Đến đây kết thúc quá trình phân quyền.

**Bước 5:** Kiểm tra kết quả phân quyền:

- Thực hiện đăng nhập vào tài khoản Administrator, đăng nhập vào các thư mục Bài giảng, Tài liệu, Thực hành sinh viên. Mỗi thư mục tạo thư mục con tương ứng với tài khoản Administrator. Nếu tạo thành công tiếp tục thực hiện xóa thư mục vừa tạo.



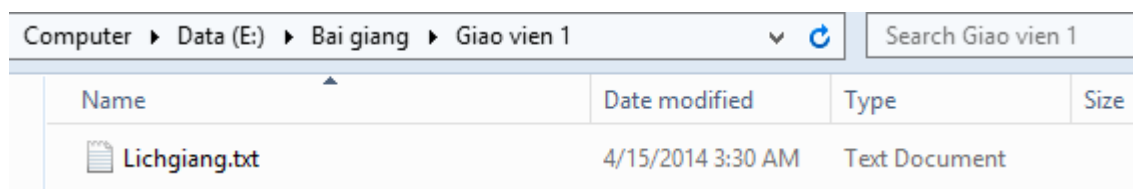
Name	Date modified	Type
Administrator	4/15/2014 3:25 AM	File folder
Giao vien 1	4/15/2014 2:41 AM	File folder
Giao vien 2	4/4/2014 3:58 AM	File folder

Thực hiện thành công.

- Thực hiện đăng nhập vào tài khoản giáo viên 1:



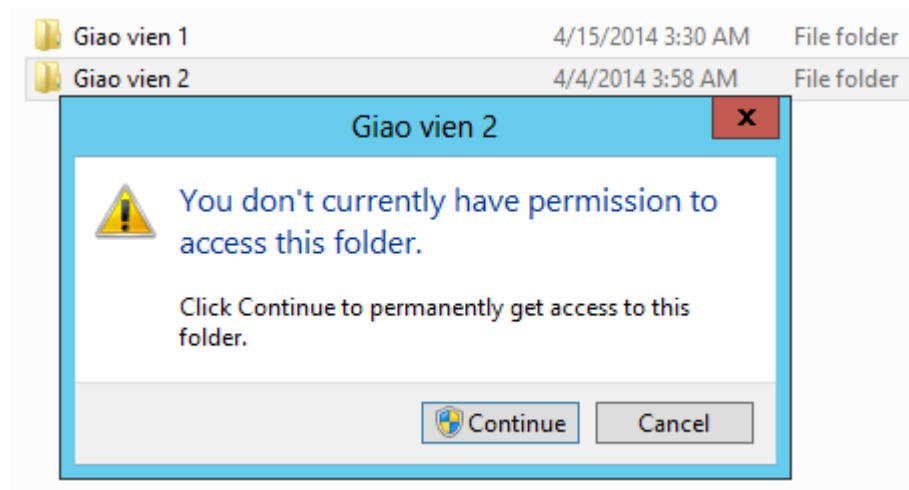
Thực hiện truy cập vào thư mục của giáo viên 1 và tạo tệp tin Lichgiang.txt



Name	Date modified	Type	Size
Lichgiang.txt	4/15/2014 3:30 AM	Text Document	

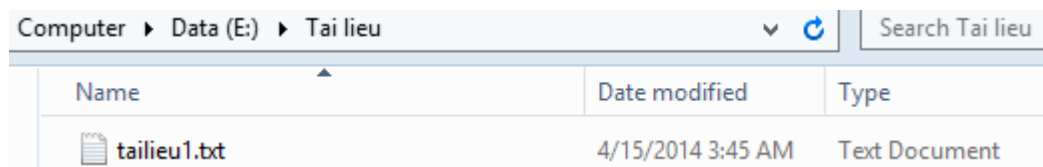
Thực hiện thành công.

Thử truy cập vào thư mục của giáo viên 2:



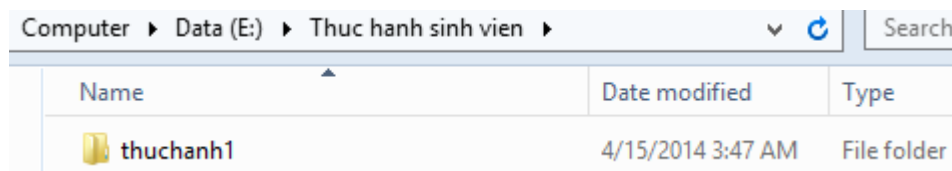
Kết quả không truy cập được vào thư mục của giáo viên 2 vì đã phân quyền cấm giáo viên 1 truy cập vào.

Truy cập vào thư mục Tài liệu và tạo tệp tin tailieu1.txt



Kết quả thành công.

Truy cập vào thư mục Thực hành sinh viên và tạo thư mục thuchanh1

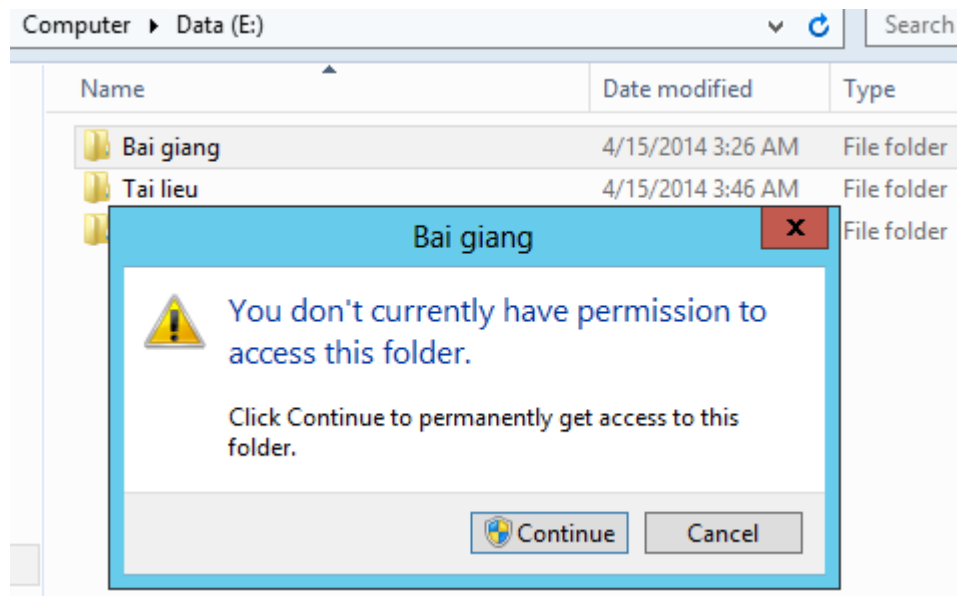


Kết quả thành công.

- Thực hiện đăng nhập vào tài khoản sinh viên 1:

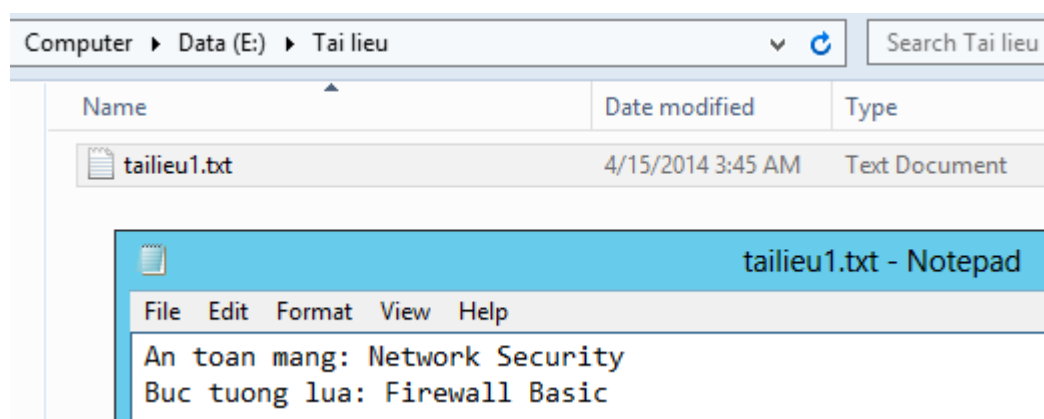


Thử truy cập vào thư mục Bài giảng:



Không truy cập được vì đã phân quyền cấm như trên.

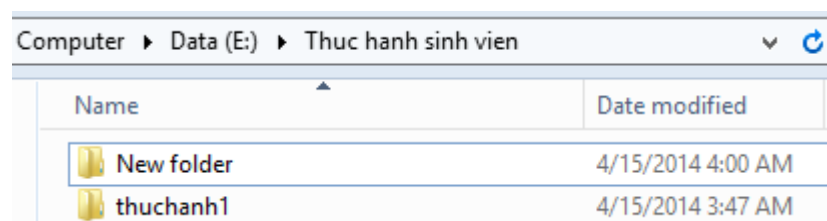
Truy cập vào thư mục Tài liệu, đọc nội dung tệp tin tailieu1.txt



Kết quả thành công vì Group sinh viên có quyền List folder contents, Read.

Thử thêm thông tin vào tệp tin này và lưu lại. Kết quả không có quyền thực hiện.

Thực hiện truy cập vào thư mục Thực hành sinh viên, tạo thư mục mới:



Thành công vì tài khoản sinhvien1 có quyền Write, nhưng không thay đổi được tên thư mục vì không có quyền Modify.

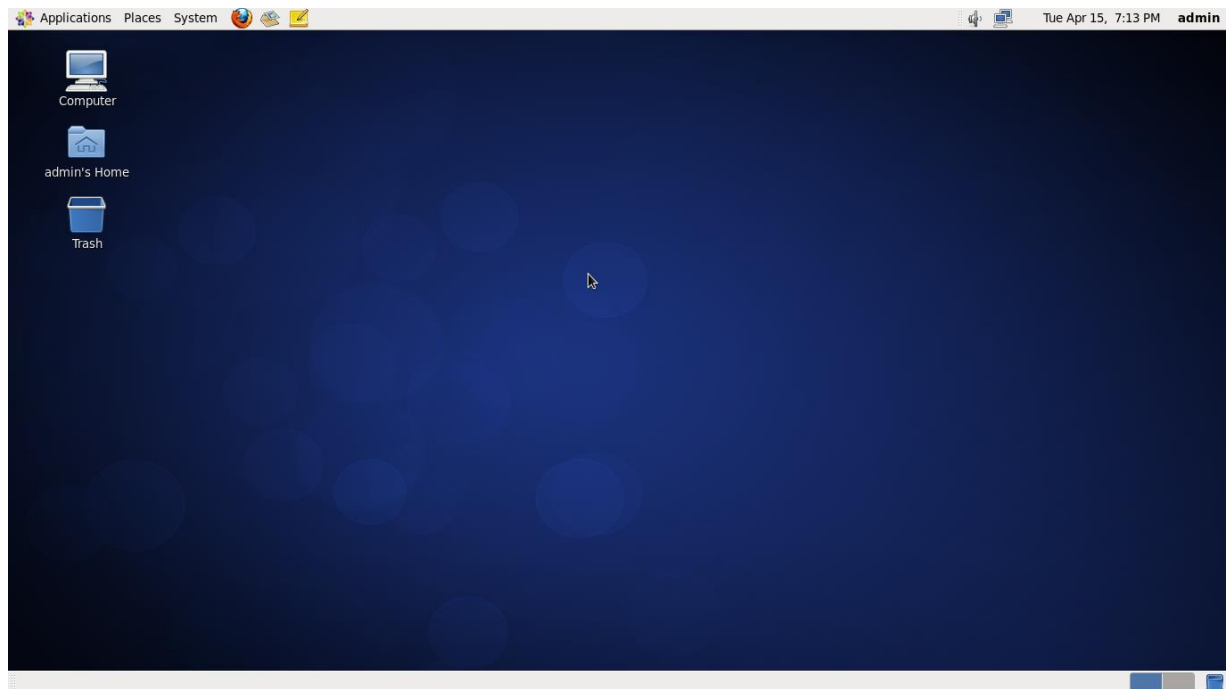


Như vậy các bước thực hiện phía trên đã hướng dẫn thực hiện và kiểm tra việc phân quyền tới tài nguyên lưu trữ trên Window Server 2012. Việc thực hiện trên Windows Server 2008 và 2003 thực hiện tương tự.

### *1.1.2 Thiết lập kiểm soát truy cập tới tài nguyên lưu trữ trên Linux*

Bài thực hành này hướng dẫn cấu hình phân quyền tới tài nguyên lưu trữ trên hệ điều hành Linux CentOS 6.5.

Hệ điều hành Linux CentOS 6.5 sau khi đã cài đặt thành công:

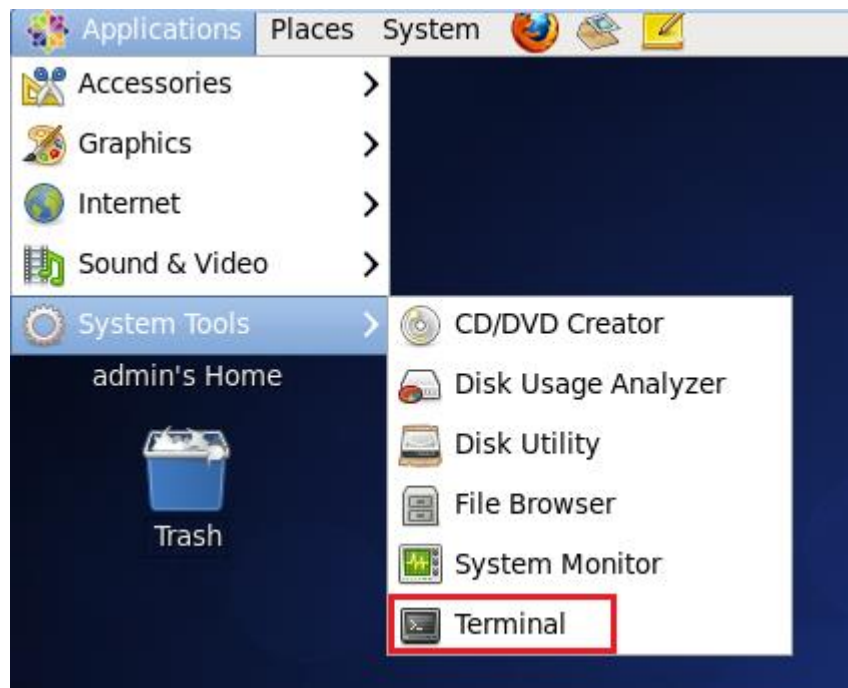


Các bước thực hiện, tất cả thao tác đều thực hiện bằng dòng lệnh:

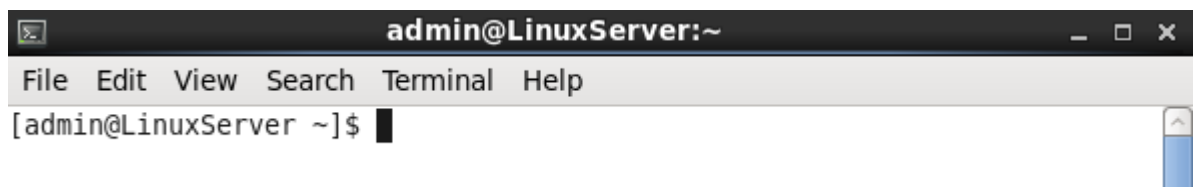
**Bước 1:** Thực hiện tạo người dùng, tạo nhóm. Đưa người dùng vào nhóm tương ứng.

Truy cập theo đường dẫn để mở cửa sổ dòng lệnh:

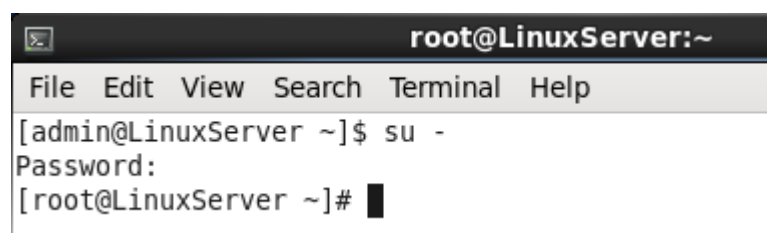
Applications → System Tools → Terminal



Cửa sổ dòng lệnh như sau:



Tuy nhiên tài khoản hiện tại chỉ có quyền người dùng thường (có ký hiệu là \$ ngay phía đầu của dòng lệnh). Để có thể thực hiện thao tác tạo người dùng phải chuyển qua tài khoản quản trị cao nhất là Root (có ký hiệu # ngay phía đầu dòng lệnh) bằng lệnh:



Trong bài này các đối tượng người dùng và nhóm vẫn tạo như bài thực hành đối với Windows Server 2012.

- Thực hiện gõ lệnh sau để tạo các đối tượng nhóm:

```
[root@LinuxServer ~]# useradd giaovien  
[root@LinuxServer ~]# useradd sinhvien  
[root@LinuxServer ~]#
```

Sau khi tạo xong sử dụng lệnh sau để kiểm tra thông tin nhóm đã tạo:

```
[root@LinuxServer ~]# cat /etc/group  
giaovien:x:501:  
sinhvien:x:502:  
[root@LinuxServer ~]#
```

Thông tin ở 2 dòng trên cho ta thấy:

Cột đầu tiên là tên nhóm, cột thứ 2 là mật khẩu của nhóm (trống vì không được sử dụng), cột thứ 3 là GID là định danh của nhóm, mỗi nhóm có 1 định danh duy nhất: giaovien – 501, sinhvien – 502.

- Thực hiện gõ lệnh sau để tạo các đối tượng người dùng:

```
[root@LinuxServer ~]# useradd giaovien1 -g giaovien  
[root@LinuxServer ~]# useradd giaovien2 -g giaovien  
[root@LinuxServer ~]# useradd sinhvien1 -g sinhvien  
[root@LinuxServer ~]# useradd sinhvien2 -g sinhvien  
[root@LinuxServer ~]#
```

4 câu lệnh trên đây đã tạo 4 người dùng giaovien1, giaovien2, sinhvien1, sinhvien2 và thêm người dùng giaovien1, giaovien2 vào nhóm giaovien, sinhvien1, sinhvien2 vào nhóm sinhvien.

Tiếp tục đặt mật khẩu lần lượt cho từng người dùng:

```
[root@LinuxServer ~]# passwd giaovien1  
Changing password for user giaovien1.  
New password:  
BAD PASSWORD: it is too simplistic/systematic  
BAD PASSWORD: is too simple  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@LinuxServer ~]#
```

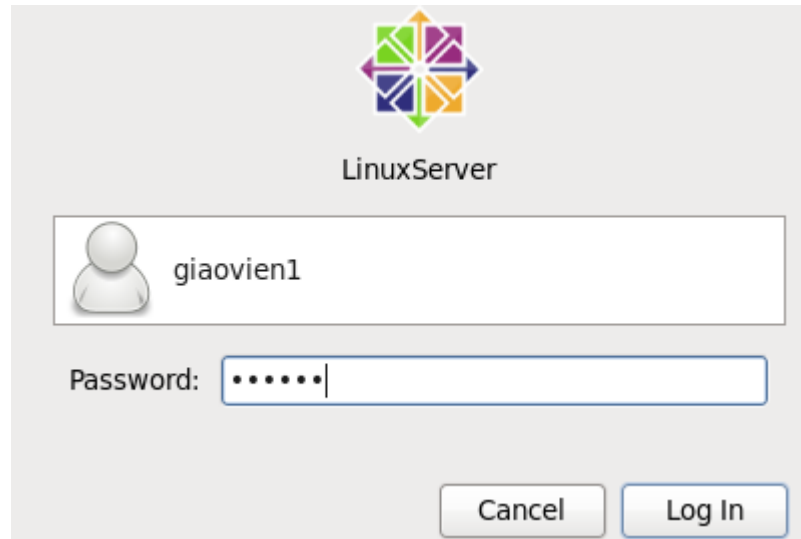
1 thông báo mật khẩu đơn giản, tuy nhiên hệ thống vẫn chấp nhận.

Để xem thông tin và thuộc tính của đối tượng người dùng đã tạo sử dụng lệnh sau:

```
[root@LinuxServer ~]# cat /etc/passwd  
giaovien1:x:503:501::/home/giaovien1:/bin/bash  
giaovien2:x:504:501::/home/giaovien2:/bin/bash  
sinhvien1:x:505:502::/home/sinhvien1:/bin/bash  
sinhvien2:x:506:502::/home/sinhvien2:/bin/bash  
[root@LinuxServer ~]#
```

- Cột thứ nhất là tên người dùng: giaovien1, sinhvien1...
- Cột thứ 2 chỉ ra mật khẩu được mã hóa và lưu ở tập tin Shadow.
- Cột thứ 3 UID là định danh duy nhất của người dùng: 503, 504, 505...

- Cột thứ 4 là định danh của nhóm chỉ ra người dùng thuộc nhóm nào, ví dụ: giaovien1 có GID là 501, mà 501 là GID của nhóm giaovien.
  - Cột thứ 5 thư mục của người dùng,
  - Cột thứ 6 đường dẫn dòng lệnh.
- Thử đăng nhập các tài khoản đã tạo:



Kết quả thành công.

## **Bước 2:** Tạo tài nguyên lưu trữ.

Đăng nhập bằng tài khoản Root tạo các thư mục: Bai\_giang, Tai\_lieu, Thuc\_hanh\_sinh\_vien. Vị trí các thư mục này nằm ngay sau gốc thư mục ký hiệu /:

Dòng lệnh như sau:

```
[root@LinuxServer ~]# mkdir /Bai_giang
[root@LinuxServer ~]# mkdir /Tai_lieu
[root@LinuxServer ~]# mkdir /Thuc_hanh_sinh_vien
[root@LinuxServer ~]#
```

Tạo thư mục cho từng giáo viên:

```
[root@LinuxServer ~]# mkdir /Bai_giang/giaovien1
[root@LinuxServer ~]# mkdir /Bai_giang/giaovien2
```

Xem thuộc tính quyền hiện tại áp dụng tới các thư mục trên:

```
drwxr-xr-x.  4 root root  4096 Apr 15 20:35 Bai_giang
drwxr-xr-x.  2 root root  4096 Apr 15 20:34 Tai_lieu
drwxr-xr-x.  2 root root  4096 Apr 15 20:34 Thuc_hanh_sinh_vien
```

- Cột thứ nhất là quyền áp dụng đối với thư mục, ký tự d chỉ đây là thư mục.

- Cột thứ 2 là các số nguyên chỉ liên kết tới thư mục.
- Cột thứ 3,4 là chủ sở hữu và nhóm sở hữu thư mục, ở đây là root.
- Cột 5 chỉ dung lượng của thư mục (byte).
- Cột 6,7,8 chỉ thời gian tạo.
- Cột 9 chỉ tên thư mục.

### Bước 3: Phân quyền

Bài thực hành này vẫn giữ các quyền của các đối tượng người dùng áp dụng tới các thư mục đã tạo như bài thực hành Windows Server 2012.

- Đối với thư mục Bai\_giang: thu về quyền chủ sở hữu là giaovien1, nhóm sở hữu là giaovien bằng lệnh sau:

```
[root@LinuxServer ~]# chown giaovien1:giaovien /Bai_giang
```

Xem thuộc tính:

```
[root@LinuxServer ~]# ls -l /
drwxr-xr-x.  4 giaovien1 giaovien 4096 Apr 15 20:35 Bai_giang
```

Kết quả thành công.

Phân quyền đối với thư mục Bai\_giang: thành viên trong nhóm giaovien có toàn quyền, thành viên trong nhóm sinhvien không được phép truy cập. Sử dụng lệnh sau:

```
[root@LinuxServer ~]# chmod 770 /Bai_giang
[root@LinuxServer ~]# ls /
drwxrwx---.  4 giaovien1 giaovien 4096 Apr 15 21:19 Bai_giang
```

Giải thích dòng lệnh:

Chmod là lệnh phân quyền, 770 (111-111-000) chủ sở hữu toàn quyền, nhóm toàn quyền, người dùng khác cấm. Riêng người dùng root vẫn có toàn quyền.

Tiếp tục phân quyền cho thư mục con giaovien1, giaovien2. Thư mục giaovien1 chỉ có tài khoản giaovien1 được toàn quyền, giaovien2 không được phép truy cập.

```
[root@LinuxServer ~]# chown giaovien1:giaovien /Bai_giang/giaovien1
[root@LinuxServer ~]# chown giaovien2:giaovien /Bai_giang/giaovien2
[root@LinuxServer ~]# chmod 700 /Bai_giang/giaovien1
[root@LinuxServer ~]# chmod 700 /Bai_giang/giaovien2
```

```
[root@LinuxServer ~]# ls -l /Bai_giang/
total 8
drwx-----. 2 giaovien1 giaovien 4096 Apr 15 20:35 giaovien1
drwx-----. 2 giaovien2 giaovien 4096 Apr 15 20:35 giaovien2
[root@LinuxServer ~]# █
```

Giải thích:

2 lệnh chown đầu tiên để lấy về quyền chủ sở hữu thư mục tương ứng.

Phân quyền 700 (111-000-000): chủ sở hữu toàn quyền, nhóm và người dùng khác cấm truy cập.

Lệnh ls -l để xem thuộc tính.

- Đối với thư mục Tai\_lieu:

Đăng nhập bằng tài khoản root, thu về quyền chủ sở hữu và nhóm sở hữu là giaovien1:giaovien:

```
[root@LinuxServer ~]# chown giaovien1:giaovien /Tai_lieu/
[root@LinuxServer ~]# ls -l /

drwxr-xr-x.  2 giaovien1 giaovien  4096 Apr 15 20:34 Tai_lieu
```

Phân quyền với nhóm giaovien quyền tạo, xóa, chỉnh sửa, sao chép. Thành viên trong nhóm sinh viên chỉ được phép đọc, sao chép.

```
[root@LinuxServer ~]# chmod 775 /Tai_lieu/
[root@LinuxServer ~]# ls -l /

drwxrwxr-x.  2 giaovien1 giaovien  4096 Apr 15 20:34 Tai_lieu
```

Giải thích dòng lệnh:

Phân quyền với lệnh chmod, 775 (111-111-101) người dùng và nhóm người dùng giaovien quyền tạo, xóa, chỉnh sửa, sao chép. Người dùng khác (sinhvien) chỉ có quyền truy cập thư mục và tệp tin đọc nội dung nhưng không được chỉnh sửa.

- Đối với thư mục Thuc\_hanh\_sinh\_vien:

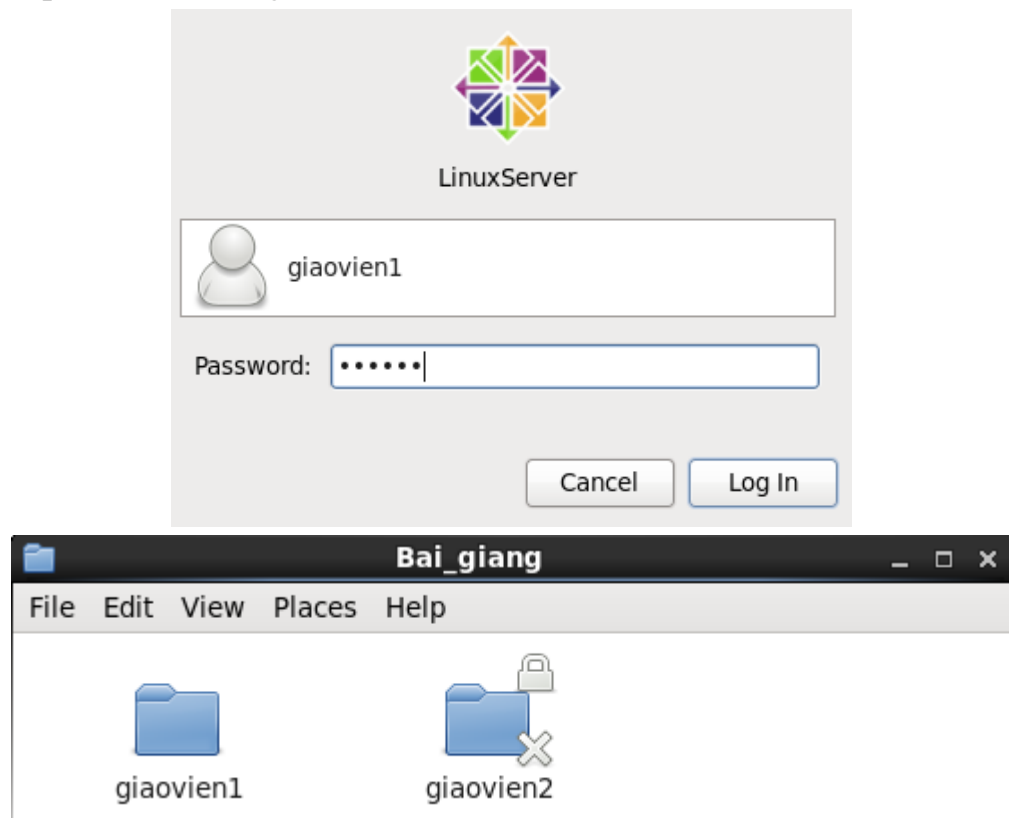
Trong Linux chức năng phân nhỏ quyền không bằng Windows nên thư mục này nếu gán quyền tạo thư mục, tệp tin cho nhóm sinhvien thì phải đi kèm với quyền thực thi để truy cập thư mục. Vì vậy gán quyền là 777 cho thư mục Thuc\_hanh\_sinh\_vien:

```
[root@LinuxServer ~]# chmod 777 /Thuc_hanh_sinh_vien/
[root@LinuxServer ~]# ls -l /

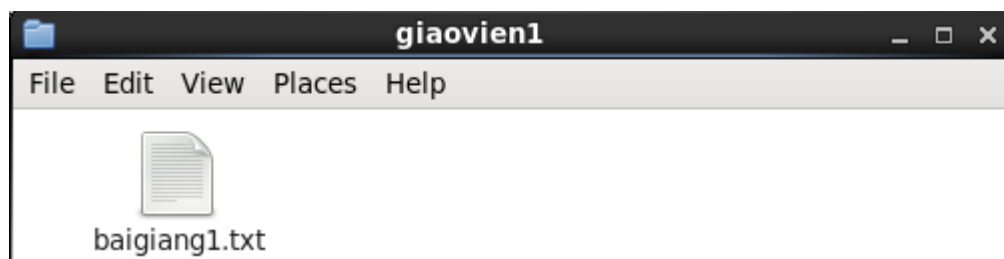
drwxrwxrwx.  2 giaovien1 giaovien  4096 Apr 15 20:34 Thuc_hanh_sinh_vien
```

**Bước 4:** Kiểm tra kết quả

- Đăng nhập bằng tài khoản giaovien1: truy cập vào thư mục Bai\_giang, truy cập tiếp vào thư mục giaovien1.

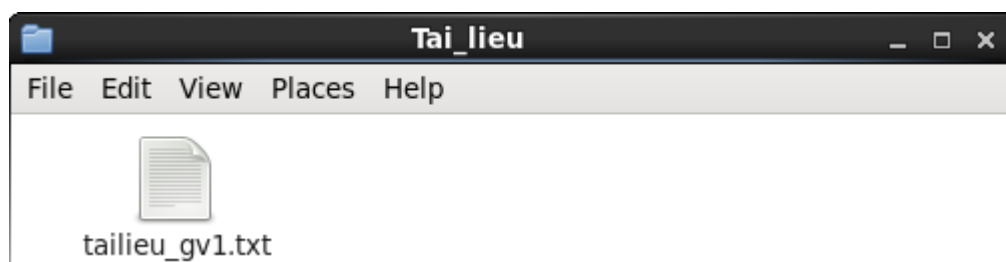


Ta thấy thư mục giaovien2 có biểu tượng khóa và dấu nhân → cấm người khác truy cập (chỉ có giaovien2 và root mới được phép truy cập). Truy cập vào thư mục của giaovien 1 và tạo tệp tin baigiang1.txt



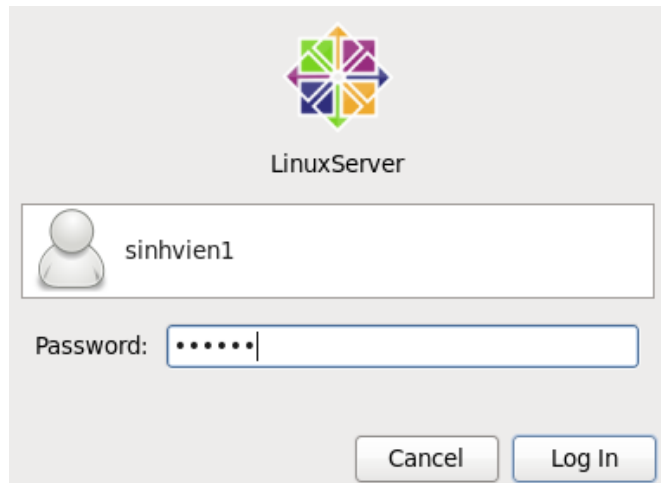
Thành công.

Truy cập vào thư mục Tai\_lieu, tạo tệp tin tailieu\_gv1.txt

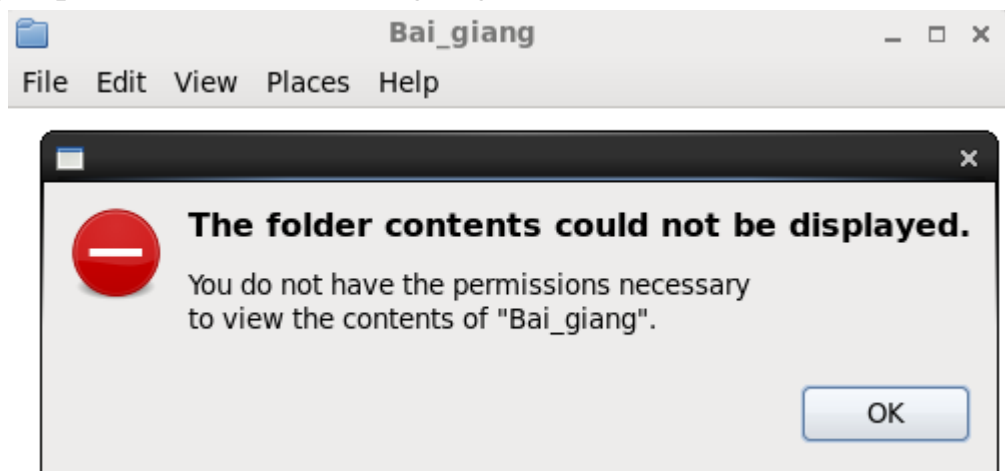


Thành công.

- Đăng nhập bằng tài khoản sinhvien1:

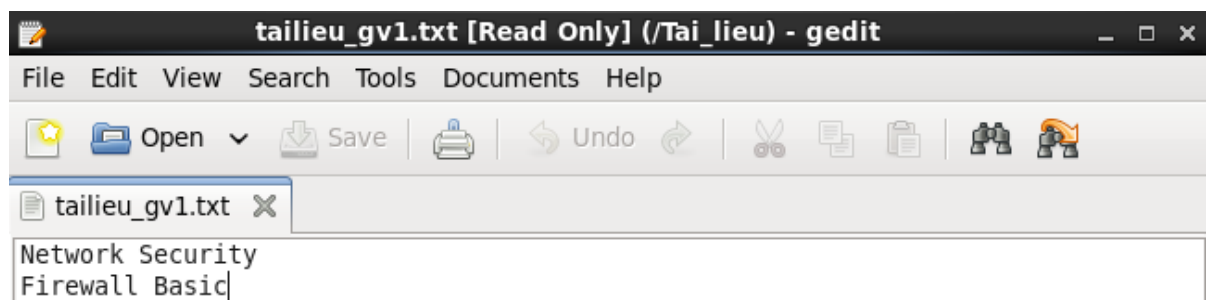
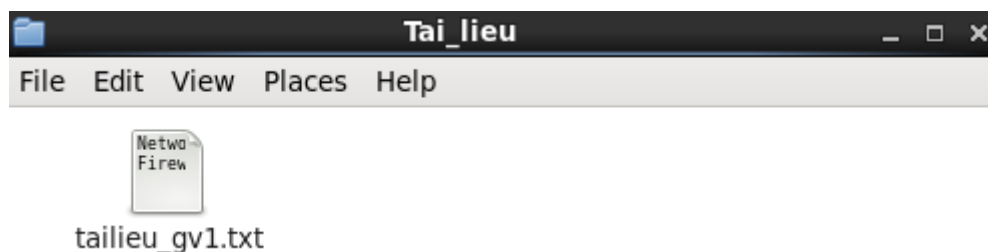


Truy cập thử vào thư mục Bai\_giang:



Thông báo hiển thị rằng người dùng sinhvien1 không có quyền truy cập.

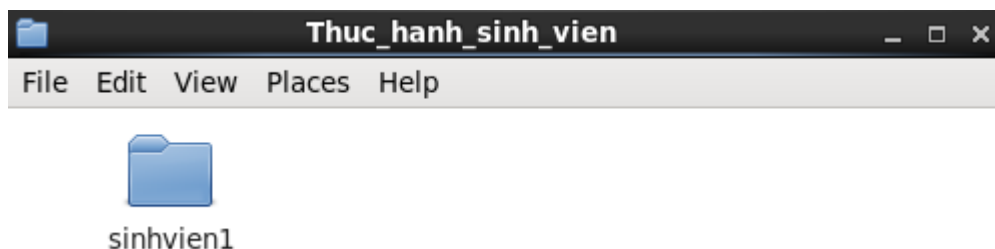
Truy cập vào thư mục Tai\_lieu và đọc nội dung của tệp tin tailieu\_gv1.txt





Kết quả thành công. Tuy nhiên sinhvien1 không có quyền tạo (Read Only).

Truy cập vào thư mục Thuc\_hanh\_sinh\_vien: Tạo thư mục sinhvien1



Kết quả thành công.

## 1.2 Thiết lập kiểm soát truy cập tới tài nguyên chia sẻ

### 1.2.1 Phân quyền tới tài nguyên chia sẻ trên Windows Server 2012

Trong bài thực hành này vẫn sử dụng các đối tượng người dùng và tài nguyên thư mục ở bài thực hành trên gồm:

Đối tượng người dùng: giaovien1, giaovien2 trong nhóm giaovien.

Sinhvien1, sinhvien2 trong nhóm sinhvien.

Thư mục: Bai giang, Tai lieu, Thuc hanh sinh vien.

**Bước 1:** Xác định quyền chia sẻ cho mỗi nhóm. Nhưng trong bài thực hành này phân quyền chia sẻ đối với các thư mục trên như sau:

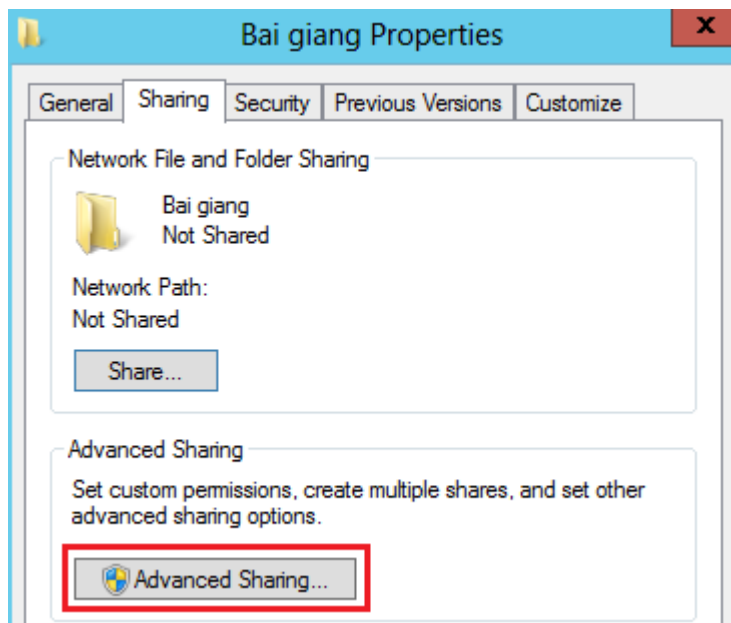
- Thư mục Bai giang: Chia sẻ với quyền chỉ cho phép thành viên trong nhóm giáo viên truy cập. Mỗi giáo viên chỉ được phép truy cập tới thư mục của mình. Thành viên trong nhóm sinh viên không được phép truy cập vào thư mục này.
- Thư mục Tai lieu: Chia sẻ với quyền thành viên nhóm giáo viên được phép truy cập, đọc, tạo, xóa, chỉnh sửa. Thành viên nhóm sinh viên chỉ được phép truy cập, đọc, sao chép.
- Thư mục Thuc hanh sinh vien: Cả thành viên của 2 nhóm đều có quyền truy cập, đọc, tạo, xóa, chỉnh sửa.

**Bước 2:** Thiết lập, để thực hành được các yêu cầu trên đây thực hiện theo các bước sau:

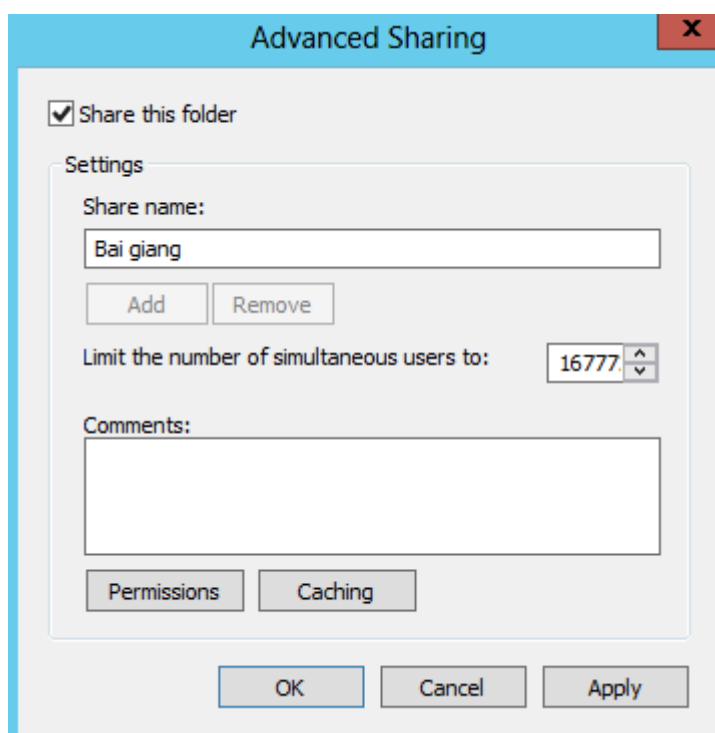
Đăng nhập Windows Server 2012 bằng tài khoản Administrator và thiết lập theo thứ tự các thư mục:

**Bước 3:** Thiết lập quyền chia sẻ cho thư mục Bai giang:

Chuột phải vào thư mục chọn Properties. Chọn tab Sharing:



Chọn thiết lập chia sẻ nâng cao (Advanced Sharing), hộp thoại thiết lập xuất hiện, tích chọn Share this folder như hình dưới:

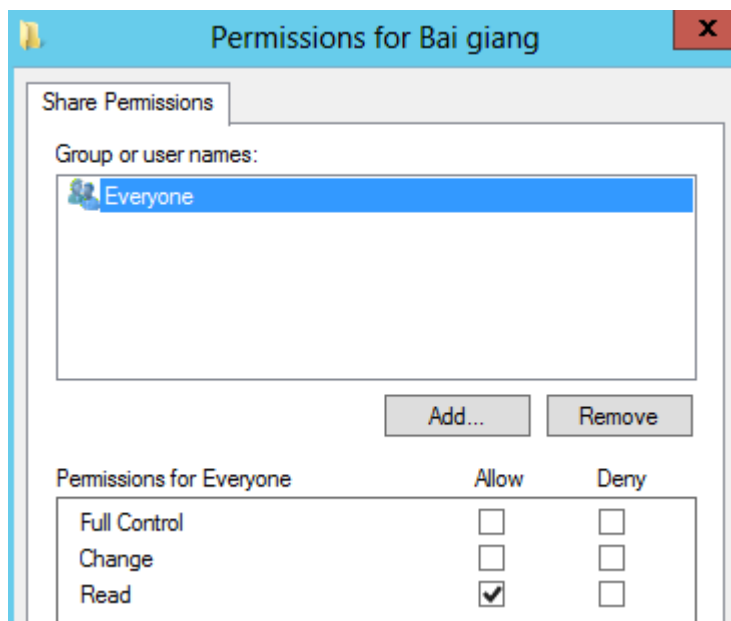


Với Share name: đang hiển thị tên mặc định của thư mục, tuy nhiên có thể thay đổi cho phù hợp với yêu cầu chia sẻ.

Thiết lập cho phép số lượng người dùng truy cập đồng thời ở dòng Limit the number of simultaneous users to: mặc định là 16777 người dùng.

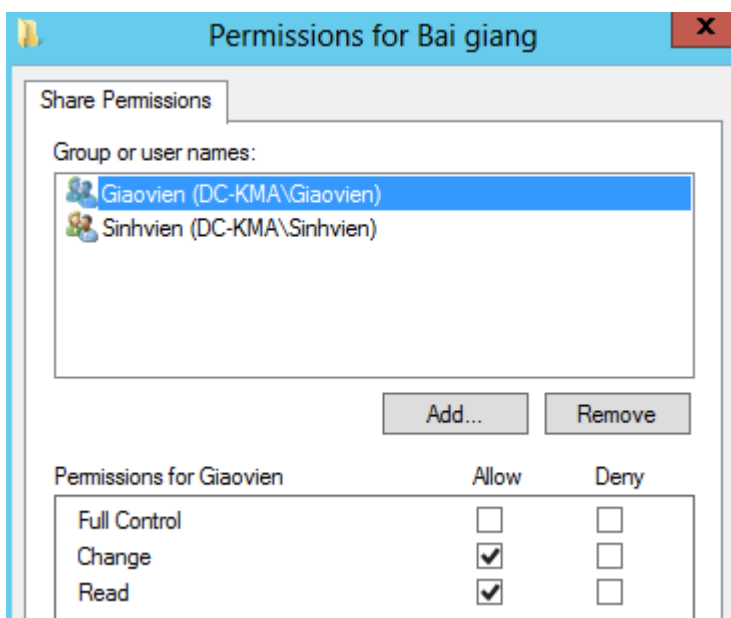
Dòng Comments: dòng chú thích chia sẻ.

Để thiết lập quyền người dùng vào Permissions:

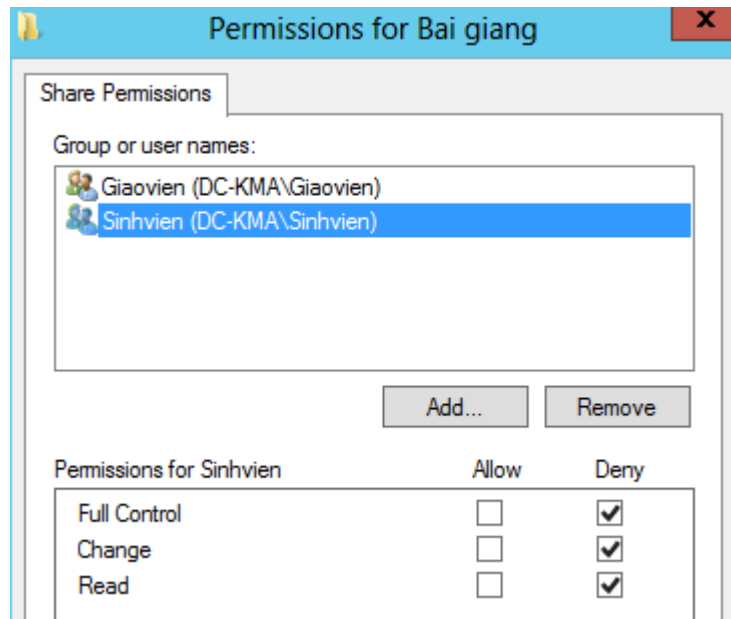


Với người dùng mặc định là Everyone quyền tương ứng Read, tuy nhiên phải gỡ bỏ tài khoản này đi chọn Remove.

Tiếp tục thêm các tài khoản group giaovien, group sinhvien và quyền tương ứng như sau:



+ Group giaovien có quyền Change, Read: Tạo, xóa, đọc, chỉnh sửa.

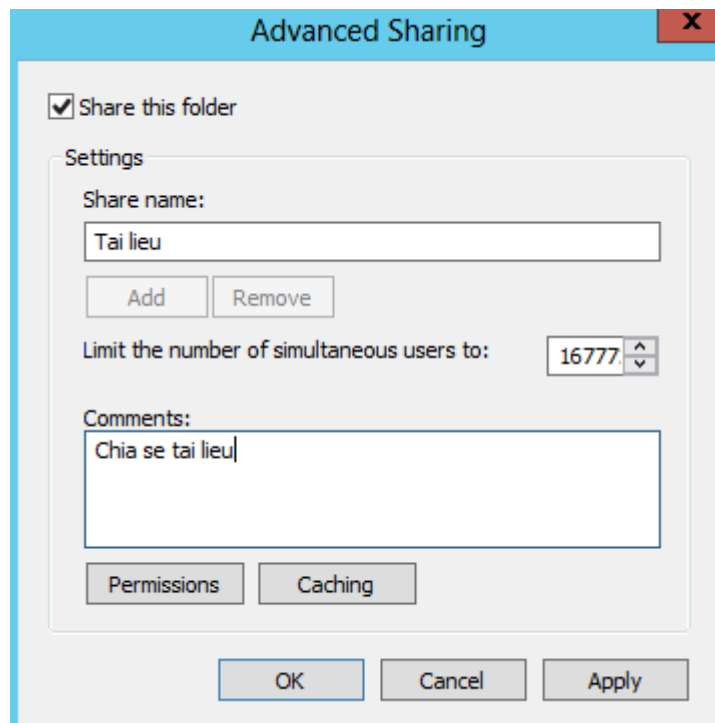


+ Group sinhvien cấm toàn quyền.

Apply → OK. Thiết lập xong cho thư mục Bai giang.

**Bước 4:** Thiết lập quyền chia sẻ cho thư mục Tai lieu:

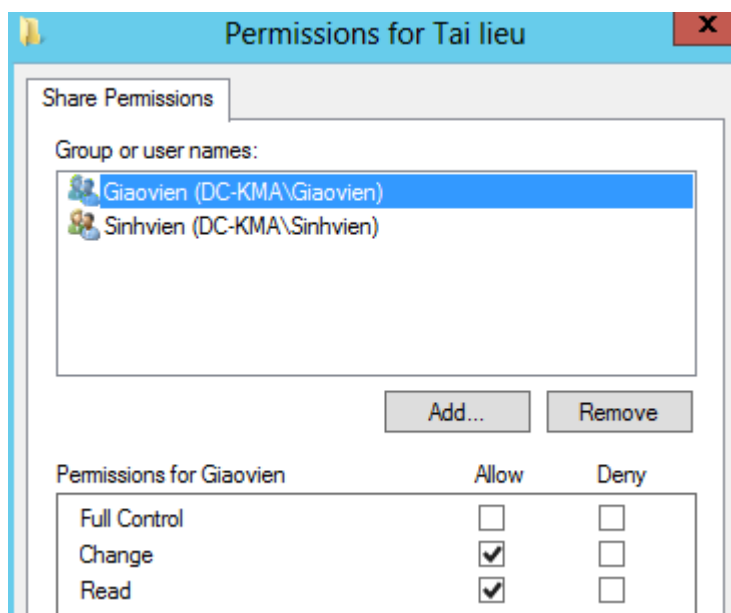
Chuột phải vào thư mục chọn Properties. Chọn tab Sharing → Advanced Sharing



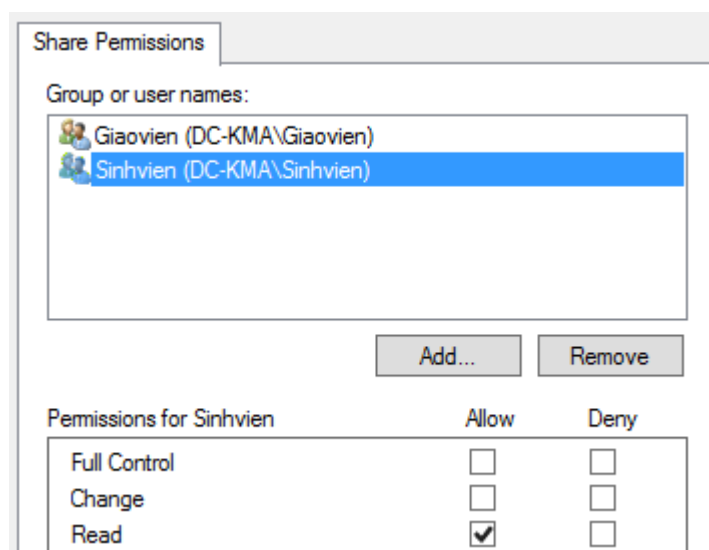
Tích vào tùy chọn Share this folder, tương tự như thư mục Bài giảng số lượng người truy cập đồng thời mặc định là 16777.

Chọn Permissions, gỡ bỏ nhóm người dùng mặc định Everyone. Thêm nhóm người dùng group giaovien và group sinhvien.

Với các quyền cho nhóm giaovien là Change, Read: đọc, sửa, xóa, tạo



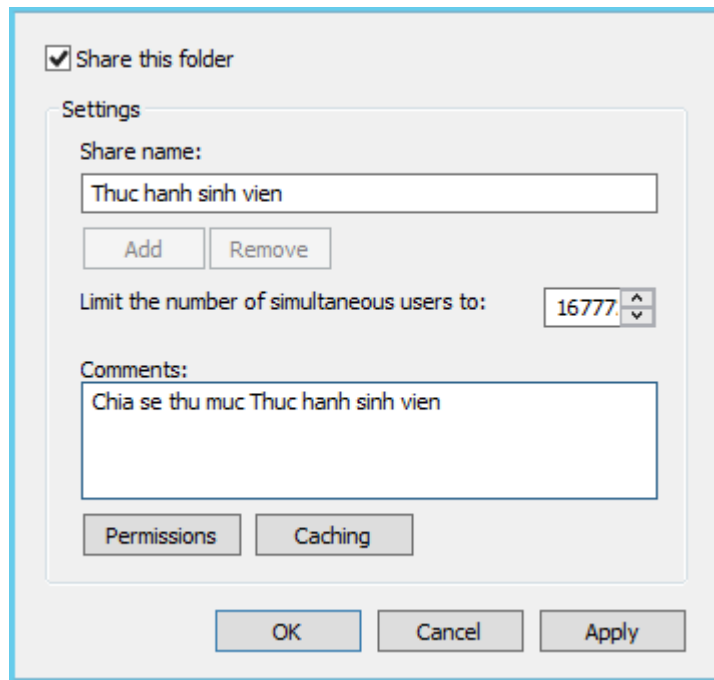
Với các quyền cho nhóm sinhvien là Read: chỉ được phép đọc.



Apply → OK

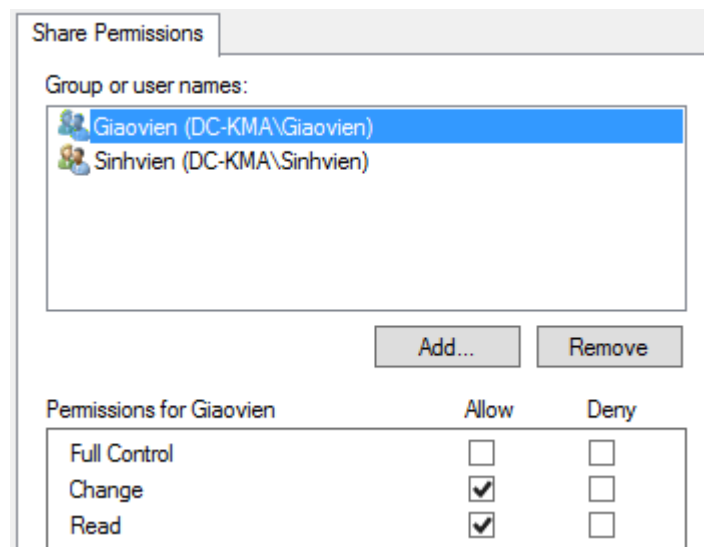
**Bước 5:** Thiết lập quyền chia sẻ cho thư mục Thuc hanh sinh vien:

Chuột phải vào thư mục chọn Properties. Chọn tab Sharing → Advanced Sharing

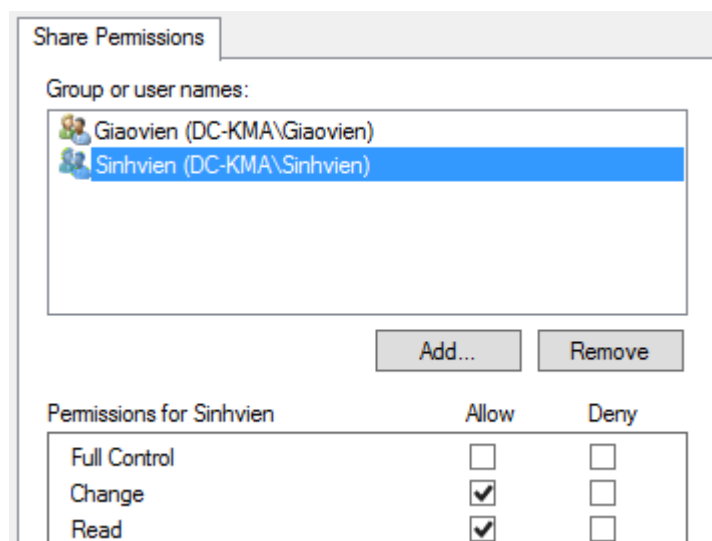


Chọn Permissions, gỡ bỏ nhóm người dùng truy cập mặc định Everyone, thêm nhóm group giaovien, group sinhvien.

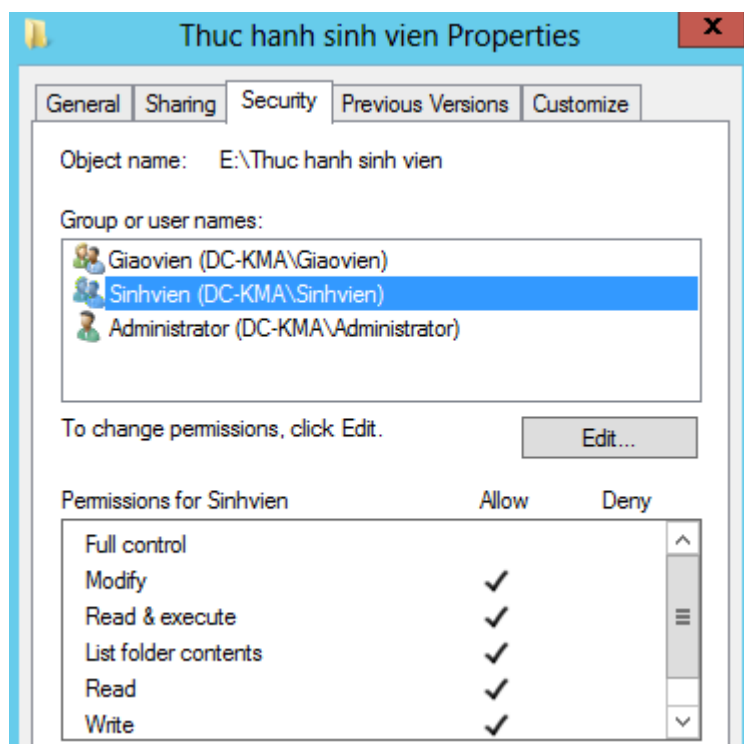
Group giaovien có quyền đọc, chỉnh sửa, xóa, tạo: Read, Change



Group sinhvien có quyền đọc, chỉnh sửa, xóa, tạo: Read, Change



Ngoài ra đối với thư mục Thuc hanh sinh vien cần phải thiết lập thêm quyền Modify trong tab Security:

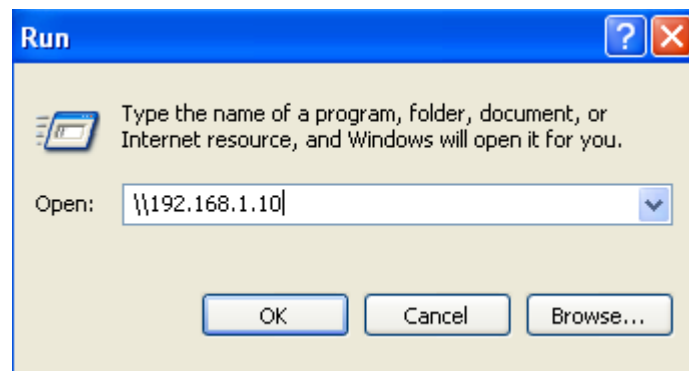


Apply → OK

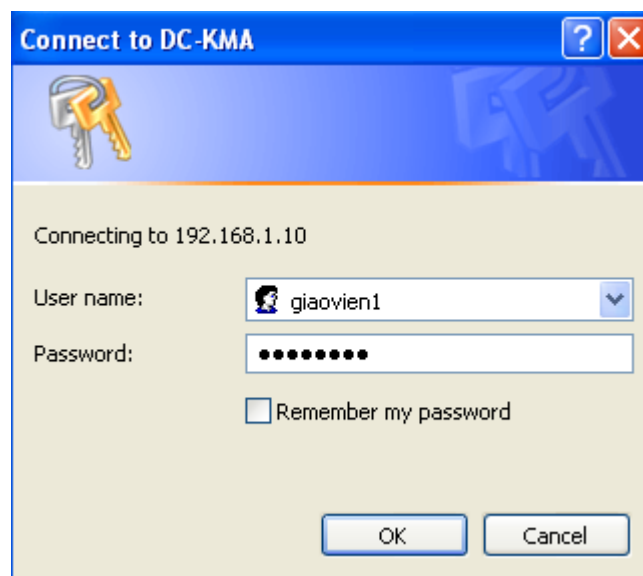
#### **Bước 6:** Kiểm tra kết quả

- Đăng nhập tài khoản giaovien1 từ 1 máy trạm chạy hệ điều hành Windows 7 hoặc XP có kết nối mạng LAN với máy chủ Server 2012.

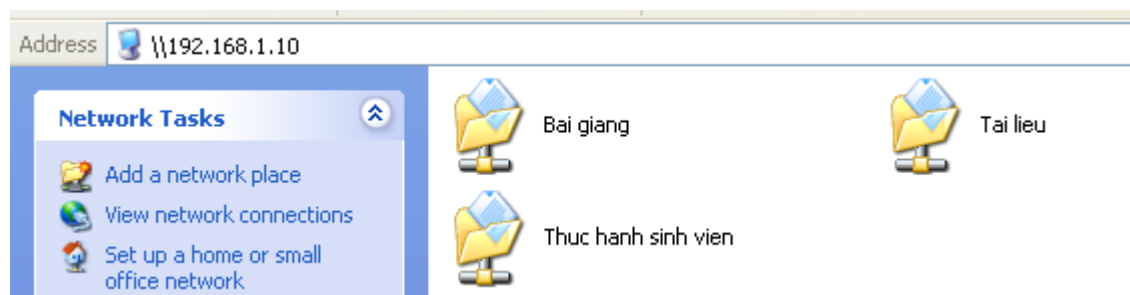
Vào Run gõ đường dẫn IP của máy chủ 2012



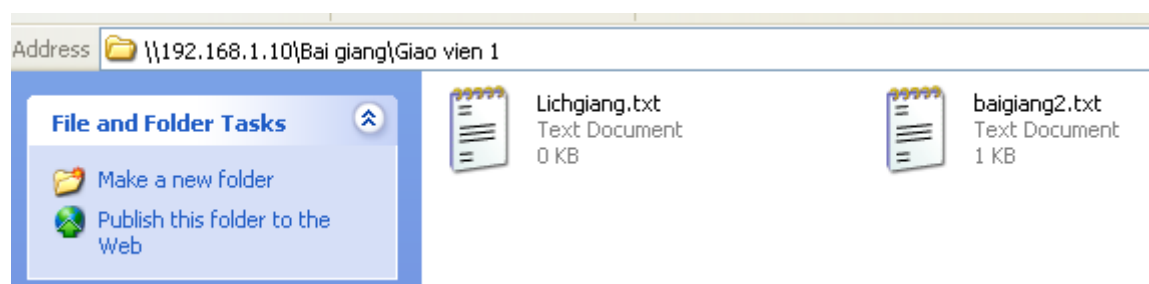
Một cửa sổ xác thực người dùng hiện ra, nhập tên và mật khẩu của giaovien1:



Sau khi xác thực thành công, tài nguyên chia sẻ hiện ra như sau:



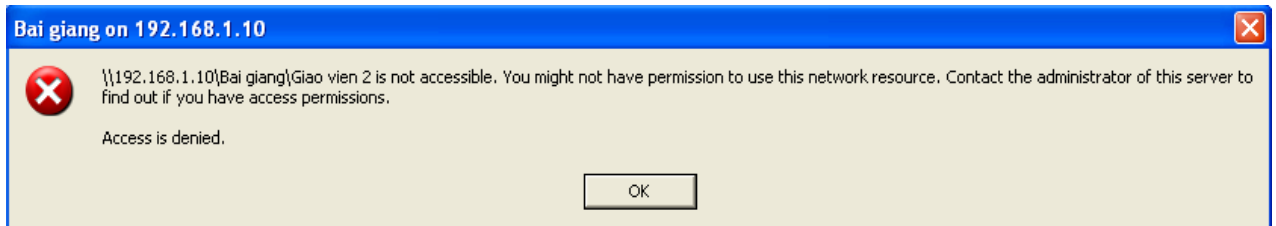
Truy cập vào thư mục bài giảng → truy cập vào thư mục giaovien1 → tạo tệp tin baigiang2.txt





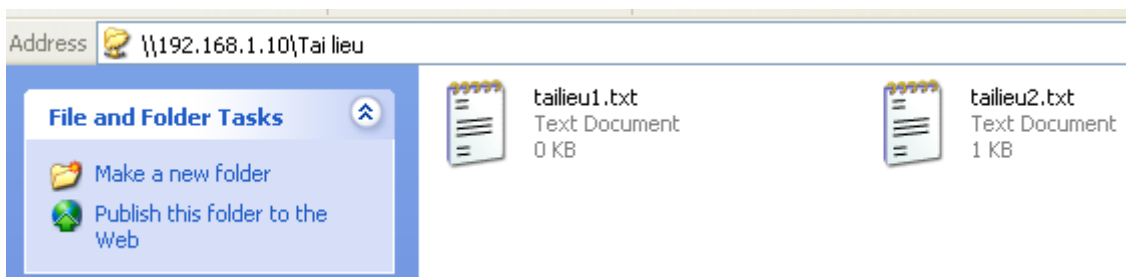
Kết quả thành công.

Truy cập vào thư mục giaovien2



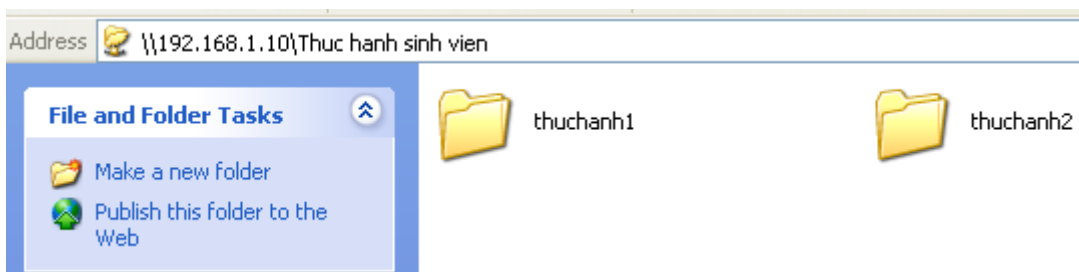
Kết quả không truy cập được vì đã thiết lập quyền cấm, và chỉ cho phép giaovien2 truy cập.

Truy cập vào thư mục Tai lieu và tạo tệp tin tailieu2.txt



Kết quả thành công.

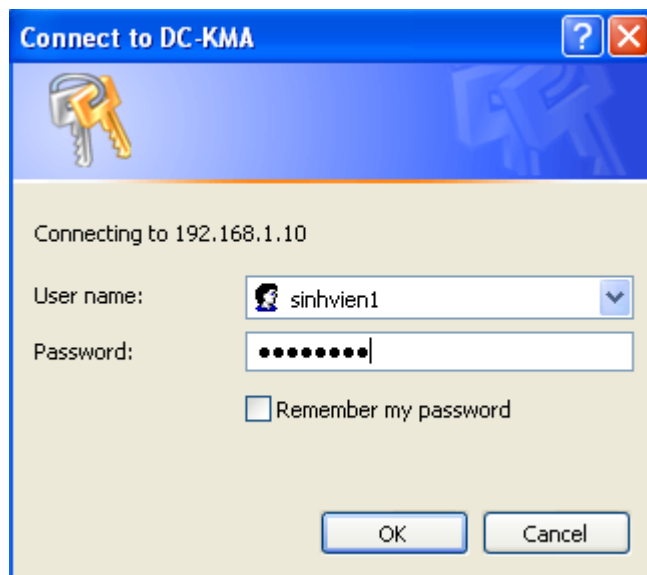
Truy cập vào thư mục Thuc hanh sinh vien và tạo thư mục thuchanh2:



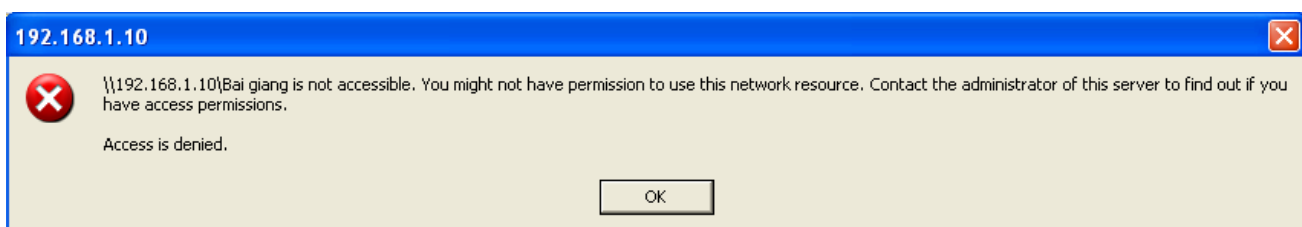
Kết quả thành công.

Như vậy với thiết lập quyền chia sẻ như trên đã đáp ứng yêu cầu chia sẻ tài nguyên và phân quyền đúng với người dùng trong nhóm giaovien.

- Đăng nhập tài khoản sinhvien1:

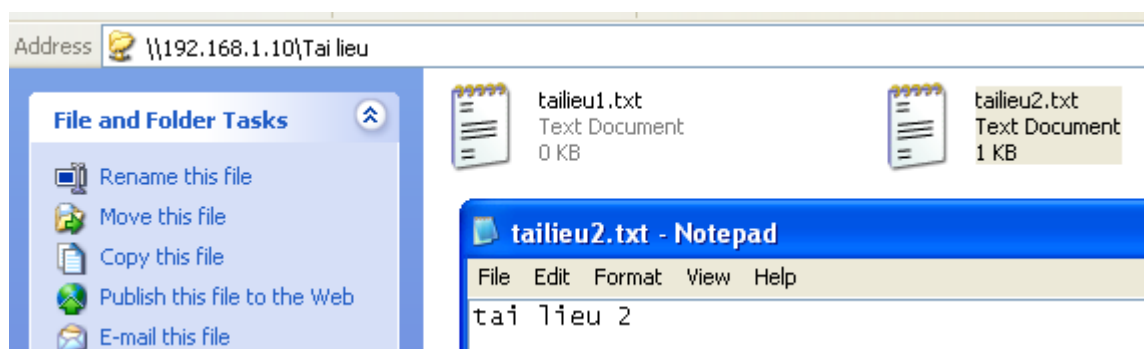


Truy cập vào thư mục Bai giang:



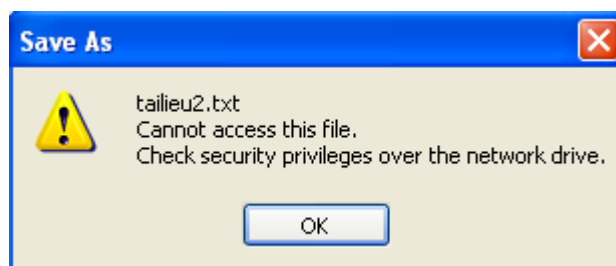
Thông báo không được phép truy cập vì đã thiết lập ở trên đây.

Truy cập vào thư mục Tai lieu, mở tệp tin tailieu2.txt đọc nội dung:



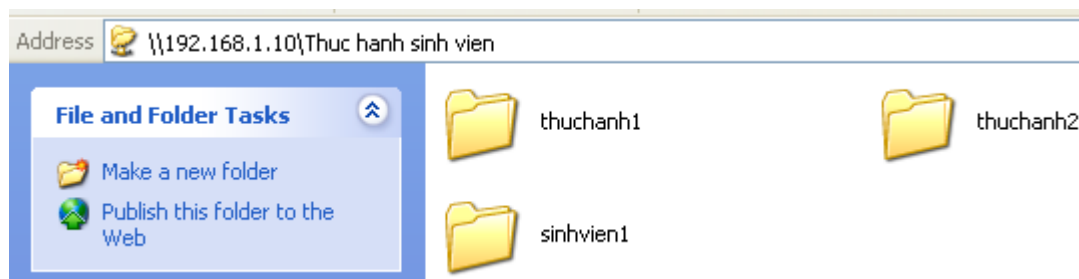
Kết quả thành công.

Thử chỉnh sửa tệp tin này và lưu lại:



Thông báo hiển thị không thể truy cập tới tệp tin và yêu cầu kiểm tra lại quyền. Bởi vì đã thiết lập nhóm người dùng sinhvien chỉ được xem mà không được chỉnh sửa ở trên đây.

Truy cập tới thư mục Thuc hanh sinh vien, tạo thư mục sinhvien1



Thực hiện thành công.

Như vậy bài thực hành đã hướng dẫn các bước thiết lập và kiểm tra quyền chia sẻ dữ liệu trên Windows Server 2012, đối với Server 2008 và 2003 thiết lập tương tự.

### 1.2.2 Phân quyền tới tài nguyên chia sẻ trên Linux CentOS 6.5

Để chia sẻ dữ liệu giữa máy chủ CentOS và máy trạm Windows thì chúng ta phải cài đặt phần mềm có tên Samba. Thực hành theo các bước sau đây:

**Bước 1:** Truy cập với tài khoản root vào máy chủ Linux CentOS 6.5, thực hiện cài đặt gói phần mềm Samba theo dòng lệnh sau:

```
yum -y install samba
```

Installed:

```
samba.i686 0:3.6.9-168.el6_5
```

Dependency Updated:

```
libsmbclient.i686 0:3.6.9-168.el6_5
```

```
samba-common.i686 0:3.6.9-168.el6_5
```

```
samba-winbind.i686 0:3.6.9-168.el6_5
```

```
samba-winbind-clients.i686 0:3.6.9-168.el6_5
```

Complete!

```
[root@LinuxServer ~]#
```

## BÀI 2. THỰC HÀNH THIẾT LẬP MẬT KHẨU AN TOÀN

### 2.1 Thực hành thiết lập mật khẩu an toàn

#### Mục đích bài thực hành:

Trong các hệ điều hành Windows và Linux mật khẩu được thiết lập mặc định không đảm bảo an toàn, vì vậy mà bài thực hành hướng dẫn cấu hình chính sách và thiết lập mật khẩu an toàn trong hệ điều hành Windows và Linux.

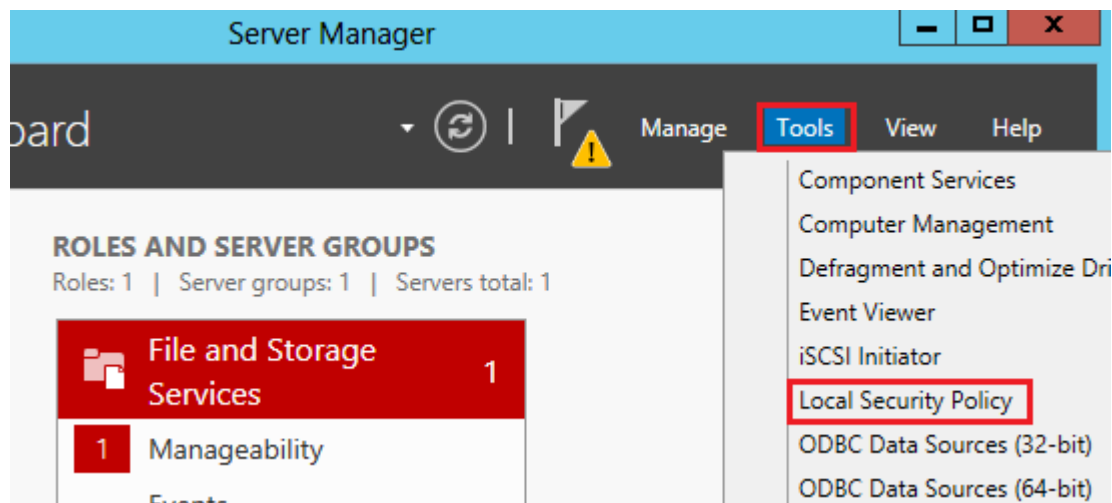
#### Yêu cầu hệ thống:

- Máy chủ chạy hệ điều hành Windows Server 2012.
- Máy trạm chạy hệ điều hành Windows 7
- Máy chủ chạy hệ điều hành Linux CentOS 6.5

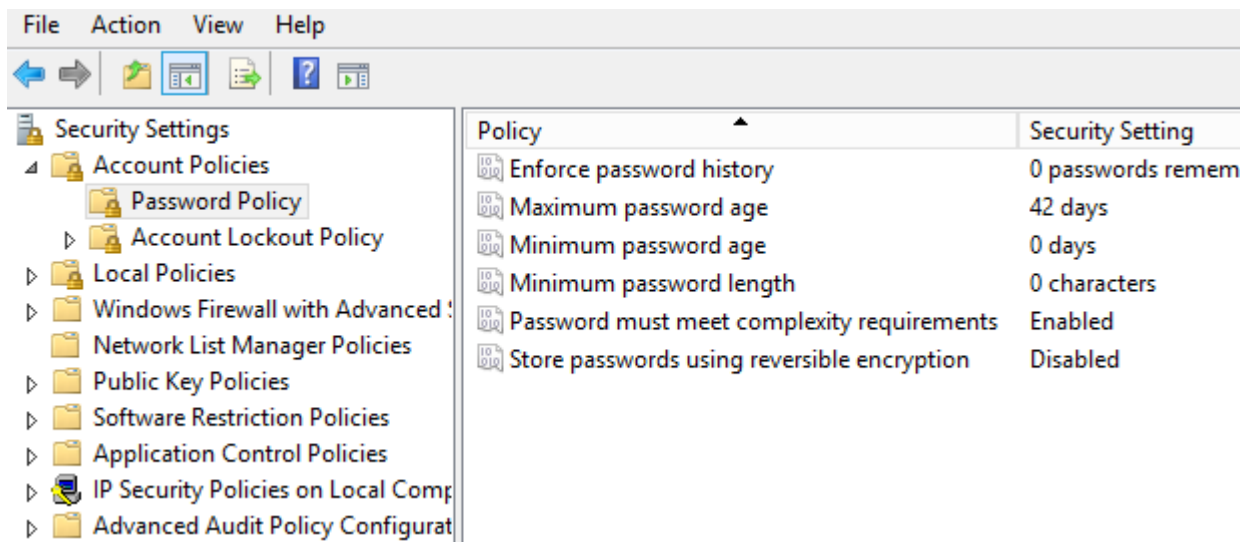
#### 2.1.1 Thiết lập mật khẩu an toàn Windows Server 2012

Các bước thực hiện:

**Bước 1:** Đăng nhập bằng tài khoản Administrator (cục bộ) vào máy chủ Windows Server 2012. Truy cập theo đường dẫn: Server Manager → Tools → Local Security Policy như hình sau đây:



Giao diện của ứng dụng Local Security Policy

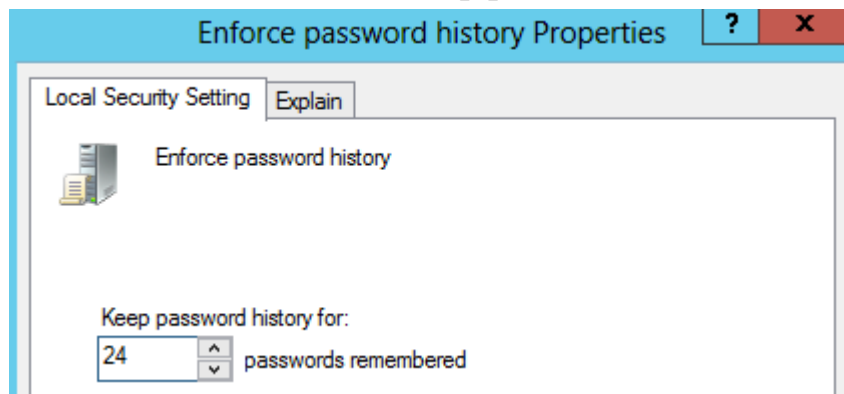


Đây là những thiết lập mặc định của hãng Microsoft sau khi cài đặt xong hệ điều hành.

Nhưng cần phải thay đổi lại một số chính sách để đảm bảo độ an toàn của mật khẩu. Ví dụ: Mật khẩu phải kết hợp chữ số, chữ in hoa, chữ thường, ký tự đặc biệt. Độ dài của mật khẩu phải lớn hơn 6 ký tự. Số lần lưu mật khẩu cũ trong bộ nhớ là 24 mật khẩu. Để làm được yêu cầu trên phải thiết lập như sau:

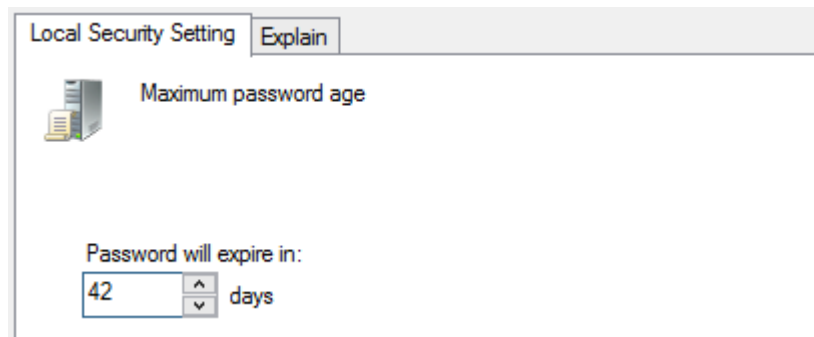
**Bước 2:** Trong các tùy chọn của Password Policy phải thiết lập:

- Enforce password history (lưu mật khẩu cũ vào bộ nhớ): giá trị là 24. Nghĩa là các mật khẩu khi được thiết lập phải khác với 24 mật khẩu trước đó:



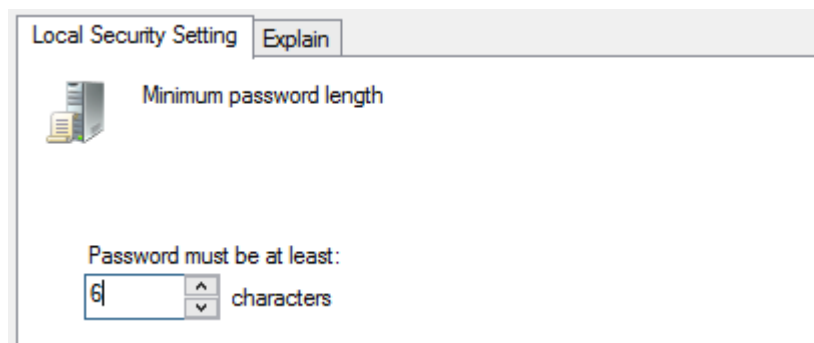
Apply - OK

- Maximum password age: Số ngày tối đa mà mật khẩu được sử dụng là 42 ngày. Sau 42 ngày này mật khẩu phải thay đổi mới:



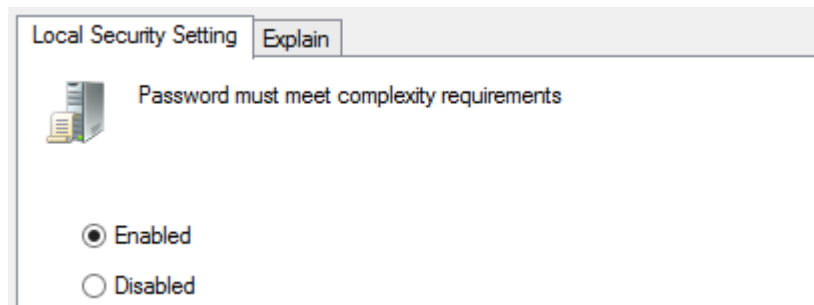
Apply - OK

- Minimum password age: Số ngày tối thiểu của 1 mật khẩu để mặc định.
- Minimum password length: Độ dài tối thiểu của mật khẩu 6 ký tự:



Apply - OK

- Password must meet complexity requirements: Yêu cầu mật khẩu phải có độ phức tạp: ký tự hoa, ký tự thường, chữ số, ký tự đặc biệt...Enabled



Sau khi thiết lập xong ta có:

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	6 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Thoát khỏi giao diện thiết lập Local Security Policy.

**Bước 3:** Áp dụng chính sách đã thiết lập

Vào Run → cmd, gõ lệnh gpupdate /force

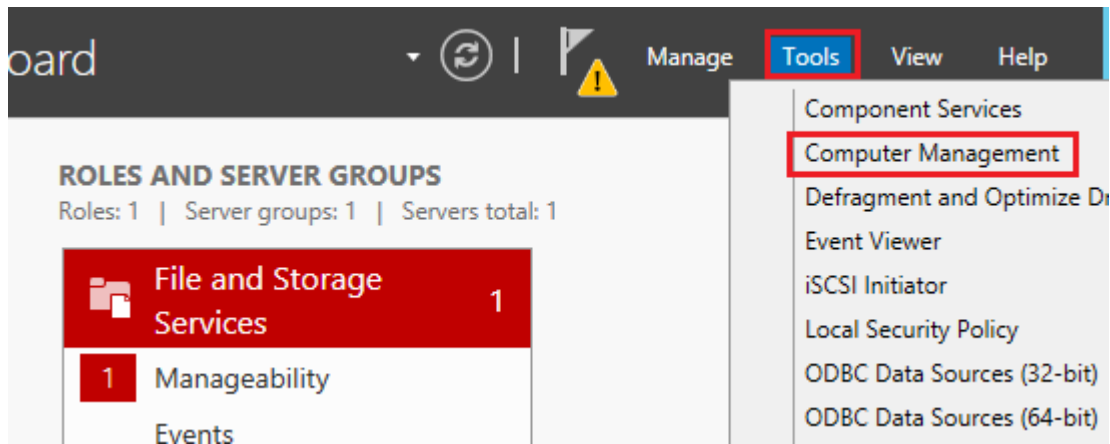
```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

**Bước 4:** Vào giao diện tạo tài khoản người dùng theo đường dẫn:

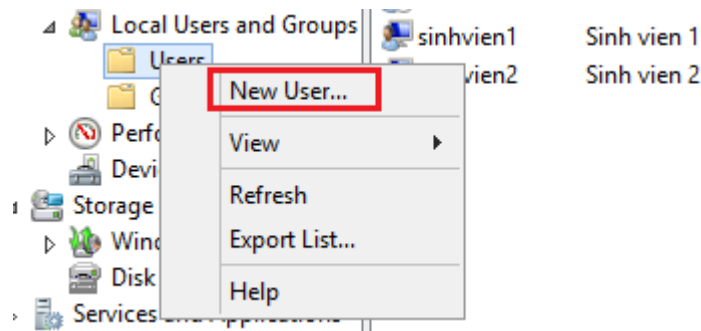
Server Manager → Tools → Computer Management



Giao diện tạo tài khoản người dùng:

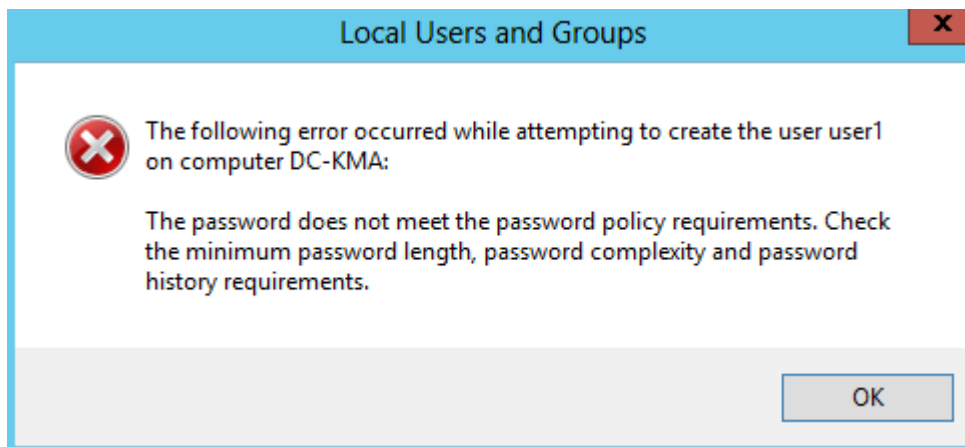


**Bước 5:** Tạo tài khoản người dùng với mật khẩu dễ: chỉ có chữ số 123

A screenshot of the 'New User' dialog box. It contains the following fields and options:

- User name: user1
- Full name: người dùng 1
- Description: (empty)
- Password: (masked with dots)
- Confirm password: (masked with dots)
- Options:
  - ☐ User must change password at next logon
  - ☐ User cannot change password
  - ☒ Password never expires
  - ☐ Account is disabled

Nhấn Create..



Một thông báo hiển thị rằng: không thể tạo ra user1 do không đáp ứng yêu cầu an toàn của mật khẩu mà đã tạo chính sách ở trên.

Tạo người dùng user2 với mật khẩu: Amin@123\*



User name:

Full name:

Description:

---

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

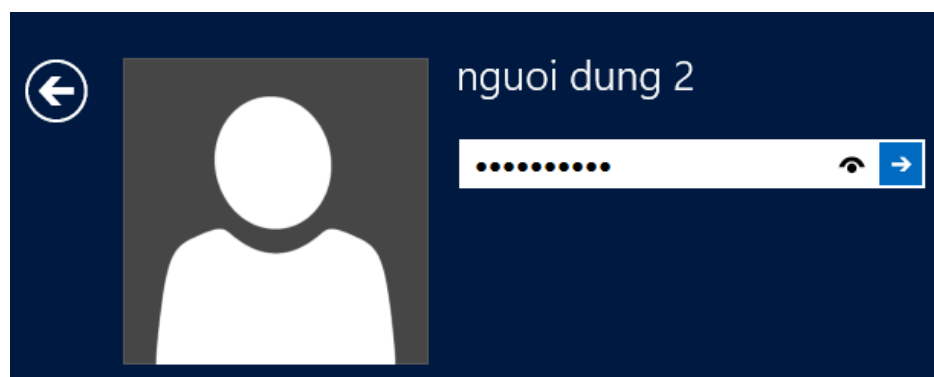
☒ Password never expires

☐ Account is disabled

Name	Full Name	Description
Administrator		Built-in account for administering...
giaovien1	Giao vien 1	Tai khoan giao vien 1
giaovien2	Giao vien 2	Tai khoan giao vien 2
Guest		Built-in account for guest access t...
sinhvien1	Sinh vien 1	Tai khoan sinh vien 1
sinhvien2	Sinh vien 2	Tai khoan sinh vien 2
user2	ngươi dung 2	

Kết quả tạo thành công người dùng user2 vì mật khẩu đảm bảo đúng chính sách đã tạo.

Đăng nhập máy chủ với tài khoản user2 đã tạo:



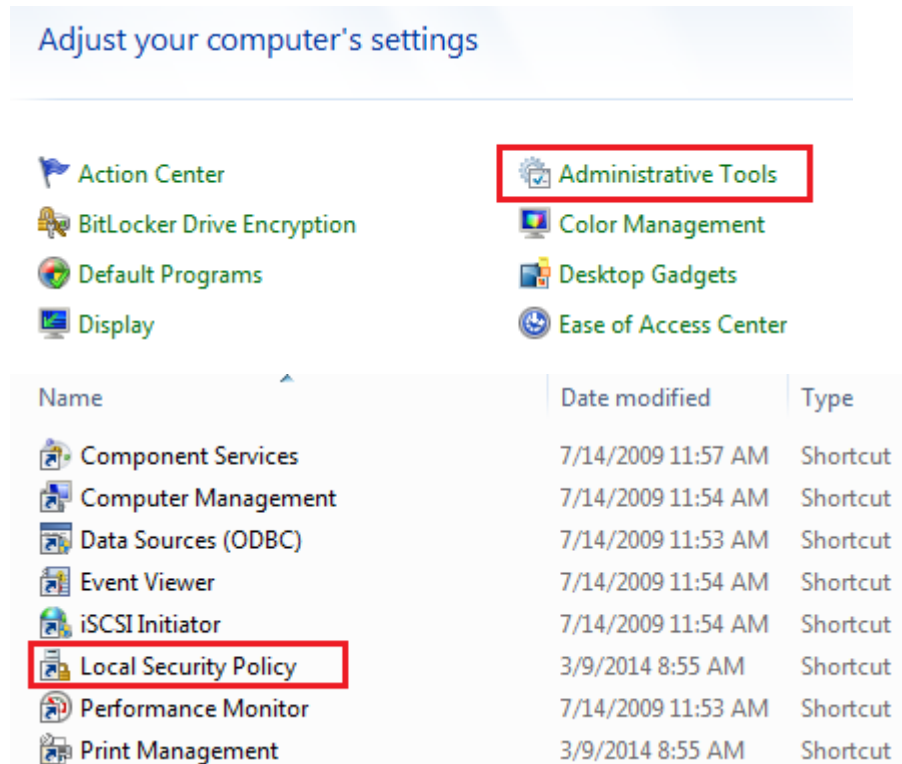
Kết quả đăng nhập thành công.

### 2.1.2 Thiết lập mật khẩu an toàn trên hệ điều hành Windows 7

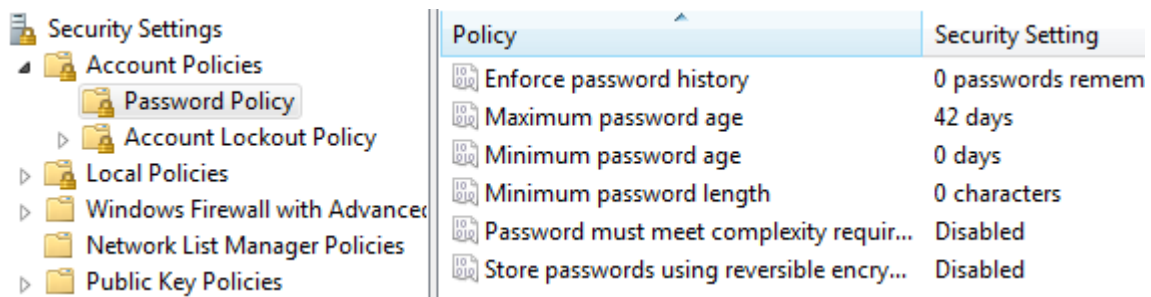
Các bước thực hiện:

**Bước 1:** Truy cập theo đường dẫn sau để vào Local Security Policy

Start → Control Panel → Administrative Tools → Local Security Policy



Các chính sách mặc định cũng tương tự như trong Server 2012.



**Bước 2:** Thực hiện thiết lập các chính sách tương tự như bước 2 trong bài Lab thiết lập mật khẩu cho Server 2012.

Kết quả sau khi thiết lập:

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	6 characters
Password must meet complexity requir...	Enabled
Store passwords using reversible encry...	Disabled

**Bước 3:** Áp dụng chính sách đã thiết lập:

Vào Run → cmd → gpupdate /force

```
C:\Users\admin>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

**Bước 4:** Tạo người dùng với mật khẩu đơn giản: abc

#### Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

Nguoi dung 1

☒ Standard user

Standard account users can use most software and change system settings the security of the computer.

Nhấn Create...

Tiếp tục chọn Change the password:

#### Make changes to Nguoi dung 1's account

[Change the account name](#)

[Change the password](#)

[Remove the password](#)

[Change the picture](#)

[Set up Parental Controls](#)

[Change the account type](#)

[Delete the account](#)

[Manage another account](#)



Nguoi dung 1

Standard user

Password protected

## Change Người dùng 1's password

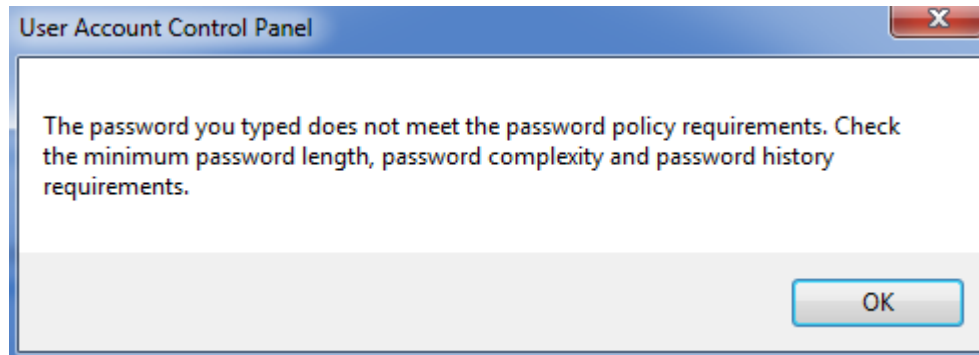


Người dùng 1  
Standard user  
Password protected

You are changing the password for Người dùng 1. If you do this, Ng files, personal certificates, and stored passwords for Web sites or net  
To avoid losing data in the future, ask Người dùng 1 to make a passv

Nhấn Change password



Thông báo xuất hiện với nội dung mật khẩu không phù hợp với chính sách đã tạo.

**Bước 5:** Tạo mật khẩu cho Người dùng 1 với các ký tự: Admin@123\*

## Change Người dùng 1's password



Người dùng 1  
Standard user  
Password protected

You are changing the password for Người dùng 1. If you do this, Người dùng 1 will lo: files, personal certificates, and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask Người dùng 1 to make a password reset floppy c

If the password contains capital letters, they must be typed the same way every time.

Chọn Change password → Thành công vì đáp ứng yêu cầu chính sách mật khẩu.

**Bước 6:** Kiểm thử

Đăng nhập bằng tài khoản Người dùng 1 với mật khẩu Admin@123\*



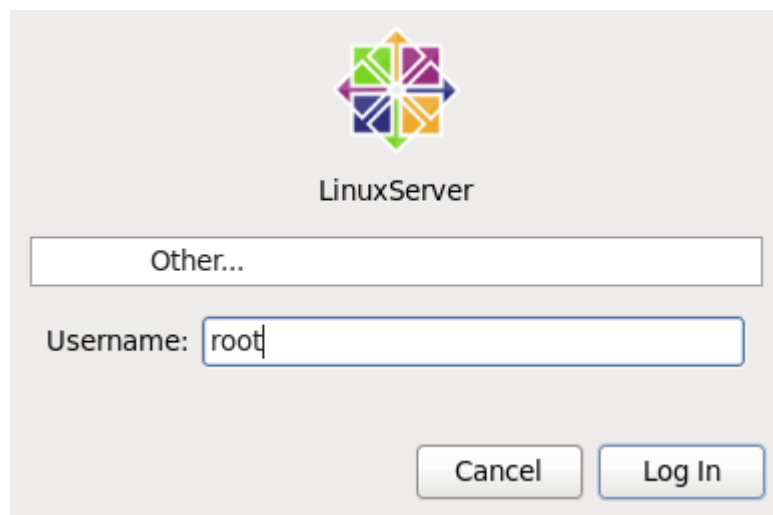
Kết quả đăng nhập thành công với mật khẩu Admin@123\*

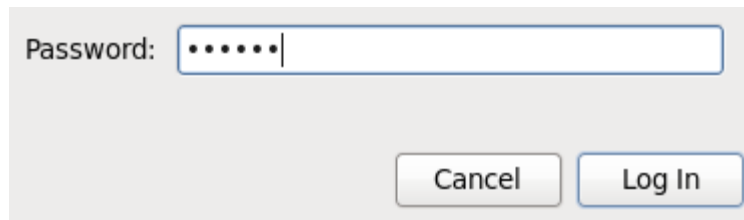
### 2.1.3 Thiết lập mật khẩu an toàn trên hệ điều hành Linux CentOS 6.5

- Thiết lập mật khẩu cho tài khoản toàn quyền root:

#### **Bước 1:** Đăng nhập tài khoản

Mặc định trong quá trình cài đặt hệ điều hành CentOS 6.5 đã yêu cầu nhập mật khẩu cho tài khoản root. Vì vậy để quản trị được mật khẩu người dùng cần phải đăng nhập vào tài khoản root:





Nhấn Log In để đăng nhập vào hệ thống.

### **Bước 2:** Bật cửa sổ dòng lệnh

Truy cập theo đường dẫn để mở cửa sổ dòng lệnh: Applications → System Tools → Terminal.

### **Bước 3:** Thiết lập mật khẩu:

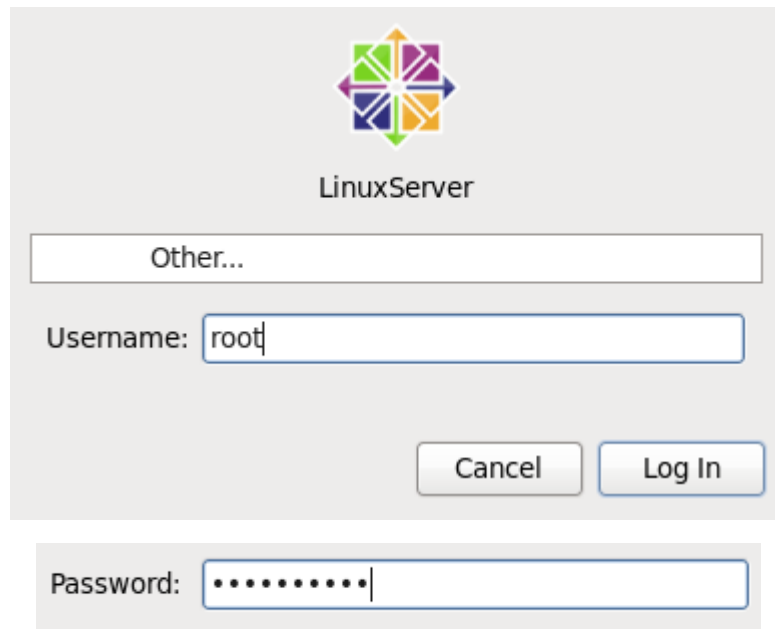
Từ cửa sổ dòng lệnh gõ lệnh: `passwd root` để thay đổi mật khẩu cho người dùng root. Thiết đặt mật khẩu phải bao gồm chữ số, chữ hoa, chữ thường, ký tự đặc biệt: Admin@123\*

```
root@LinuxServer:~  
File Edit View Search Terminal Help  
[root@LinuxServer ~]# passwd root  
Changing password for user root.  
New password:  
BAD PASSWORD: it is based on a dictionary word  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@LinuxServer ~]#
```

Thay đổi thành công.

### **Bước 4:** Kiểm thử

Đăng nhập lại tài khoản root để kiểm tra:

A login dialog box for LinuxServer. At the top is a logo consisting of a stylized 'X' made of four colored squares (green, yellow, blue, red) and the text 'LinuxServer' below it. Below the logo is a text field containing 'Other...'. Underneath that is a 'Username:' label followed by a text field containing 'root'. At the bottom right are two buttons: 'Cancel' and 'Log In'. Below the main dialog box is a 'Password:' label followed by a text field containing ten dots, indicating a masked password.

Đăng nhập thành công. Với mật khẩu dạng này kẻ tấn công rất khó có thể đoán được, hoặc sử dụng công cụ để tấn công.

- Thiết lập mật khẩu cho người dùng thường:

Để có thể thiết lập mật khẩu cho người dùng thì phải sử dụng tài khoản root. Đăng nhập bằng tài khoản root và mở cửa sổ dòng lệnh.

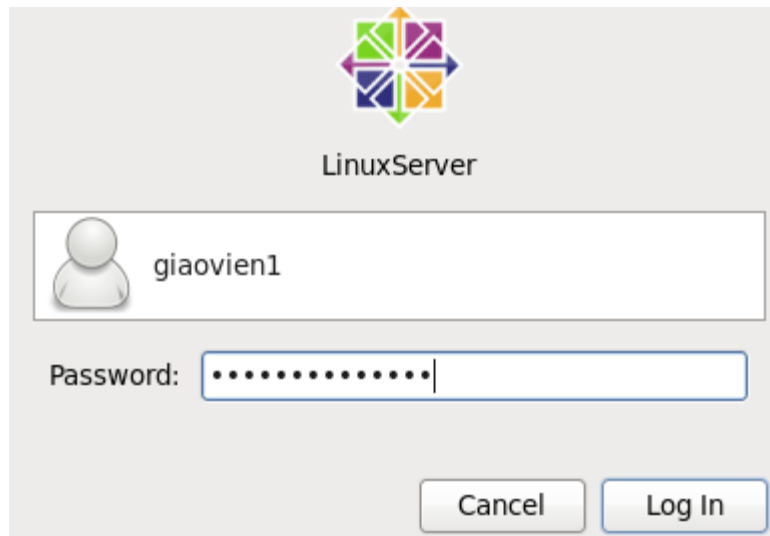
Để thay đổi hoặc nhập mật khẩu mới cho người dùng nào chỉ cần gõ lệnh theo cú pháp:

```
#passwd ten_nguoi_dung
```

Ví dụ: thay đổi mật khẩu cho giaovien1, mật khẩu an toàn: giaovien1\*@987

```
[root@LinuxServer ~]# passwd giaovien1
Changing password for user giaovien1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@LinuxServer ~]# █
```

Đăng nhập bằng tài khoản giaovien1 với mật khẩu giaovien1\*@987:

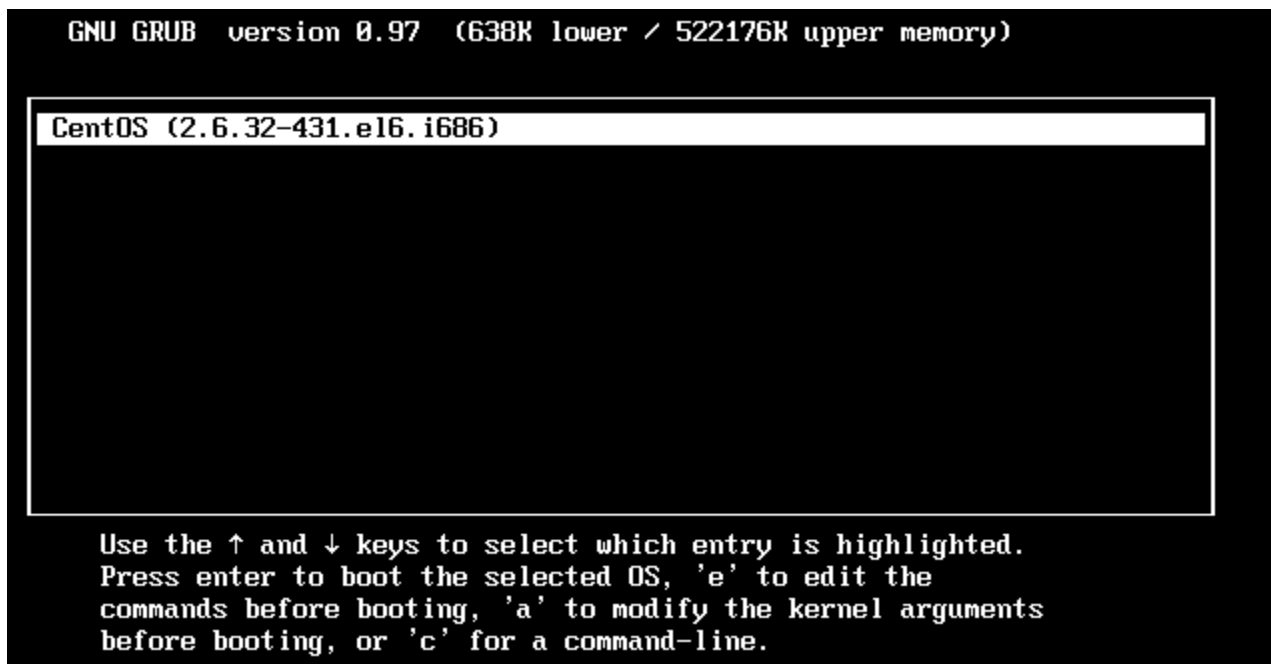


Nhấn Log In để đăng nhập. Kết quả đăng nhập thành công.

- Thiết lập mật khẩu bảo vệ Grub boot loader

Mặc định khi cài xong hệ điều hành Linux CentOS 6.5 hoặc các phiên bản thấp hơn, thì Grub boot loader chưa được đặt mật khẩu bảo vệ. Kẻ tấn công có thể vào chế độ này để thay đổi mật khẩu của tài khoản root và các tài khoản khác. Vì vậy cần thiết phải có mật khẩu để bảo vệ Grub boot loader chống lại truy cập không được phép.

Giao diện Grub boot loader:



Nhấn phím e để vào chỉnh sửa tùy chọn boot.



```
root (hd0,0)
kernel /vmlinuz-2.6.32-431.el6.i686 ro root=UUID=04e0529d-b96e-4672-9→
initrd /initramfs-2.6.32-431.el6.i686.img
```

Chọn dòng thứ 2 và tiếp tục nhấn phím e để chỉnh sửa:

```
[ Minimal BASH-like line editing is supported. For the first
lists possible command completions. Anywhere else TAB lists
completions of a device/filename. ESC at any time cancels.
at any time accepts your changes.]

<c KEYTABLE=us rd_NO_DM rhgb quiet -s
```

Thêm ký tự -s vào cuối dòng (chế độ single mode). Nhấn Enter để chấp nhận.

Nhấn phím b để khởi động hệ điều hành ở chế độ single mode. Giao diện hiển thị như sau:

```
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling local filesystem quotas: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
[root@LinuxServer /]# _
```

Tại bước này kẻ tấn công có thể sử dụng lệnh passwd để thay đổi mật khẩu hoặc thực hiện các lệnh quan trọng khác. Như vậy nếu không đặt mật khẩu cho Grub boot loader thì rất nguy hiểm cho hệ điều hành.

Để bảo vệ Grub boot loader ta phải đặt mật khẩu cho nó. Thực hiện theo các bước sau đây:

**Bước 1:** Đăng nhập vào hệ điều hành bằng tài khoản root:

```
root@LinuxServer:~
File Edit View Search Terminal Help
[root@LinuxServer ~]#
```

**Bước 2:** Sử dụng lệnh grub-md5-crypt để tạo password:

```
[root@LinuxServer ~]# grub-md5-crypt
Password:
Retype password:
$1$9Rbqg1$0HVLqA3DJlRz80ofT2X8C.
[root@LinuxServer ~]# █
```

Với mật khẩu đầu vào là Admin@123\* thì thuật toán sẽ sinh ra chuỗi:  
\$1\$9Rbqg1\$0HVLqA3DJlRz80ofT2X8C

**Bước 3:** Mở tệp tin grub.conf theo đường dẫn để thêm chuỗi đã sinh ở bước 2.

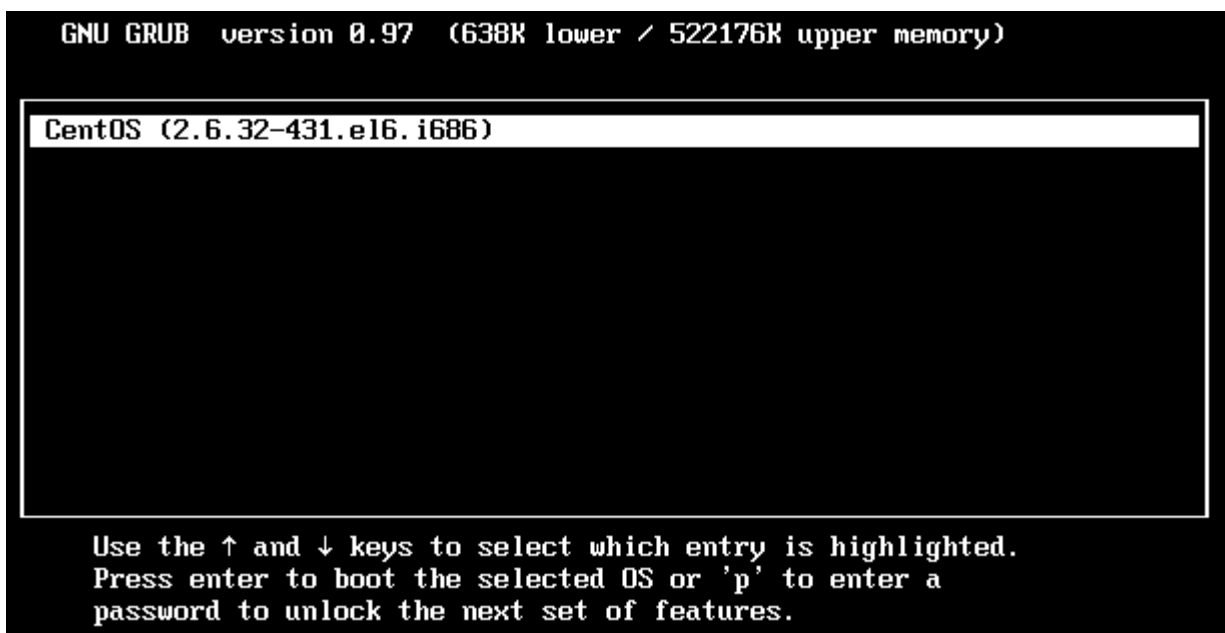
```
[root@LinuxServer ~]# gedit /boot/grub/grub.conf

#           kernel /vmlinuz-version ro root=/dev/sda2
#           initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
password --md5 $1$9Rbqg1$0HVLqA3DJlRz80ofT2X8C.
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-431.el6.i686)
    root (hd0,0)
```

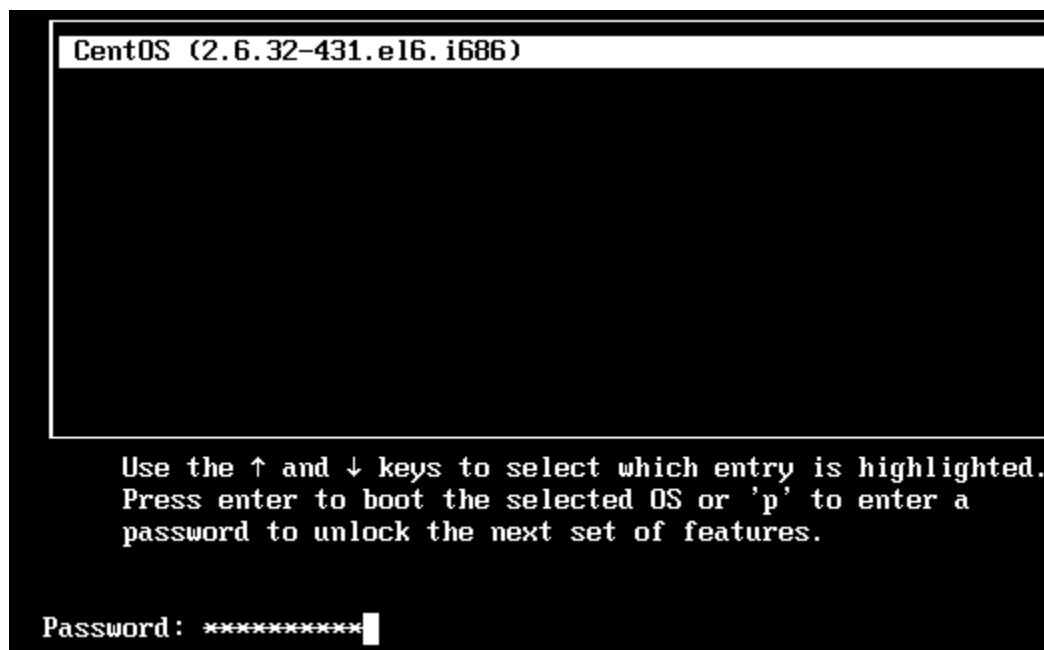
Lưu tệp tin và khởi động lại hệ điều hành

**Bước 4:** Kiểm thử

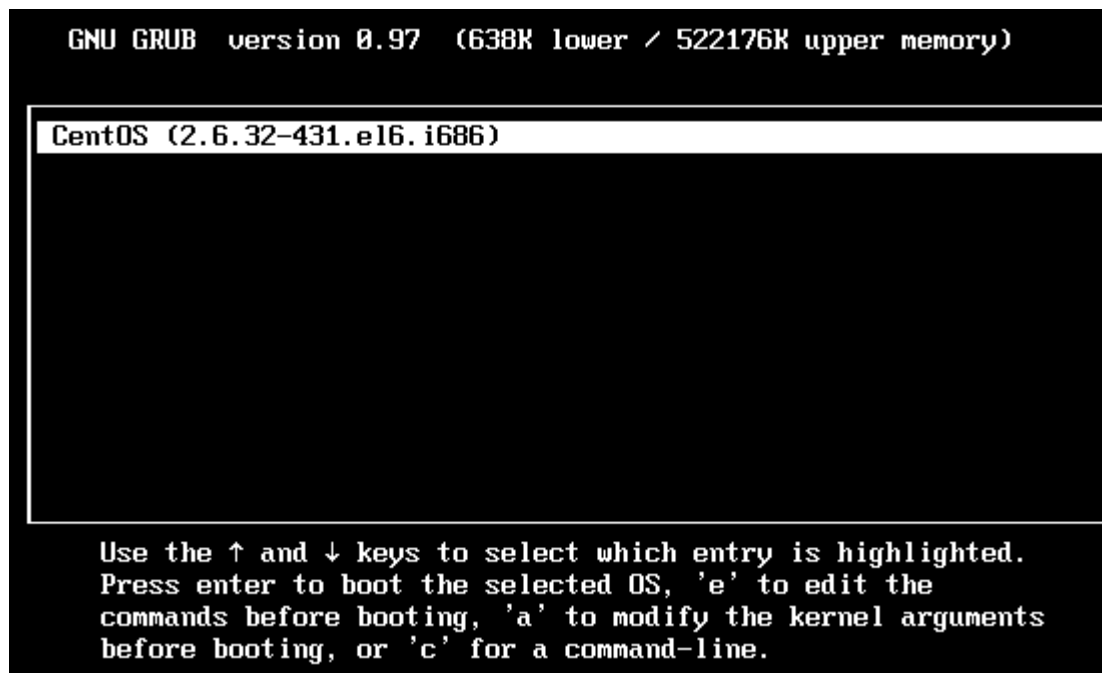
Khởi động lại hệ điều hành, màn hình xuất hiện:



Tại màn hình này để truy cập và chỉnh sửa được boot loader phải có mật khẩu mới vào được. Và mật khẩu chỉ có người quản trị thiết lập mới biết. Nhấn p để nhập mật khẩu:



Sau khi nhập mật khẩu hợp lệ, màn hình tiếp theo có thể chỉnh sửa boot loader:



Kết luận: Cần phải thiết lập mật khẩu có mức độ phức tạp cho các tài khoản trên hệ thống, và mật khẩu cũng phải tuân thủ các chính sách để đảm bảo an toàn.

## **BÀI 3. THỰC HÀNH THIẾT LẬP SỬ DỤNG SSL ĐỂ MÃ HÓA CHO DỊCH VỤ WEB, MAIL**

### **3.1 Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ web**

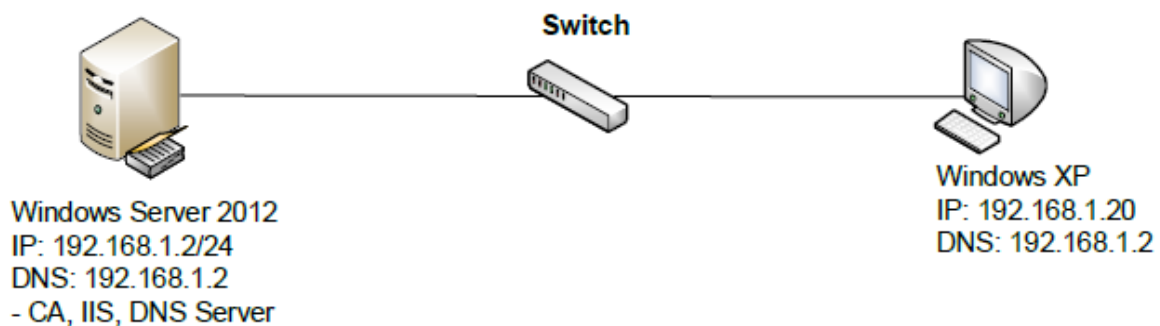
#### **Mục đích bài thực hành:**

Bài thực hành hướng dẫn sinh viên cài đặt, cấu hình các dịch vụ phân giải tên miền DNS, cài đặt và cấu hình cho dịch vụ Web IIS 8. Cài đặt dịch vụ cung cấp chứng thư số Certification Authority (CA). Xin chứng thư và cấu hình SSL cho dịch vụ web IIS. Nhằm mục đích bảo mật dữ liệu trên đường truyền giữa máy trạm web client và máy chủ web.

#### **Yêu cầu hệ thống:**

- 01 Máy chủ chạy hệ điều hành Windows Server 2012.
- 01 máy trạm chạy hệ điều hành Windows XP
- Cả 2 máy trên kết nối được với nhau.

#### **Mô hình triển khai:**



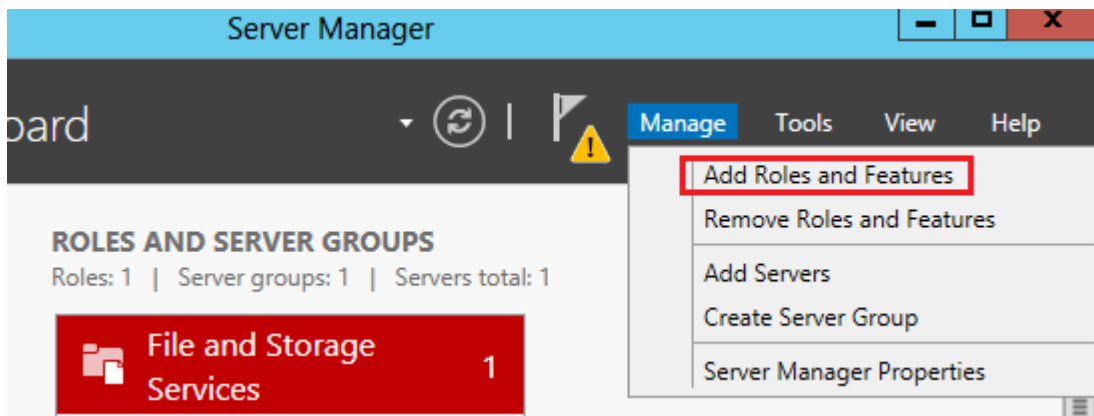
#### **Các bước triển khai:**

##### **3.1.1 Cài đặt DNS trên máy chủ Windows Server 2012**

**Bước 1:** Đăng nhập bằng tài khoản quản trị Administrator vào máy chủ Windows Server 2012.

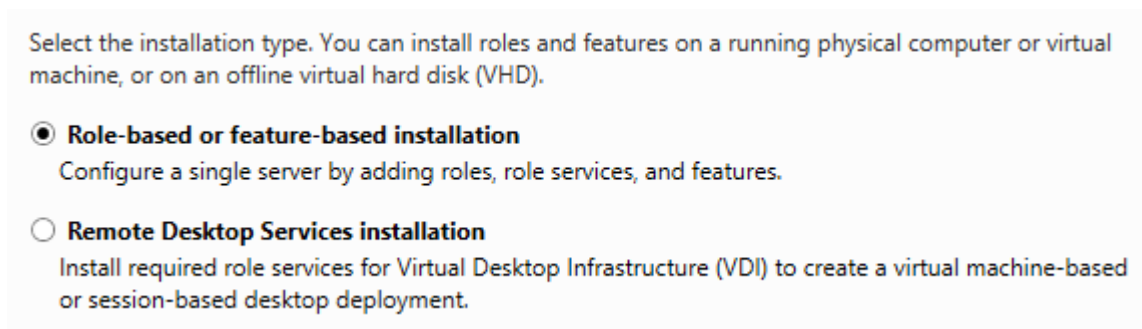
**Bước 2:** Truy cập theo đường dẫn để cài đặt dịch vụ DNS:

Server Manager → Manage → Add Roles and Features



**Bước 3:** Cửa sổ Add Roles and Features xuất hiện chọn Next để bắt đầu quá trình cài đặt.

Trong lựa chọn Select installation type → chọn Role-based or feature-based installation để cài đặt các dịch vụ và tính năng cho máy chủ.



Chọn Next để tiếp tục cài đặt.

Trong tùy chọn Select destination server → Chọn Select a server from the server pool.

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool  
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
DC-KMA	192.168.1.2	Microsoft Windows Server 2012 Release Candidate Data

<  >

1 Computer(s) found

Chọn Next để tiếp tục cài đặt.

#### Bước 4: Lựa chọn dịch vụ

Trong tùy chọn Select server roles → tích vào dịch vụ DNS server

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server
- ☐ Fax Server

Chọn Next để tiếp tục cài đặt.

Trong tùy chọn Select features để mặc định và chọn Next để tiếp tục.

Trong tùy chọn Confirm installation selection tích vào tùy chọn Restart the destination server automatically if required

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Chọn Install để cài đặt dịch vụ

View installation progress



Feature installation



Installation started on DC-KMA

DNS Server

Remote Server Administration Tools

Role Administration Tools

DNS Server Tools

Sau khi cài đặt thành công, trên giao diện Server Manager xuất hiện thêm chức năng giám sát dịch vụ DNS.

#### ROLES AND SERVER GROUPS

Roles: 2 | Server groups: 1 | Servers total: 1



DNS

1

1

Manageability

Events

Services

Performance

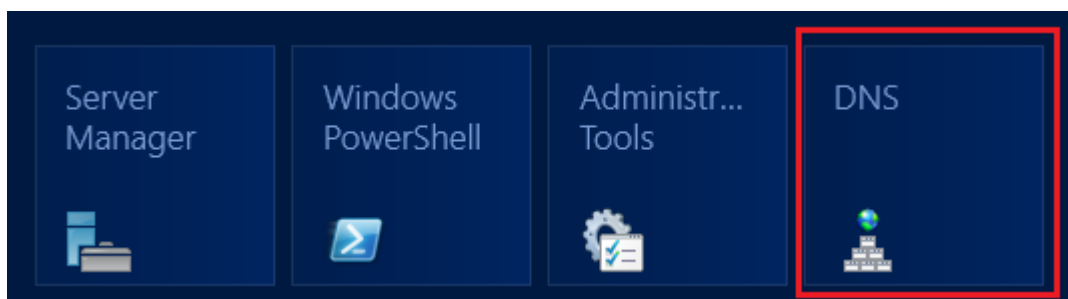
BPA results

5/5/2014 9:13 PM

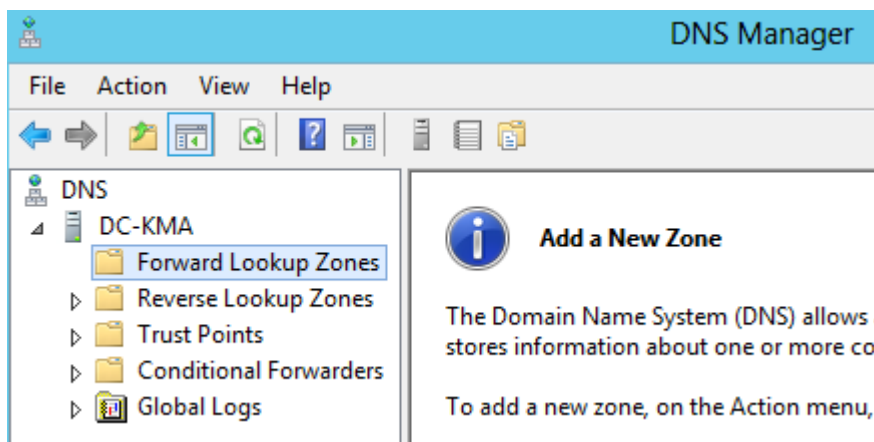
**Bước 5:** Cấu hình dịch vụ DNS để phân giải tên miền

Nhấn phím Start chọn DNS





Cửa sổ cấu hình DNS xuất hiện



**Bước 6:** Cấu hình phân giải xuôi:

Chuột phải vào mục Forward Lookup Zones → chọn New Zone

Trong mục Zone Type → chọn Primary zone

#### Zone Type

The DNS server supports various types of zones and storage.

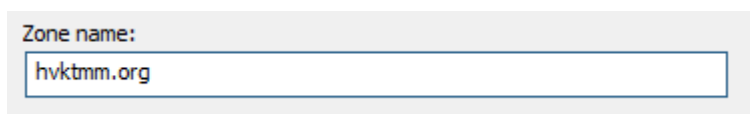
Select the type of zone you want to create:

☒ Primary zone

Creates a copy of a zone that can be updated directly on this server.

Chọn Next để tiếp tục

Trong mục Zone Name → điền tên miền: hvktmm.org



Trong mục Zone File để mặc định → Next

### Zone File


You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

Trong mục Dynamic Update → chọn Allow both nonsecure and secure dynamic update

☐ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.

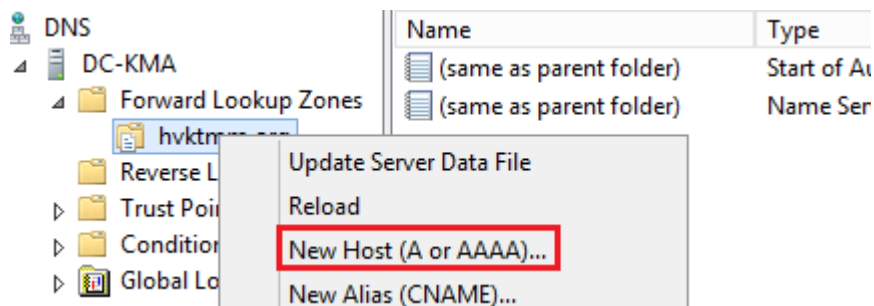
☒ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Chọn Next → Finish

### Bước 7: Tạo bản ghi Host A (www)

Chuột phải vào mục hvktmm.org chọn New Host



**New Host**

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

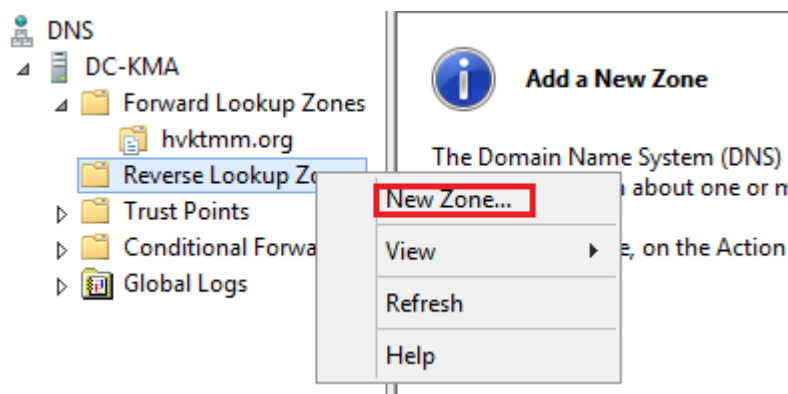
☒ Create associated pointer (PTR) record

Trong mục Name nhập www

Trong mục IP address nhập địa chỉ IP của Server → Add Host

### **Bước 8:** Cấu hình phân giải ngược

Chuột phải vào mục Reverse Lookup Zone chọn New Zone



Trong mục Zone Type → chọn Primary Zone

Trong mục Reverse Lookup Zone Name → chọn Ipv4 Lookup zone → Next

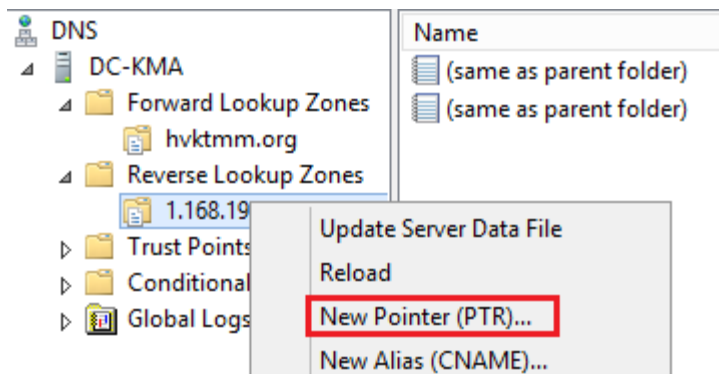
Trong mục Network ID nhập dải địa chỉ IP máy chủ sử dụng: 192.168.1 → Next

Trong mục Zone file để mặc định → Next

Trong mục Dynamic Update chọn Allow both nonsecure and secure dynamic update → Next → Finish

### **Bước 9:** Tạo bản ghi phân giải ngược PTR

Chuột phải vào dải IP đã khai báo chọn New Pointer



Nhập IP của Server (192.168.1.2)

Trở đến bản ghi Host A trong phân giải xuôi.

Nhấn OK → Finish

### **Bước 10:** Kiểm tra phân giải tên miền

Bật cửa sổ dòng lệnh CMD, sử dụng lệnh nslookup để kiểm tra

```
C:\Users\Administrator>nslookup
Default Server: www.hvktmm.org
Address: 192.168.1.2

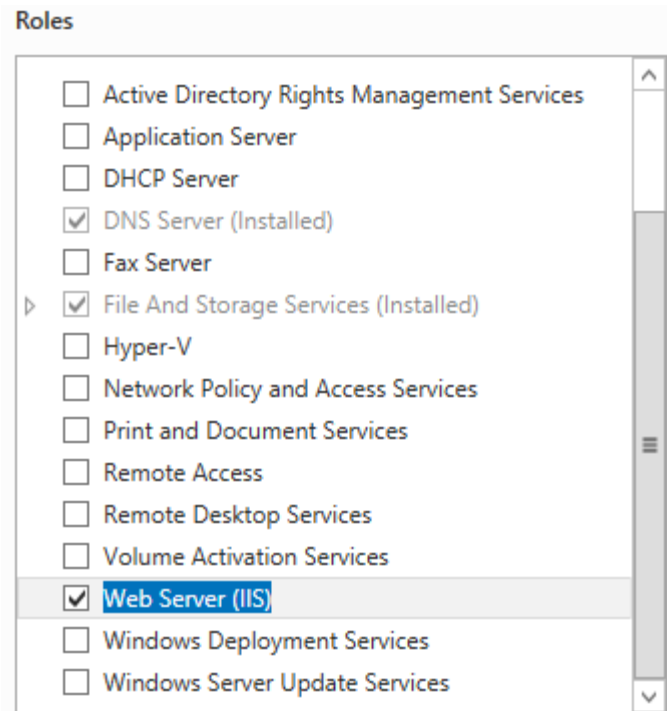
> www.hvktmm.org
Server: www.hvktmm.org
Address: 192.168.1.2

Name: www.hvktmm.org
Address: 192.168.1.2
```

Kết quả trả về đã có IP tương ứng với tên miền đã tạo.

### *3.1.2 Cài đặt dịch vụ web IIS 8 trên máy chủ Windows Server 2012*

Thực hiện lại bước 2 và 3 trong mục 3.1.1 để vào mục Select server roles. Tích chọn dịch vụ Web server (IIS).

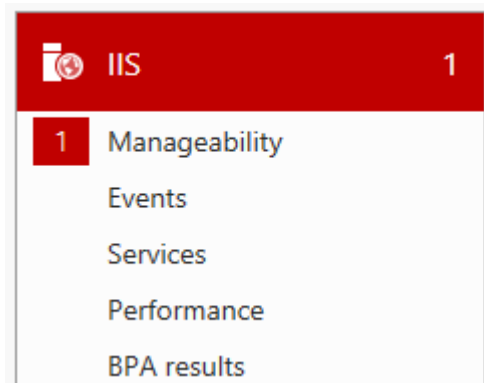


Chọn Next để tiếp tục.

Trong mục Select features để mặc định → chọn Next để tiếp tục.

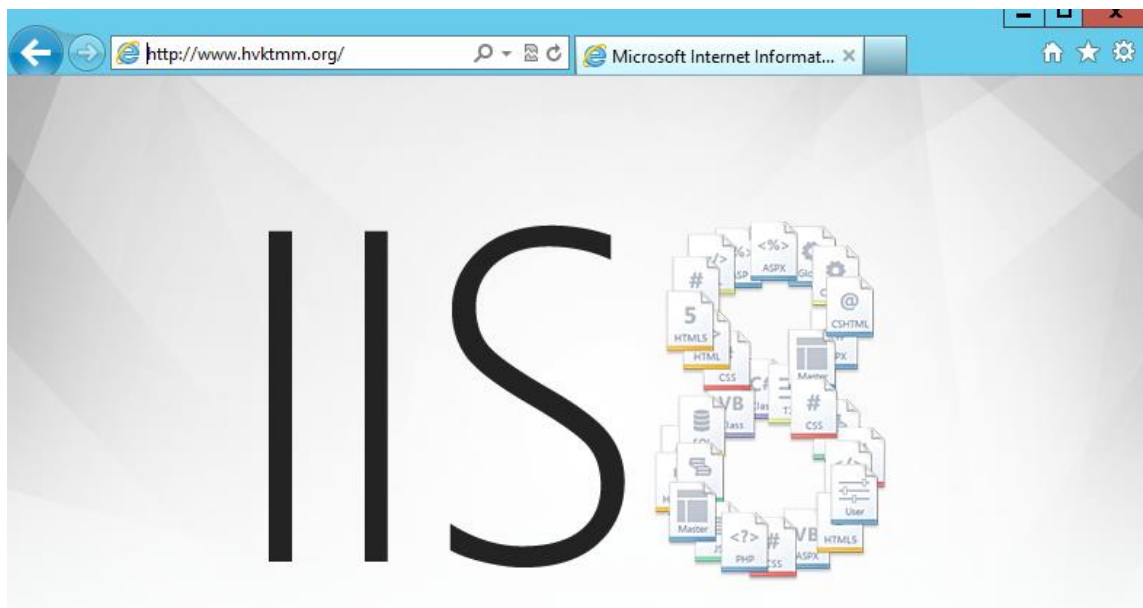
Các bước tiếp theo để mặc định → Install

Sau khi cài đặt thành công trong Server Manager xuất hiện giao diện giám sát dịch vụ IIS.



Bước 4: Kiểm tra hoạt động của web server

Bật trình duyệt web IE và gõ tên miền đã tạo ở trên: [www.hvktmm.org](http://www.hvktmm.org)



Giao diện xuất hiện trang web mặc định của IIS 8.

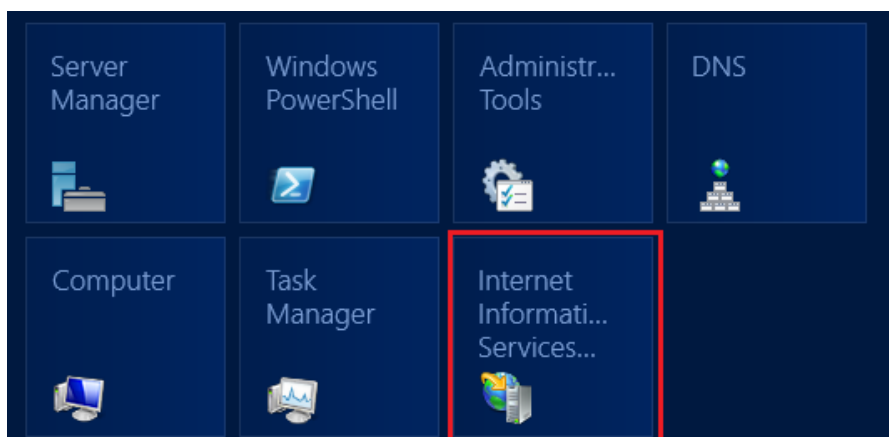
**Bước 5:** Tạo trang web riêng

Truy cập vào thư mục lưu trữ web của IIS theo đường dẫn: C:\inetpub\wwwroot

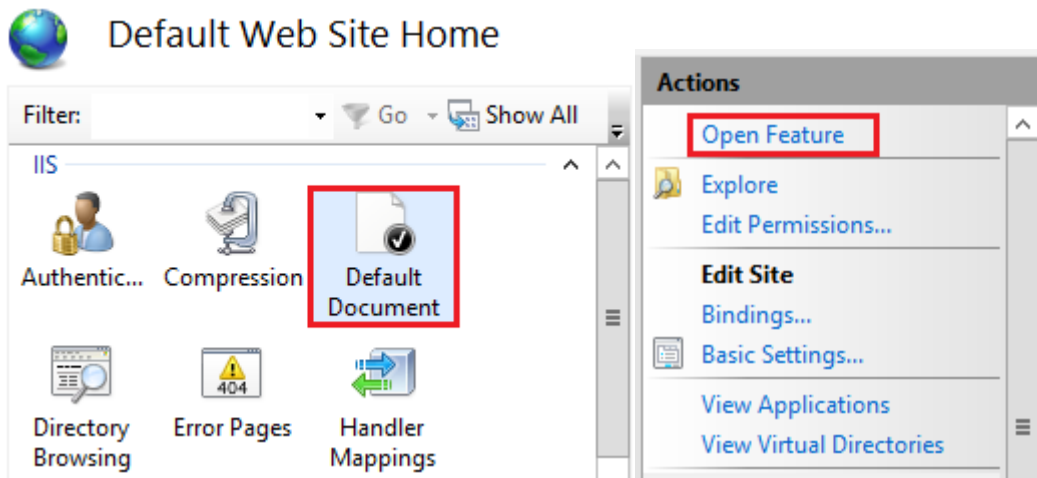
Tạo tệp tin mới có tên index.html, chỉnh sửa nội dung của file theo ý muốn.

**Bước 6:** Cấu hình để IIS nhận tệp tin index.html

Thực hiện theo đường dẫn: Start → Internet Information Service

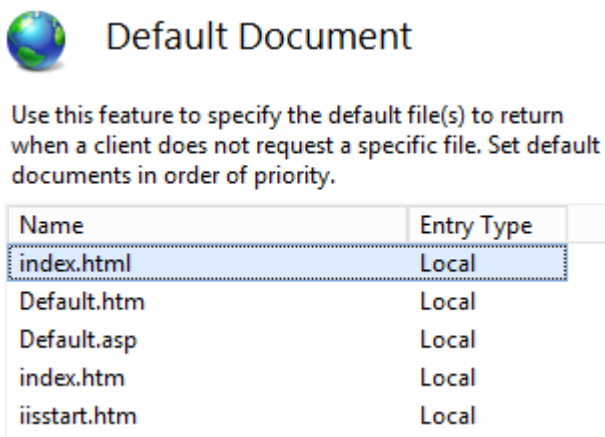


Truy cập vào website mặc định: Default Web Site



Chọn Default Document → Open feature.

Di chuyển vị trí của file index.html lên trên cùng như hình dưới đây:



OK.

### Bước 7: Kiểm tra kết quả

Bật trình duyệt web IE và truy cập theo tên miền đã tạo ở trên.

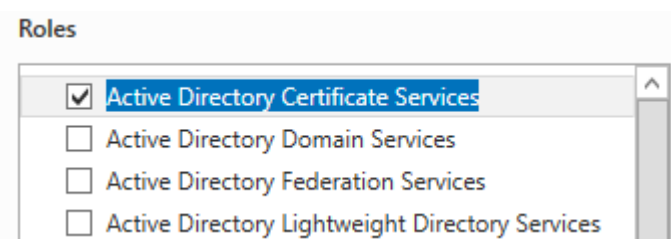


Trang web mặc định hiển thị trang index.html đã tạo ở trên.

### 3.1.3 Cài đặt dịch vụ Certification Authority (CA)

**Bước 1:** Thực hiện lại bước 2 và 3 trong mục 3.1.1 để truy cập đến các dịch vụ cần cài đặt.

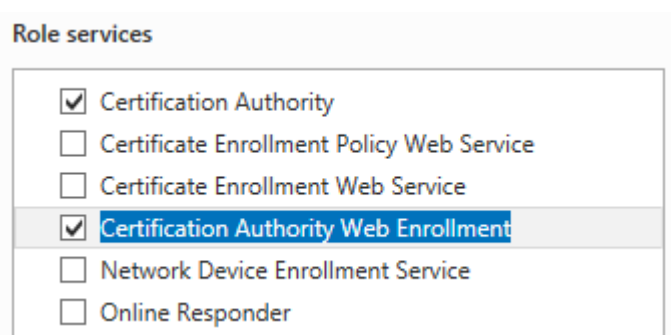
**Bước 2:** Tích chọn dịch vụ Active Directory Certificate Service



Chọn Next để tiếp tục.

Trong mục Select features để mặc định → Next

Trong mục Select role services chọn 2 dịch vụ: Certification Authority và Certification Authority Web Enrollment.

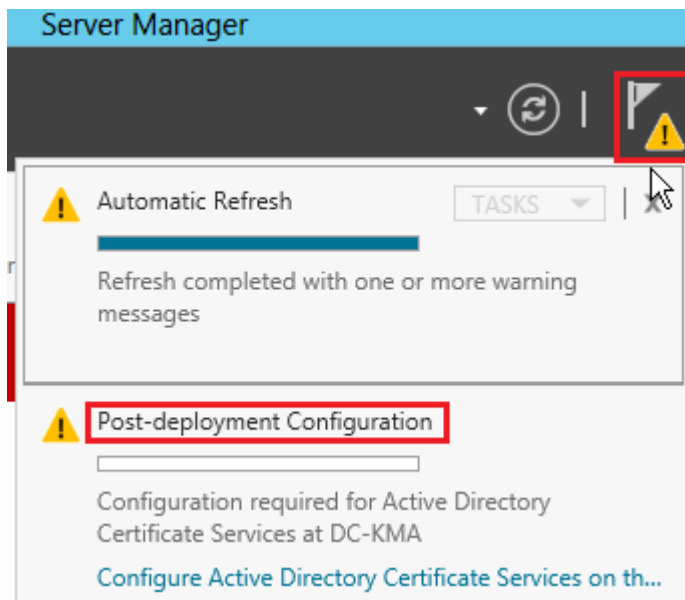


Chọn Next để tiếp tục, chọn Install để cài đặt dịch vụ.

**Bước 3:** Cấu hình dịch vụ CA

Sau khi cài đặt dịch vụ CA thành công, chúng ta phải cấu hình tiếp cho CA. Kích chọn vào biểu tượng hình lá cờ trong giao diện Server Manager như hình dưới đây:

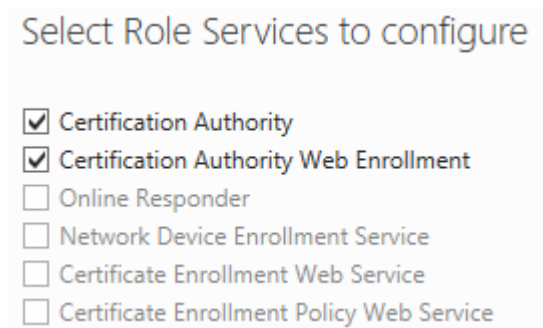




Tiếp tục chọn Configure Active Directory Certificate Services

Trong giao diện Credential để mặc định → chọn Next

Trong giao diện Role Services tích chọn 2 tùy chọn Certification Authority và Certification Authority Web Enrollment.



Trong giao diện Setup Type chọn Standalone CA → Next.

Trong giao diện CA Type chọn Root CA → Next.

Trong giao diện Private Key chọn Create a new private key → Next.

Trong giao diện Cryptography for CA chọn mặc định → Next.

Trong giao diện CA Name đặt tên cho CA → Next.

Trong giao diện Validity Period để mặc định là 5 năm → Next.

Trong giao diện CA database để mặc định

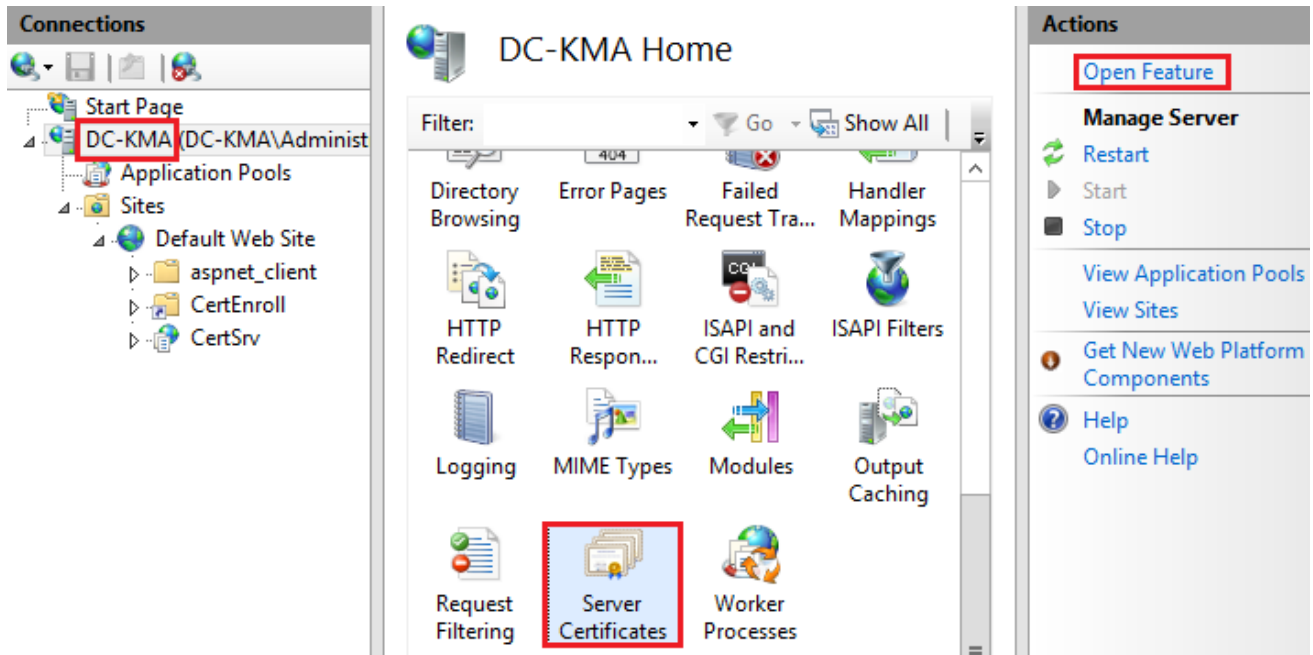
Cuối cùng chọn Configure → Finish

Hoàn tất quá trình cài đặt và cấu hình dịch vụ cung cấp chứng thư số CA.

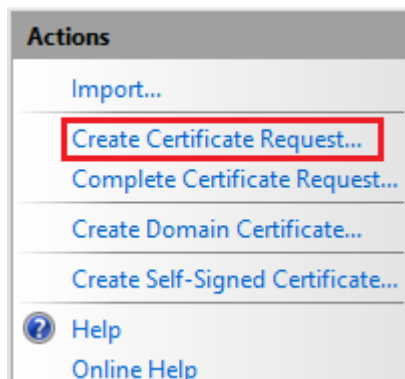
### 3.1.4 Cấu hình SSL cho dịch vụ Web

#### **Bước 1:** IIS gửi yêu cầu chứng thư số tới CA

Bật dịch vụ IIS lên, chọn tên của máy chủ web (DC-KMA), trong giao diện ở giữa DC-KMA Home tìm đến dịch vụ Server Certificates → Open feature



Trong giao diện của Server Certificates, ở cột Action chọn Create Certificate Request



Trong giao diện tiếp theo nhập các thông tin về máy chủ IIS. Đặc biệt trong mục Common name phải nhập tên chính xác của tên miền web.

Common name:	<input type="text" value="www.hvktmm.org"/>
Organization:	<input type="text" value="kma"/>
Organizational unit:	<input type="text" value="kma"/>
City/locality	<input type="text" value="ha noi"/>
State/province:	<input type="text" value="ha noi"/>
Country/region:	<input type="text" value="VN"/>

Chọn Next để tiếp tục.

Trong giao diện tiếp theo tùy chọn của độ dài khóa mã, mặc định là 1024 bit.

Trong giao diện tiếp theo File Name, trở đến nơi lưu trữ file và đặt tên cho file. File này lưu trữ thông tin về khóa.

Specify a file name for the certificate request:

Chọn Finish để kết thúc.

## Bước 2: Gắn thông tin về khóa với chứng thư số

- Bật trình duyệt Web IE lên và truy cập theo tên miền vào đường dẫn của CA:

<http://www.hvktmm.org/certsrv>

- Chọn tùy chọn Request a Certificate → Advanced certificate request → Submit a certificate request by using...

- Mở file key1.txt vừa tạo ở trên, copy nội dung của file và dán vào ô Saved Request

### Saved Request:

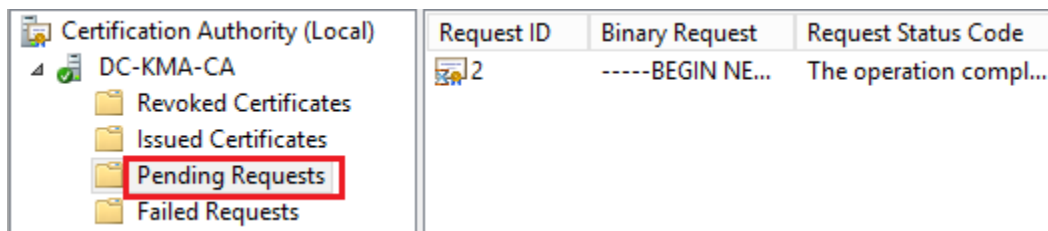
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<pre> BBYEFBOJgBvPTW7SiXjG++30V39hFbCvMA0GCSqG. s8RKDULsdPv3xGWWja1xX+vxG1F6XUnJdJ7OX6aq: //uWDBq1FAhlwc+GWDp93AQQDxCcab+nS29rx05ml DZSWF5M6ihuO2PkesedXgRBgcobBax9nGnmI -----END NEW CERTIFICATE REQUEST----- </pre>
---	---

Chọn Submit.

Yêu cầu chứng thư số kèm với thông tin của khóa mã đã được gửi tới CA.

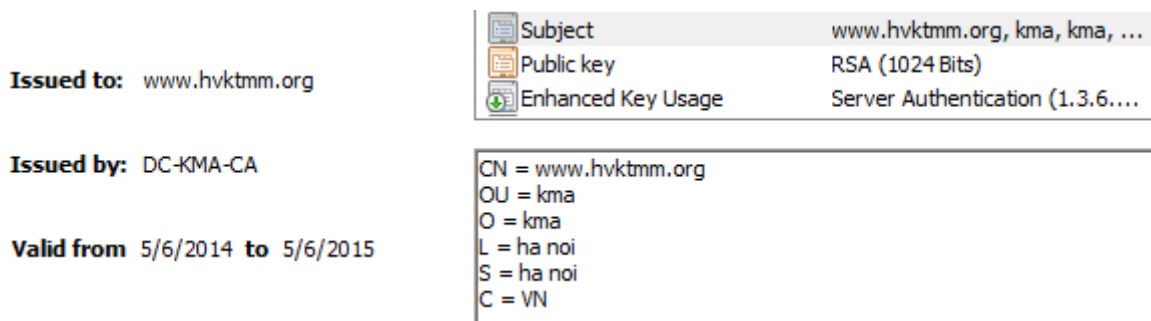
## Bước 3: Cấp chứng thư số cho IIS

- Bật dịch vụ CA lên, truy cập vào mục Pending Requests, thấy có 1 chứng thư đang chờ đợi duyệt của CA.



- Chuột phải vào chứng thư số có ID là 2 và chọn All Tasks → Issue

Bây giờ trong mục Issued Certificates thấy có chứng thư ID 2 đã được cấp với các thông tin như đã khai báo lúc yêu cầu.



- Tiếp tục thực hiện như ở bước 2, truy cập IE theo đường dẫn:

<http://www.hvktmm.org/certsrv>

- Chọn tùy chọn View the status of a pending certificate request

**Select a task:**

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Kích vào đường dẫn Saved-Request Certificate để lưu chứng thư.

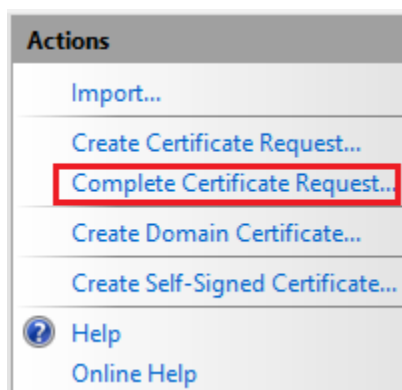
### View the Status of a Pending Certificate Request

Select the certificate request you want to view:

[Saved-Request Certificate \(Tuesday May 6 2014 8:34:15 PM\)](#)

**Bước 4:** Cài đặt chứng thư cho máy chủ IIS

- Bật dịch vụ IIS, chọn máy chủ IIS, chọn Server Certificates, trong mục Action chọn Open feature
- Chọn Complete Certificate Request



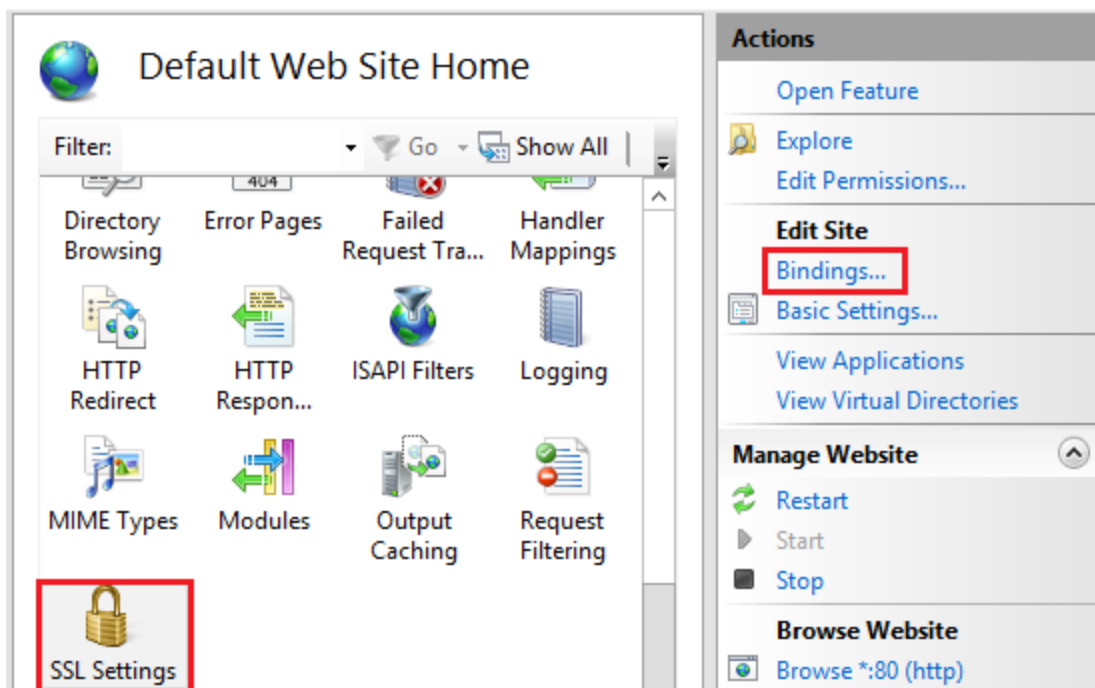
Tiếp tục trở đến nơi lưu trữ chứng thư đã tải về từ bước 3.

A screenshot of the 'Import and Export Certificate' dialog box. It has three main sections. The first section is 'File name containing the certification authority's response:' with a text box containing 'C:\Users\Administrator\Downloads\certnew.cer' and a browse button (...). The second section is 'Friendly name:' with a text box containing 'kma'. The third section is 'Select a certificate store for the new certificate:' with a dropdown menu showing 'Personal'.

Nhấn OK để kết thúc.

### **Bước 5:** Cấu hình để máy chủ IIS chạy dịch vụ SSL

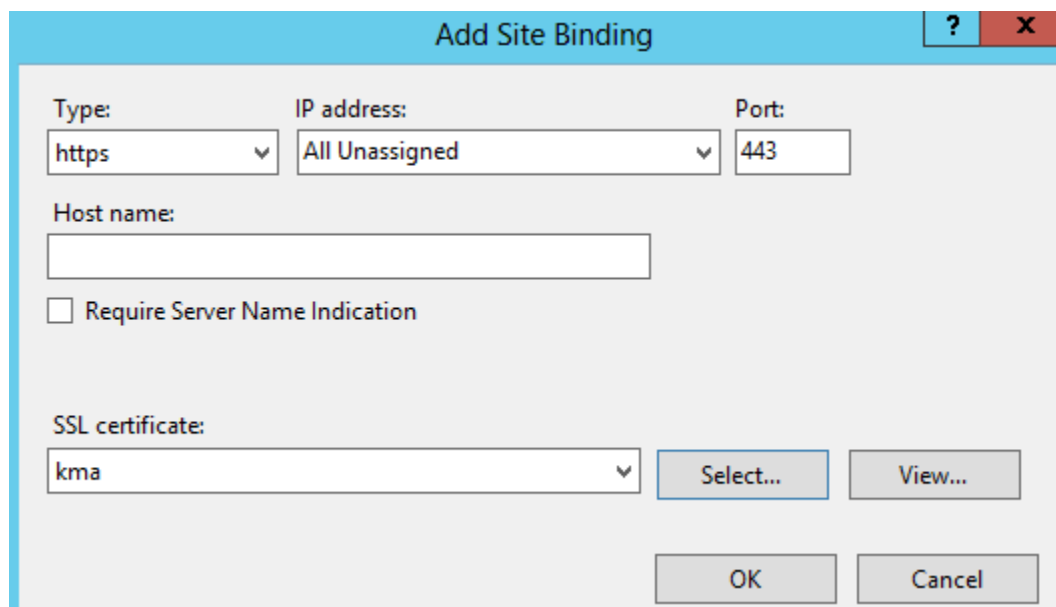
- Từ giao diện quản trị của IIS truy cập tới Sites → Default Web Site, trong các chức năng ở cột giữa Default Web Site Home tìm đến chức năng SSL setting
- Trong mục Action chọn Bindings...



- Giao diện Site Bindings chọn Add

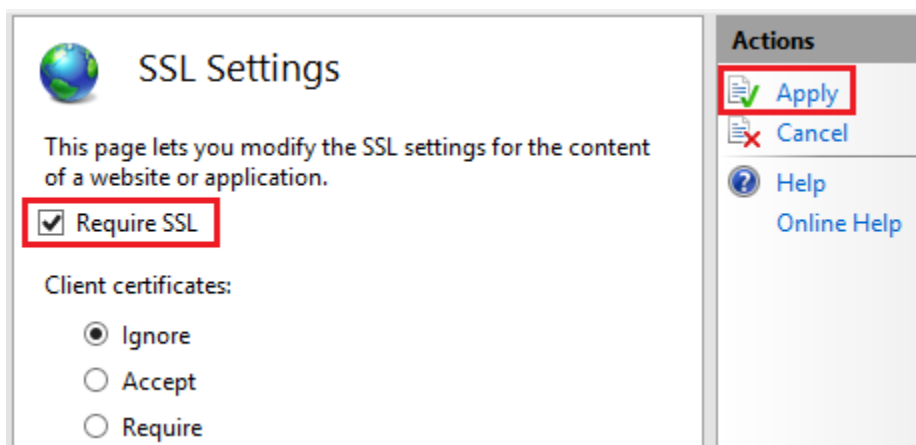
Trong mục Type chọn https : Port 443

Trong mục SSL Certificate → Select → chọn chứng thư đã cài đặt



Chọn OK để kết thúc.

- Trở lại giao diện Default Web Site Home chọn SSL Settings, mục Action chọn Open feature. Tích chọn vào yêu cầu SSL, mục Action chọn Apply



Kết thúc cài đặt và cấu hình SSL.

Bước 6: Kiểm thử

- Bật trình duyệt web IE và gõ tên miền với https



→ Thành công.

- Từ một máy tính chạy hệ điều hành XP kết nối vào mạng của máy chủ IIS và truy cập tên miền với https



→ Thành công.

### 3.2 Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ Mail

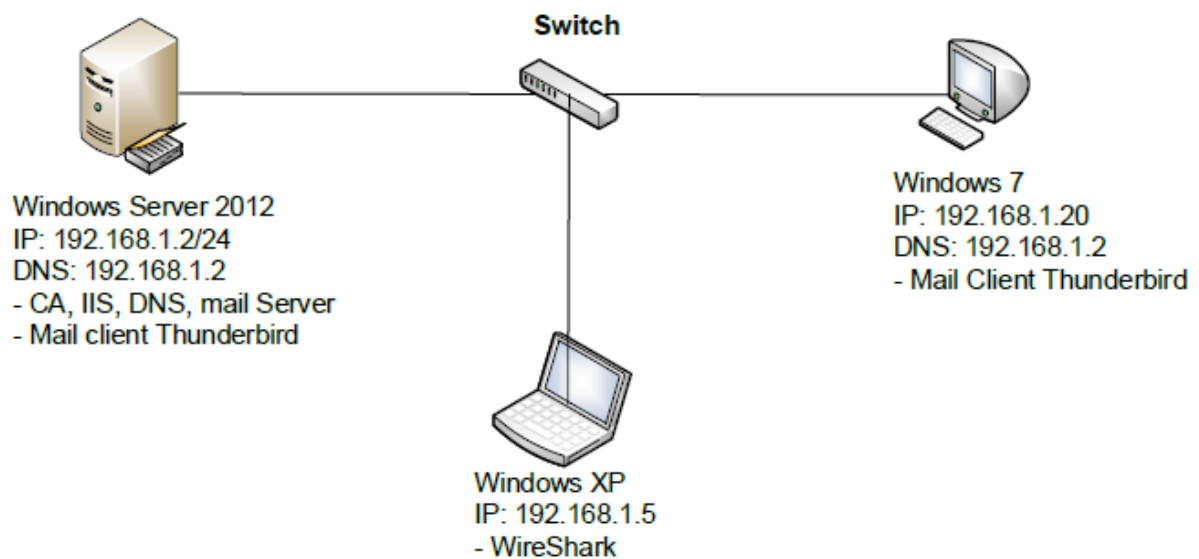
#### Mục đích bài thực hành:

Bài thực hành hướng dẫn sinh viên cài đặt và cấu hình máy chủ dịch vụ mail MDaemon V10, cài đặt và cấu hình phần mềm mail client Thunderbird, xin và cấp chứng thư số cho các tài khoản mail client sử dụng CA, cấu hình các chứng thư số tương ứng để người dùng mã hóa và ký số mail khi gửi từ người dùng này đến người dùng khác. Nhằm mục đích đảm bảo tính bí mật và toàn vẹn nội dung mail khi gửi trên đường truyền.

## **Yêu cầu hệ thống:**

- Máy chủ chạy hệ điều hành Windows Server 2012. Đã cài đặt các dịch vụ:
  - Dịch vụ phân giải tên miền DNS.
  - Dịch vụ cấp chứng thư số Certification Authority.
  - Dịch vụ Web IIS.
- Phần mềm máy chủ dịch vụ mail server MDAemon V10.
- Phần mềm máy trạm mail Thunderbird Setup 24.5.0.
- Phần mềm phân tích lưu lượng mạng Wireshark-win32-1.8.6.
- Máy trạm chạy hệ điều hành Windows 7, Windows XP kết nối với máy chủ Windows Server 2012.

## **Mô hình mạng:**



## **Các bước thực hiện:**

### *3.2.1 Tạo bản ghi MX trong DNS, tắt tường lửa của Server 2012*

#### **Bước 1:** Tạo bản ghi MX để xác định máy chủ mail

- Bật dịch vụ DNS và tạo bản ghi Host A với tên mail:



Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

☒ Create associated pointer (PTR) record

- Tiếp tục tạo bản ghi MX

Mail Exchanger (MX)

Host or child domain:

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) of mail server:

Mail server priority:

Nhấn OK để kết thúc.

**Bước 2:** Tắt tường lửa của Windows để cho phép dịch vụ mail kết nối tới máy chủ mail.

- Bật dịch vụ Server Manager truy cập theo đường dẫn: Tools → Windows Firewall with Advanced Security
- Click vào chức năng Windows Firewall Properties

**Public Profile is Active**

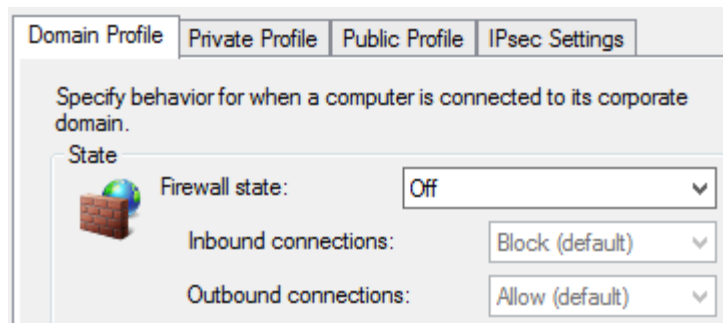
☒ Windows Firewall is on.

☐ Inbound connections that do not match a rule are blocked.

☒ Outbound connections that do not match a rule are allowed.

☒ [Windows Firewall Properties](#)

- Trong các Tab Domain Profile, Private Profile, Public Profile chuyển sang trạng thái Firewall state: Off



Apply → OK → Kết thúc cấu hình tường lửa.

### 3.2.2 Cài đặt phần mềm Mdaemon, tạo tài khoản mail client

Bài thực hành này vẫn kế thừa một số thiết lập ở bài 3.1 như: sử dụng CA, DNS, IIS và vẫn sử dụng https để truy cập tên miền.

**Bước 1:** Cài đặt phần mềm MDAemon V10 làm máy chủ mail

- Copy phần mềm MDAemon V10 vào máy chủ Windows Server 2012 và tiến hành cài đặt.
- Quá trình cài đặt Mdaemon cần một số thiết lập như sau:  
Nhập thông tin đăng ký phần mềm:

- Trong mục Domain Name nhập: hvktnm.org
- Thiết lập First Account:

Full name (ex: Frank Thomas)

Mailbox (ex: Frank - don't include a domain name)

Password (ex: SwordFish - no spaces)

- Thiết lập DNS là địa chỉ của DNS server:

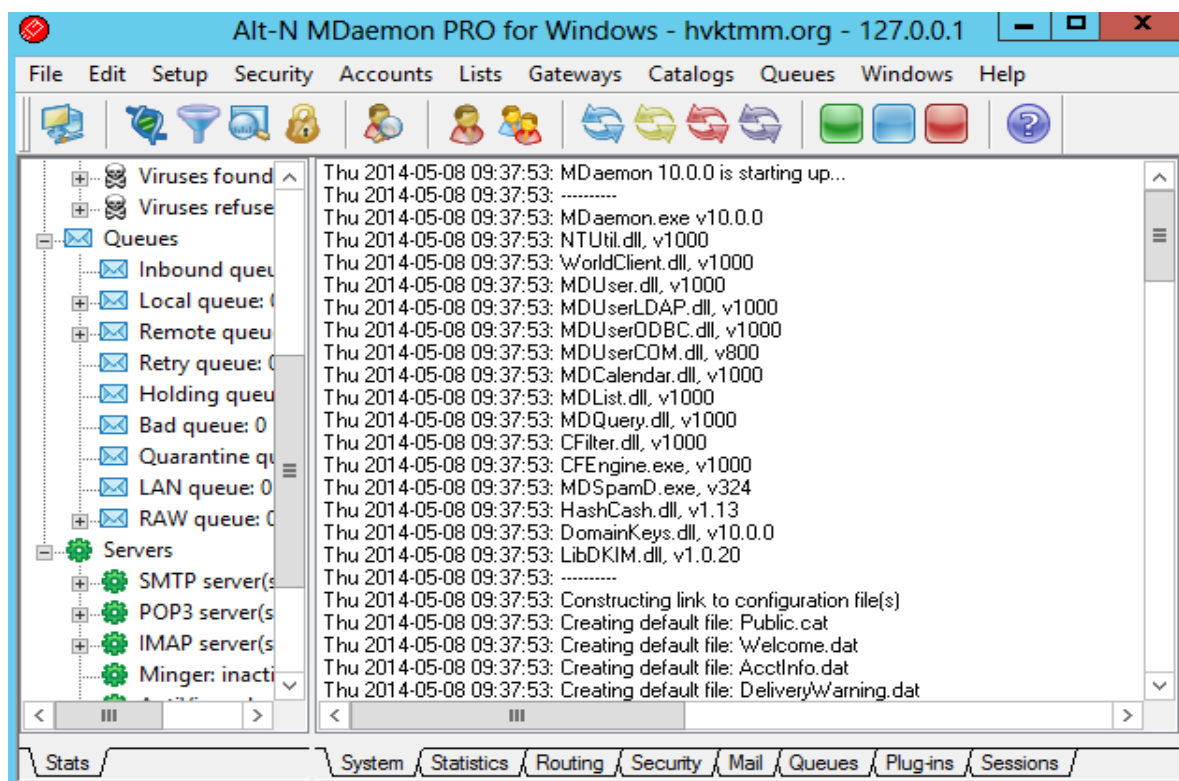
☒ Use Windows DNS settings

Primary DNS IP Address  (optional)

Backup DNS IP Address  (optional)

- Next → Finish

Sau khi cài đặt xong và bật máy chủ mail hoạt động



## Bước 2: Thiết lập tài khoản mail cho người dùng

Truy cập giao diện quản trị mail server và theo đường dẫn như sau:

Main menu → Tab Account → New Account

Trong giao diện tạo tài khoản mới hiện ra, nhập thông tin cho tài khoản, ví dụ:

Chọn OK để kết thúc.

Tương tự tạo tiếp tài khoản có tên là user2.

### 3.2.3 Cài đặt phần mềm Mail Client để gửi và nhận mail

#### Bước 1: Cài đặt tại máy chủ Windows Server 2012

- Copy phần mềm Thunderbird Setup 24.5.0 vào máy chủ Windows Server và tiến hành cài đặt theo chỉ dẫn mặc định.
- Sau khi cài đặt và khởi động phần mềm Thunderbird sẽ hỏi người dùng thiết lập tài khoản. Click vào tùy chọn use my existing email:

- Nhập các thông tin về tài khoản của người dùng user1:

Chọn Continue để tiếp tục. Thunderbird sẽ truy vấn đến tên miền tìm địa chỉ mail đã khai báo.

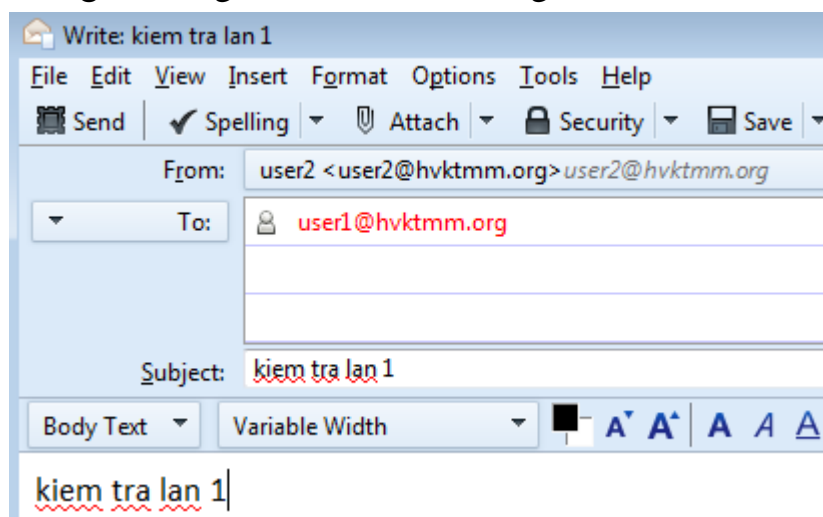
- Kết quả như sau:

Nhấn Done để kết thúc cấu hình.

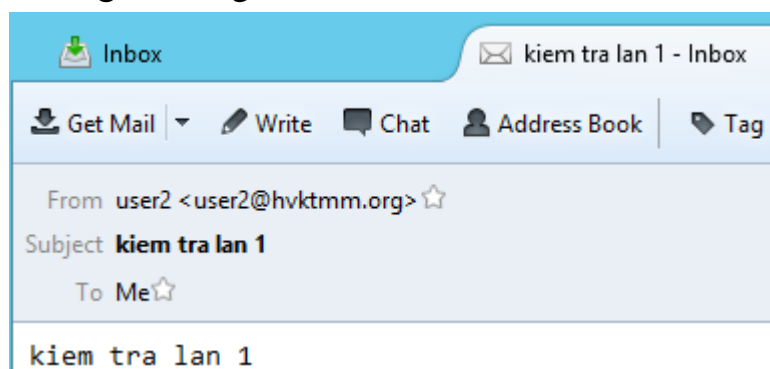
**Bước 2:** Thực hiện tương tự như bước 1 nhưng cài đặt trên máy Windows 7 và tài khoản là của user2.

**Bước 3:** Kiểm tra gửi và nhận mail giữa 2 người dùng user1 và user2.

- Từ người dùng user2 soạn mail và gửi cho user1



- Bên người dùng user1 đã nhận được mail:



**Bước 4:** Chặn bắt thông tin truyền

- Từ máy chạy Windows XP cài phần mềm WireShark chặn bắt thông tin không được mã hóa giữa người dùng user1 gửi cho user2.
- Kết quả chặn bắt

```

MAIL FROM:<user2@hvktmm.org> SIZE=377
250 <user2@hvktmm.org>, Sender ok
RCPT TO:<user1@hvktmm.org>
250 <user1@hvktmm.org>, Recipient ok
DATA
354 Enter mail, end with <CRLF>.<CRLF>
Message-ID: <536BD69E.1050005@hvktmm.org>
Date: Thu, 08 May 2014 12:10:22 -0700
From: user2 <user2@hvktmm.org>
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101
MIME-Version: 1.0
To: user1@hvktmm.org
Subject: kiểm tra lần 2
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

kiểm tra lần 2
.
250 ok, message saved <Message-ID: 536BD69E.1050005@hvktmm.org>

```

Kết quả chặn bắt cho thấy kẻ tấn công có thể biết được người gửi và người nhận, tiêu đề của mail, và quan trọng là biết được nội dung của mail.

### 3.2.4 Cấp chứng thư số cho người dùng user1 và user2

**Bước 1:** Cấp chứng thư số cho người dùng user1 trên máy chủ Windows Server 2012

- Bật trình duyệt web IE và truy cập theo đường dẫn  
<https://www.hvktmm.org/certsrv>
- Trong giao diện web xuất hiện chọn Request a certificate:  
**Select a task:**  
[Request a certificate](#)  
[View the status of a pending certificate request](#)  
[Download a CA certificate, certificate chain, or CRL](#)
- Tiếp tục chọn Advanced certificate request.
- Tiếp tục chọn Create and submit a request to this CA.
- Trong mục Identifying Information: Nhập thông tin của user1
- Trong mục Type of Certificate Needed: chọn E-mail protection certificate
- Trong mục Key options: tích chọn Mark keys as exportable

### Identifying Information:

Name:	user1
E-Mail:	user1@hvktmm.org
Company:	kma
Department:	ha noi
City:	ha noi
State:	ha noi
Country/Region:	vn

### Type of Certificate Needed:

E-Mail Protection Certificate ▼

### Key Options:

☒ Create new key set   ☐ Use existing key set

CSP: Microsoft Enhanced RSA and AES Cryptographic Provider

Key Usage: ☐ Exchange   ☐ Signature   ☒ Both

Key Size: 1024   Min: 384   Max: 16384   (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

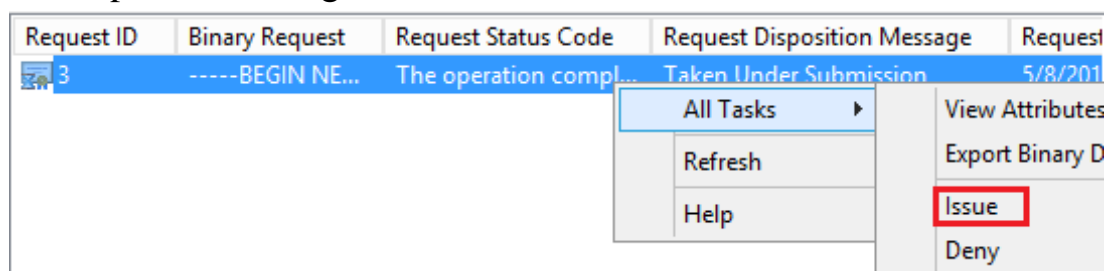
☒ Automatic key container name   ☐ User specified key c

☒ Mark keys as exportable

- Nhấn Submit để gửi yêu cầu tới CA.

**Bước 2:** Truy cập vào dịch vụ CA để cấp phát chứng thư cho người dùng user1

- Truy cập vào mục Pending requests ta thấy có 1 chứng thư đang chờ đợi đồng ý.
- Chuột phải vào chứng thư chọn All Tasks → Issue



- Như vậy chứng thư đã được cấp cho người dùng user1

**Bước 3:** Cài đặt chứng thư của user1 vào máy chủ Windows Server 2012

- Truy cập vào trình duyệt web IE theo đường dẫn:  
<https://www.hvktmm.org/certsrv>
- Trong mục Select a task chọn View the status of a pending certificate request:

**Select a task:**

[Request a certificate](#)

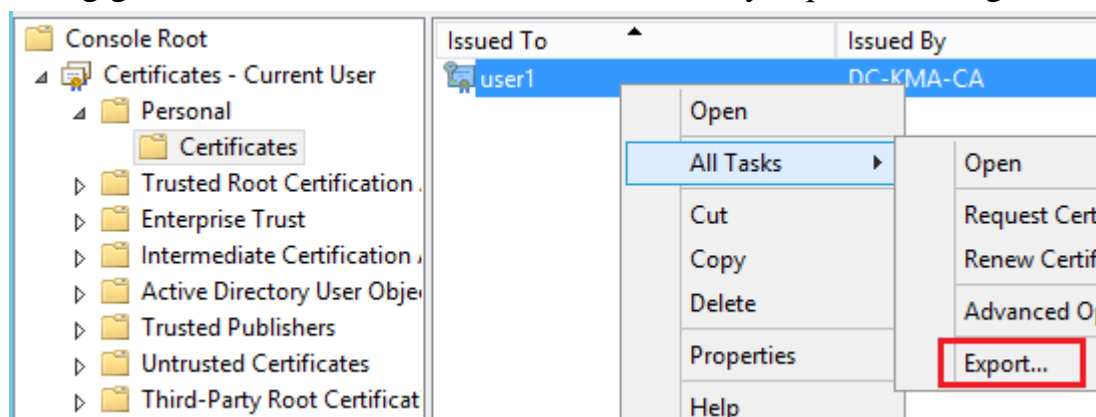
[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

- Chọn E-Mail Protection Certificate.
- Tiếp tục chọn Install this certificate.

**Bước 4:** Trích xuất chứng thư của người dùng user1 thành 2 định dạng để import vào phần mềm Thunderbird.

- Bật công cụ MMC từ Run.
- Chọn File → Add/Remove Snap-in → Certificates → Add (My user account) → OK
- Trong giao diện MMC với dịch vụ Certificate truy cập theo đường dẫn:



Chuột phải vào chứng thư của user1 chọn All Tasks → Export.

- Giao diện truy xuất chứng thư xuất hiện chọn Next để tiếp tục.
- Giao diện tiếp theo chọn No, do not export the private key:

Do you want to export the private key with the certificate?

- ☐ Yes, export the private key
- ☒ No, do not export the private key

Chọn Next để tiếp tục.

- Trong định dạng của chứng thư chọn encoded binary X.509:

Select the format you want to use:

- ☒ DER encoded binary X.509 (.CER)
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)



- Chọn Next để tiếp tục, chọn nơi lưu trữ file và đặt tên chứng thư là user1.cer
- Tiếp tục lại quá trình trích xuất chứng thư của user1 nhưng lần này trích xuất cả khóa bí mật của user1:

Do you want to export the private key with the certificate?



- ☒ Yes, export the private key  
☐ No, do not export the private key

- Định dạng:

- ☒ Personal Information Exchange - PKCS #12 (.PFX)  
☒ Include all certificates in the certification path if possible  
☐ Delete the private key if the export is successful  
☐ Export all extended properties

- Trong mục Security: nhập mật khẩu để bảo vệ khóa.
- Tiếp tục chọn nơi lưu và đặt tên cho chứng thư.

Kết thúc quá trình trích xuất chứng thư với 2 định dạng là user1.cer, và user1-key.pfx

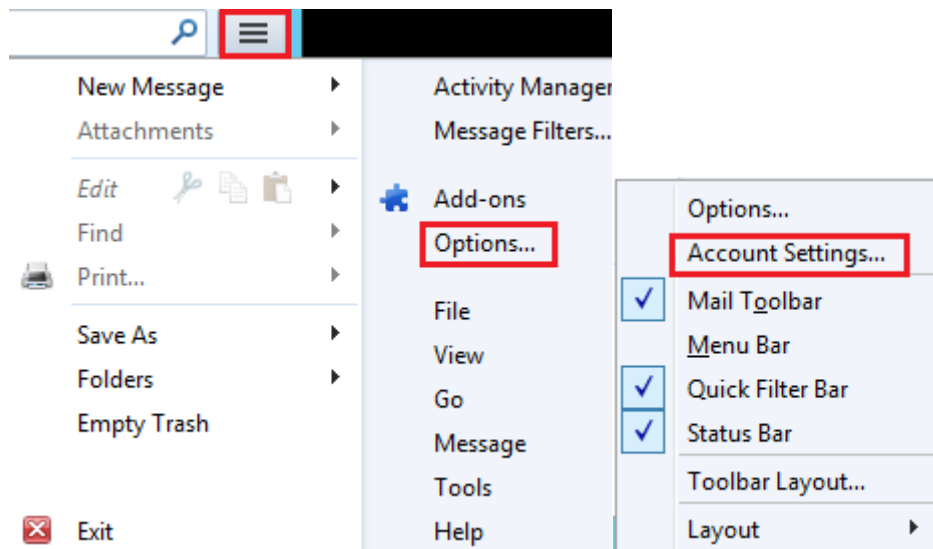
Name	Date modified	Type	Size
 user1.cer	5/8/2014 11:00 AM	Security Certificate	1 KB
 user1-key.pfx	5/8/2014 11:05 AM	Personal Informati...	3 KB

### **Bước 5:** Trích xuất chứng thư của CA để Import vào Thunderbird

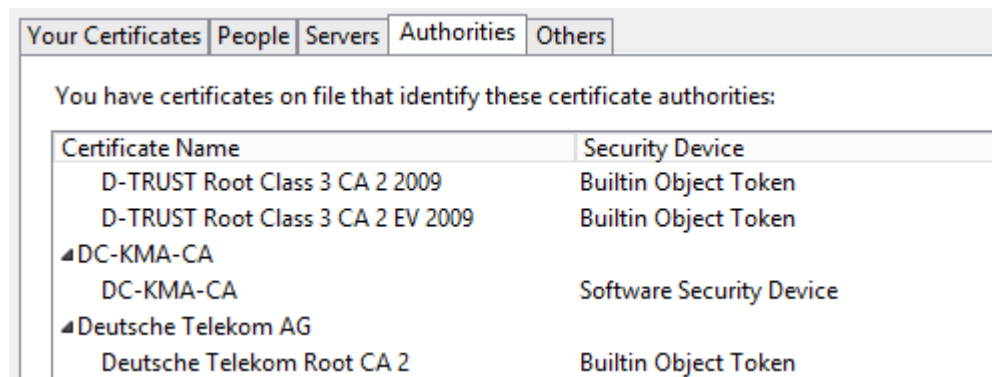
- Trong giao diện MMC Console Root → Trusted Root Certification Authorities chọn chứng thư của CA → All Tasks → Export
- Đặt tên cho chứng thư là CA.cer và chọn nơi lưu trữ.

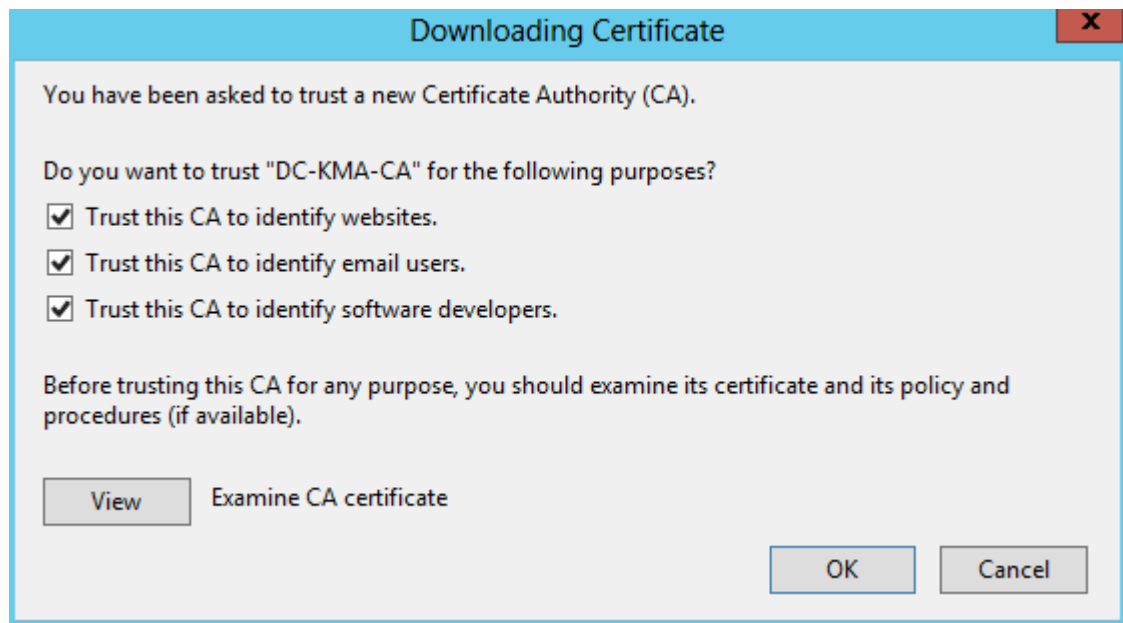
### **Bước 6:** Import 2 chứng thư của user1 vào Thunderbird

- Bật Thunderbird lên và thực hiện theo đường dẫn: chọn biểu tượng 3 dấu gạch ngang ở phía góc của Thunderbird → Chọn Options, thanh công cụ hiện ra chọn Account Settings



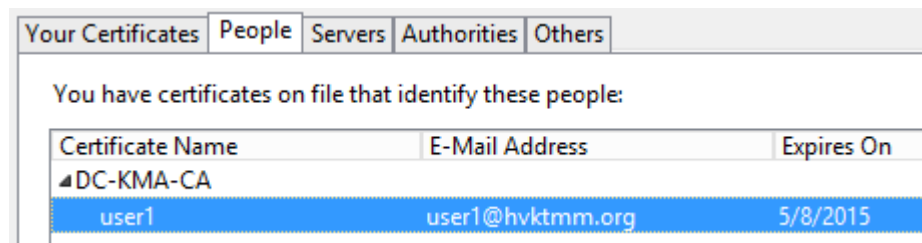
- Trong giao diện Account Setting chọn tab Security
- Trong mục Certificates chọn View certificate
- Giao diện Certificate Manager xuất hiện chọn Tab Authorities → Chọn Import và trở đến nơi lưu trữ chứng thư của CA đã trích xuất ở bước 5.



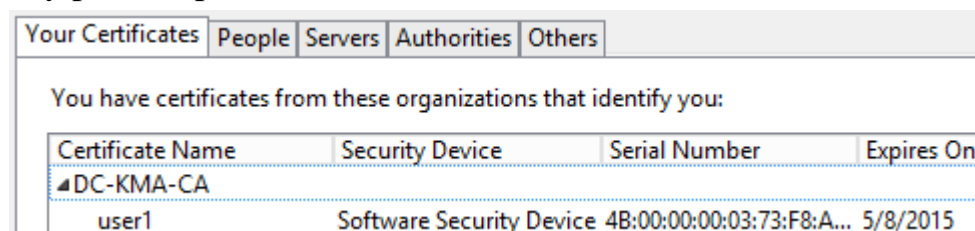


Chọn OK

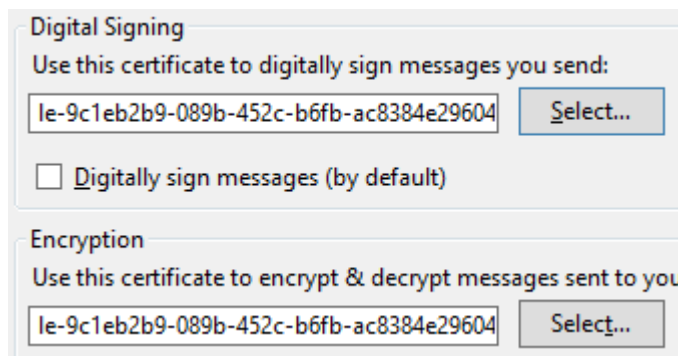
- Trong Tab People Import chứng thư của user1 với định dạng user1.cer



- Trong Tab People Import chứng thư của user2 với định dạng user2.cer (sau khi đã trình xuất ở phần sau)
- Trong Tab Your Certificates Import chứng thư của user1 với định dạng user1-key.pfx, nhập mật khẩu bảo vệ:



- Nhấn OK để kết thúc.
- Từ giao diện Account Setting trong mục Digital Signing và Encryption trở đến chứng thư đã Import:



- Nhấn OK để kết thúc cấu hình chứng thư cho người dùng user1.

**Bước 7:** Cấp chứng thư, cài đặt chứng thư và Import chứng thư của người dùng user2 vào Thunderbird trên máy Windows 7

- Các bước thực hiện tương tự từ bước 1 đến bước 6 cho người dùng user1 trên máy chủ Windows Server 2012.
- Import thêm chứng thư của người dùng user1 với định dạng user1.cer vào Tab People

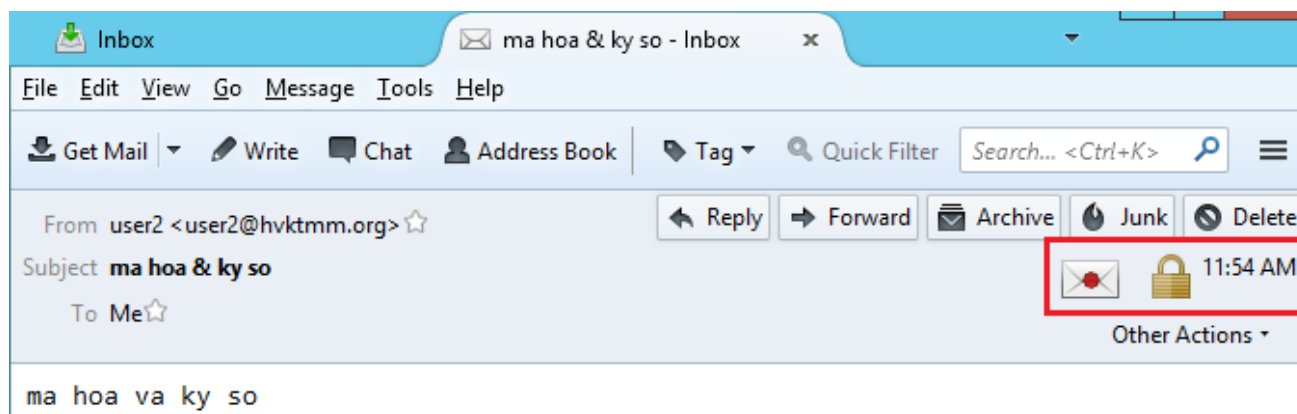
### 3.2.5 Gửi thư có mã hóa và ký số

**Bước 1:** Từ người dùng user2 soạn thư có mã hóa và ký số gửi cho user1



Gửi cho user1

**Bước 2:** chuyển sang tài khoản của user1 để kiểm tra kết quả



Kết quả người dùng user1 đã nhận được mail, trong mail có 2 biểu tượng ký số và mã hóa.

### Bước 3: Chặn bắt thông tin truyền

- Từ một máy chạy hệ điều hành XP và cài phần mềm Wireshark để chặn bắt thông tin truyền giữa máy Windows 7 và Windows Server 2012.
- Kết quả chặn bắt và phân tích thông tin.

```

Message-ID: <536BD4AE.1080709@hvktmm.org>
Date: Thu, 08 May 2014 12:02:06 -0700
From: user2 <user2@hvktmm.org>
User-Agent: Mozilla/5.0 (windows NT 6.1; rv:24.0) Gecko/20100101 Thunderb
MIME-Version: 1.0
To: user1@hvktmm.org
Subject: ky so & ma hoa
Content-Type: application/pkcs7-mime; name="smime.p7m"; smime-type=envelo
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxgGKMIHCAgEAMCswFDESMBAGA1UEAXMJREMTS01BLUNB
AhNLAAAAA3P4pgpgHZMMAAAAAAADMA0GCSqGSIb3DQEBAQUABIGASH4OXH19LcC5d4pQytPV
wfUPPGCAKKJhvexkrALT02Quu+UexREFKml6hiy5wv5lGphHts2GctHa0Qhq33QgKRijcwjN
OnP8HAXPJW5aTaQeZkhXctU+jD77CY2YJPLGx06U6lDc7E7GeCLYd1113jgchfADh1J19P58
73Cs ch8wgCICAQAwKZAUMRIWEAYDVQQDEW1EQY1LTUetQ0ECE0sAAAAEtFXddPgmaCAAAAA

```

Trong kết quả chặn bắt này, kẻ tấn công có thể biết được người gửi và người nhận, tiêu đề của mail, nhưng không biết được nội dung của mail, bởi vì đã được mã hóa.

### **Tài liệu tham khảo**

- [1] Microsoft. Windows Server 2012: Evaluation Guide. Năm 2012.
  - [2] Microsoft Official. Administering Windows Server 2012. Wiley. Năm 2013.
  - [3] Tom Adelstein, Bill Lubanovic. Linux System Administration. O'Reilly Media. Năm 2007.
  - [4] Remo Suppi Boldrito, Josep Jorba Esteve. GNU/Linux Advanced Administration. Năm 2008.
  - [5] Daniel P. Bovet, Marco Cesati. Understanding the Linux Kernel, 3rd Edition. O'Reilly Media. Năm 2005.
  - [6] Juliet Kemp. Linux System Administration Recipes: A Problem-Solution Approach. Apress. Năm 2009.
  - [7] Evi Nemeth, Garth Snyder. UNIX and Linux System Administration Handbook (4th Edition). Prentice Hall. Năm 2010.
  - [8] Configure the GRUB boot loader.
- Website:<http://www.tldp.org/HOWTO/Remote-Serial-Console-HOWTO/configure-boot-loader-grub.html>