การติดตั้ง Active Directory บน Windows Server 2003

Windows Server 2003 Server Roles

โดยทั่วไปนั้น หลังจากทำการติดตั้ง Windows Server 2003 การทำงานของเครื่องเซิร์ฟเวอร์จะเป็นแบบ Standalone server และเป็นสมาชิกของเวิร์กกรุ๊ป (Workgroup) โดยจะยังไม่ได้เป็นสมาชิกของโดเมน จากนั้นเมื่อทำการการติดตั้ง Active Directory เสร็จเรียบร้อย และมีการเพิ่มเครื่องเซิร์ฟเวอร์ Windows Server 2003 เข้าเป็นสมาชิกของโดยเมน จะมีบทบาท 2 บทบาทที่เครื่องเซิร์ฟเวอร์จะเป็นได้ คือ Member Server คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมน (Domain Member) และ เซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์ (Domain Controller)

บทบาทของเครื่องเซิร์ฟเวอร์ Windows Server 2003 ในการใช้งานรูปแบบต่างๆ

1. เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่ไม่เป็นสมาชิกของโดเมน จะเรียกเซิร์ฟเวอร์แบบนี้ว่า Stand-alone server ซึ่งจะเป็นสมาชิกของ Workgroup และจะเก็บฐานข้อมูลของยูสเซอร์ไว้ที่เครื่องตัวเอง ในไฟล์ชื่อว่า Security Accounts Manager (SAM)

2. เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่เป็นสมาชิกของ (Domain member) จะมีบทบาท 2 บทบาท คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมน (Domain Member Server) และ เซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์ (Domain Controller Server)

Member Server

Member Server คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมน (Domain member) เหมาะสำหรับการใช้งานเป็น file/print server, application server, database server และ web server เพราะสามารถที่จะบริหารจัดการได้โดยผ่าน Domain Controller โดยเซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมนนั้น จะเก็บฐานข้อมูลของยูสเซอร์ไว้ที่ตัวเองเรียกว่า Security Accounts Manager (SAM) แต่สามารถที่จะถูกควบคุมผ่านทางโดเมนได้

Domain Controller

Domain Controller คือ เซิร์ฟเวอร์ที่ทำหน้าที่จัดเก็บฐานข้อมูลของโดเมน (Domain database) และจัดการการสื่อสารระหว่างยูสเซอร์กับโดเมน และยังทำหน้าที่ให้บริการตรวจสอบการล็อกออน (Logon Authentication) เข้าโดเมนของเครื่องคอมพิวเตอร์ลูกข่าย (Client computer) และ ผู้ใช้ (User)

หน้าที่ของโดเมนคอนโทรลเลอร์ในโดเมน

ในแต่ละโดเมน (Domain) นั้นจะต้องมี Domain Controller (DC) อย่างน้อย 1 ตัว โดยเซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์ (Domain Controller Server) จะมีหน้าที่มี 3 อย่างดังนี้

1. ให้บริการและตรวจสอบการ Logon (Authentication) ของ User
2. ให้บริการและจัดการการให้บริการ Directory Service
3. เก็บและจัดการ Active Directory Database

บทบาทของโดเมนคอนโทรลเลอร์ในโดเมน

เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่เป็นโดเมนคอนโทรลเลอร์ในโดเมนนั้น จะมีบทบาท 3 บทบาทด้วยกัน ดังนี้

Operations Master Roles

Active Directory Domain นั้นจะรองรับการทำ Multi Master Replication Model คือ การแลกเปลี่ยนข้อมูลระหว่างโดเมนคอนโทรลเลอร์ทุกๆ ตัวจะมีระดับชั้นการทำงานเท่ากัน แต่จะมีโดเมนคอนโทรลเลอร์หนึ่งตัวที่ทำหน้าที่เป็น Operations Master ซึ่งจะทำหน้าที่ให้บริการการร้องขอการเปลี่ยนแปลงต่างๆ ของ Active Directory แก่โดเมนคอนโทรลเลอร์ตัวอื่นๆ โดยในแต่ละฟอเรสต์ (Forest) นั้นจะมี Operations Master Roles จำนวน 5 อย่างด้วยกัน ซึ่ง Operations Master Roles จะถูกกำหนดให้กับโดเมนคอนโทรลเลอร์เครื่องใดเครื่องหนึ่ง หรือหลายเครื่องก็ได้ โดย Operations Master Roles นั้นมี 2 ประเภท คือ Forest-Wide Operation master Roles และ Domain-Wide Operation master Roles

Forest-Wide Operation master Roles

Operations Master Roles แบบ Forest-Wide นั้น จะถูกกำหนดให้กับโดเมนคอนโทรลเลอร์ได้เพียงเครื่องเดียวในแต่ละฟอเรสต์ (Forest) ซึ่งมีอยู่ 2 ชนิด คือ

1. Schema Master จะทำหน้าที่ควบคุมการอัพเดตและการเปลี่ยนแปลงแก้ไข Schema ในแต่ละฟอเรสต์ (Forest)

2. Domain Naming Master จะทำหน้าที่ควบคุมการเพิ่มหรือลบโดเมน (Domain) ในแต่ละฟอเรสต์ (Forest)

Domain-Wide Operation master Roles

Operations Master Roles แบบ Domain-Wide นั้น จะถูกกำหนดให้กับโดเมนคอนโทรลเลอร์ได้เพียงเครื่องเดียวในแต่ละโดเมน (Domain) ซึ่งมีอยู่ 3 ชนิดคือ

1. Relative Identifier (RID) Master ทำหน้าที่สร้าง Relative Identification (RID) ให้กับโดเมนคอนโทรลเลอร์ทุกตัวในโดเมน (Domain) การมี RID Master นั้น ก็เพื่อรับประกันว่าหมายเลข Security ID ของ Object ทุกๆ ตัวในแต่ละโดเมน (Domain) มีค่าไม่ซ้ำกัน

2. PDC Emulator Master ทำหน้าที่ดังนี้

2.1 จำลองตัวเป็น PDC ของ Windows NT4.0 เพื่อให้สามารถทำการซิงโครไนซ์ (Synchronize) ยูสเซอร์แอคเคาต์และพาสเวิร์ดกับ BDC ของ Windows NT4.0 ได้

2.2 จำลองตัวเป็น PDC ของ Windows NT 4.0 เพื่อให้เครื่องไคลเอนต์ที่เป็น Windows 95/98 สามารถใช้งานได้ตามปกติ ในกรณีที่ ต่อมาได้ทำการอัพเดต Windows NT4.0 BDC ไปเป็น Windows Server 2003 บทบาทการเป็น PDC Emulator จะยังคงอยู่ แต่ว่าการทำหน้าที่จะเปลี่ยนไป คือ เมื่อยูสเซอร์ทำการเปลี่ยนพาสเวิร์ดบนโดเมนคอนโทรลเลอร์ตัวใดๆ ก็ตาม โดเมนคอนโทรลเลอร์ตัวนั้นจะทำการส่งสัญญาณไปยัง เซิร์ฟเวอร์ที่เป็น PDC Emulator จากนั้นจะทำการเรพลิเคต (Replicate) ไปยังโดเมนคอนโทรลเลอร์อื่นๆ ทุกตัวภายในโดเมน เมื่อยูสเซอร์ทำการล็อกออน (Logon) ด้วยพาสเวิร์ดใหม่ที่โดเมนคอนโทรลเลอร์ตัวอื่น ซึ่งอาจจะยังไม่ได้รับการ เรพลิเคต

(Replicate) โดเมนคอนโทรลเลอร์ตัวนั้นจึงยังไม่รู้ว่าพาสเวิร์ดมีการเปลี่ยนแปลง แต่ก่อนที่โดเมนคอนโทรลเลอร์จะแจ้งยูสเซอร์ว่าใส่พาสเวิร์ดผิด โดเมนคอนโทรลเลอร์ตัวนั้นจะถามไปยัง เซิร์ฟเวอร์ที่เป็น PDC Emulator ก่อน ซึ่งเซิร์ฟเวอร์ที่เป็น PDC Emulator จะทราบว่ามีการเปลี่ยนพาสเวิร์ดและแจ้งกลับไปยังโดเมนคอนโทรลเลอร์ตัวที่สอบถามมา ดังนั้นโดเมนคอนโทรลเลอร์ก็จะทราบว่ามีการเปลี่ยนพาสเวิร์ด จึงยอมให้ยูสเซอร์ล็อกออนเข้าใช้งานด้วยพาสเวิร์ดตัวใหม่ได้

3. Infrastructure Master ทำหน้าที่ติดตามการเปลี่ยนแปลงสมาชิกของกรุ๊ปต่างๆ และคอยอัพเดตการเปลี่ยนแปลงดังกล่าวให้กับยังโดเมนคอนโทรลเลอร์ทุกตังในโดเมน เพื่อให้ยังโดเมนคอนโทรลเลอร์มีข้อมูลที่ทันสมัยเสมอ

Global Catalog Server

นอกจาก Forest-Wide Operation master Roles และ Domain-Wide Operation master Roles แล้ว ในแต่ละฟอเรสต์จะต้องมีโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ (Global Catalog Server) คือ เซิร์ฟเวอร์ที่ทำหน้าที่เก็บรวบรวมค่าต่างๆ ของ attribute ที่สำคัญและถูกใช้งานบ่อย ของแต่ละออบเจ็กต์ โกลบอลแค็ตตาล็อกเซิร์ฟเวอร์จะทำหน้าที่เพิ่มความรวดเร็วในการค้นหาออบเจ็กต์ในฟอเรสต์ โดยในแต่ละฟอเรสต์จะต้องมีโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์อย่างน้อย 1 เครื่อง โดยค่าดีฟอลท์นั้น เครื่องโดเมนคอนโทรลเลอร์เครื่องแรกของฟอเรสต์จะทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์โดยอัตโนมัติ แต่มีข้อกำหนดของการทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ คือ ในกรณีที่มีโดเมนคอนโทรลเลอร์มากกว่า 1 เครื่อง โดเมนคอนโทรลเลอรที่ทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ จะต้องเป็นโดเมนคอนโทรลเลอร์คนละตัวกับที่ทำหน้าที่เป็น Infrastructure Master เนื่องจากโดยดีฟอลท์นั้น เครื่องโดเมนคอนโทรลเลอร์เครื่องแรกของโดเมนจะทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์โดยอัตโนมัติ แต่อย่างไรก็ตามเราสามารถเปลี่ยนเครื่องโดเมนคอนโทรลเลอร์ที่ทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ในภายหลังได้ นอกจากนี้ยังสามารถเพิ่มเครื่องโดเมนคอนโทรลเลอร์ให้ทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ได้ตามความเหมาะสม โดยรายละเอียดจะกล่าวถึงในภายหลัง

การติดตั้ง Active Directory

1. การวางแผนการติดตั้ง Active Directory

ก่อนการติดตั้ง Active Directory บนเครื่อง Windows Server 2003 นั้น แอดมินจะต้องวางแผนการติดตั้งว่าจะมีลักษณะแบบใด และต้องเตรียมข้อมูลพื้นฐานของระบบเครือข่าย เช่น หมายเลขไอพีและซับเน็ตมาสก์ที่ใช้ หมายเลขไอพีของเซิร์ฟเวอร์ DNS หมายเลขไอพีของดีฟอลท์เกตเวย์ (Default Gateway) และในกรณีที่เราไม่ได้ดูแลระบบเองทั้งหมด ก็ต้องประสานงานกับแอดมินที่เป็นผู้ดูแลเครื่องเซิร์ฟเวอร์ต่างๆ เพื่อทำการคอนฟิกในส่วนที่เกี่ยวข้อง เช่น DNS เซิร์ฟเวอร์ เป็นต้น

โดยทั่วไป ก่อนทำการติดตั้ง Active Directory บนเครื่อง Windows Server 2003 จะต้องวางแผนหรือเตรียมข้อมูลต่างๆ ดังนี้

- ติดตั้งเป็น New Forest หรือ Existing Forest
- ติดตั้งเป็น New Domain ใน Existing Forest หรือเป็น New Child Domain ใน Existing Forest
- ชื่อของโดเมนหลักและโดนเมนย่อยต่างๆ (Domain name/ Child Domain name)

- IP Address สำหรับเซิร์ฟเวอร์ทุกตัว
- ซับเน็ตมาสก์ (Subnet Mask)
- IP Address ของดีฟอลท์เกตเวย์
- IP Address ของ DNS เซิร์ฟเวอร์

ดำเนินการติดตั้ง Active Directory บนเครื่อง Windows Server 2003

หลังจากติดตั้งวินโดวส์เซิร์ฟเวอร์ 2003 เสร็จเรียบร้อยแล้ว ก่อนดำเนินการติดตั้ง Active Directory ให้ทำการตรวจสอบการคอนฟิกต่างๆ ให้แน่ใจว่าถูกต้องแล้ว จากนั้นให้ทำการล็อกออนเข้าเครื่องเซิร์ฟเวอร์ด้วยยูสเซอร์ที่เป็นโลคอลแอดมิน โดยดีฟอลท์นั้นวินโดวส์จะเปิดหน้าต่าง Manage Your Server ซึ่งจะเป็นตัวอำนวยความสะดวกและช่วยเหลือในการจัดการวินโดวส์เซิร์ฟเวอร์ 2003 ในด้านต่างๆ เช่น Adding Roles to Your Server ซึ่งจะอำนวยความสะดวกในการเพิ่มหน้าที่ให้กับวินโดวส์เซิร์ฟเวอร์ และ Managing Your Server Roles ซึ่งจะอำนวยความสะดวกในการจัดการการทำงานต่างๆ ของเซิร์ฟเวอร์

ขั้นตอนการติดตั้ง Domain Controller และ Active Directory

ในตัวอย่างนี้ จะแสดงถึงขั้นตอนการติดตั้ง Active Directory โดยการติดตั้งวินโดวส์เซิร์ฟเวอร์ 2003 เป็นโดเมนคอนโทรลเลอร์ใน New Domain และ New Forest ซึ่งมีขั้นตอนดังนี้

การ Active Directory แบบ New Domain และ New Forest นั้นมีวิธีการทำดังนี้

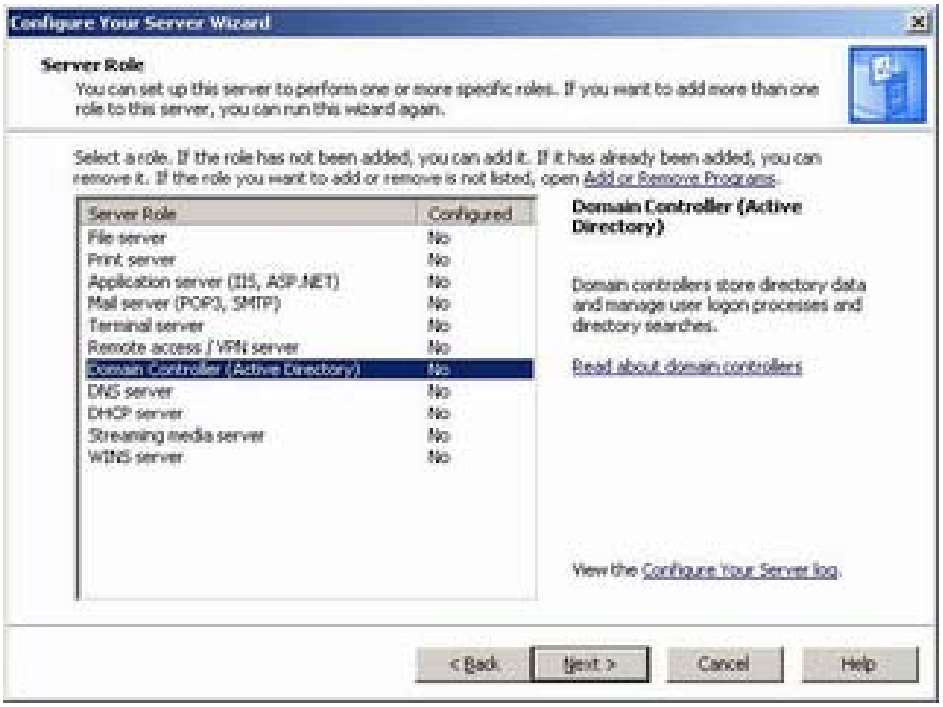
1. ทำการล็อกออนเข้าเครื่องเซิร์ฟเวอร์ด้วยยูสเซอร์ที่เป็นโลคอลแอดมิน จากนั้นในหน้า Manage Your Server ให้คลิกที่ Add or remove a role จะได้หน้าไดอะล็อกบ็อกซ์ Preliminary Steps

Manage Your Server

2. ในหน้าต่าง Preliminary Steps ให้คลิก Next

3. ในหน้าไดอะล็อกบ็อกซ์ Configuration Options ให้คลิกเลือก Custom Configuration เสร็จแล้วคลิก Next

4. ในหน้าไดอะล็อกบ็อกซ์ Server Role ให้คลิกเลือก Domain Controller (Active Directory) เสร็จแล้วคลิก Next



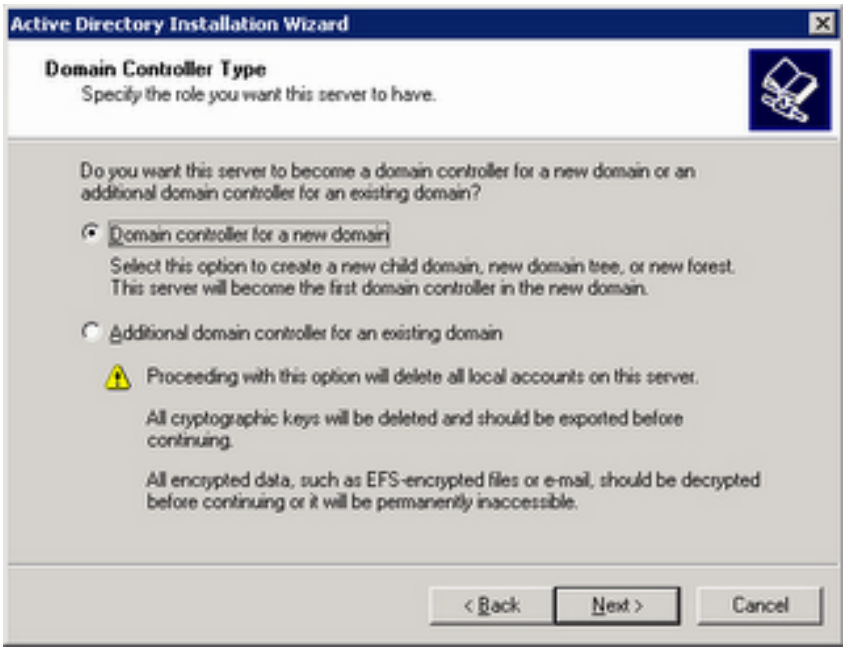
Server Role

5. ในหน้าไดอะล็อกบ็อกซ์ Summary of Selections ให้คลิก Next

6. ในหน้าไดอะล็อกบ็อกซ์ Active Directory Installation Wizard ให้คลิก Next

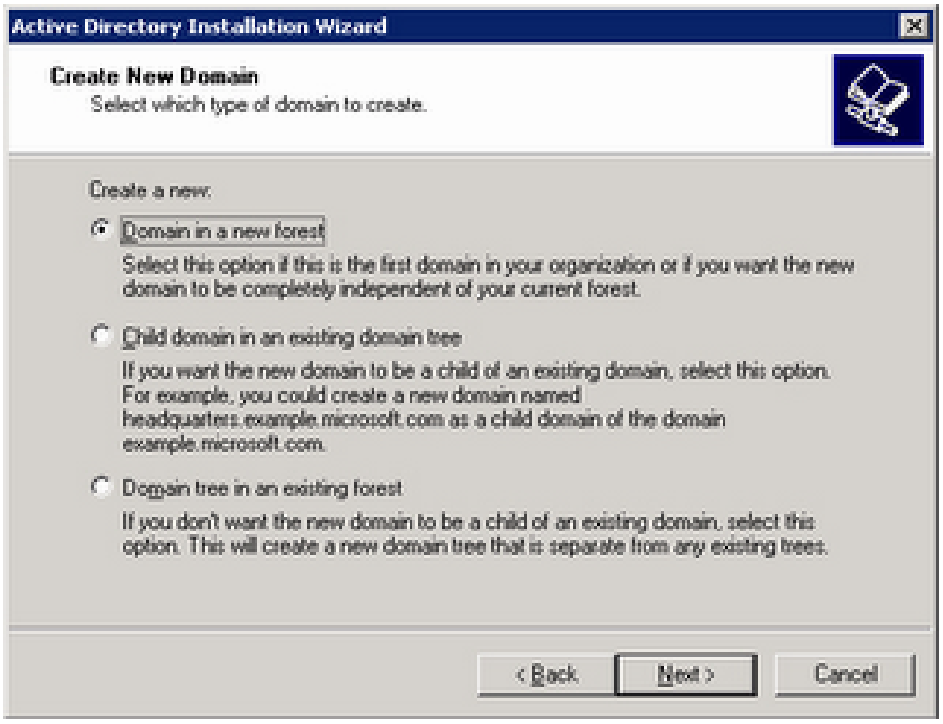
7. ในหน้าไดอะล็อกบ็อกซ์ Operating System Compatibility ให้คลิก Next

8. ในหน้าไดอะล็อกบ็อกซ์ Domain Controller Type ให้คลิกเลือก Domain Controller for a new domain เสร็จแล้วคลิก Next



Domain Controller Type

9. ในหน้าไดอะล็อกบ็อกซ์ Create New Domain ให้คลิกเลือก Domain in a new forest เสร็จแล้วคลิก Next



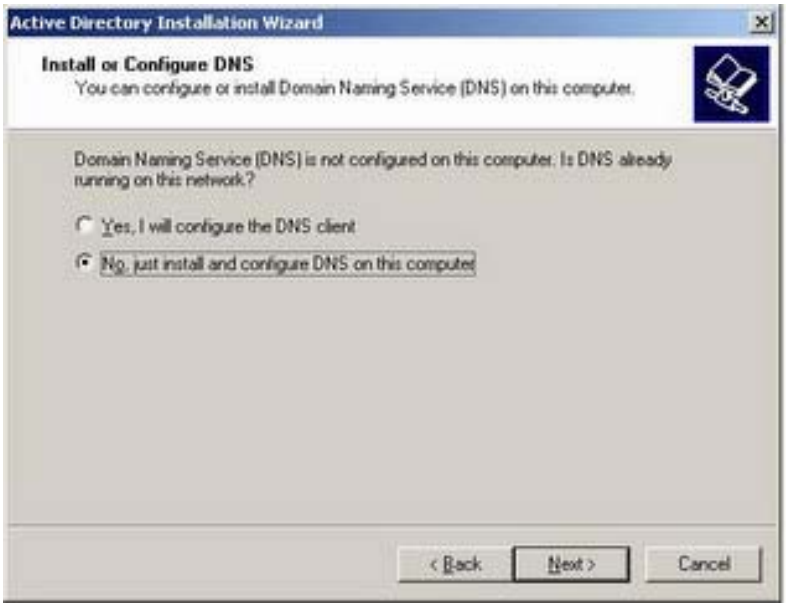
Create New Domain

หมายเหตุ:

1. หากต้องการการติดตั้งวินโดวส์เซิร์ฟเวอร์ 2003 เป็นโดเมนคอนโทรลเลอร์ใน New Domain ของ Existing Forest ให้เลือกเป็น Domain tree in an existing Forest

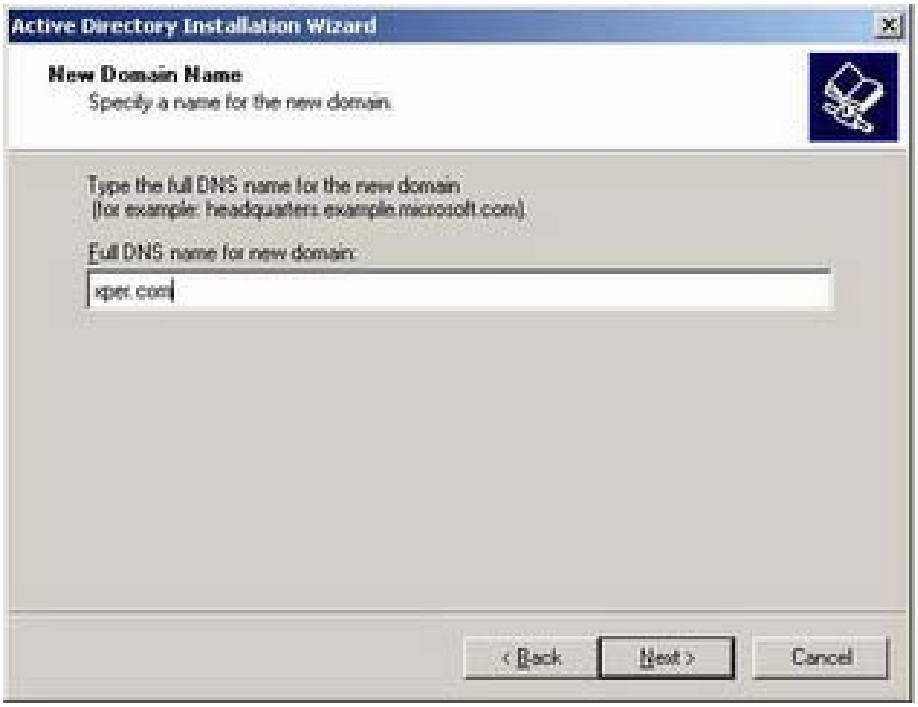
2. หากต้องการการติดตั้งวินโดวส์เซิร์ฟเวอร์ 2003 เป็นโดเมนคอนโทรลเลอร์ใน Child Domain ให้เลือกเป็น Child domain in an existing domain

10. ในหน้าไดอะล็อกบ็อกซ์ Install or configure DNS ให้คลิกเลือก No, just install and configure DNS on this computer เสร็จแล้วคลิก Next



Install or configure DNS

11. ในหน้าไดอะล็อกบ็อกซ์ New Domain Name ให้พิมพ์ชื่อเต็มของ Domain ในช่อง Full DNS name for new domain เสร็จแล้วคลิก Next



New Domain Name

12. ในหน้าไดอะล็อกบ็อกซ์ NetBIOS Domain Name ให้คลิก Next

13. ในหน้าไดอะล็อกบ็อกซ์ Database and Log Folders ในช่อง Database folder ให้ใช้ค่าที่ระบบกำหนดให้โดยอัตโนมัติ ส่วนในช่อง Log folder นั้นหากเครื่องเซิร์ฟเวอร์มี partition เดียวก็ให้ใช้ค่าที่กำหนดให้อัตโนมัติ แต่หากมี partition อื่นก็ให้เลือกเป็น partition อื่นก็ได้ เสร็จแล้วคลิก Next

14. ในหน้าไดอะล็อกบ็อกซ์ Shared System Volume ให้ใช้ค่าที่กำหนดให้อัตโนมัติ เสร็จแล้วให้คลิก Next

15. ในหน้าไดอะล็อกบ็อกซ์ Permissions ให้คลิกเลือก Permission ที่ต้องการ เสร็จแล้วคลิก Next

16. ในหน้าไดอะล็อกบ็อกซ์ Directory Services Restore Mode Administrator Password ให้ใส่พาสเวิร์ดที่ต้องการในช่อง Restore Mode Password และ ในช่อง Confirm password เสร็จแล้วคลิก Next

17. ในหน้าไดอะล็อกบ็อกซ์ Summary ให้คลิก Next แล้วรอให้ระบบจะทำการติดตั้ง Active Directory

18. ในหน้าไดอะล็อกบ็อกซ์ Completing the Active Directory Installation Wizard ให้คลิก Finish

19. ทำการรีสตาร์ทเครื่องโดยคลิก Restart Now

20. เมื่อเซิร์ฟเวอร์พร้อมใช้งาน ให้ทำการล็อกออนด้วยยูสเซอร์โดเมนแอดมิน

21. ในหน้าไดอะล็อกบ็อกซ์ Configure Your Server Wizard จะแจ้งว่า ขณะนี้เครื่องเซิร์ฟเวอร์ทำหน้าที่เป็นโดเมนคอนโทรลเลอร์ ให้คลิก Finish