

ACTIVE DIRECTORY

A. Khái Quát Về Active Directory

Trong bài viết này sẽ tập trung phân tích, giải thích một cách tổng quan về Active Directory để các bạn có thể hiểu rõ được các vấn đề sau:

- Chức năng của Directory Service
- Mục đích của Active Directory
- Các tính năng của Active Directory

I. Hiểu biết cơ bản về Directory Services (UNDERSTANDING DIRECTORY SERVICES)

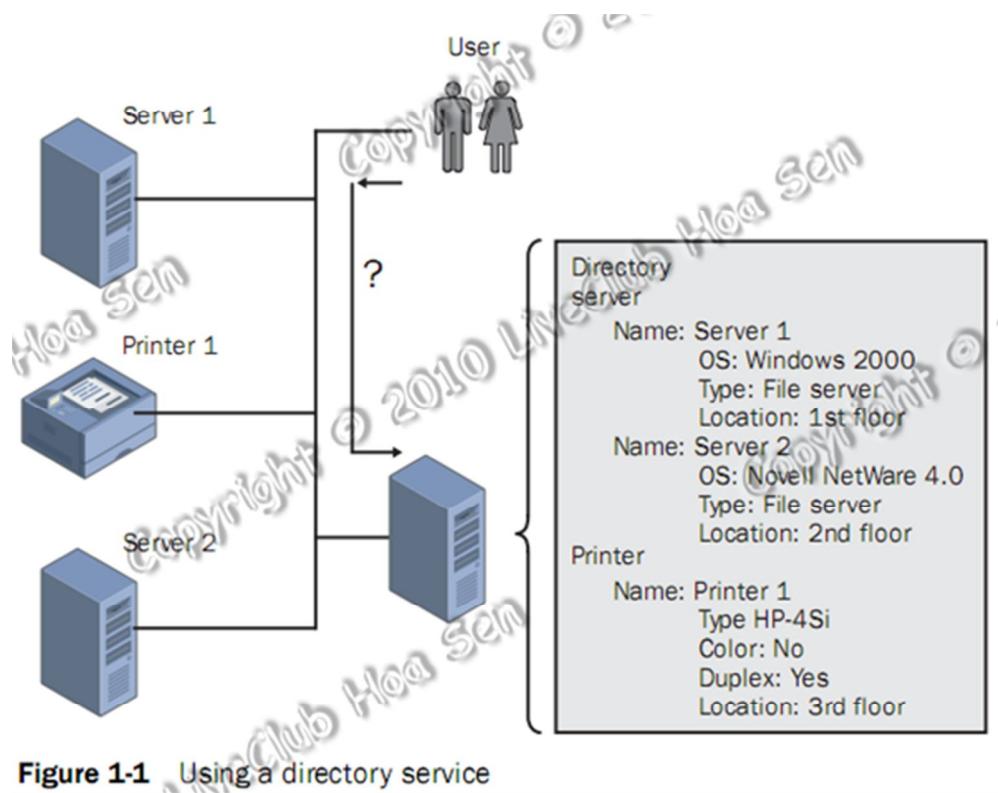
- Directory là một mô hình tổ chức thông tin, dữ liệu mà trong đó các thông tin dữ liệu có mối quan hệ chặt chẽ với nhau, ta có thể dễ dàng nắm được thông qua ví dụ Danh bạ điện thoại, với Tên trên danh bạ, ta có thể dễ dàng tra ra được số điện thoại tương ứng.

- Trong các hệ thống máy tính phân tán hoặc trong mạng máy tính, có rất nhiều đối tượng được tổ chức, lưu trữ theo cấu trúc Directory như users, máy tính, file, server, máy in, máy fax ... Và khi người dùng cuối cùng là user, muốn sử dụng những đối tượng trên thì sao, ví dụ như user muốn dùng máy in thì sao? Do đó cần có một dịch vụ hỗ trợ user có thể xác định được đối tượng và cho phép user sử dụng nó, vì thế mà ta có định nghĩa Directory Service. Directory Service được áp dụng trong việc lưu trữ các thông tin, dữ liệu theo kiến trúc tổ chức Directory và quản lý tập trung các đối tượng, đơn giản hóa quá trình xác định và quản lý resources.

- Directory Service là một dịch vụ hoạt động như một switchboard chính trong các hệ điều hành máy chủ, nó hỗ trợ các nguồn Resources độc lập và phân tán có thể làm việc với nhau, có thể kết nối với nhau. Directory Service cung cấp một nền tảng cho các chức năng của một hệ điều hành máy chủ, đảm bảo tính bảo mật, nâng cao hiệu năng khi thiết kế và triển khai các hệ thống mạng, đồng thời giúp người quản trị có thể dễ dàng quản trị được hệ thống.

II. Vì sao cần phải có Directory Service (WHY HAVE A DIRECTORY SERVICE?):

- Directory Service cung cấp một phương tiện hỗ trợ việc tổ chức và đơn giản hóa việc truy xuất Resources. Người dùng và ngay cả người quản trị không cần biết chính xác về đối tượng mà họ đang cần. Họ chỉ cần biết 1 số yêu tố về đối tượng đó.



Trong hình trên, ta dễ dàng thấy được Directory Service truy vấn trên Directory để lấy ra thông tin của các Object thông qua một số yếu tố của Object. Directory Service vừa là một dịch vụ hỗ trợ quản trị hệ thống, cũng là công cụ hỗ trợ người dùng cuối (User) trong việc quản trị hệ thống.

III. Vậy Active Directory là gì (HOW ABOUT ACTIVE DIRECTORY?)

- Active Directory là một sự ứng dụng của Directory Service, được tích hợp vào trong họ các phiên bản Windows Server, được xem như trái tim của cả hệ thống mạng và cũng góp phần mang đến sự thành công của Windows Server. Active Directory lưu trữ thông tin và tài nguyên trong hệ thống mạng dưới mô hình tổ chức Directory và hoạt động với cơ chế là 1 dịch vụ, đó chính là nguyên tắc hoạt động cơ bản của Active Directory, tóm lại Active Directory hoạt động với cơ chế của Directory Service, tuy nhiên bên trong Active Directory còn rất nhiều điều huyền bí cho anh em IT Pro tự mình nghiên cứu, tìm hiểu và ứng dụng nó.

IV. Active Directory có những tính năng gì (WHAT CAN ACTIVE DIRECTORY DO?)

- Là một dịch vụ được tích hợp sẵn trong họ các sản phẩm Windows Server của Microsoft, Active Directory cung cấp cho tựi mình một số tính năng quan trọng, phải nói là rất nhiều giúp công việc thiết kế, triển khai và quản trị hệ thống của anh em mình được dễ dàng hơn, chặt chẽ hơn. Vậy các tính năng, dịch vụ đó là gì?

- **Centralized Data Store** – Lưu trữ dữ liệu tập trung: Toàn bộ dữ liệu, thông tin trong hệ thống được lưu trữ một cách tập trung, cho phép người dùng có thể truy cập dữ liệu từ bất cứ nơi đâu, bất cứ lúc nào đồng thời nâng cao hiệu năng quản trị của hệ thống, giảm thiểu độ rủi ro cho tài nguyên.
- **Scalability** – khả năng linh hoạt với nhu cầu: Active Directory cung ứng một cách linh hoạt các giải pháp quản trị khác nhau cho từng nhu cầu cụ thể trên nền tảng hạ tầng xác định của các doanh nghiệp.
- **Extensibility** – Cơ sở dữ liệu của Active Directory cho phép nhà quản trị có thể customize và phát triển, ngoài ra ta còn có thể phát triển các ứng dụng sử dụng cơ sở dữ liệu này, giúp tận dụng hết khả năng, hiệu năng của Active Directory
- **Manageability** – khả năng quản trị linh hoạt dễ dàng: Active Directory được tổ chức theo cơ chế của Directory Service dưới mô hình tổ chức Directory giúp các nhà quản trị có cái nhìn tổng quan nhất đối với cả hệ thống, đồng thời giúp user có thể dễ dàng truy xuất và sử dụng tài nguyên hệ thống.
- **Integration with Domain Name System (DNS)** DNS là một partner rất cần thiết đối với Active Directory, trong một hệ thống mạng, các dịch vụ của Active Directory chỉ hoạt động được khi dịch vụ DNS được cài đặt. DNS có trách nhiệm dẫn đường, phân giải các Active Directory Domain Controller trong hệ thống mạng, và càng quan trọng hơn trong môi trường Multi Domain. DNS được dễ dàng tích hợp vào Active Directory để nâng cao độ bảo mật và khả năng đồng bộ hóa giữa các Domain Controller với nhau trong môi trường nhiều Domain.
- **Client Configuration Management:** Active Directory cung cấp cho chúng ta một khả năng quản trị các cấu hình phía client, giúp quản trị hệ thống dễ dàng hơn và nâng cao khả năng di động của user.
- **Policy – based administration:** Trong Active Directory, việc quản trị hệ thống được đảm bảo một cách chắc chắn qua các chính sách quản trị tài nguyên, các quyền truy xuất trên các site, domain và các organization unit. Đây là một trong những tính năng quan trọng nhất được tích hợp vào Active Directory.

- **Replication of information:** Active Directory cung cấp khả năng đồng bộ dữ liệu thông tin giữa các domain, trên nền tảng, môi trường nhiều domain nhằm mục đích giảm thiểu đến mức tối đa rủi ro và nâng cao khả năng hoạt động của hệ thống mạng.
- **Flexible, secure authentication and authorization:** Active Directory cung cấp nhiều cơ chế authentication như Kerberos, Secure Socket Layer và Transport Layer Security giúp cho việc bảo mật thông tin của user khi xác thực thông tin truy xuất tài nguyên.
- **Security integration:** Active Directory được tích hợp mặc định trong các phiên bản Windows Server, do đó Active Directory làm việc rất dễ dàng và linh hoạt, truy xuất điều khiển trên hệ thống được định nghĩa trên từng đối tượng, từng thuộc tính của đối tượng. Không những thế, các chính sách bảo mật được áp dụng không phải đơn thuần trên local mà còn được áp dụng trên các site, domain hay ou xác định.
- **Directory – enable applications and infrastructure:** Active Directory là một môi trường tuyệt hảo cho các nhà quản trị thiết lập các cấu hình và quản trị các ứng dụng trên hệ thống. Đồng thời Active Directory cung cấp một hướng mở cho các nhà phát triển ứng dụng (developer) xây dựng các ứng dụng trên nền tảng Active Directory thông qua Active Directory Service Interfaces
- **Interoperability with other directory services:** Active Directory được xây dựng trên giao thức directory service chuẩn gồm 2 giao thức là Lightweight Directory Access Protocol (LDAP) và Name Service Provider Interface (NSPI), do đó Active Directory có khả năng tương thích với các dịch vụ khác được xây dựng trên nền tảng directory service thông qua các giao thức này. Vì LDAP là một giao thức directory chuẩn, do đó ta có thể phát triển, tích hợp các sản phẩm ứng dụng trao đổi, chia sẻ thông tin với Active Directory thông qua giao thức LDAP. Còn giao thức NSPI được hỗ trợ bởi Active Directory nhằm mục đích đảm bảo và nâng cao khả năng tương thích với directory của Exchange.
- **Signed and encrypted LDAP traffic:** Mặc định là công cụ Active Directory trong windows server sẽ tự động xác thực và mã hóa thông tin, dữ liệu truyền tải trên giao thức LDAP. Việc xác thực giao thức nhằm đảm bảo thông tin được gửi đến từ 1 nguồn chính thức và không bị giả mạo.

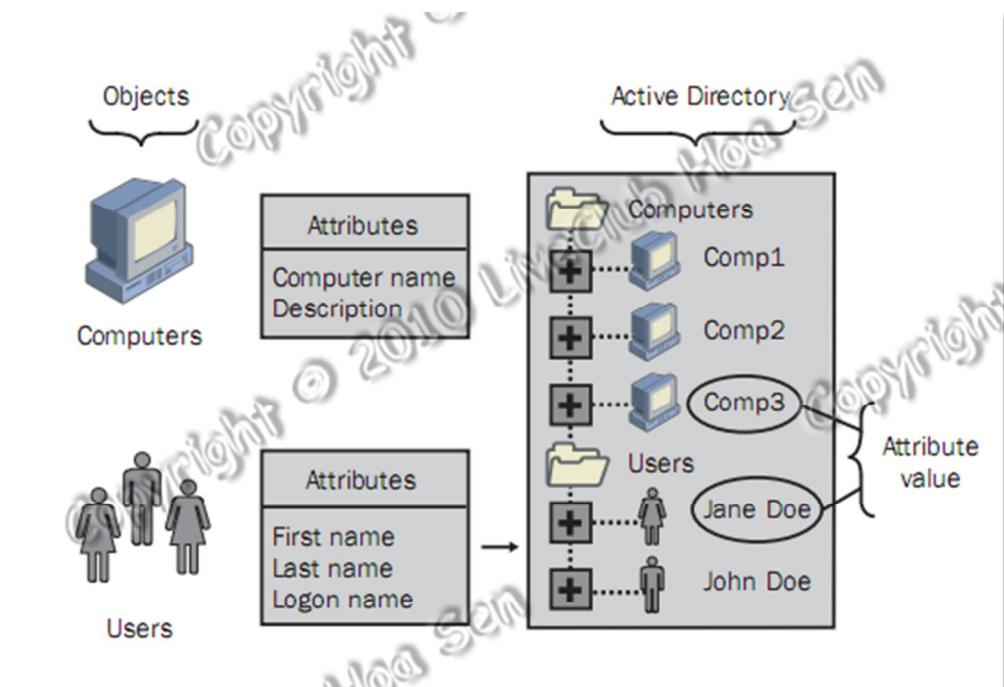
B. Kiến trúc Active Directory

Trong bài viết này sẽ tập trung tìm hiểu sâu hơn và giải thích 1 số vấn đề về kiến trúc của Active Directory :

- Kiến trúc database của Active Directory
- Kiến trúc tổ chức của Active Directory

I. ACTIVE DIRECTORY OBJECTS

- Dữ liệu trong Active Directory như là thông tin users, máy in, server, database, groups, computers và security policies được tổ chức như các objects (đối tượng). Mỗi object có những thuộc tính riêng đặc trưng cho object đó, ví dụ như object user có các thuộc tính liên quan như First Name, Last Name, Logon Name, ... và Computer Object có các thuộc tính như computer name cùng description. Một số object đặc biệt bao gồm nhiều object khác bên trong được gọi là các “container”, ví dụ như domain là một container bao gồm nhiều user và computer account.



II. ACTIVE DIRECTORY SCHEMA

- Trong Active Directory, database lưu trữ chính là AD Schema, Schema định nghĩa các đối tượng được lưu trữ trong Active Directory. Nhưng Schema lưu trữ các đối tượng thế nào? Thực chất, schema là một danh sách các định nghĩa xác định các loại đối tượng và các loại thông tin về đối tượng lưu trữ trong Active Directory. Về bản chất, schema cũng được lưu trữ như 1 object.
- Schema được định nghĩa gồm 2 loại đối tượng (object) là schema class objects và schema Attribute objects.

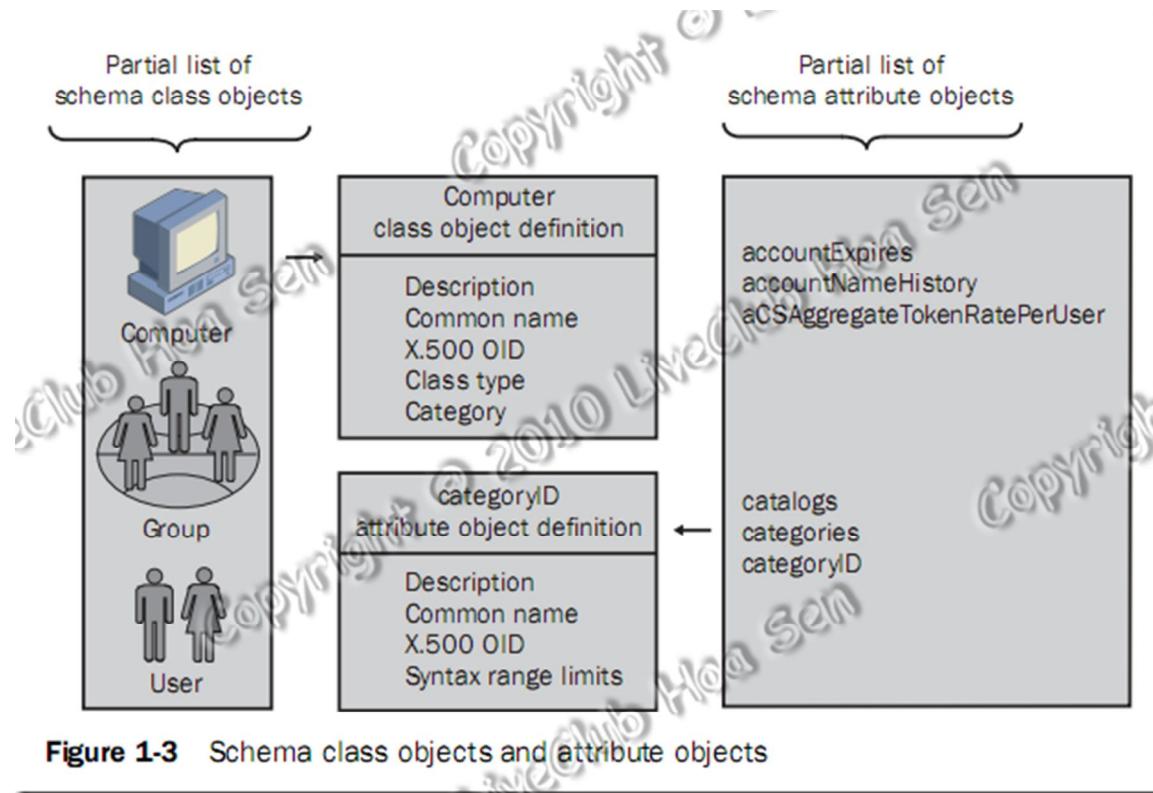


Figure 1-3 Schema class objects and attribute objects

- Schema Class có chức năng như một template cho việc tạo mới các đối tượng trong AD. Mỗi Schema Class là một tập hợp các thuộc tính của đối tượng(Schema Attribute Objects). Khi bạn tạo một đối tượng thuộc về một loại Schema Class thì Schema Attribute sẽ lưu trữ các thuộc tính của đối tượng đó tương ứng với loại Schema Class của đối tượng.
- Schema Attribute định nghĩa các Schema Class tương ứng với nó. Mỗi thuộc tính chỉ được định nghĩa một lần trong Active Directory và có thể thuộc nhiều Schema Class theo quan hệ một nhiều (1-m).

- Mặc định thì một tập hợp các Schema Class và Schema Attribute được đóng gói sẵn chung với Active Directory. Tuy nhiên Schema của Active Directory mở ra một khả năng phát triển mở rộng Schema Class trên các Attribute có sẵn hay là tạo mới các Attribute SCHEMA. Tuy nhiên cái nào cũng có cái lợi và cái hại, để có thể mở rộng phát triển với schema, bạn cần chuẩn bị kỹ lưỡng thông qua các bản thiết kế rõ ràng và xem xét là có cần thiết hay không, vì độ rủi ro trong việc này khá cao đối với các hệ thống đang hoạt động ổn định, còn về vấn đề làm Virtual Lab thì anh em mình cứ thoải mái thôi, không có vấn đề gì cả, ^^.

III. ACTIVE DIRECTORY COMPONENTS

- Trong mô hình mạng doanh nghiệp, các components của Active Directory được sử dụng, áp dụng để xây dựng nên các mô hình phù hợp với nhu cầu các doanh nghiệp. Xét về khía cạnh mô hình kiến trúc của AD thì ta phân làm 2 loại là Physical và Logical.

1. Logical Structure:

- Trong AD, việc tổ chức tài nguyên theo cơ chế Logical Structure, được ánh xạ thông qua mô hình domains, OUs, trees và forest. Nhóm các tài nguyên được tổ chức một cách luận lí cho phép bạn dễ dàng truy xuất đến tài nguyên hơn là phải nhớ cụ thể vị trí vật lí của nó.

a) Domain:

- Cốt lõi của kiến trúc tổ chức luận lí trong AD chính là Domain, nơi lưu trữ hàng triệu đối tượng (objects). Tất cả các đối tượng trong hệ thống mạng trong một domain thì do chính domain đó lưu trữ thông tin của các đối tượng. Active Directory được kiến tạo bởi một hay nhiều domain và một domain có thể triển khai trên nhiều physical structure. Việc access vào domain được quản trị thông qua Access Control Lists (ACLs), quyền truy xuất trên domain tương ứng với từng đối tượng.

b) OUs:

- OU là một container được dùng để tổ chức các đối tượng trong một domain thành các nhóm quản trị luận lí (logical). OUs cung cấp phương tiện thực hiện các tác vụ quản trị trong hệ thống như là quản trị user và resources, đó là những scope đối tượng nhỏ nhất mà bạn có thể ủy quyền xác thực quản trị. OUs bao gồm nhiều đối tượng khác như là user accounts, groups, computers và các OUs khác tạo nên các cây OUs trong cùng một domain. Các cây OUs trong một domain độc lập với kiến trúc các cây OUs thuộc các domain khác.

c) Trees:

- Trees là một nhóm các domain được tổ chức theo cấu trúc hình cây với mô hình parent-child ánh xạ từ thực tế tổ chức của doanh nghiệp, tổ chức. Một domain có 1 hoặc nhiều child domain nhưng 1 child domain chỉ có 1 parent-domain mà thôi.

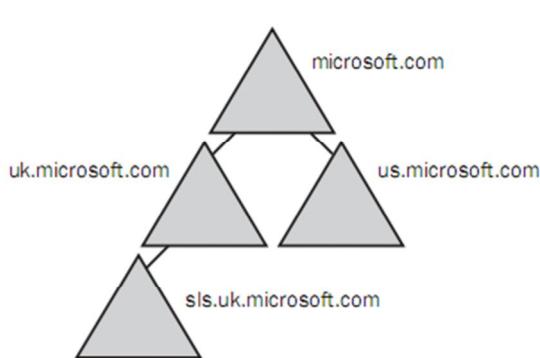


Figure 1-6 A domain tree

d) Forests:

- Forest là một thuật ngữ được đặt ra nhằm định nghĩa 1 mô hình tổ chức của AD, 1 forest gồm nhiều domain trees có quan hệ với nhau, các domain trees trong forest là độc lập với nhau về tổ chức, nghe ra có vẻ mâu thuẫn trong mối quan hệ nhưng ta sẽ dễ hiểu hơn khi mối quan hệ giữa các domain trees là quan hệ Trust 2 chiều như các partners với nhau.
- Một forest phải đảm bảo thoả các đặc tính sau:

- Toàn bộ domain trong forest phải có 1 schema chia sẻ chung
- Các domain trong forest phải có 1 global catalog chia sẻ chung
- Các domain trong forest phải có mối quan hệ trust 2 chiều với nhau
- Các tree trong 1 forest phải có cấu trúc tên(domain name) khác nhau
- Các domain trong forest hoạt động độc lập với nhau, tuy nhiên hoạt động của forest là hoạt động của toàn bộ hệ thống tổ chức doanh nghiệp.

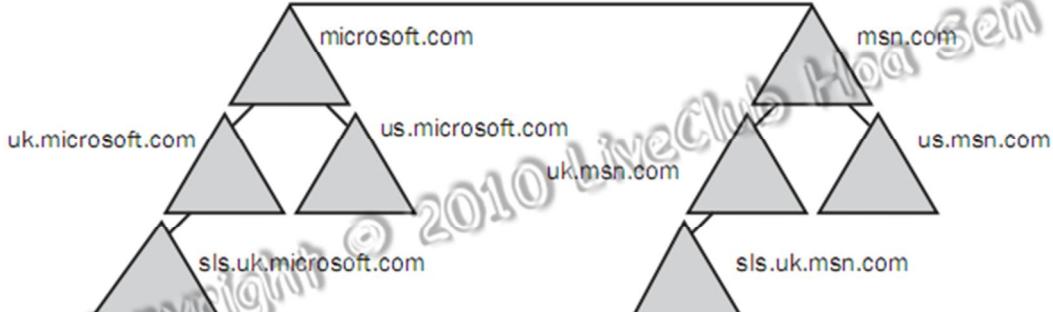


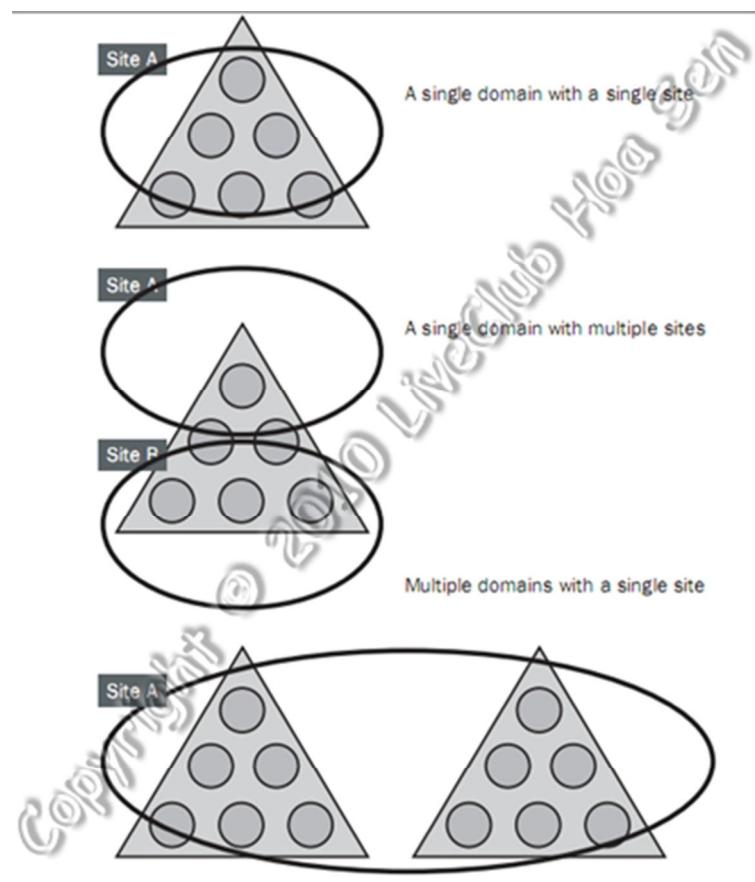
Figure 1-7 A forest of trees

2. Physical Structure:

- Xét về khía cạnh physical component của AD thì gồm 2 phần là Sites và Domain Controllers. Với vị trí là một administrator, bạn sẽ phải dùng các components này để thiết kế và triển khai các mô hình kiến trúc phù hợp với nhu cầu doanh nghiệp tổ chức.

a) Sites:

- Site là một thuật ngữ được dùng đến khi nói về vị trí địa lý của các domain trong hệ thống. Khi hệ thống các domain được phân tán ở những vị trí địa lý, những nơi khác nhau và có quan hệ với nhau thì những nơi đặt các domain này chính là các Site.



- Trong hình trên, ta có thể thấy được với mỗi site có thể có một hoặc nhiều domain khác nhau hay mỗi domain thuộc nhiều site khác nhau.
- Ví dụ nhưng công ty A có 2 chi nhánh là Hà Nội và Thành Phố Hồ Chí Minh, tại các chi nhánh, nhân viên thường xuyên phải đăng nhập vào domain để làm việc. Tuy nhiên hạ tầng mạng và đường truyền rất hạn chế, vậy giải pháp nào là hợp lý cho công ty A? Với nhu cầu của công ty A, ta có thể triển khai một domain tại Hà Nội, 1 domain tại Thành Phố Hồ Chí Minh và 2 domain này có quan hệ với nhau, các domain sẽ tiến hành replicate dữ liệu, thông tin theo 1 schedule xác định, các nhân viên tại Hà Nội và Tp Hồ Chí Minh chỉ cần đăng nhập vào hệ thống phù hợp với vị trí của mình.

b) Domain Controllers:

- Domain Controller là 1 máy tính hay server chuyên dụng được setup Windows Server và lưu trữ bản sao của Domain Directory (local domain database). Một domain có thể có 1 hay nhiều domain controller, mỗi domain controller đều có bản sao dữ liệu của Domain Directory. Domain Controller chịu trách nhiệm chứng thực cho users và chịu trách nhiệm đảm bảo các chính sách bảo mật được thực thi.
- Các chức năng chính của domain controller:
 - Mỗi domain controller lưu trữ các bản sao thông tin của Active Directory cho chính domain đó, chịu trách nhiệm quản lý thông tin và tiến hành đồng bộ dữ liệu với các domain controller khác trong cùng một domain.
 - Domain Controller trong một Domain có khả năng tự động đồng bộ dữ liệu với các domain controller khác trong cùng một domain. Khi bạn thực hiện một tác vụ đối với thông tin lưu trữ trên domain controller, thì thông tin này sẽ tự động được đồng bộ hóa đến các domain controller khác. Tuy nhiên để đảm bảo sự ổn định cho hệ thống mạng, chúng ta cần phải có một chính sách hợp lý cho các domain trong việc đồng bộ hóa thông tin dữ liệu với một thời điểm phù hợp.
 - Domain Controller tự động đồng bộ hóa ngay lập tức các thay đổi quan trọng đối với cả Domain như disable một user account.
 - Active Directory sử dụng việc đồng bộ hóa dữ liệu theo cơ chế multimaster, nghĩa là không có domain controller nào đóng vai trò là master cả, mà thay vào đó thì tất cả domain controller đều ngang hàng với nhau, mỗi domain controller lưu trữ một bản sao của database hệ thống. Các domain controller lưu trữ các thông tin dữ liệu khác nhau trong một khoảng thời gian ngắn cho đến khi thông tin các domain controller trong hệ thống đều được đồng bộ với nhau, hay nói cách khác là thông nhất dữ liệu cho toàn domain.

- Mặc dù là Active Directory hỗ trợ hoàn toàn việc đồng bộ dữ liệu theo cơ chế multimaster nhưng thực tế thì không phải lúc nào cũng theo cơ chế này (việc thực thi không được cho phép ở nhiều nơi trong hệ thống mạng trong cùng một thời điểm). Operations master roles là các roles đặc biệt được assigned với 1 hoặc nhiều domain controllers khác để thực hiện đồng bộ theo cơ chế single-master, ta có thể dễ dàng nhận thấy việc thực thi operations của multimaster là sự thực thi của nhiều single-master đồng thời.
 - Hệ thống có nhiều hơn một domain hỗ trợ trong trường hợp dự phòng backup domain controller, khi một domain controller có vấn đề xảy ra thì các domain sẽ tự động chạy dự phòng, đảm bảo hệ thống luôn được ổn định.
 - Domain Controller quản lý các vấn đề trong việc tương tác với domain của users, ví dụ xác định đối tượng trong Active Directory hay xác thực việc logon của user.
- Là một người quản trị hệ thống, bạn phải đặt các domain controller trên các sites để đạt hiệu quả cao nhất cho việc đồng bộ dữ liệu và đăng nhập hệ thống của user.

C. Cài đặt và cấu hình Active Directory

* Nội dung:

- Hướng dẫn cấu hình AD với domain liveclubhoasen.com và joint client vào domain.

I. CHUẨN BỊ:

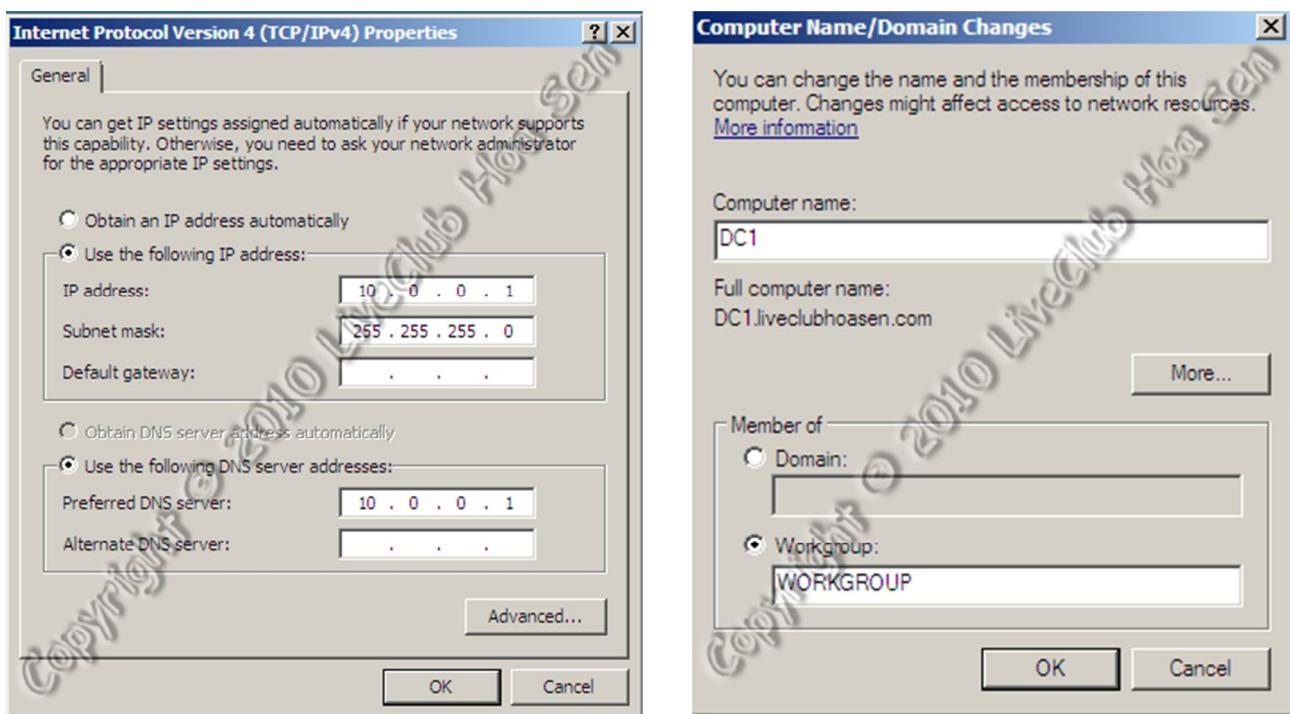
- Thiết lập địa chỉ IP cho card mạng của server hoặc bạn có thể thiết lập địa chỉ IP của các DNS Server trong hệ thống. Nếu server này là Domain Controller và DNS Server đầu tiên, quá trình cài đặt AD DS sẽ bao gồm cả việc cài đặt DNS Server.
- Nếu muốn bổ sung server này vào một forest đã tồn tại trên Windows Server 2000, Windows Server 2003 bạn phải cập nhật thông tin về forest bằng lệnh `adprep /forestprep`.
- Nếu muốn bổ sung server này vào một domain đã tồn tại trên Windows Server 2000, Windows Server 2003, bạn phải cập nhật thông tin về domain và group policy bằng lệnh `adprep /domainprep /gpprep`.
- Nếu muốn cài đặt một Read-Only Domain Controller, bạn phải chuẩn bị forest bằng lệnh `adprep /rodcprep`.
- Xây dựng các DNS Server trong hệ thống mạng nếu có, trong quá trình cài đặt AD DS sẽ có cài đặt DNS Server

- Ở Windows 2003 bước chuẩn bị này cần phải thêm source Windows 2003 nhưng qua tới Windows 2008 đã được tích hợp sẵn trên hệ điều hành lúc này ta không cần dùng tới đĩa source cài đặt.

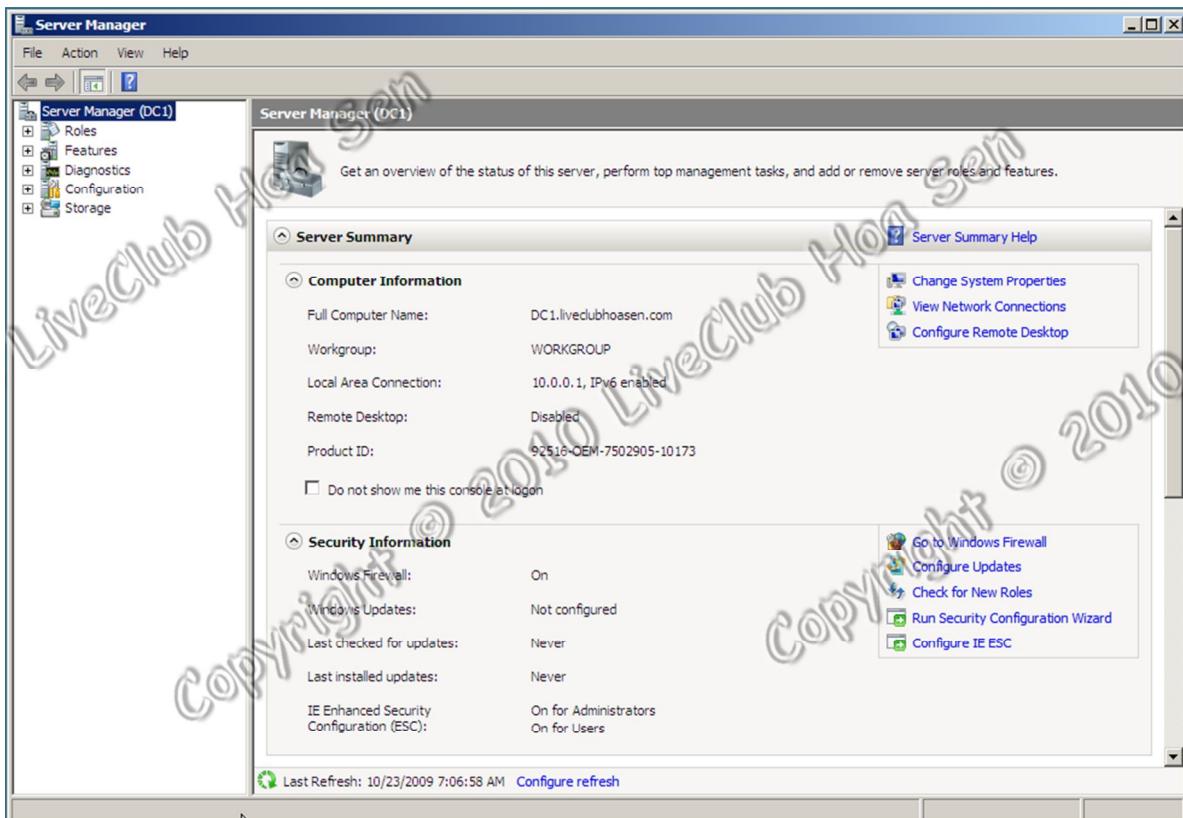
II. CẤU HÌNH:

1. Trên máy Server

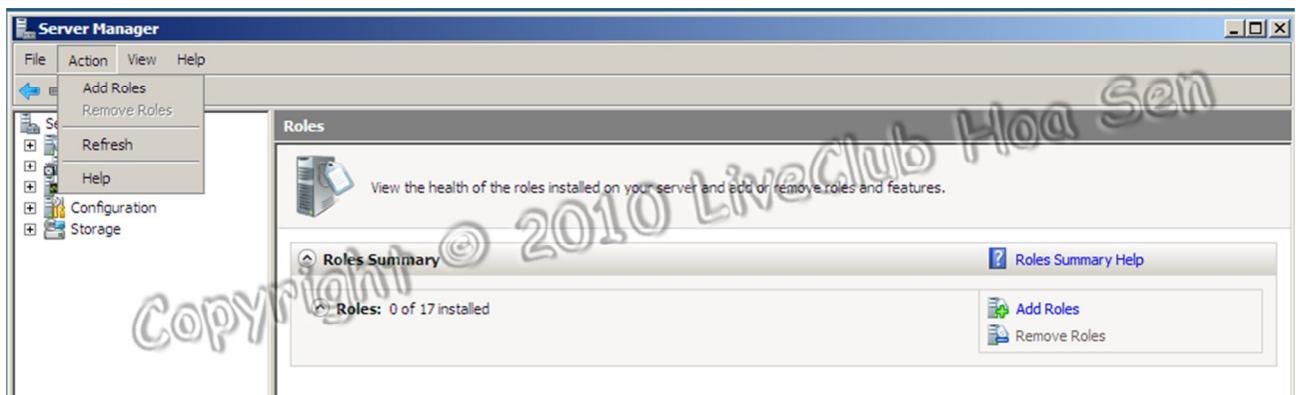
- Ban đầu kiểm tra lại các thông số cần thiết ở bước chuẩn bị:



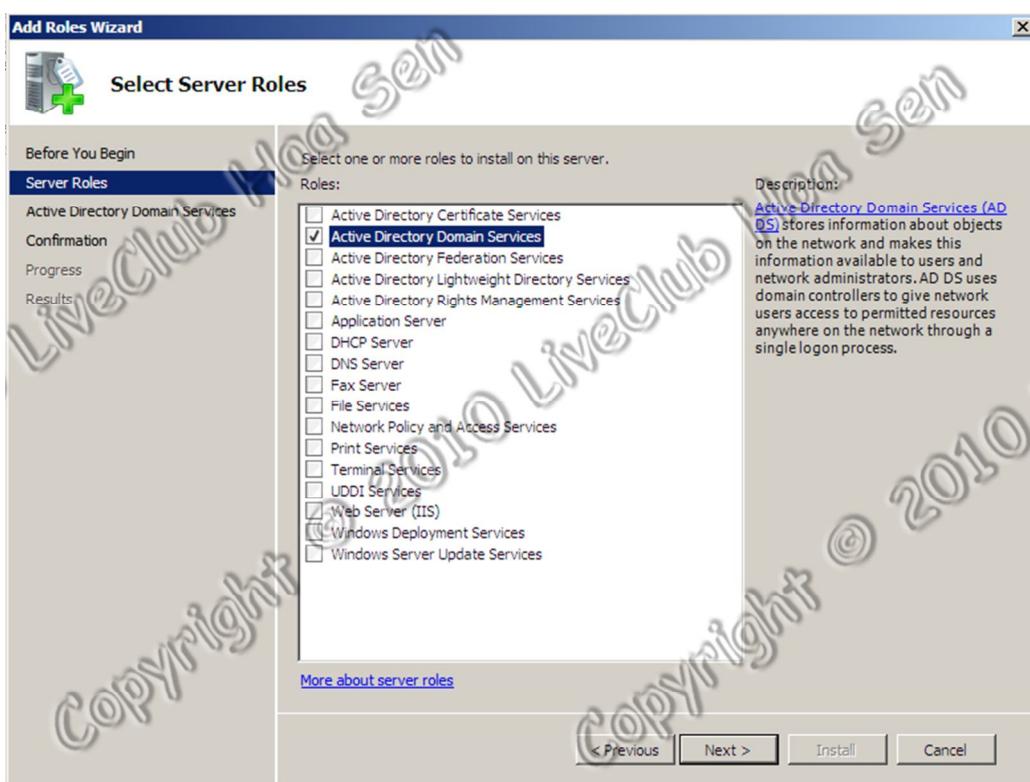
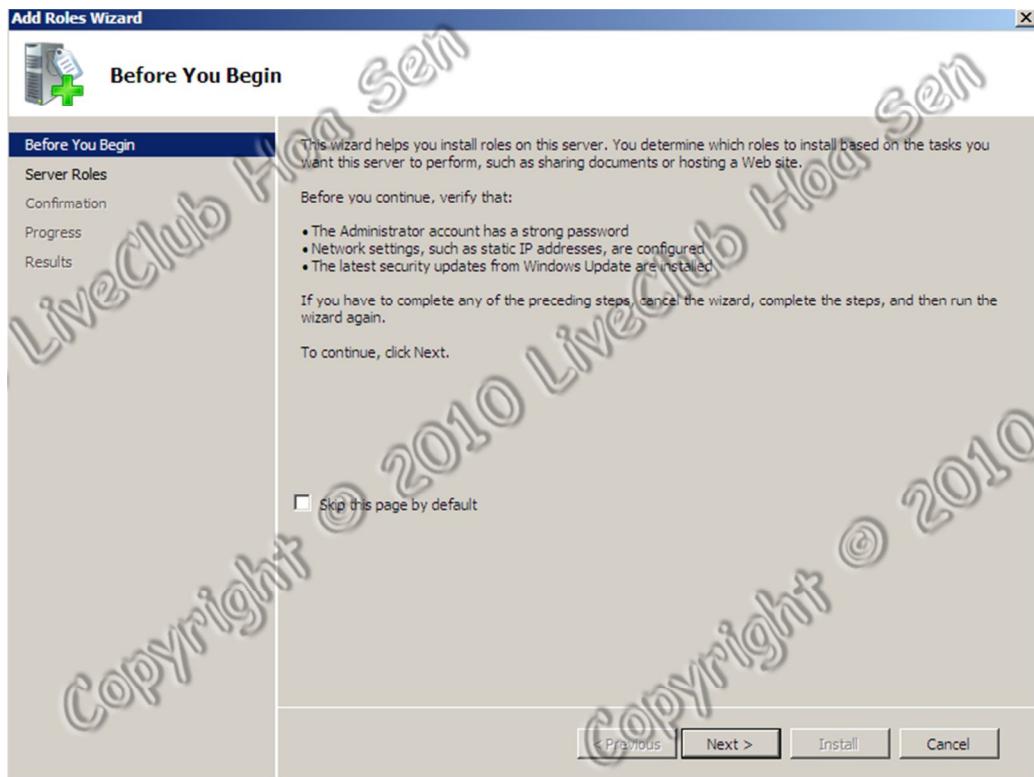
- Ở Windows Server 2003, các dịch vụ được cài đặt ở **Add/Remove Windows Components**. Qua tới Windows Server 2008 được thay thế bằng công cụ quản trị **Server Manager** với các định nghĩa mới là Roles và Features. Và mặc định Windows Server 2008 chưa cài đặt các dịch vụ nên bạn phải cài đặt dịch vụ AD DS trước khi lên Domain Controller.
- Vào **Administrator Tool → Server Manager** (hoặc nhìn bên góc trái màn hình kề nút Start sẽ thấy biểu tượng server manager).



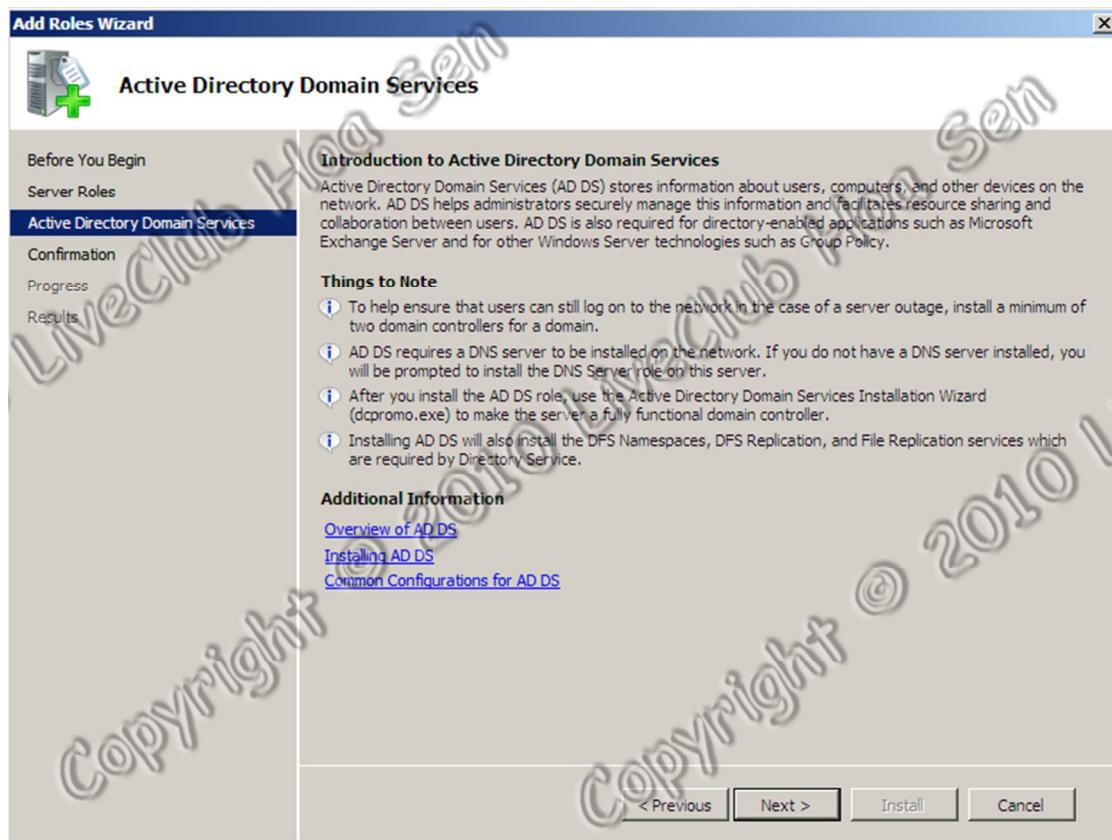
- Trong mục Roles chọn Add roles (hoặc vào menu Action → Add roles).



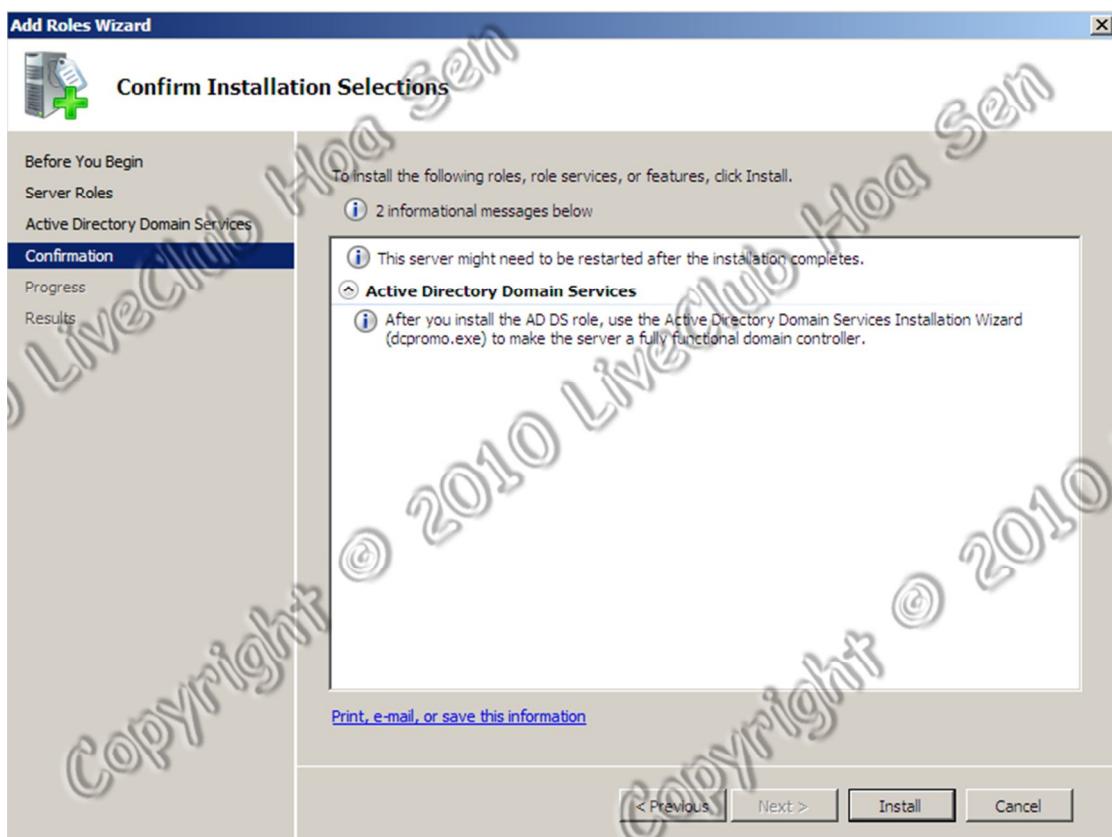
- Chọn Next → chọn dịch vụ **Active Directory Domain Services (ADDS)**.



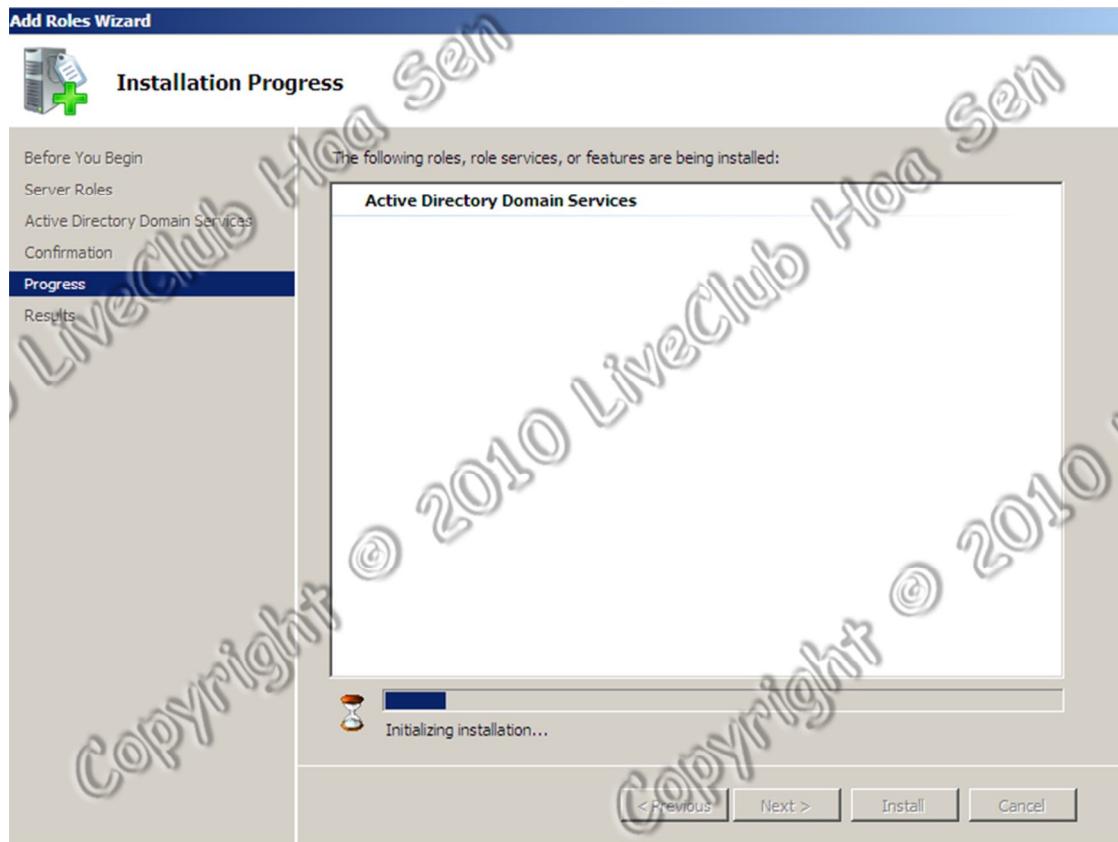
- Nhấn Next, mục này mô tả về ADDS và những chú ý **Things to Note**.



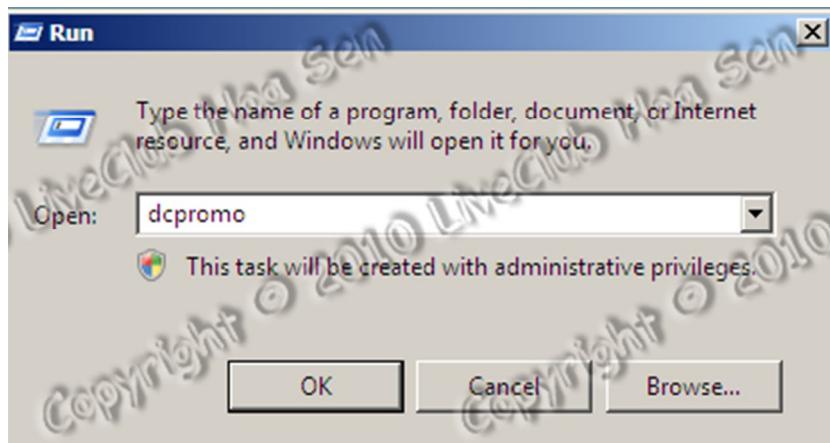
- Tiếp tục Next, mục này xác nhận lần cuối trước khi cài đặt dịch vụ.



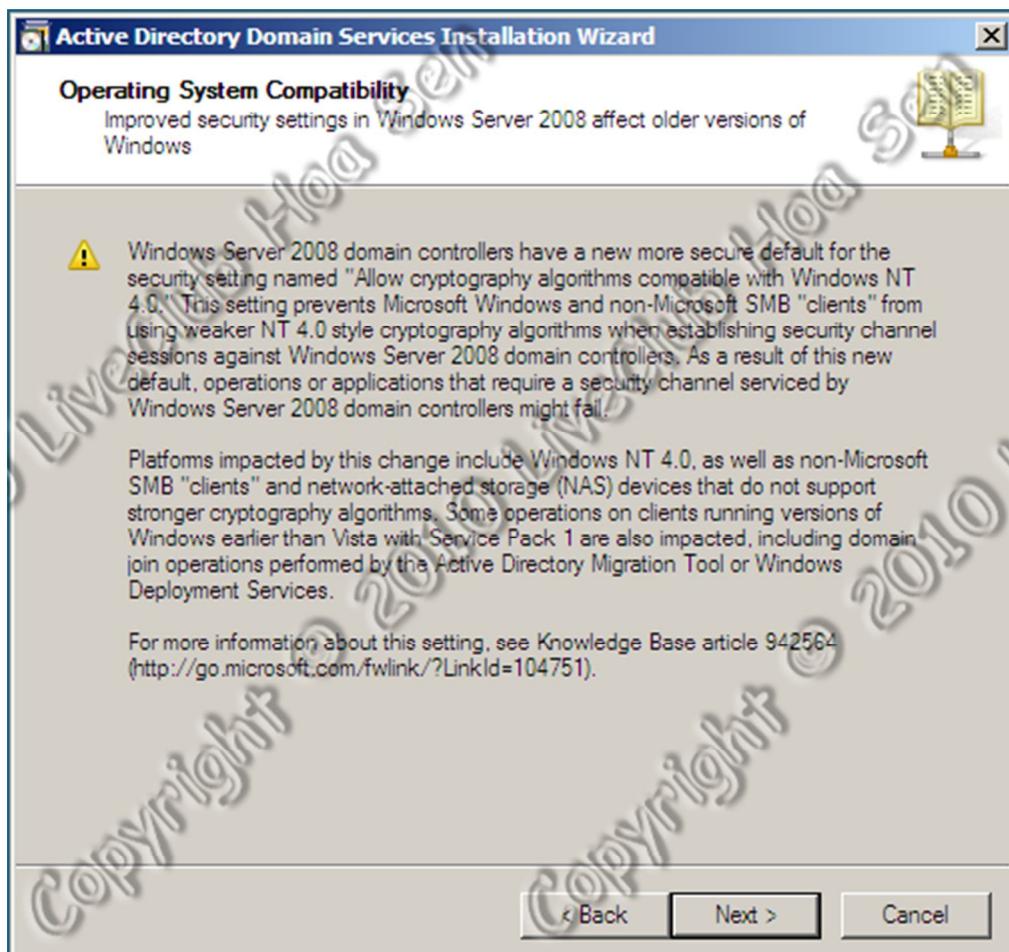
- Next → tiến trình đang cài đặt dịch vụ.



- Tiến trình cài đặt dịch vụ kết thúc sẽ hiện ra câu thông báo yêu cầu nâng cấp lên domain bằng lệnh `dcpromo` như Windows Server 2003.



- Tại bảng Welcome to the Active Directory Domain Services Installation Wizard chọn **Next**.

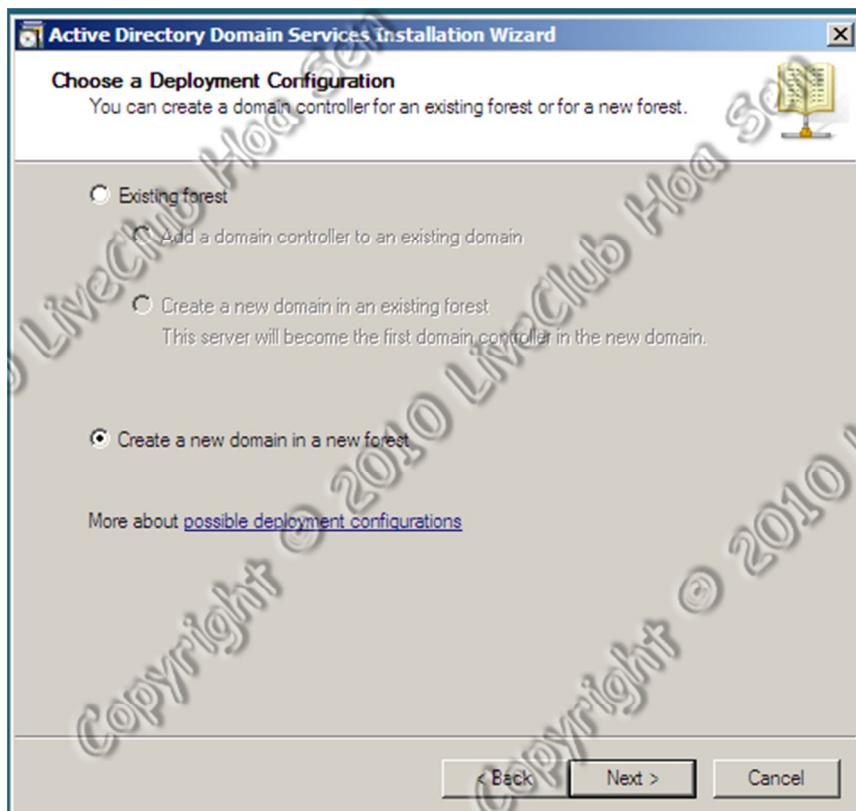


- Tại bảng Operating System Compatibility cho biết tính tương thích của Windows Server 2008.

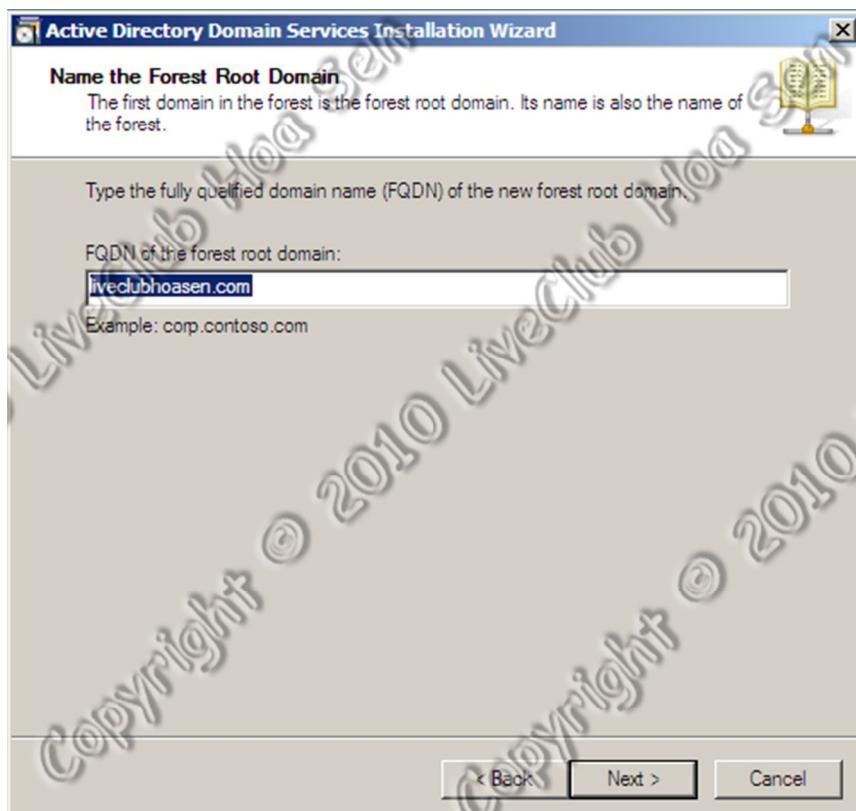
- Tiếp tục Next. Ở bảng tiếp theo, chúng ta có 2 lựa chọn chính là:

- Tạo một domain mới trong một forest mới.
- Tạo một domain mới trong một forest đã có.

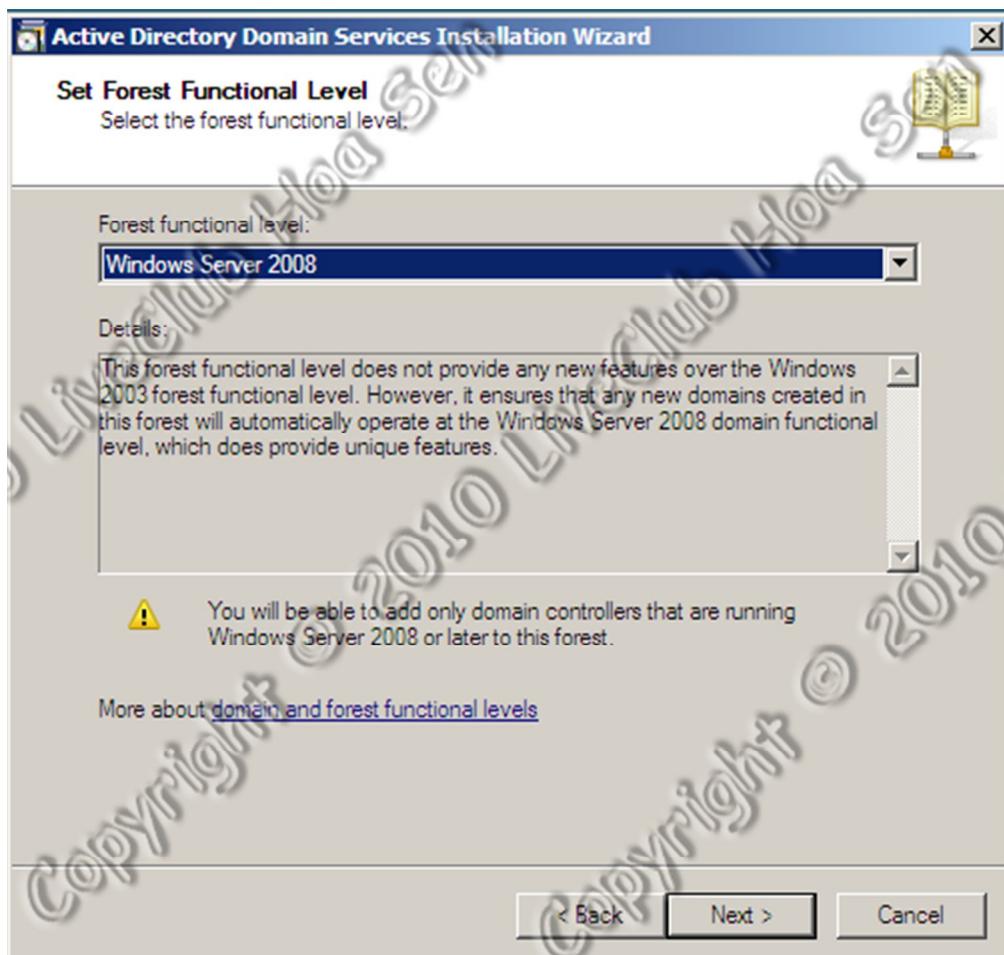
nhưng ở đây chúng ta dựng 1 domain mới nên sẽ stick vào mục **Creat a new domain in a new forest** và click Next.



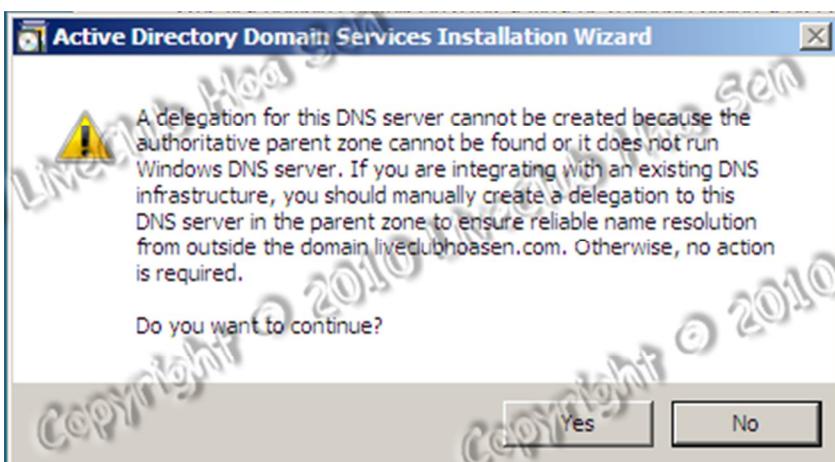
- Bảng tiếp sau đây là mục tên Domain của bạn. Ở đây chúng tôi chọn tên domain là **liveclubhoasen.com** sau đó nhấn **Next** để hệ thống kiểm tra domain này đã tồn tại hay chưa.



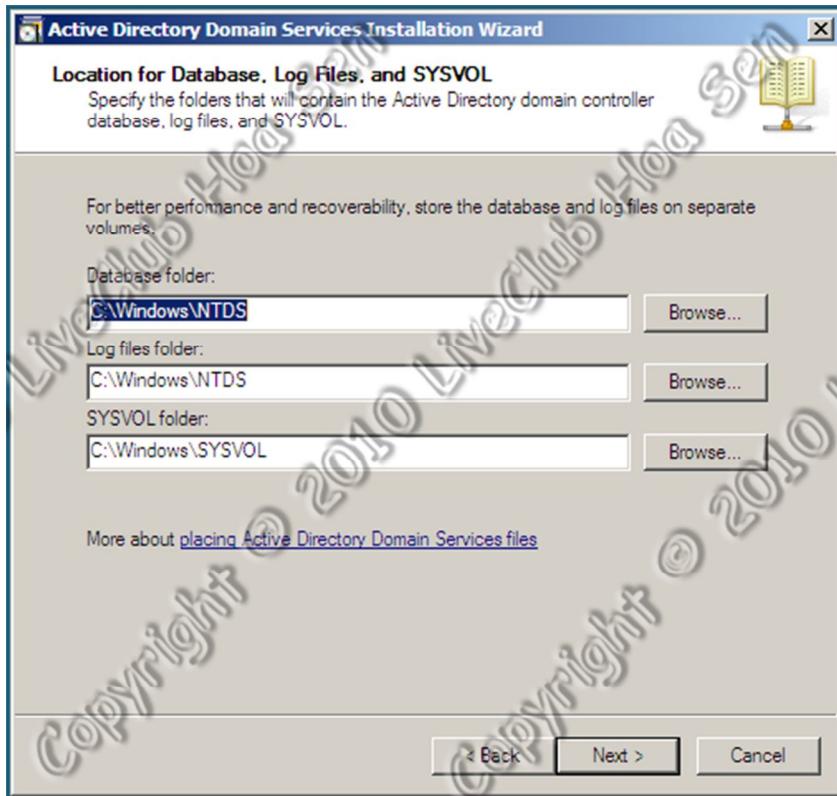
- Tiếp theo chọn functional là Windows Server 2008 để có đầy đủ tính năng mới nhất trên Windows Server 2008. Nhấn Next.



- Đến mục tiếp theo hệ thống thông báo chưa có DNS và hỏi chúng ta có muốn cài đặt hay không. Chọn cài đặt và nhấn Next tiếp tục.

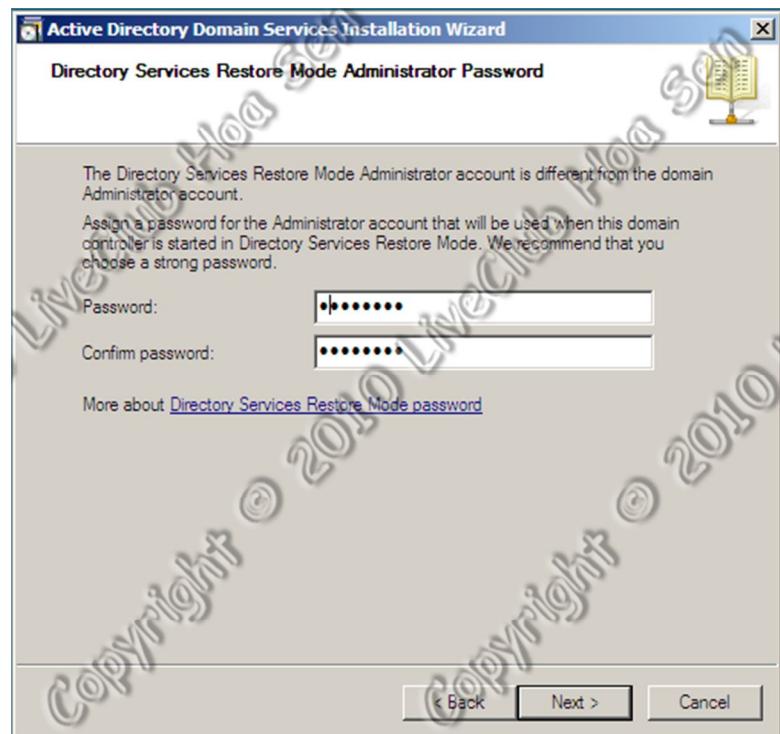


- Bảng tiếp theo là đường dẫn thư mục mặc định chứa các file hệ thống gồm:

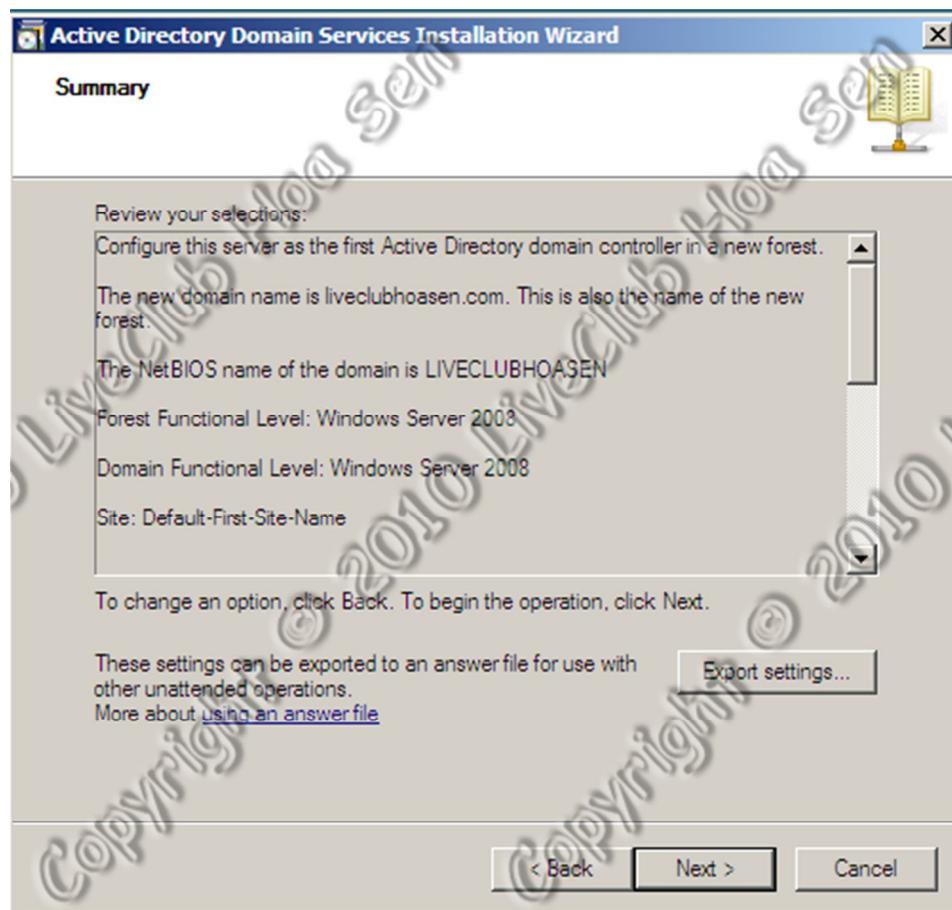


- Database
 - Log File : thư mục ghi là các cảnh báo các hành động của hệ thống
 - SYSVOL : là folder trên các Domain Controller (DC) của Domain Network. Nội dung SYSVOL chứa các dữ liệu được đồng bộ (Replication) giữa các DC trong cùng Domain.
Xem thêm <http://support.microsoft.com/kb/315457>
- Ở đây là demo nên chúng tôi để mặc định. Nhấn Next tiếp tục.

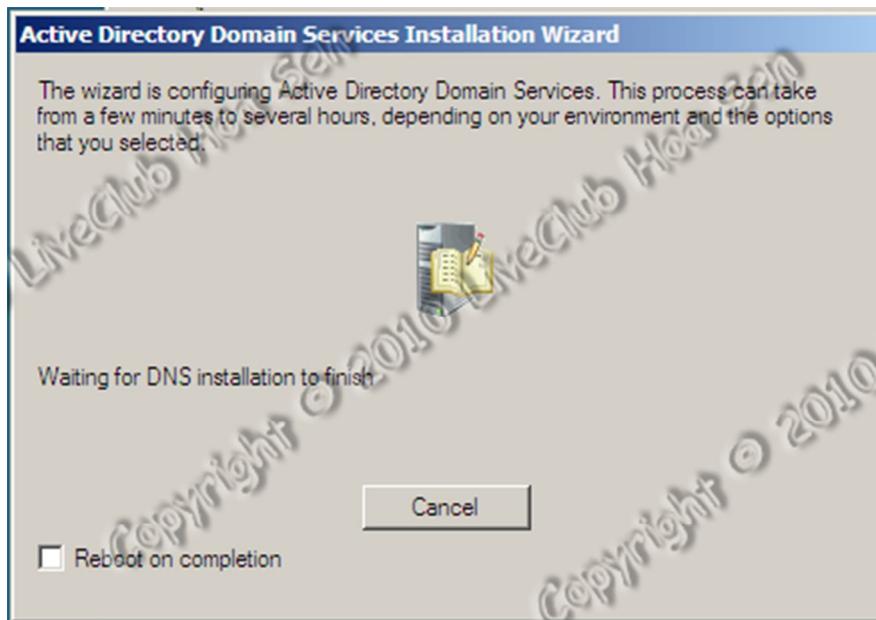
- Tiếp theo là mật khẩu dành cho công đoạn restore hệ thống ADDS . Lưu ý, password này không phải là password của tài khoản Administrator trong domain và password phải theo kiểu complexity (gồm các ký tự a,A,@,1....)



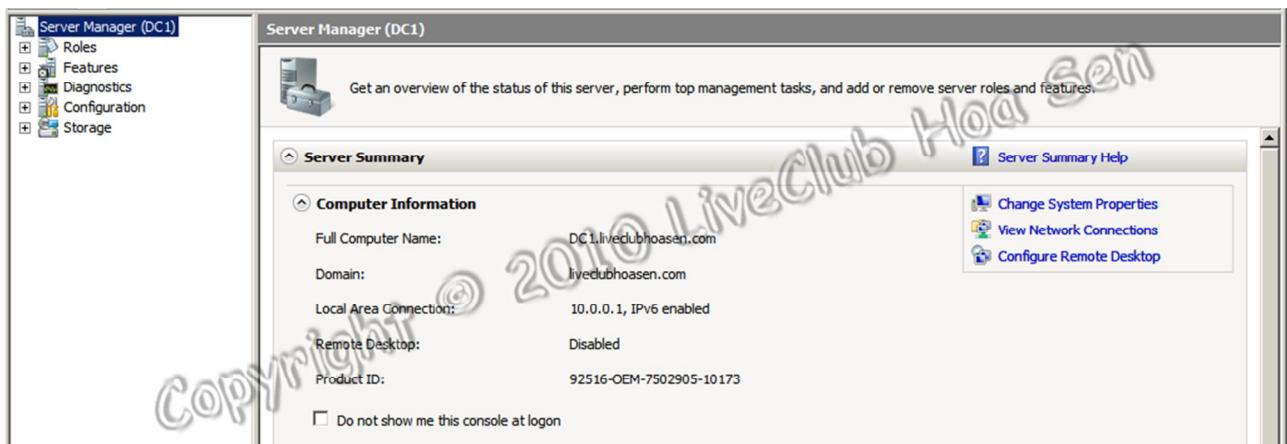
- Nhấn Next → kiểm tra lại thông số khởi tạo ban đầu để tiến hành cài đặt dịch vụ



- Nhấn Next để cài đặt

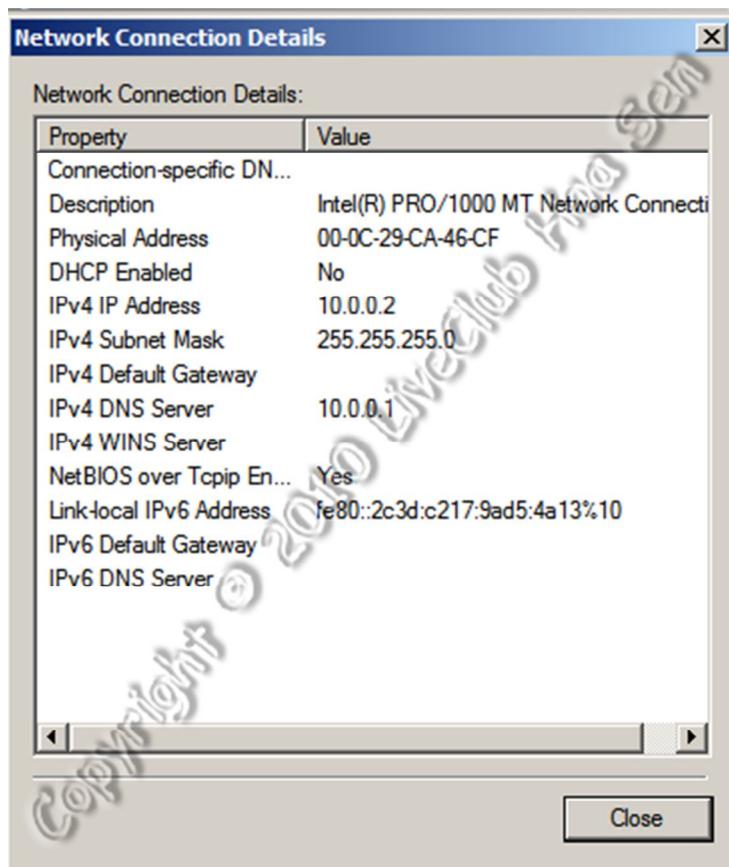


- Sau khi cài đặt hoàn tất reboot hệ thống, log on kiểm tra hệ thống.

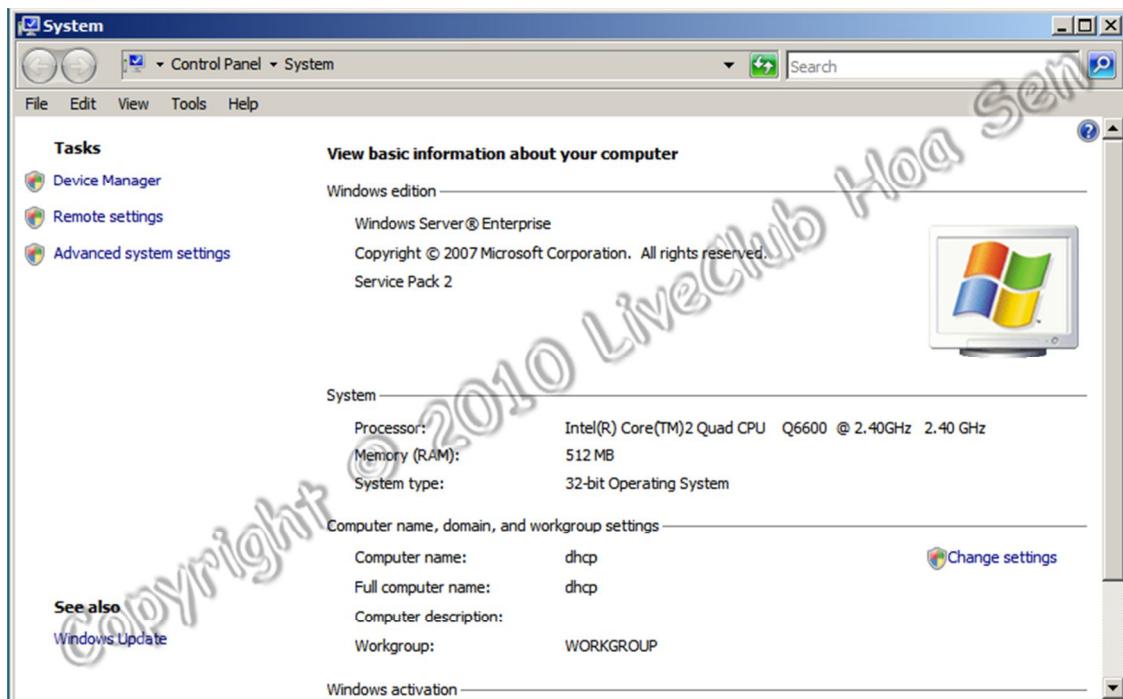


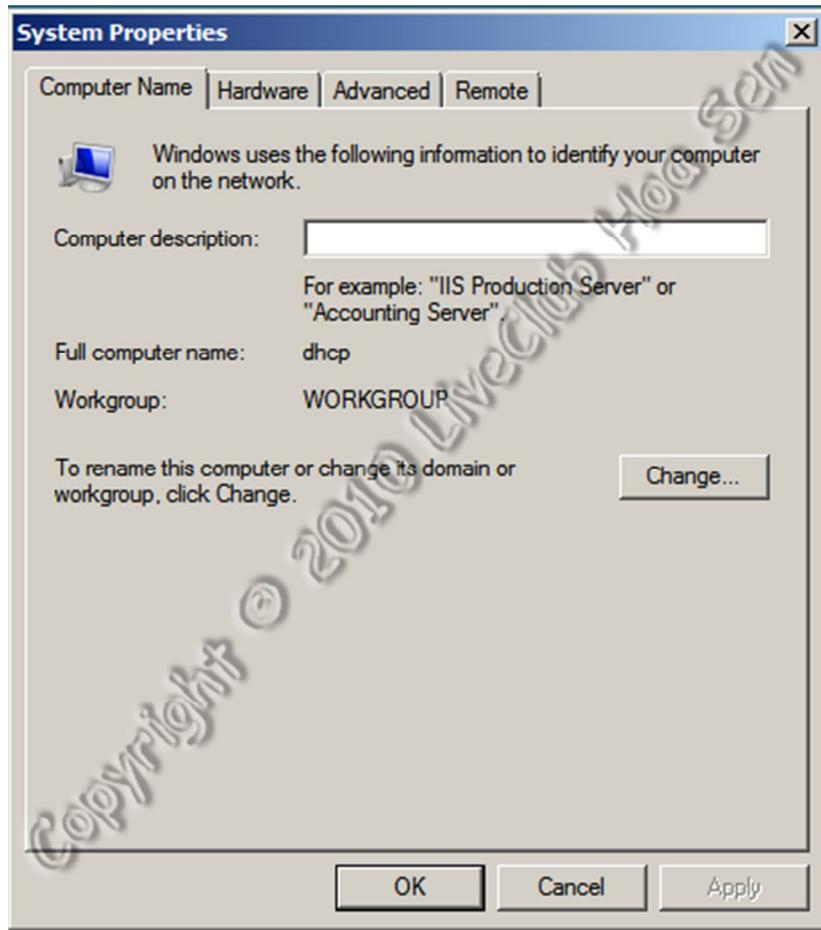
2. Client join domain: (máy client là 2k8 làm tương tự trên Win vista và Win 7)

- * Client phải cùng net với DC và preferDNS về DNS server trong mạng (ở đây DNS server là DC).

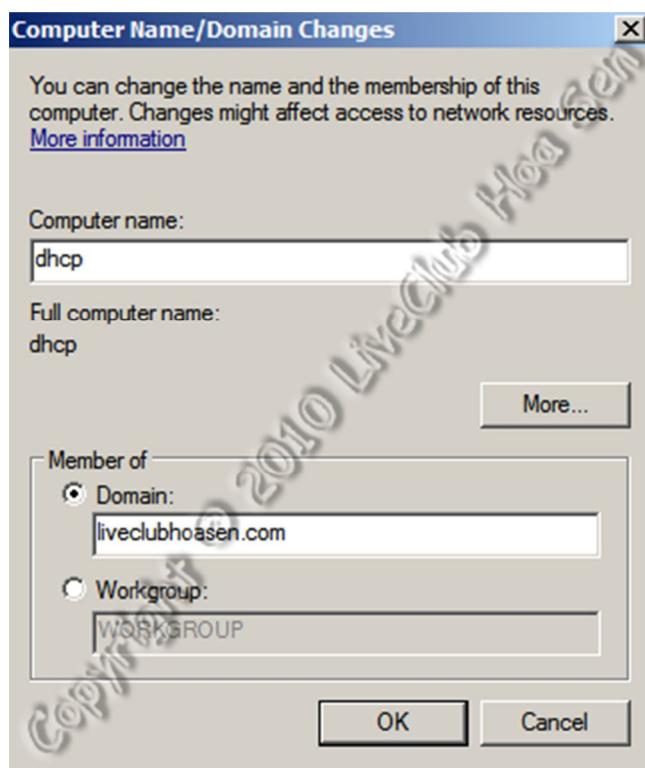


- Vào Computer → Properties → Advanced system settings



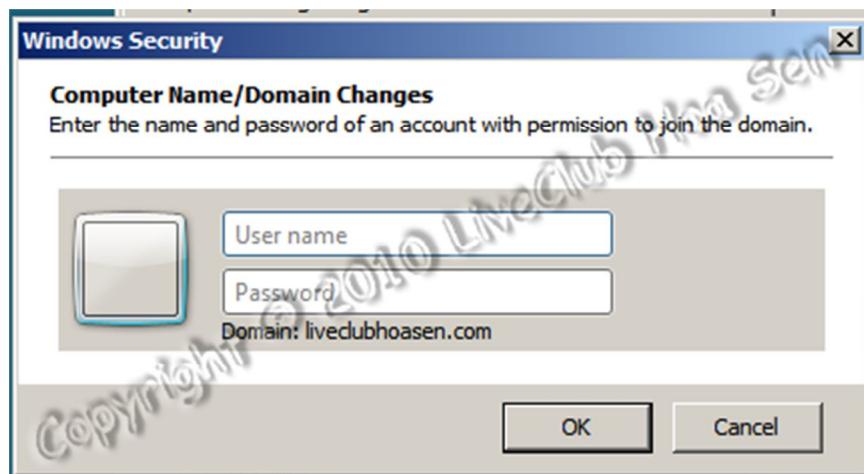


- Nhấn **Change**



- ✓ **Computer Name:** đánh tên máy vào đây nếu muốn đổi tên ở đây chúng tôi chọn là dhcp
- ✓ Tiếp theo stick vào phần **Domain** nhập vào domain của bạn ở đây domain của chúng tôi là **liveclubhoasen.com**

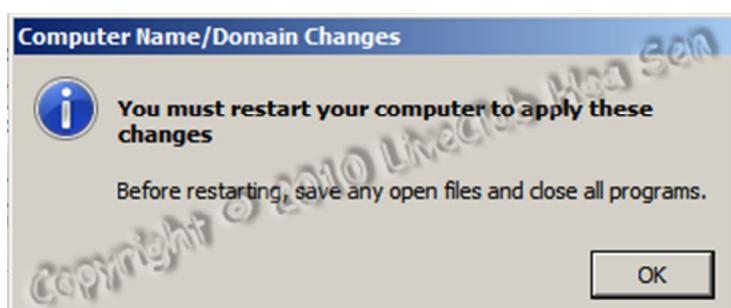
- Nhấn OK hệ thống check DNS server DC của domain liveclubhoasen.com, bảng thông báo hiện ra yêu cầu nhập tài khoản user được quyền joindomain ở đây chúng tôi chọn tài khoản Admin.



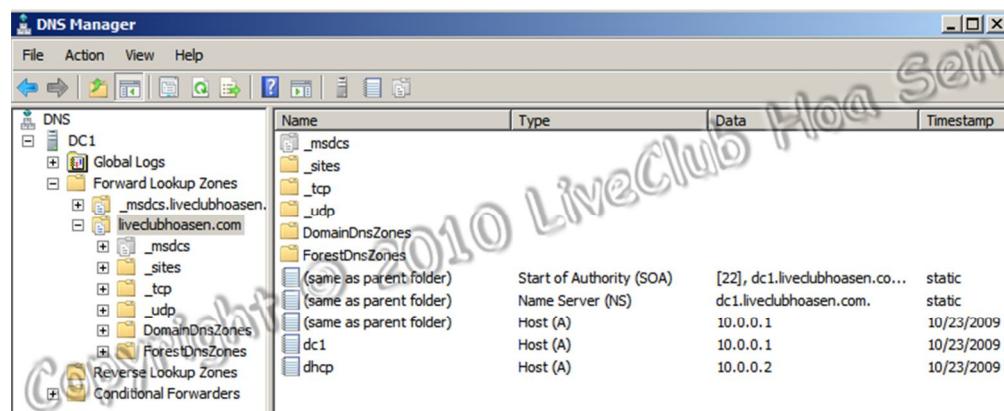
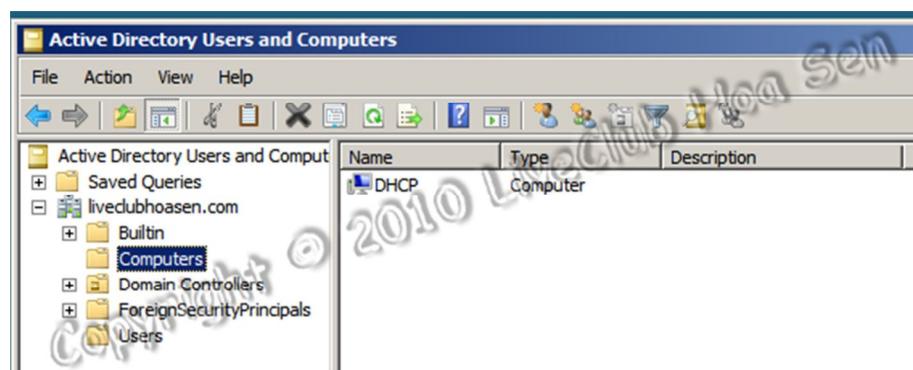
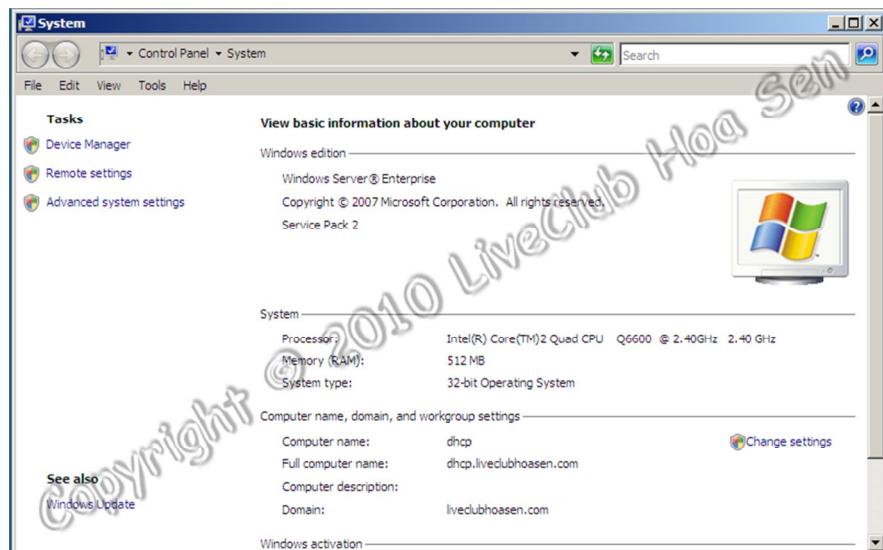
- Xác nhận hoàn tất.



- Yêu cầu Restart lại hệ thống.

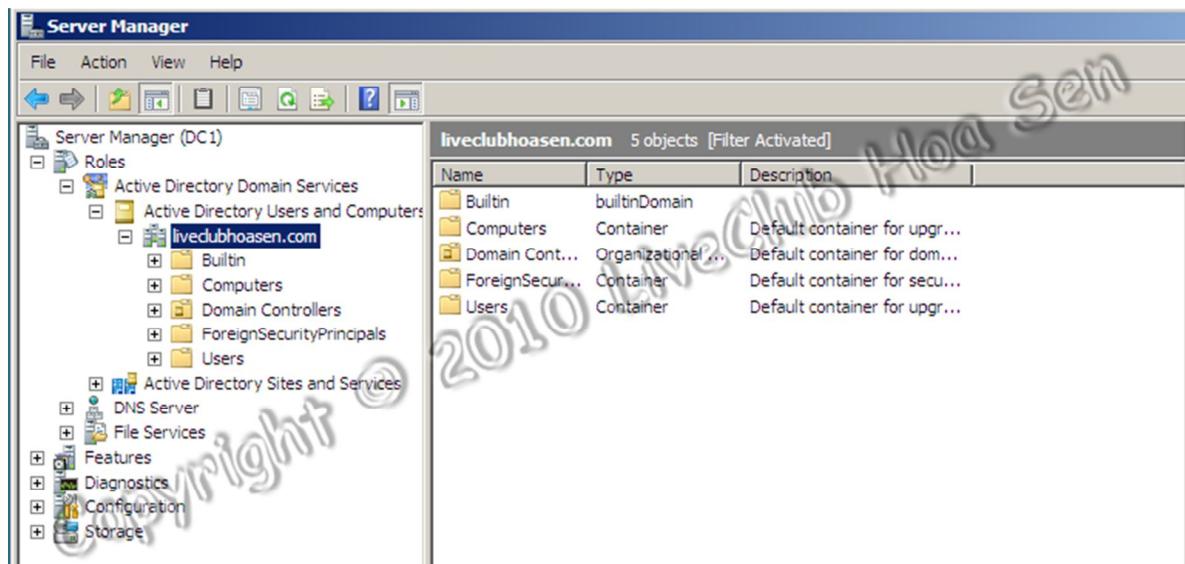


- Log on kiểm tra hệ thống máy sau khi join.



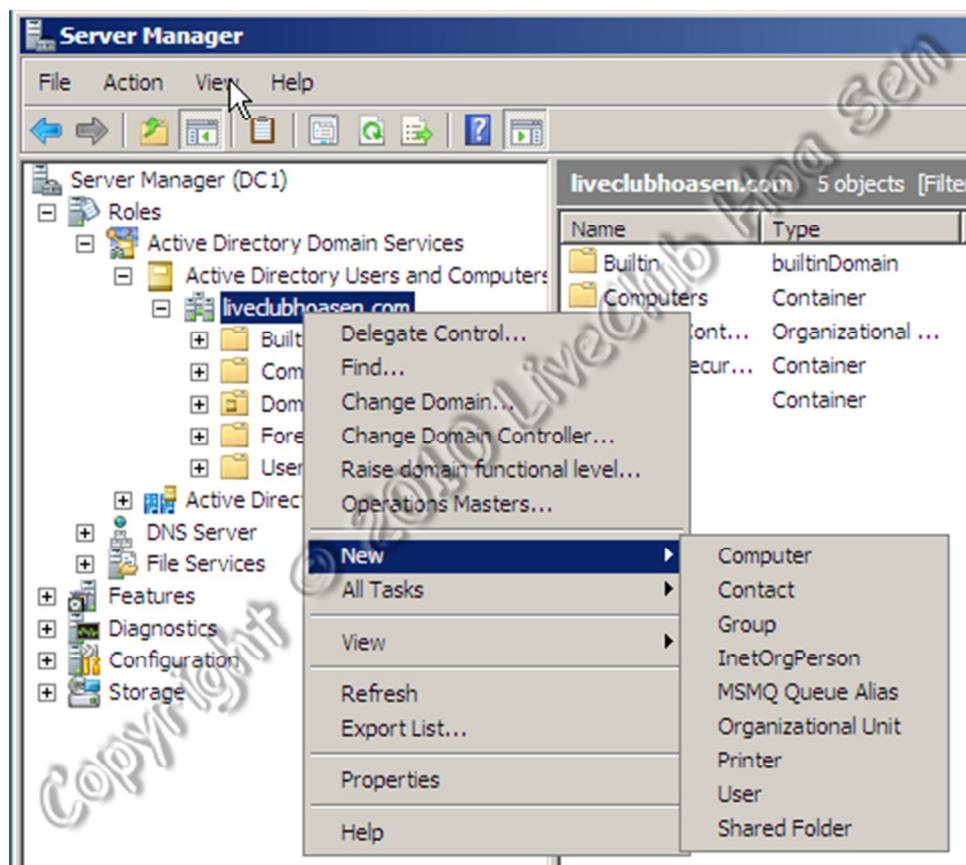
III. Quản lý User, Group, OU:

- Vào Server Management → Roles → Active Directory Domain Services → liveclubhoasen.com (p/s: tên domain của bạn).



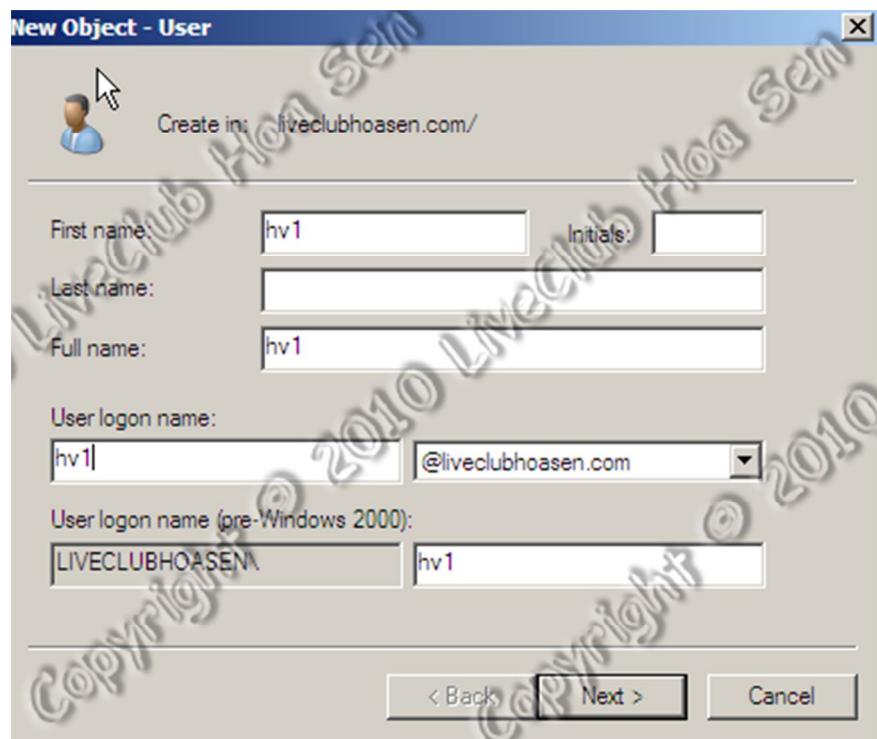
1. Tạo mới User, Group, OU:

- Chuột phải liveclubhoasen.com → New.

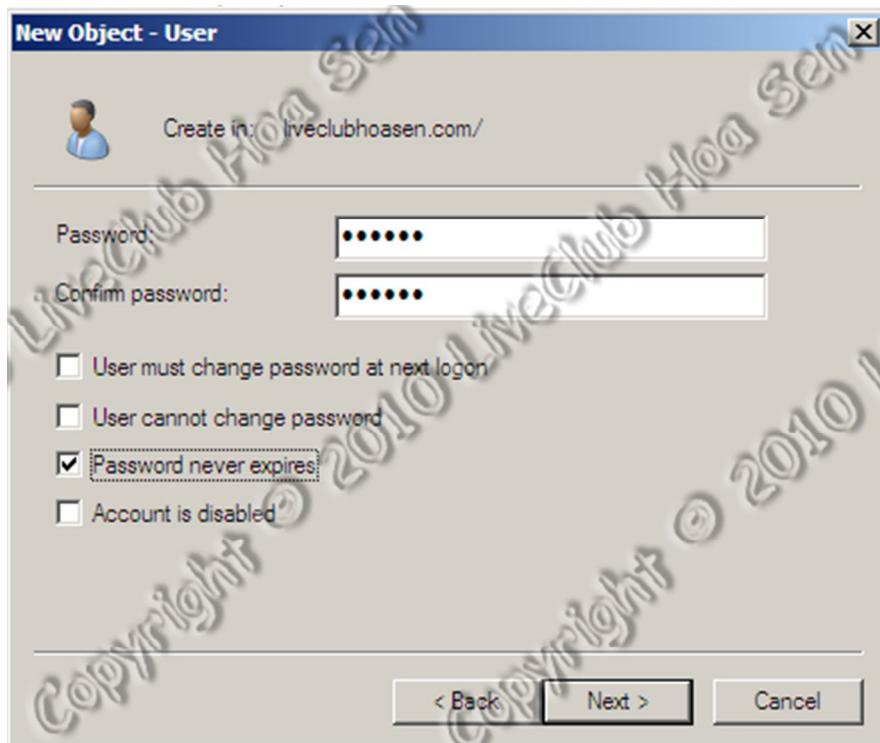


- Chúng ta sẽ tạo mới 1 user **hv1**, 1 group **lop** và 1 group **hocvien**.

a) New User:



- Điền thông tin tài khoản user → Next.



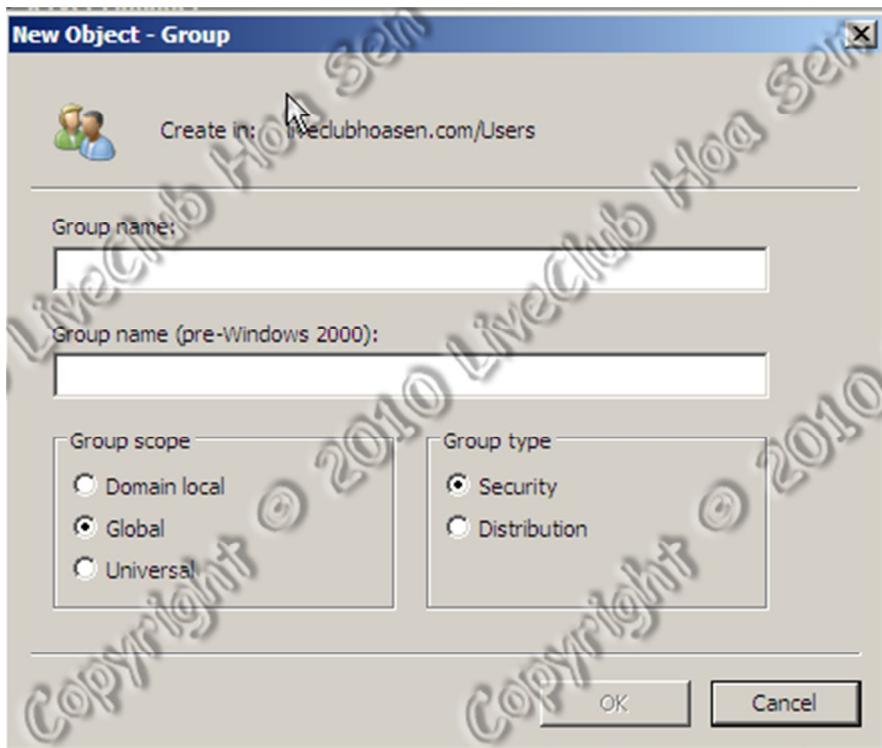
- ✓ **Password:** yêu cầu phức tạp
- ✓ **User must change password at next logon :** tài khoản sau khi tạo yêu cầu thay đổi mật khẩu ngay lần đăng nhập đầu tiên
- ✓ **User cannot change password :** tài khoản này không được quyền thay đổi mật khẩu
- ✓ **Password never expires :** mật khẩu không bao giờ hết hạn vì trong hệ thống sẽ có trường policy quản lý cứ sau 1 khoảng thời gian sẵn sẽ yêu cầu người dùng đổi mật khẩu lại để tăng mức độ bảo mật với người dùng.
- ✓ **Account Disable :** tài khoản sau khi tạo sẽ không được sử dụng ngay lập tức mà sẽ bị khóa chưa được sử dụng.

- Cuối cùng Next tạo tài khoản hoàn tất.

Lưu ý: khi xuất hiện thông báo này thì có nghĩa password tài khoản của bạn chưa phức tạp phải thay cái khác:

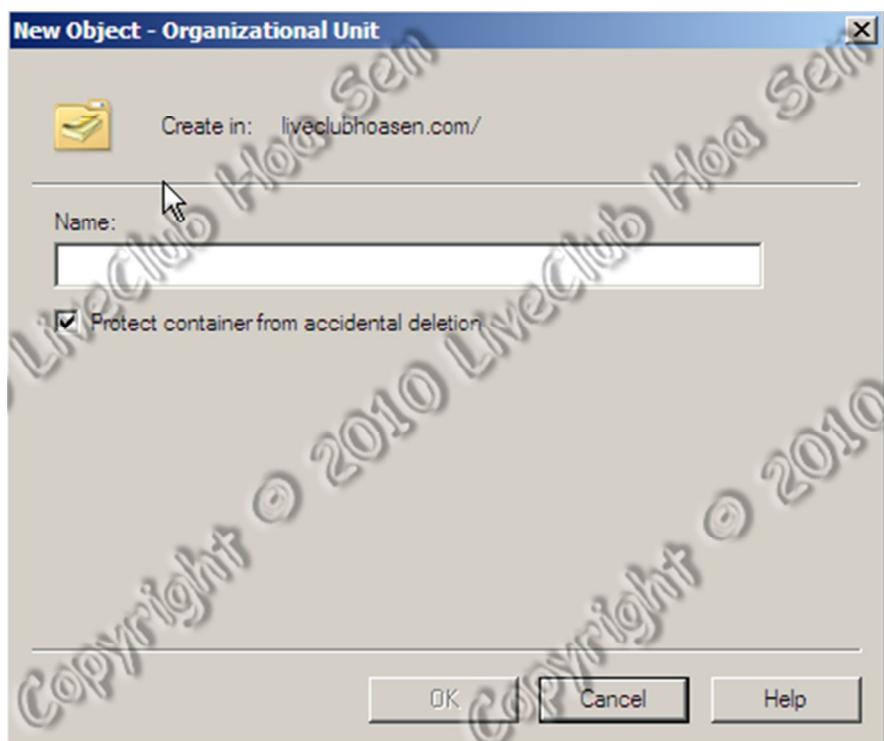


b) New Group:



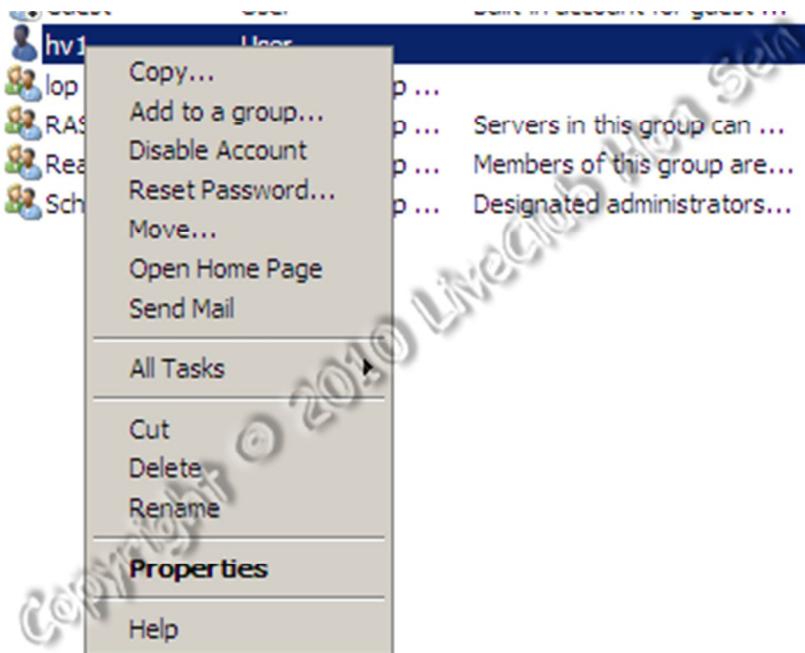
- Nhập group name → OK.

c) New Organizational Unit (OU):



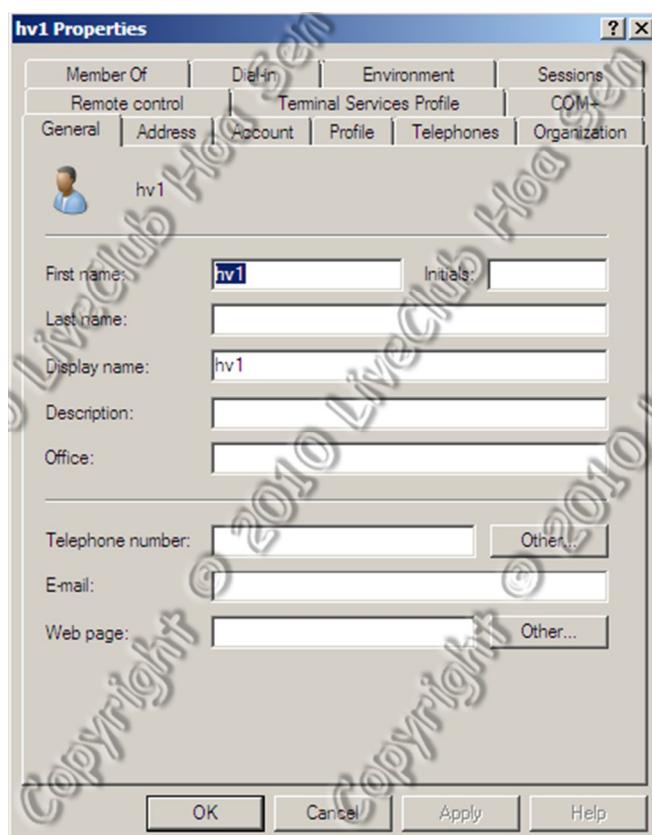
2. Làm việc với User:

- Vào thư mục user chuột phải user **hv1** vừa tạo → Properties.

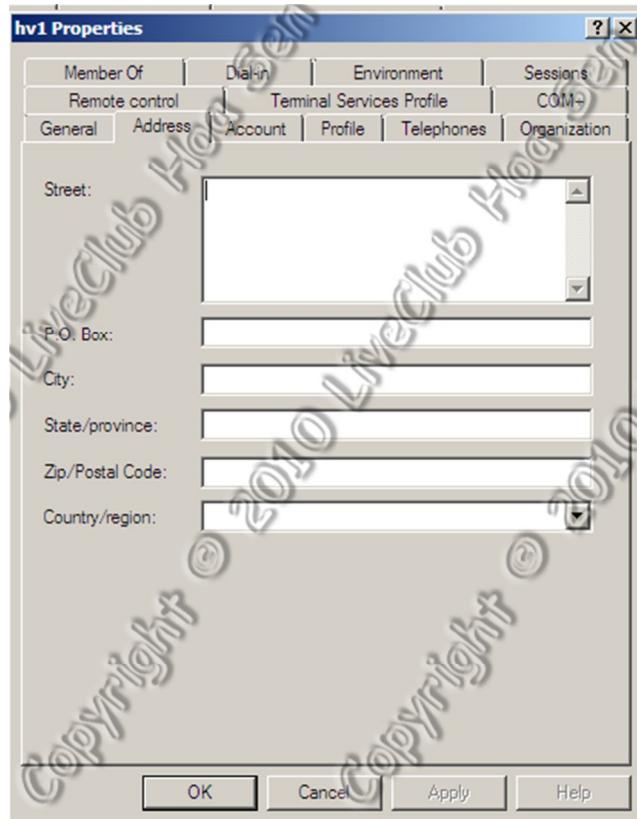


- Hộp thoại thông tin user **hv1** hiện ra. Chúng ta sẽ qua từng TAB

a) **General:** Chứa thông tin cơ bản của user như điện thoại, email, tên, ...

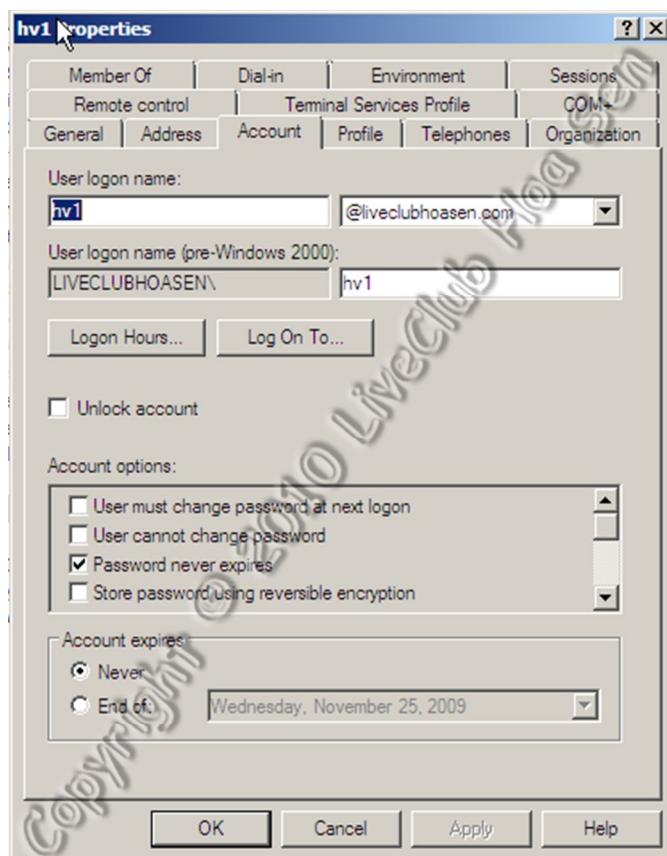


b) **Address:** chưa thông tin địa chỉ, nơi ở , văn phòng, mã vùng...

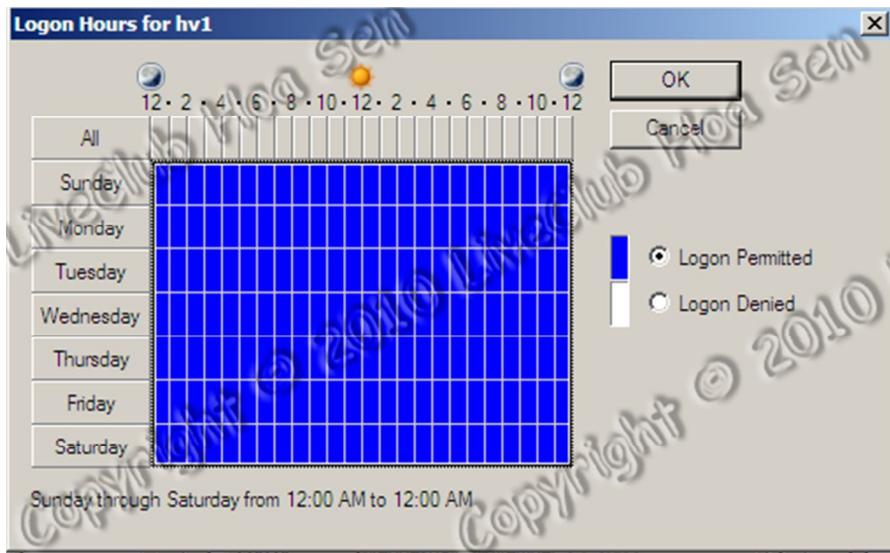


c) **Account:** chứa thông tin tài khoản bao gồm tên đăng nhập, tên domain,..

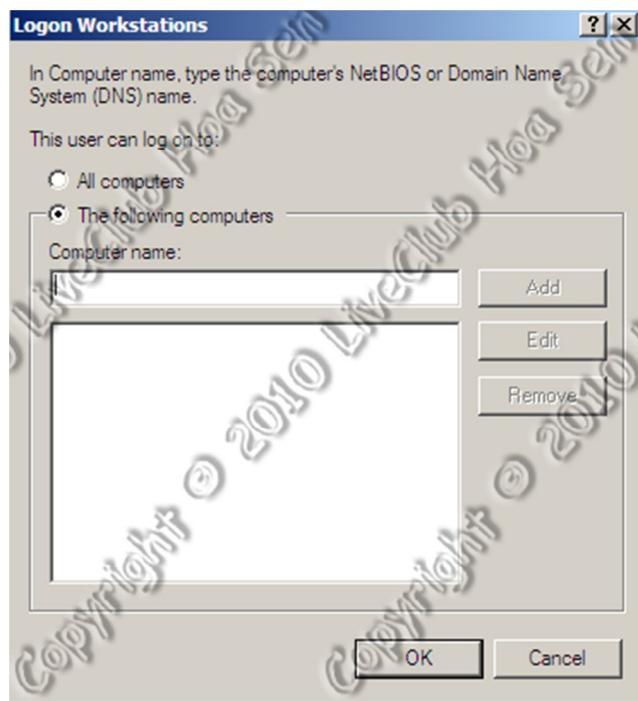
- Account options chứa những thuộc tính action áp cho tài khoản tương tự như ở mục tạo user đã nói các bạn có thể xem lại.
- Account expires quy định ngay tài khoản không còn sử dụng được nữa áp dụng cho tài khoản xài thời vụ.



- Mục **Logon Hours** → quy định thời gian cho phép sử dụng account trong ngày, trong tuần.
- + Với màu xanh ý nghĩa cho sử dụng và màu trắng là cấm.

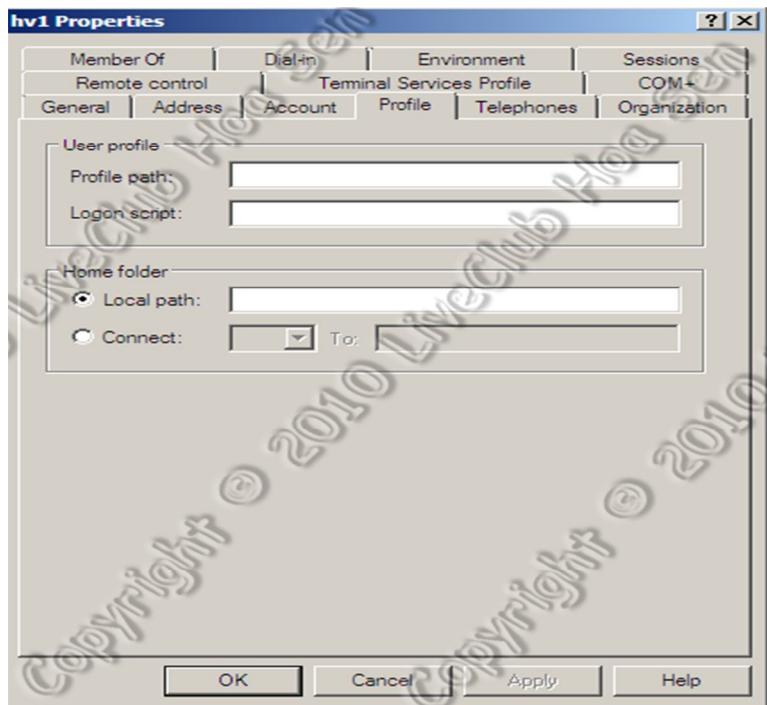


- Mục **Logon To** → quy định máy nào user có quyền logon sử dụng cò thê điền netbios name hoặc domain name của máy.



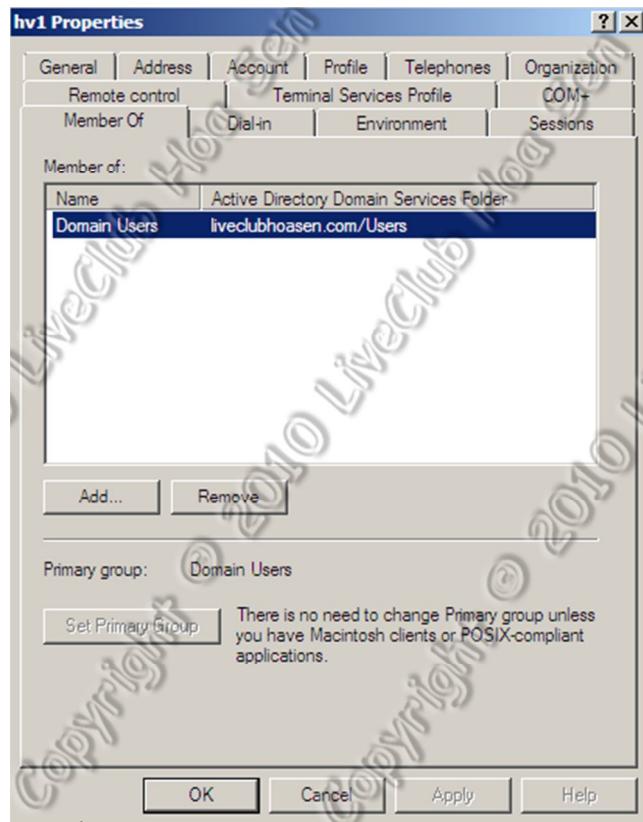
c) Profile:

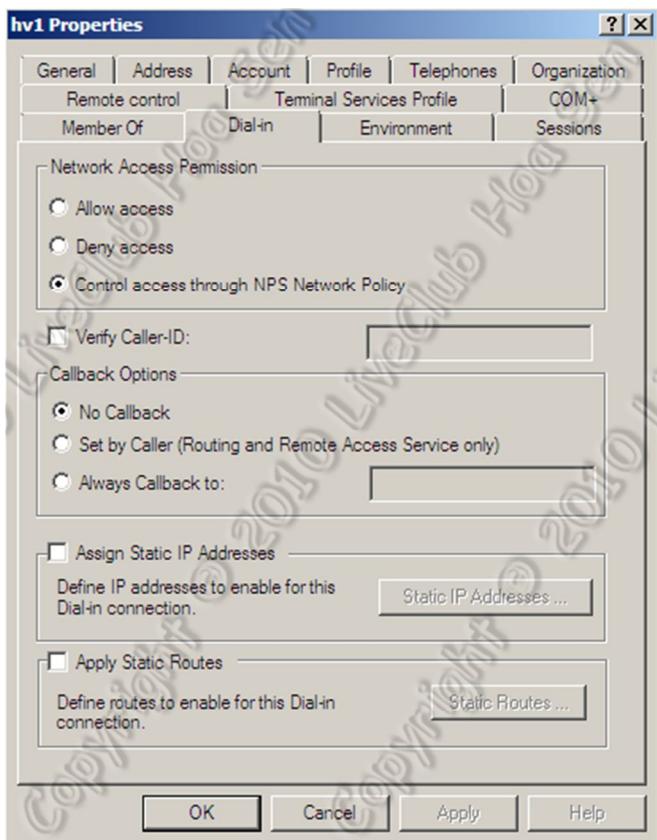
- Profile path : cho phép thay đổi thư mục chứa profile của user
- Logon script : đoạn script sẽ kích mỗi khi user logon hệ thống



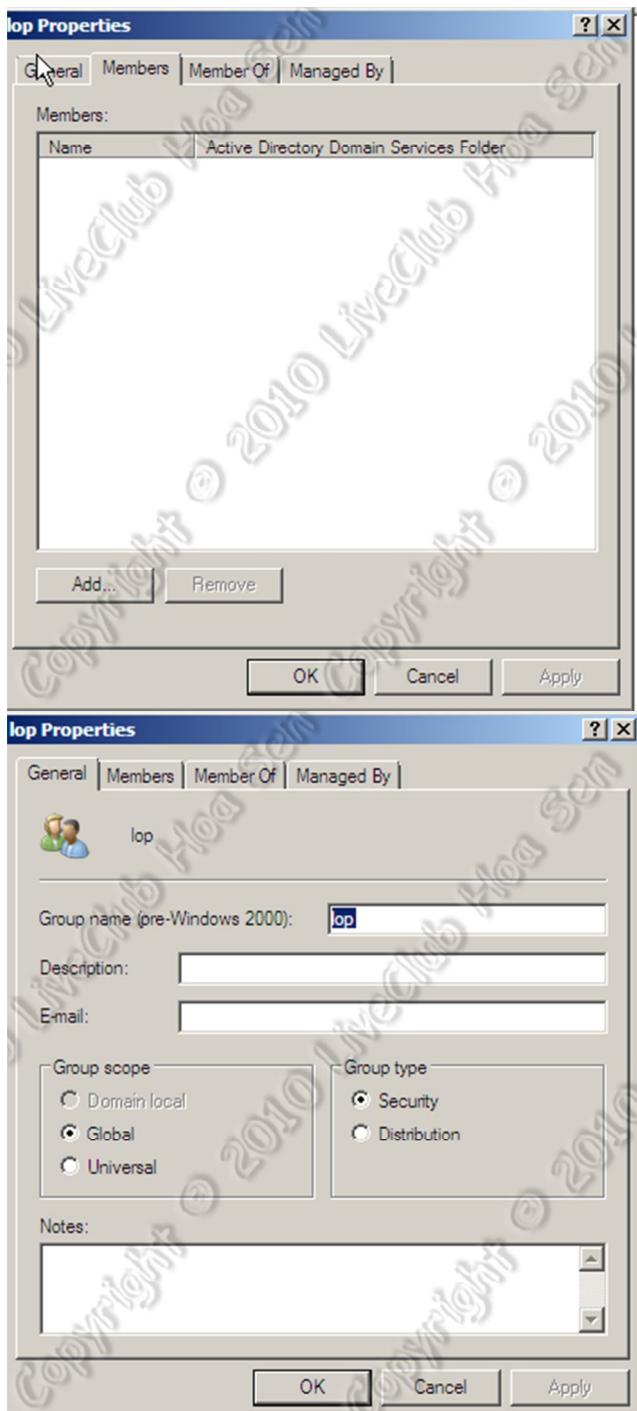
- Localpath : cho phép thay đổi đường dẫn thư mục home của user ở local máy hoặc trên hệ thống mạng thông qua cách connect.

d) Member Of: Quản lý group của user



e) Dial in: Quản lý quyền kết nối của user**3. Làm việc với Group:**

- Chuột phải group → properties.



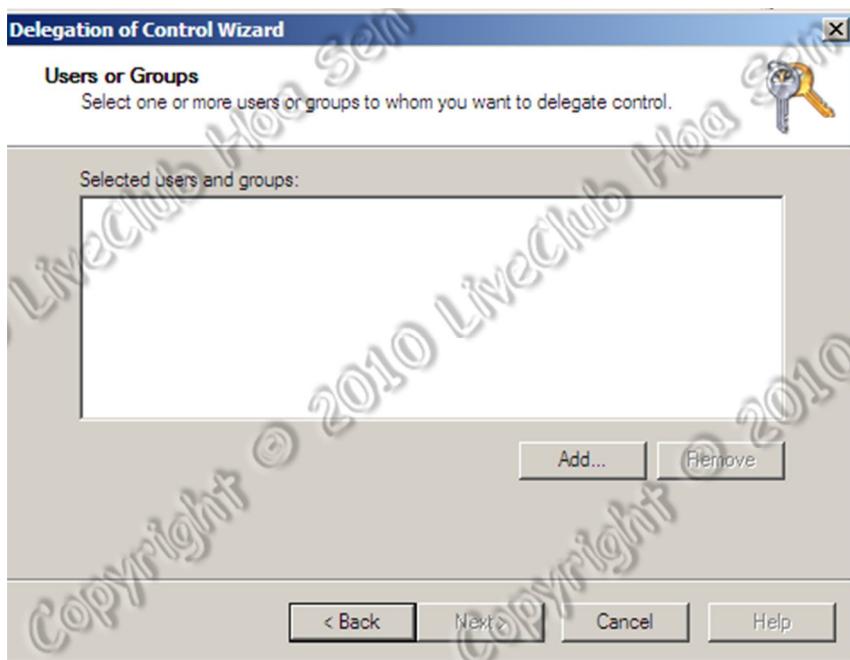
- **General** cho biết thông tin type và scope của group **Members** cho biết user nào thuộc group này **Member of** cho biết group này có nằm trong group nào nữa không, **Managed By** ủy thác cho user nào đó quản lý group.

4. Làm việc với Organizational Unit (OU):

- Có chức năng quan trọng nhất là delegate control chức năng này có nhiệm vụ ủy quyền OU cho user hoặc group quản lý với quyền hạn nhất định tùy theo Admin phân quyền.
- Bước đầu chuột phải OU → Delegate control → Next



- Add user hoặc group sẽ quản lý OU này → Next.



- Trong mục **Delegate the following common tasks** → chọn những quyền hạn có thể cho những người quản lý OU này → Next → Finish.

