

# Read-Only Domain Controllers (RODCs)

## I. Giới thiệu

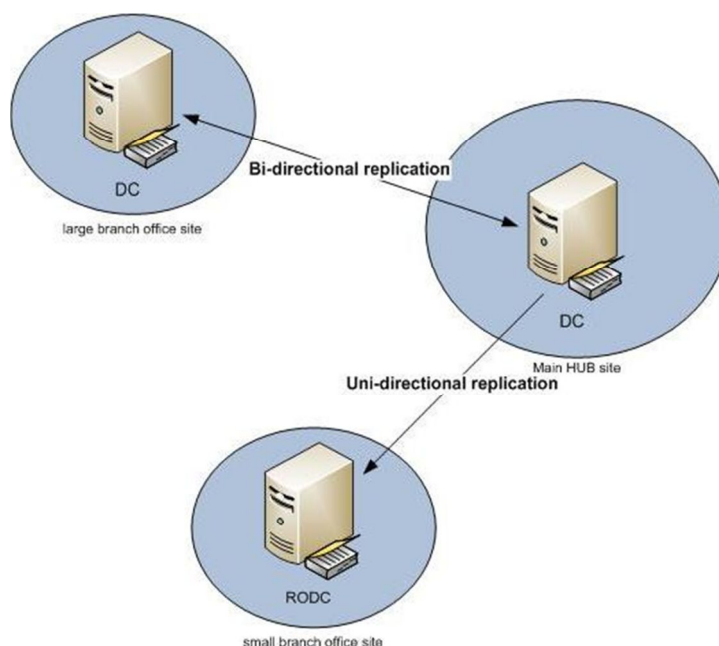
Read-Only Domain Controllers (RODCs) là một dạng mới của domain controller trong Windows Server 2008. Cùng với RODC, các tổ chức có thể dễ dàng triển khai một domain controller tại vị trí mà bảo mật thông thường không thể đảm bảo.

Mục đích chính của RODC là để củng cố an ninh trong các văn phòng chi nhánh. Ở các văn phòng chi nhánh thường rất khó để có được sự giúp đỡ cho những vấn đề cơ sở hạ tầng IT, đặc biệt là Domain Controllers chứa những dữ liệu nhạy cảm. Thông thường một DC có thể tìm thấy dưới một chiếc bàn ở văn phòng. Nếu một người nào đó có thể truy cập vật lý vào DC, không khó để tác động vào hệ thống và có thể truy cập vào dữ liệu. RODC có thể giải quyết những vấn đề này.

**Những yếu tố cần thiết cho RODC là:**

- \* *Read-Only Domain Controller*
- \* *Administrative Role Separation*
- \* *Credential Caching*
- \* *Read-Only DNS*

RODC chứa những bản copy không cho phép ghi và không cho phép đọc của cơ sở dữ liệu của Active Directory với tất cả những thuộc tính và các đối tượng. RODC chỉ hỗ trợ những bản sao đơn hướng những thay đổi của Active Directory, có nghĩa là RODC luôn sao chép trực tiếp với Domain Controllers tại vị trí HUB.



### Hình A: sao chép đến RODC

RODC sẽ thực hiện việc sao chép thông thường hướng đến từ vị trí HUB cho những thay đổi của Active Directory và DFS. RODC sẽ nhận bất kì thứ gì đến từ Active Directory nhưng những thông tin nhạy cảm, bằng những tài khoản mặc định như Domain Admins, Enterprise Admins và Schema Admins đều được loại ra khỏi việc sao chép của RODC

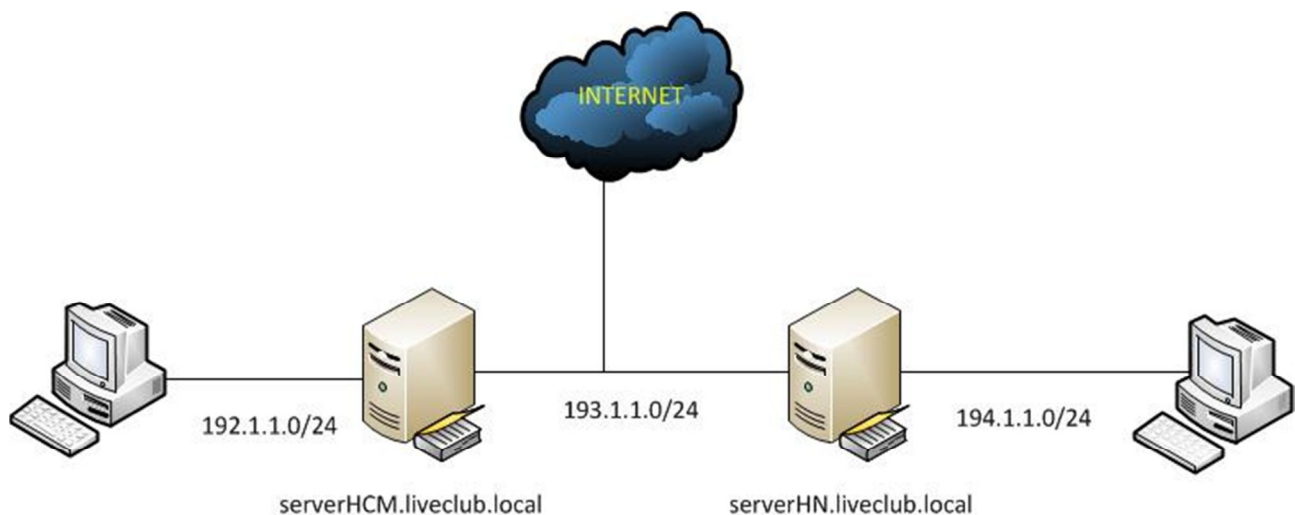
Nếu một bản sao chép cần viết truy cập đến Active Directory, RODC gửi một phản hồi chuyển đến LDAP tự động đưa ứng dụng đến một Domain Controller cho phép ghi, tại vị trí HUB chính. RODC này cũng có thể chạy Global Catalog Role để đăng nhập nhanh hơn nếu cần.

Đây là thuận lợi lớn nhất cho các văn phòng chi nhánh, bởi vì nếu có ai truy cập vật lý vào server hay thậm chí là ăn trộm nó, người này có thể crack mật mã trên tài khoản người dùng ở AD, nhưng không phải tất cả các tài khoản nhạy cảm - bởi vì chúng không tồn tại trên RODC.

Điều này có nghĩa là những tài khoản admin nhạy cảm không thể log in vào RODC nếu kết nối WAN đến vị trí HUB hiện không có sẵn.

Để thi hành RODC trong môi trường của bạn, bạn cần domain của mình và forest ở chế độ Windows Server 2003 và DC chạy bộ mô phỏng PDC cần để chạy Windows Server 2008.

## II. Mô hình



Hình B: mô hình demo

Trong mô hình này chủ yếu dùng 3 máy là chính 2 máy server và 1 máy client

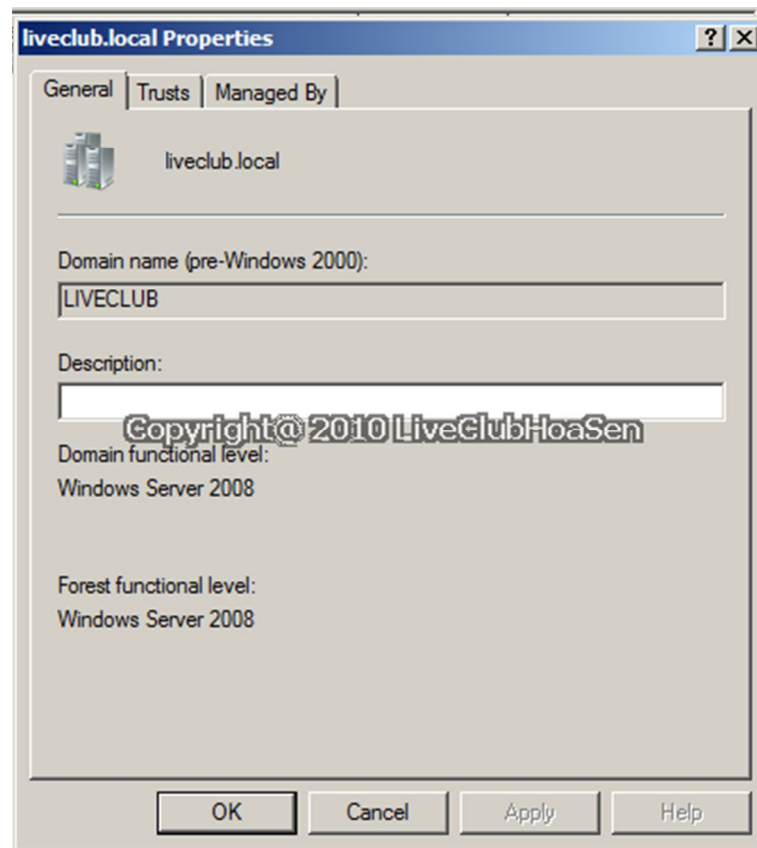
Yêu cầu ban đầu:

- ❖ Thiết lập ban đầu như mô hình có thể dùng Routing and Remote Access hoặc default route thiết lập liên lạc 2 mạng 192.1.1.0/24 và 194.1.1.0/24
- ❖ Máy ServerHCM đã lên DC liveclub.local
- ❖ Máy ServerHN đã join domain

## III. Cấu hình

### Bước 1: Kiểm tra functional level domain

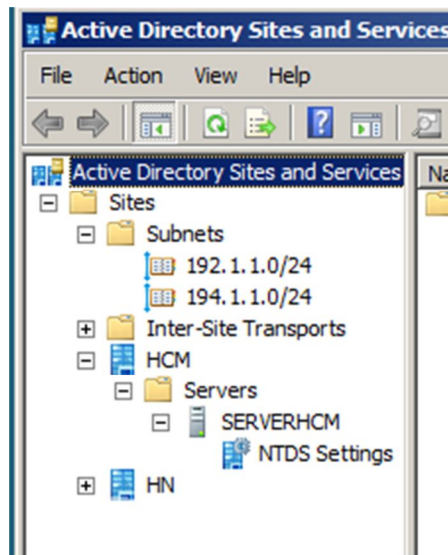
Trước khi bắt đầu, bạn phải bảo đảm rằng mức chức năng Forest đã được thiết lập cho Windows Server 2003 hoặc phiên bản cao hơn. Để thực hiện điều đó, bạn chỉ cần mở giao diện điều khiển **Active Directory Domains and Trusts**. Khi cửa sổ này được mở, hãy kích chuột phải vào **Active Directory forest** của bạn, sau đó chọn lệnh **Properties**. Như những gì bạn có thể thấy qua hình A, mức chức năng forest được liệt kê trên tab **General** của trang thuộc tính.



Nếu mức chức năng forest không có đủ thẩm quyền, khi đó bạn phải nâng mức trước khi tiếp tục. Cần lưu ý rằng điều này có nghĩa bạn sẽ không thể sử dụng các bộ điều khiển miền của Windows 2000 trong forest của bạn. Để nâng mức chức năng forest, kích **OK** để đóng trang thuộc tính. Lúc này, hãy kích phải vào danh sách forest của bạn một lần nữa và chọn mức **Raise Forest Functional level**, trên cửa sổ xuất hiện sau đó, hãy chọn tùy chọn **Windows Server 2003**, sau đó kích nút **Raise**.

## Bước 2: cấu hình chia site cho hệ thống

Vì ở đây chúng ta đang làm bài lab giả định hai trụ sở ở 2 hai vị trí địa lý khác nhau chúng ta sẽ cấu hình chia site cho hệ thống một cho HCM và một cho HN.



### Bước 3: Nâng cấp RODC

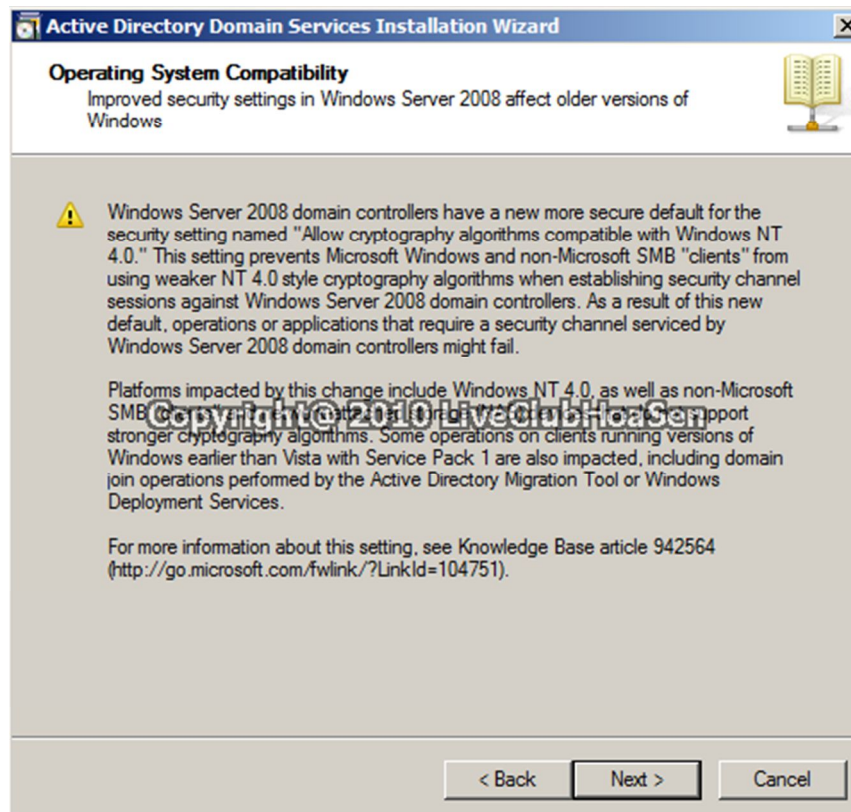
Bây giờ bắt đầu cấu hình máy chủ của bạn làm nhiệm vụ của một Read Only Domain Controller. Quá trình thực hiện khá giống với quá trình cấu hình máy chủ là một domain controller.

Bắt đầu quá trình bằng cách đăng nhập vào máy chủ qua tài khoản thành viên của nhóm quản trị viên miền. Tại đây, hãy nhập lệnh **DCPROMO** vào nhắc lệnh **Run** của máy chủ. Khi đó bạn sẽ thấy Windows khởi chạy Active Directory Domain Services Installation Wizard. Wizard sẽ thực hiện một thủ tục kiểm tra nhanh chóng để bảo đảm rằng các nhị nguyên phân Active Directory đã được cài đặt. Các nhị nguyên phân này bình thường không được cài đặt (mặc định), vì vậy wizard sẽ cài đặt chúng cho bạn.

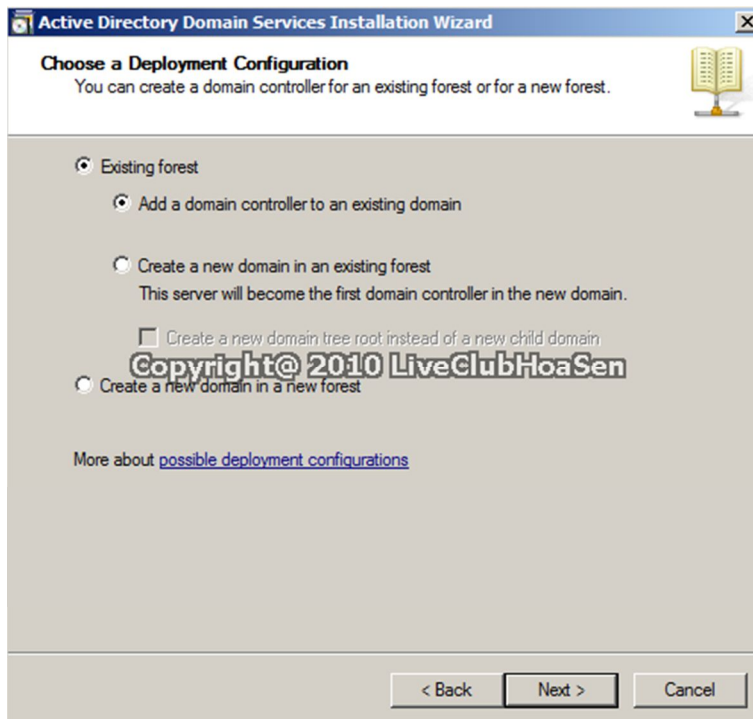
Khi Windows kết thúc việc cài đặt các nhị nguyên phân, nó sẽ hiển thị màn hình chào của wizard. Mặc dù bạn có thể kích Next và băng qua màn hình chào của wizard nhưng trong trường hợp này bạn cần tích vào hộp kiểm **Use Advanced Mode Installation**. Bước này rất quan trọng nếu thiếu mất bước này sẽ có một vài tùy chọn trong những bước sau sẽ mất đi buộc bạn phải cấu hình sau khi mà việc cài đặt hoàn tất.



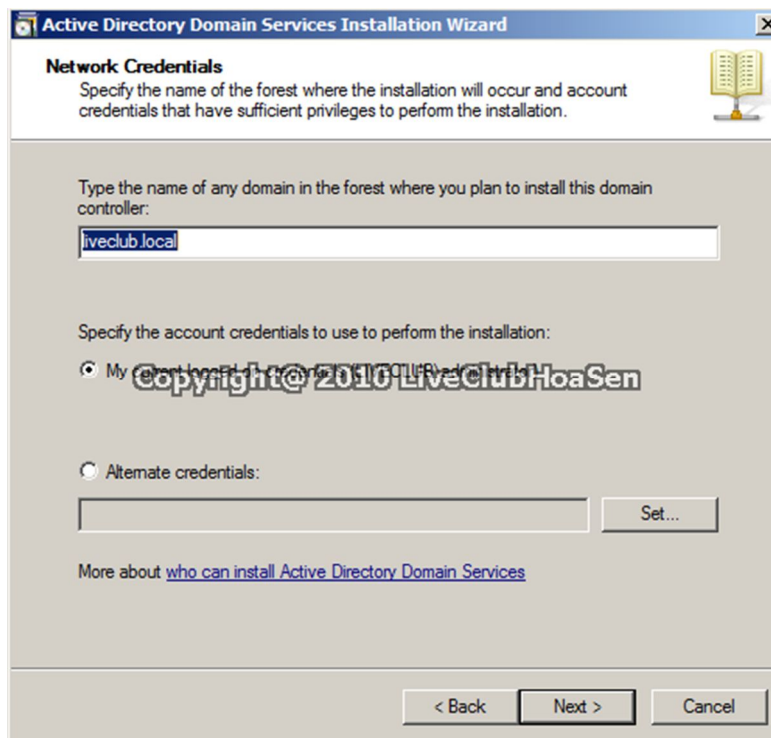
Click **Next** hộp thoại **Operating System Compatibility** hiện ra thông báo chi tiết về sản phẩm và những lưu ý khi thiết lập



Kích **Next**, khi đó wizard sẽ hỏi bạn về forest và miền nào mà domain controller mới sẽ phục vụ. Chọn tùy chọn để bổ sung domain controller vào một miền bên trong một forest đang tồn tại.

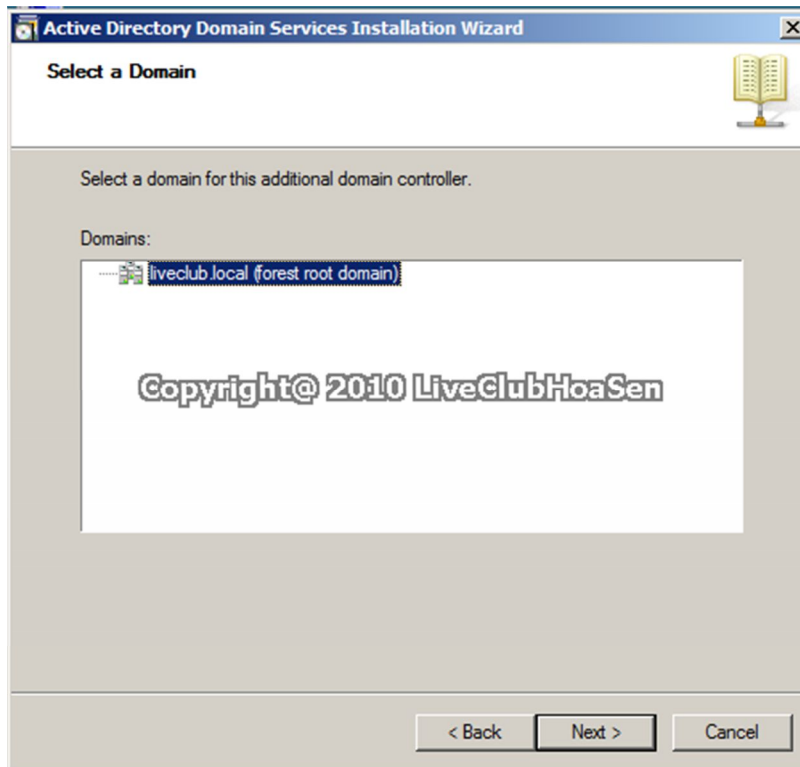


Kích **Next**, wizard sẽ nhắc nhở chỉ định tên của miền mà bạn đã lên kế hoạch cho việc bổ sung domain controller đến. Bạn cũng phải xác nhận rằng mình muốn sử dụng các tiêu chuẩn đã được đăng nhập khi được nhắc nhở tăng cấp máy chủ lên trạng thái domain controller. Khi thực hiện xong, hãy kích **Next**.

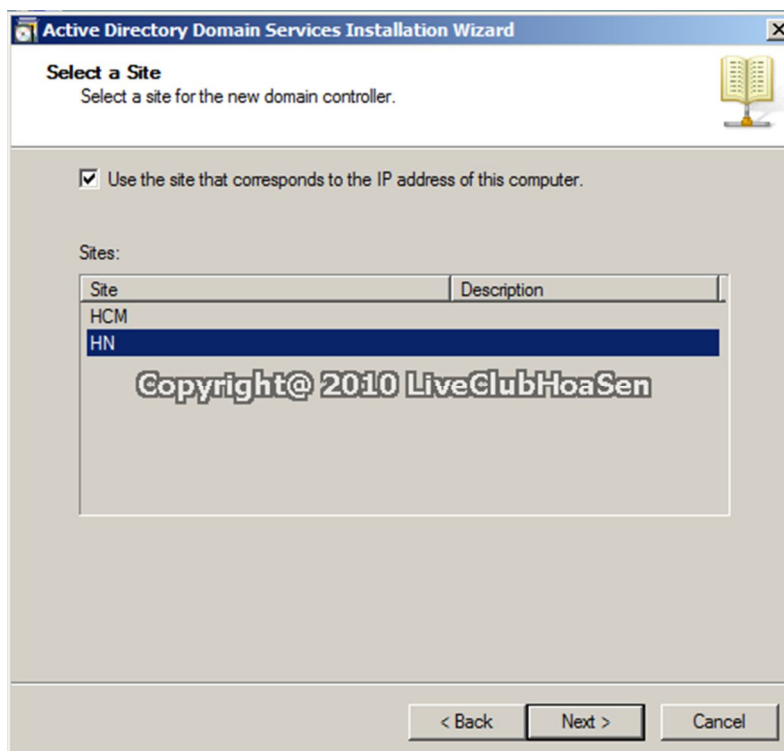




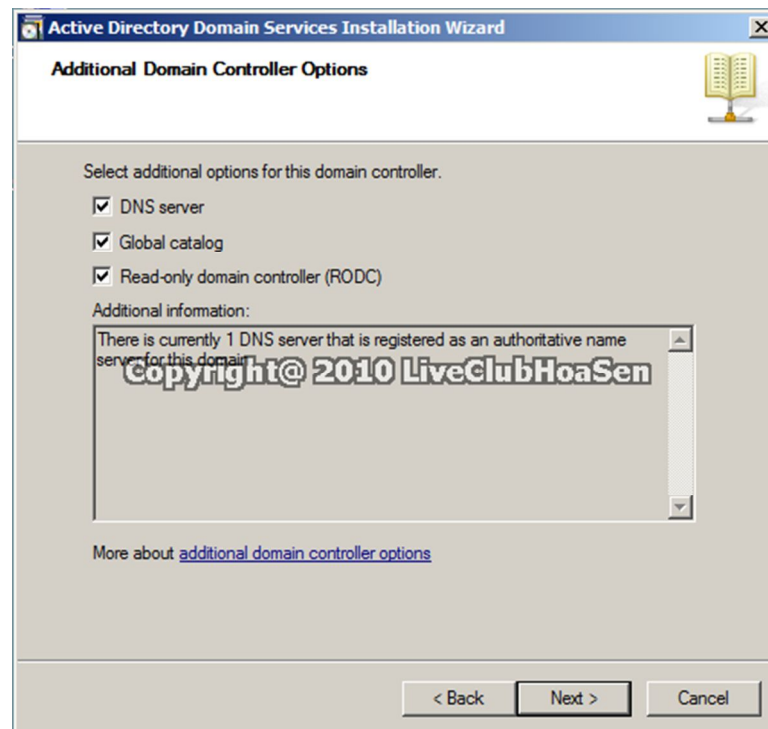
Màn hình dưới đây sẽ yêu cầu bạn xác nhận sự lựa chọn miền của mình. Sau khi thực hiện xong, kích **Next**.



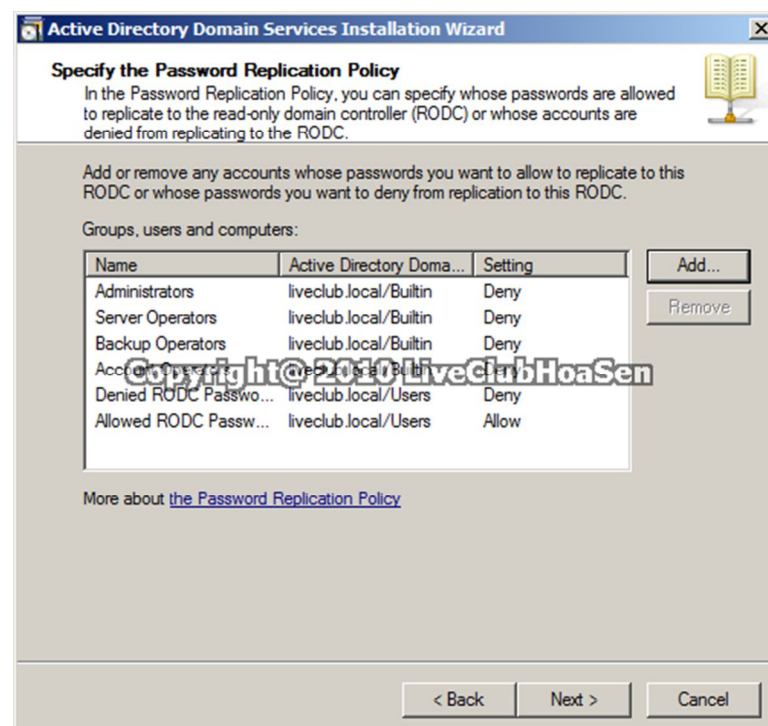
Bạn sẽ thấy một màn hình yêu cầu chỉ định tên của site mà bạn muốn đặt domain controller trong đó. Đây là một bước quan trọng đối với Read Only Domain Controllers, vì chúng thường được đặt tại các văn phòng chi nhánh, do vậy luôn nằm trong những site Active Directory độc lập.



Kích **Next**, bạn sẽ được yêu cầu chọn các tùy chọn bổ sung cho domain controller. Rõ ràng bạn sẽ muốn chọn tùy chọn **Read Only Domain Controller** nhưng bên cạnh đó bạn cũng nên tạo chọn cho domain controller các tùy chọn **DNS server** và máy chủ catalog toàn cục (**global catalog**).

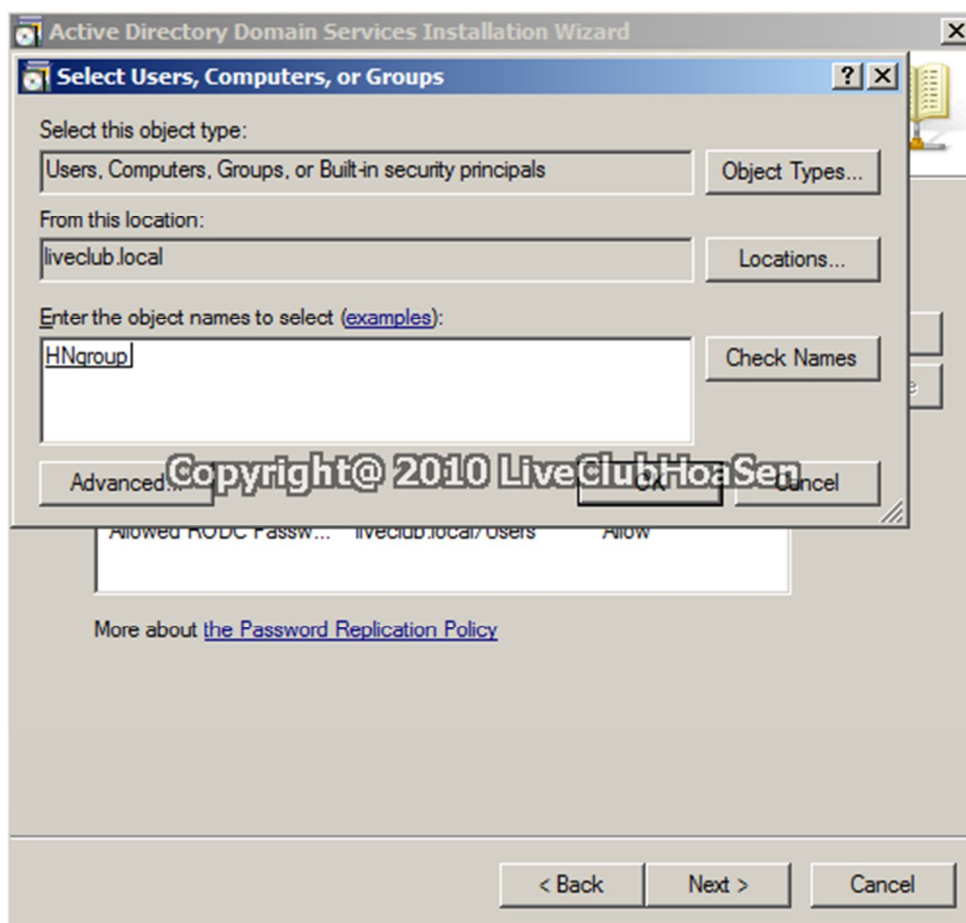
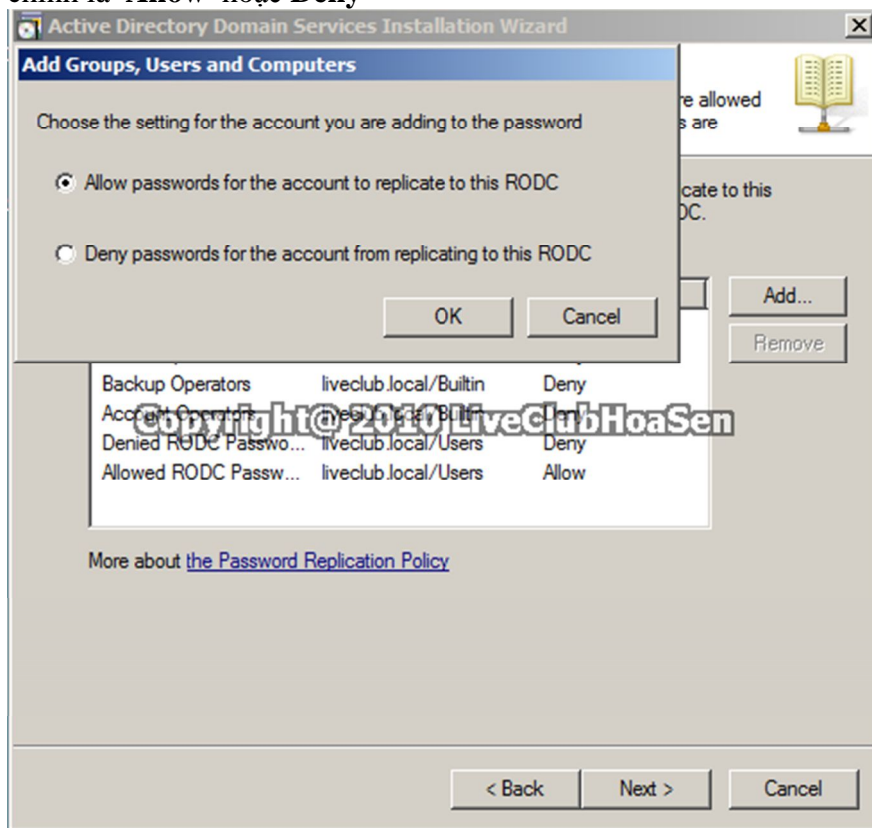


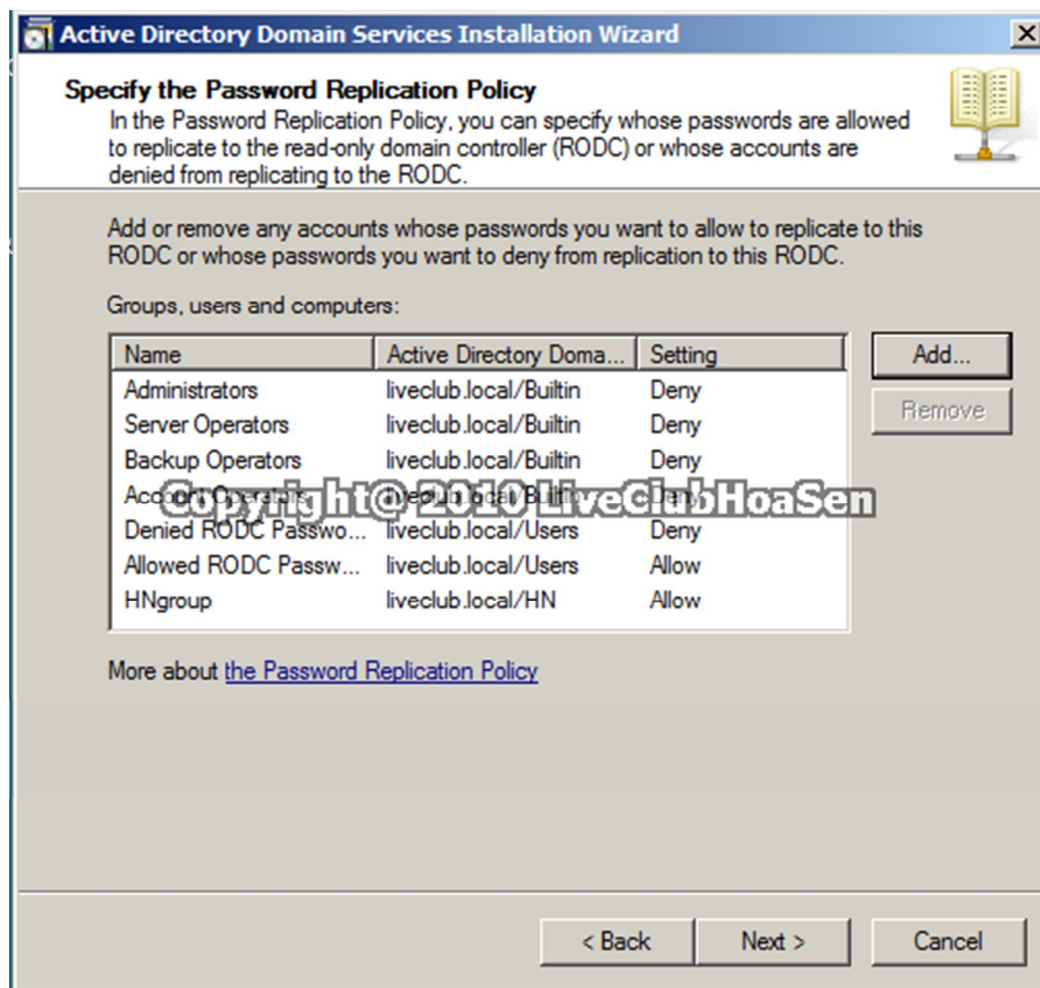
Kích **Next**, bạn sẽ được yêu cầu chỉ định **Password Replication Policy**. Đây chính là nơi bạn có thể điều khiển mật khẩu nào được phép tạo bản sao trong Read Only Domain Controller. Bạn có thể tạo bất cứ thay đổi nào cần thiết, tuy nhiên những tùy chọn mặc định làm việc cũng khá tốt.



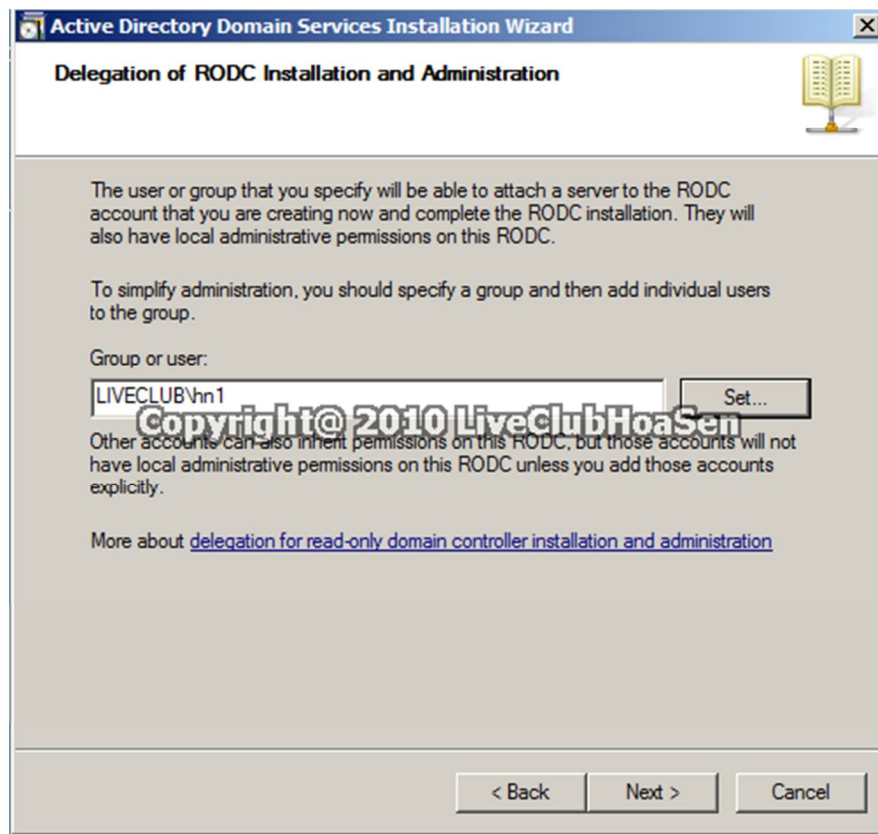


Click **AddB** để tùy biến thêm việc quản lý tài khoản nào được sao chép với 2 hành động chính là **Allow** hoặc **Deny**

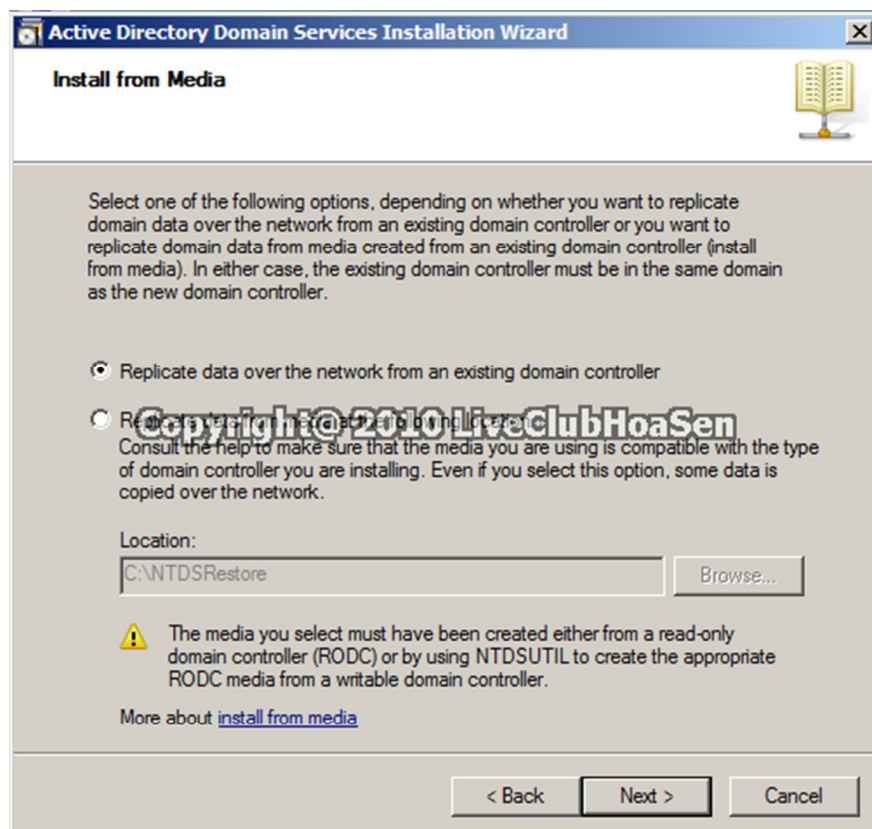




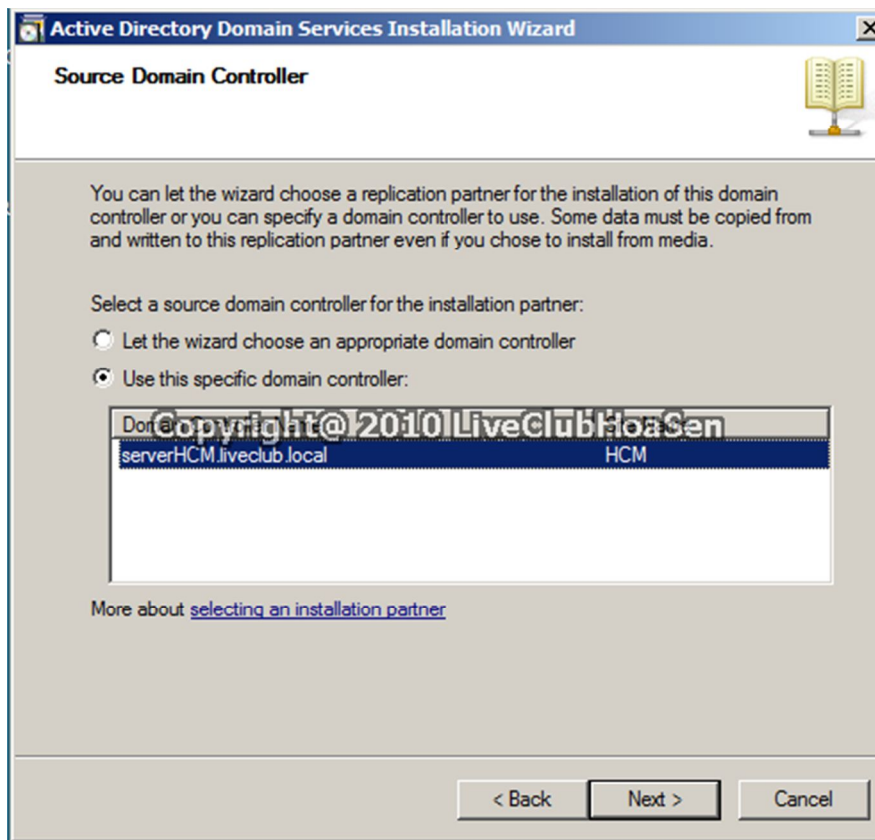
Kích **Next**, bạn sẽ có thể ủy nhiệm người dùng hoặc nhóm để hoàn tất quá trình cài đặt RODC. Không nên quá quan tâm đến các tùy chọn mà chúng tôi đã thực hiện ở đây (chỉ mang tính ví dụ).



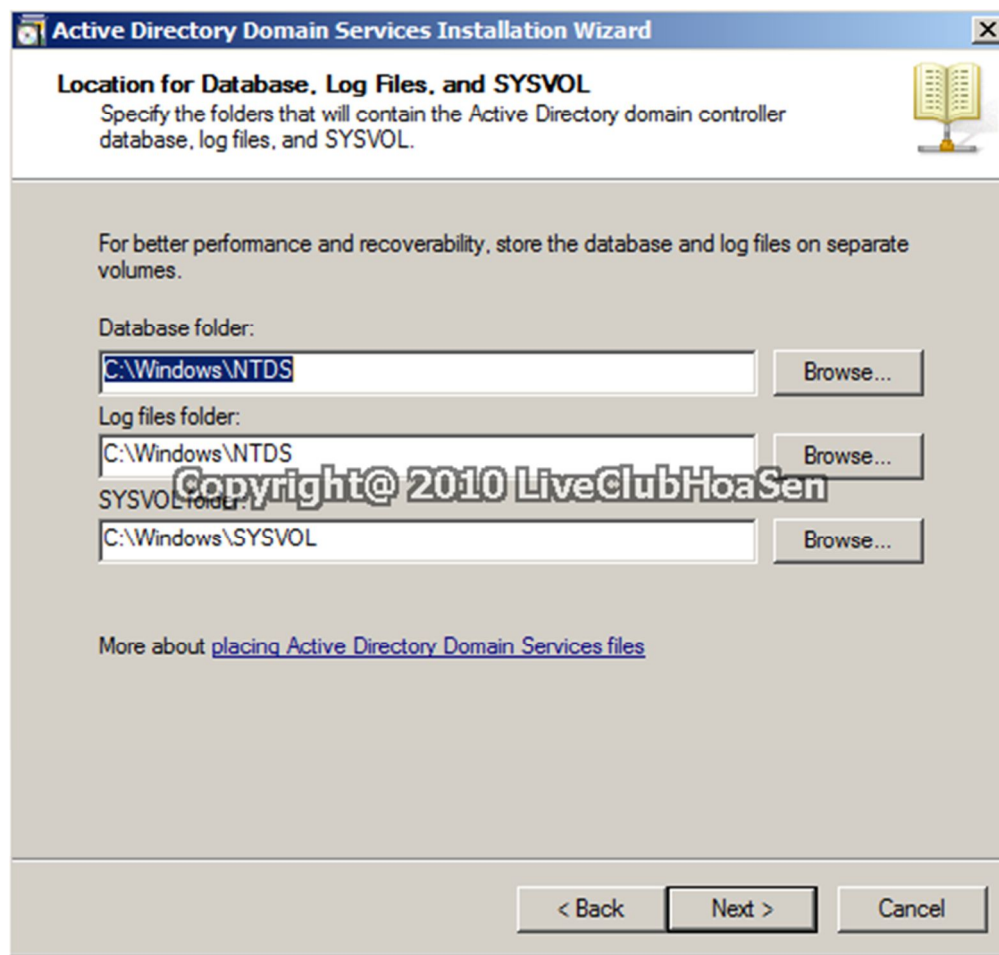
Màn hình tiếp theo mà bạn thấy sẽ cung cấp cho bạn tùy chọn tái tạo dữ liệu trên mạng từ một domain controller hay tạo một cơ sở dữ liệu Active Directory từ một file. Việc tạo một cơ sở dữ liệu Active Directory từ một file sẽ rất tiện lợi nếu bạn có một cơ sở dữ liệu lớn và kết nối chậm. Ngược lại, bạn nên chọn tái tạo dữ liệu qua mạng.



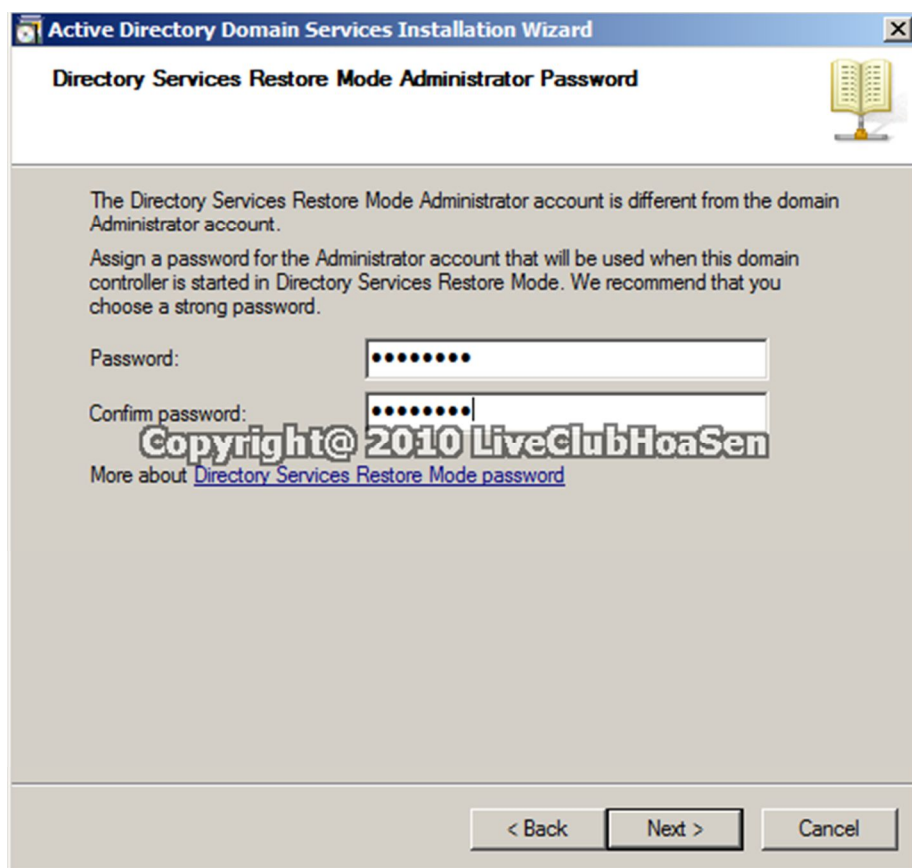
Màn hình tiếp theo yêu cầu bạn chọn đối tác tạo bản sao cho domain controller. Cách tốt nhất vẫn thường được sử dụng là cho phép Windows chọn đối tác tạo bản sao cho bạn trừ khi bạn có một lý do nào đó cho việc sử dụng một domain controller cụ thể nào đó. Ở đây chúng ta chỉ có 1 DC chính nên sẽ chọn DC chính đó làm nguồn sao chép.



Khi kích Next, bạn sẽ được đưa đến một cửa sổ trong wizard mà bạn có thể sử dụng đã quen sử dụng. Màn hình này yêu cầu bạn chỉ định vị trí cơ sở dữ liệu Active Directory sẽ được lưu. Cần đưa ra sự lựa chọn của bạn và kích Next.



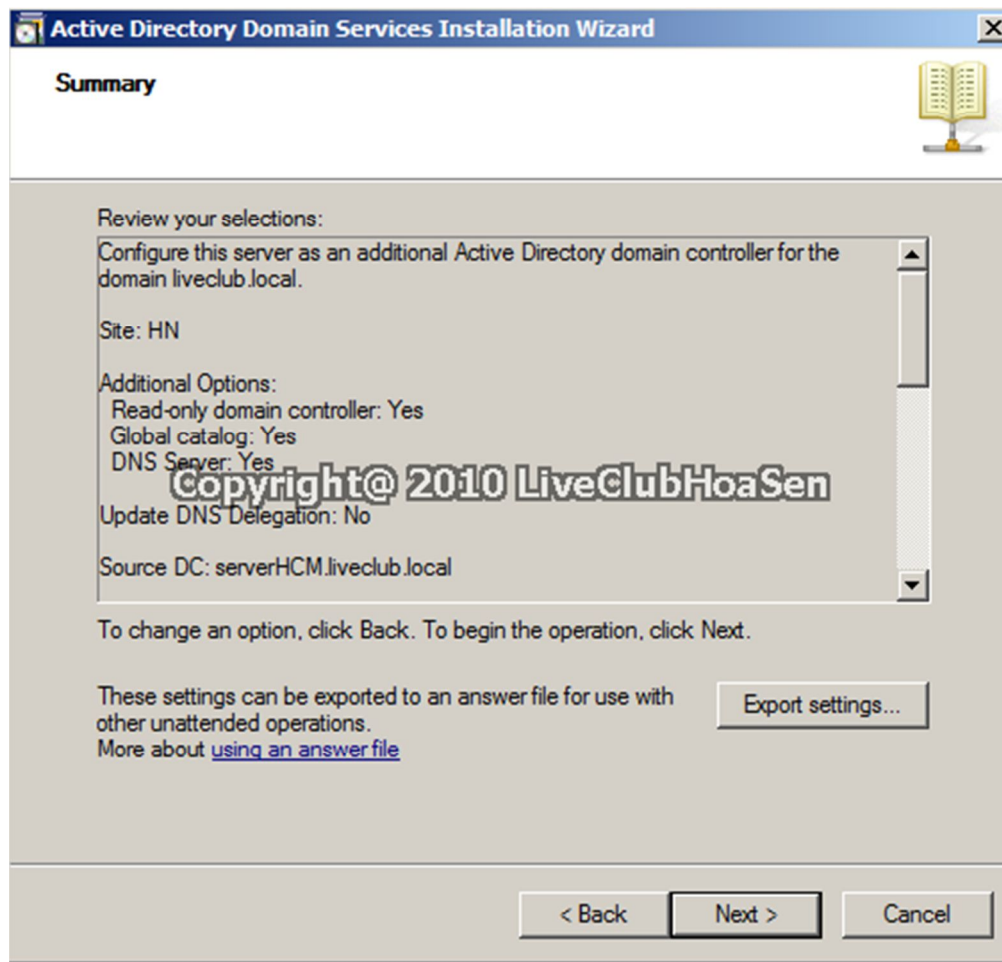
Sau đó bạn sẽ được nhắc nhở phải cung cấp mật khẩu Directory Services Restore Mode. Nhập vào mật khẩu và kích **Next**.



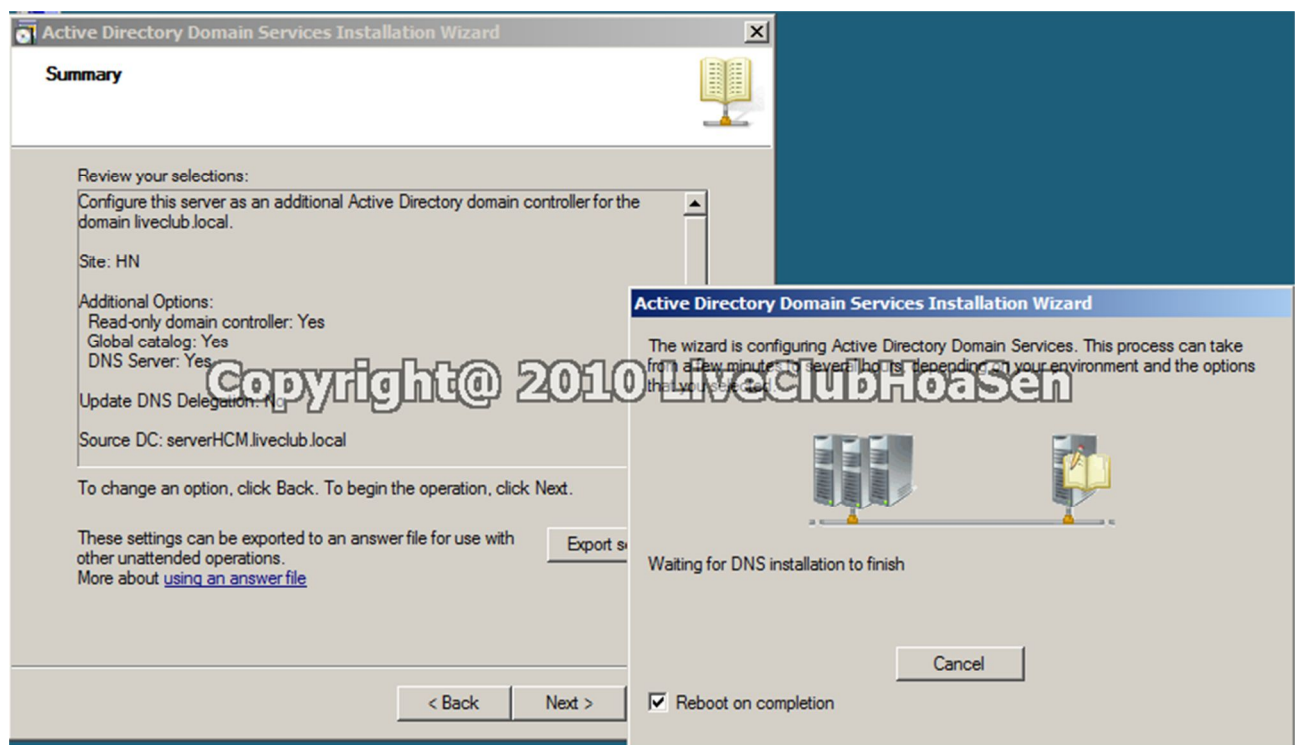
The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Directory Services Restore Mode Administrator Password'. Below this, there is an icon of an open book. The text explains that the Directory Services Restore Mode Administrator account is different from the domain Administrator account and asks the user to assign a password for the Administrator account that will be used when the domain controller is started in Directory Services Restore Mode. It recommends choosing a strong password. There are two input fields: 'Password:' and 'Confirm password:', both containing masked characters (dots). A large watermark 'Copyright@ 2010 LiveClubHoaSen' is overlaid on the screen. Below the watermark, there is a link: 'More about [Directory Services Restore Mode password](#)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Lúc này bạn sẽ thấy một bảng tóm tắt về những tùy chọn cài đặt mà bạn đã chọn. Giả dụ rằng mọi thứ xuất hiện đều đúng theo nguyện vọng của bạn.

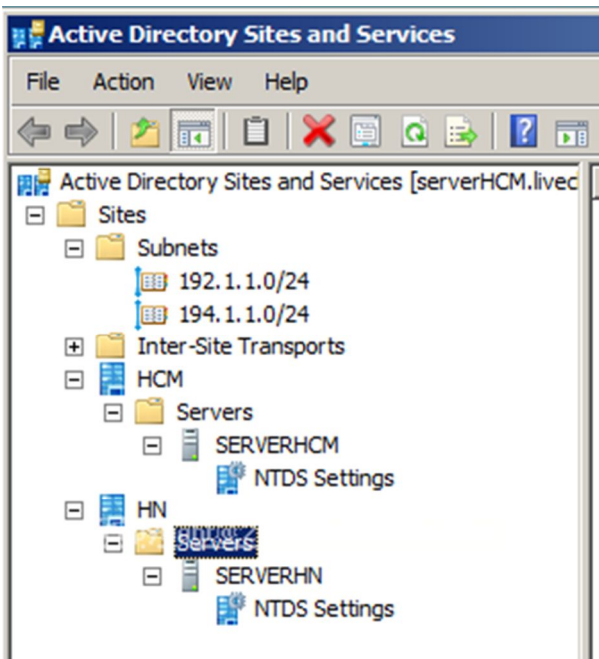




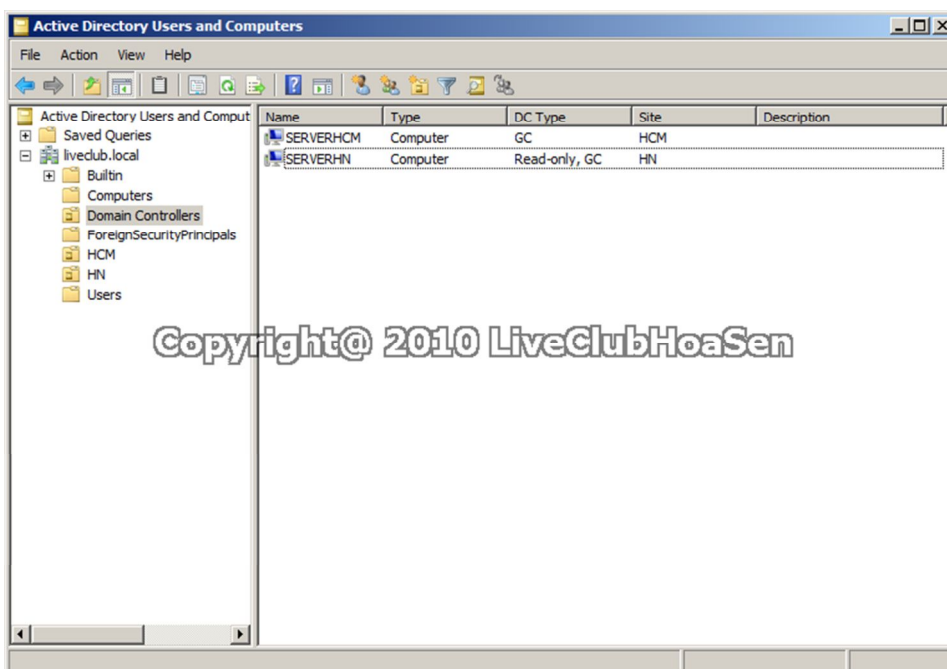
Hãy kích **Next** để bắt đầu quá trình tăng cấp cho domain controller. Khi quá trình hoàn tất, kích **Finish** và sau đó khởi động lại máy chủ.



Sau khi **finish** hoàn tất quá trình thiết lập chúng ta sẽ kiểm tra lại việc sập chép hoàn tất không xảy ra lỗi chưa.



Kiểm tra Active Directory Sites and Services ở serverHCM



The screenshot shows the Windows Server Manager console. On the left, the 'Roles' tree is expanded to 'DNS', and 'liveclub.local' is selected. The right pane displays a table of 16 DNS records for the 'liveclub.local' zone.

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[58], serverhcm.livedub.loc
(same as parent folder)	Name Server (NS)	serverhcm.livedub.local.
(same as parent folder)	Host (A)	192.1.1.1
(same as parent folder)	Host (A)	193.1.1.1
(same as parent folder)	IPv6 Host (AAAA)	2002:c010:0101:0000:0000
(same as parent folder)	IPv6 Host (AAAA)	2002:c001:0101:0000:0000
serverhcm	Host (A)	193.1.1.1
serverHN	Host (A)	192.1.1.1
serverHN	Host (A)	194.1.1.1
serverHN	Host (A)	193.1.1.2