การติดตั้ง Active Directory บน Windows Server 2003

Windows Server 2003 Server Roles

โดยทั่วไปนั้น หลังจากทำการติดตั้ง Windows Server 2003 การทำงานของเครื่องเซิร์ฟเวอร์จะเป็นแบบ Standalone server และเป็นสมาชิกของเวิร์กกรุ๊ป (Workgroup) โดยจะยังไม่ได้เป็นสมาชิกของโดเมน จากนั้นเมื่อทำ การการติดตั้ง Active Directory เสร็จเรียบร้อย และมีการเพิ่มเครื่องเซิร์ฟเวอร์ Windows Server 2003 เข้าป็นสมาชิก ของโดยเมน จะมีบทบาท 2 บทบาทที่เครื่องเซิร์ฟเวอร์จะเป็นได้ คือ Member Server คือ เซิร์ฟเวอร์ที่เป็นสมาชิก ของโดเมน (Domain Member) และ เซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์ (Domain Controller)

บทบาทของเครื่องเซิร์ฟเวอร์ Windows Server 2003 ในการใช้งานรูปแบบต่างๆ

 เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่ไม่เป็นสมาชิกของโคเมน จะเรียกเซิร์ฟเวอร์แบบนี้ว่า Standalone server ซึ่งจะเป็นสมาชิกของ Workgroup และจะเก็บฐานข้อมูลของยูสเซอร์ไว้ที่เครื่องตัวเอง ในไฟล์ชื่อว่า Security Accounts Manager (SAM)

 2. เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่เป็นสมาชิกของ (Domain member) จะมีบทบาท 2 บทบาท คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของ โคเมน (Domain Member Server) และ เซิร์ฟเวอร์ที่เป็น โคเมนคอน โทรลเลอร์ (Domain Controller Server)

Member Server

Member Server คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโคเมน (Domain member) เหมาะสำหรับการใช้งานเป็น file/print server, application server, database server และ web server เพราะสามารถที่จะบริหารจัดการได้โคยผ่าน Domain Controller โดยเซิร์ฟเวอร์ที่เป็นสมาชิกของโคเมนนั้น จะเก็บฐานข้อมูลของยูสเซอร์ไว้ที่ตัวเองเรียกว่า Security Accounts Manager (SAM) แต่สามารถที่จะถูกควบคุมผ่านทางโคเมนได้

Domain Controller

Domain Controller คือ เซิร์ฟเวอร์ที่ทำหน้าที่จัดเก็บฐานข้อมูลของโคเมน (Domain database) และจัดการ การสื่อสารระหว่างยูสเซอร์กับโคเมน และยังทำหน้าที่ให้บริการตรวจสอบการล็อกออน (Logon Authentication) เข้าโคเมนของเกรื่องคอมพิวเตอร์ลูกข่าย (Client computer) และ ผู้ใช้ (User)

หน้าที่ของโดเมนคอนโทรลเลอร์ในโดเมน

ในแต่ละ โคเมน (Domain) นั้นจะต้องมี Domain Controller (DC) อย่างน้อย 1 ตัว โคยเซิร์ฟเวอร์ที่เป็น โคเมนคอนโทรลเลอร์ (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 ที่เป็นโคเมนคอนโทรลเลอร์ในโคเมนนั้น จะมีบทบาท 3 บทบาท ด้วยกัน ดังนี้

Operations Master Roles

Active Directory Domain นั้นจะรองรับการทำ Multi Master Replication Model คือ การแลกเปลี่ยนข้อมูล ระหว่างโดเมนคอนโทรลเลอร์ทุกๆ ตัวจะมีระดับชั้นการทำงานเท่ากัน แต่จะมีโดเมนคอนโทรลเลอร์หนึ่งตัวที่ทำ หน้าที่เป็น Operations Master ซึ่งจะทำหน้าที่ให้บริการการร้องขอการเปลี่ยนแปลงต่างๆ ของ Active Directory แก่ โดเมนคอนโทรลเลอร์ตัวอื่นๆ โดยในแต่ละฟอเรสต์ (Forest) นั้นจะมี Operations Master Roles จำนวน 5 อย่าง ด้วยกัน ซึ่ง Operations Master Roles จะถูกกำหนดให้กับโดเมนคอนโทรลเลอร์เครื่องใดเครื่องหนึ่ง หรือหลาย เครื่องก็ได้ 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 จะถูกกำหนดให้กับโดเมนคอนโทรลเลอร์ได้เพียงเครื่อง เดียวในแต่ละฟอเรสต์ (Forest) ซึ่งมีอยู่ 2 ชนิด คือ

 Schema Master จะทำหน้าที่ควบคุมการอัพเคตและการเปลี่ยนแปลงแก้ไข Schema ในแต่ละฟอเรสต์ (Forest)

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

Domain-Wide Operation master Roles

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

 Relative Identifier (RID) Master ทำหน้าที่สร้าง Relative Identification (RID) ให้กับโคเมน กอนโทรลเลอร์ทุกตัวในโคเมน (Domain) การมี RID Master นั้น ก็เพื่อรับประกันว่าหมายเลง Security ID ของ Object ทุกๆ ตัวในแต่ละโคเมน (Domain) มีค่าไม่ซ้ำกัน

2. PDC Emulator Master ทำหน้าที่ดังนี้

2.1 จำลองตัวเป็น PDC ของ Windows NT4.0 เพื่อให้สามารถทำการซิงโคร ในซ์ (Synchronize) ยูสเซอร์แอกเกาต์และพาสเวิร์ดกับ BDC ของ Windows NT4.0 ได้

2.2 จำลองตัวเป็น PDC ของ Windows NT 4.0 เพื่อให้เกรื่องใคลเอนต์ที่เป็น Windows 95/98 สามารถใช้งานได้ตามปกติ ในกรณีที่ ต่อมาได้ทำการอัพเดต Windows NT4.0 BDC ไปเป็น Windows Server 2003 บทบาทการเป็น PDC Emulator จะยังคงอยู่ แต่ว่าการทำหน้าที่จะเปลี่ยนไป คือ เมื่อยูสเซอร์ทำการเปลี่ยนพาสเวิร์ด บนโดเมนคอนโทรลเลอร์ตัวใดๆ ก็ตาม โดเมนคอนโทรลเลอร์ตัวนั้นจะทำการส่งสัญญาณไปยัง เซิร์ฟเวอร์ที่เป็น PDC Emulator จากนั้นจะทำการเรพลิเคต (Replicate) ไปยังโดเมนคอนโทรลเลอร์อื่นๆ ทุกตัวภายในโดเมน เมื่อยูส เซอร์ทำการล็อกออน (Logon) ด้วยพาสเวิร์ดใหม่ที่โดเมนคอนโทรลเลอร์ตัวอื่น ซึ่งอาจจะยังไม่ได้รับการ เรพลิเคต (Replicate) โคเมนคอนโทรลเลอร์ตัวนั้นจึงยังไม่รู้ว่าพาสเวิร์คมีการเปลี่ยนแปลง แต่ก่อนที่โคเมนคอนโทรลเลอร์ จะแจ้งยูสเซอร์ว่าใส่พาสเวิร์คผิด โคเมนคอนโทรลเลอร์ตัวนั้นจะถามไปยัง เซิร์ฟเวอร์ที่เป็น PDC Emulator ก่อน ซึ่งเซิร์ฟเวอร์ที่เป็น PDC Emulator จะทราบว่ามีการเปลี่ยนพาสเวิร์คและแจ้งกลับไปยังโคเมนคอนโทรลเลอร์ตัวที่ สอบถามมา ดังนั้นโคเมนคอนโทรลเลอร์ก็จะทราบว่ามีการเปลี่ยนพาสเวิร์ค จึงยอมให้ยูสเซอร์ล็อกออนเข้าใช้งาน ด้วยพาสเวิร์คตัวใหม่ได้

 Infrastructure Master ทำหน้าที่ติดตามการเปลี่ยนแปลงสมาชิกของกรุ๊ปต่างๆ และคอยอัพเดตการ เปลี่ยนแปลงดังกล่าวให้กับยังโดเมนคอนโทรลเลอร์ทุกตังในโดเมน เพื่อให้ยังโดเมนคอนโทรลเลอร์มีข้อมูลที่ ทันสมัยเสมอ

Global Catalog Server

นอกจาก Forest-Wide Operation master Roles และ Domain-Wide Operation master Roles แล้ว ในแต่ ละฟอเรสต์จะด้องมีโกลบอลแก็ตตาล็อกเซิร์ฟเวอร์ (Global Catalog Server) กือ เซิร์ฟเวอร์ที่ทำหน้าที่เก็บรวบรวม ก่าต่างๆ ของ attribute ที่สำคัญและถูกใช้งานบ่อย ของแต่ละออบเจ็กต์ โกลบอลแก็ตตาล็อกเซิร์ฟเวอร์จะทำหน้าที่ เพิ่มความรวดเร็วในการค้นหาออบเจ็กต์ในฟอเรสต์ โดยในแต่ละฟอเรสต์จะด้องมีโกลบอลแก็ตตาล็อกเซิร์ฟเวอร์ อย่างน้อย 1 เครื่อง โดยก่าดีฟอลท์นั้น เครื่องโดเมนคอนโทรลเลอร์เครื่องแรกของฟอเรสต์จะทำหน้าที่เป็นโกลบอล แก็ตตาล็อกเซิร์ฟเวอร์โดยอัตโนมัติ แต่มีข้อกำหนดของการทำหน้าที่เป็นโกลบอลแก็ตตาล็อกเซิร์ฟเวอร์ คือ ใน กรณีที่มีโดเมนคอนโทรลเลอร์มากกว่า 1 เครื่อง โดเมนคอนโทรลเลอรที่ทำหน้าที่เป็นโกลบอลแก็ตตาล็อก เซิร์ฟเวอร์ จะด้องเป็นโดเมนคอนโทรลเลอร์คนละตัวกับที่ทำหน้าที่เป็น Infrastructure Master เนื่องจากโดยดีฟอลท์นั้น เครื่องโดเมนคอนโทรลเลอร์เครื่องแรกของโดเมนจะทำหน้าที่เป็นโกลบอลแก็ตตาล็อก เซิร์ฟเวอร์โดยอัตโนมัติ แต่อย่างไรก็ตามเราสามารถเปลี่ยนเครื่องโดเมนคอนโทรลเลอร์ที่ทำหน้าที่เป็นโกลบอล แก็ตตาล็อกเซิร์ฟเวอร์ในภายหลังได้ นอกจากนี้ยังสามารถเพิ่มเครื่องโดเมนคอนโทรลเลอร์ให้ทำหน้าที่เป็นโกลบอล แก็ตตาล็อกเซิร์ฟเวอร์ในภายหลังได้ นอกจากนี้ยังสามารถเพิ่มเครื่องโดเมนคอนโทรลเลอร์ให้ทำหน้าที่เป็นโก ลบอลแก็ตตาล็อกเซิร์ฟเวอร์ได้ตามความเหมาะสม โดยรายละเอียดจะกล่าวถึงในภายหลัง

การติดตั้ง Active Directory

1. การวางแผนการติดตั้ง Active Directory

ก่อนการติดตั้ง Active Directory บนเครื่อง Windows Server 2003 นั้น แอดมินจะต้องวางแผนการติดตั้งว่า จะมีลักษณะแบบใด และต้องเตรียมข้อมูลพื้นฐานของระบบเครือข่าย เช่น หมายเลขไอพีและซับเน็ตมาสก์ที่ใช้ หมายเลขไอพีของเซิร์ฟเวอร์ DNS หมายเลขไอพีของดีฟอลท์เกตเวย์ (Default Gateway) และในกรณีที่เราไม่ได้ ดูแลระบบเองทั้งหมด ก็ต้องประสานงานกับแอดมินที่เป็นผู้ดูแลเครื่องเซิร์ฟเวอร์ต่างๆ เพื่อทำการคอนฟิกในส่วนที่ เกี่ยวข้อง เช่น DNS เซิร์ฟเวอร์ เป็นต้น

โดยทั่วไป ก่อนทำการติดตั้ง Active Directory บนเครื่อง Windows Server 2003 จะต้องวางแผนหรือเตรียม ข้อมูลต่างๆ ดังนี้

- ติดตั้งเป็น New Forest หรือ Existing Forest

- ติดตั้งเป็น New Domain ใน Existing Forest หรือเป็น New Child Domain ใน Existing Forest

- ชื่อของโคเมนหลักและ โคนเมนย่อยต่างๆ (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 ให้ทำ การตรวจสอบการคอนฟิกต่างๆ ให้แน่ใจว่าถูกต้องแล้ว จากนั้นให้ทำการล็อกออนเข้าเครื่องเซิร์ฟเวอร์ด้วยยูสเซอร์ ที่เป็นโลคอลแอดมิน โดยดีฟอลท์นั้นวินโดวส์จะเปิดหน้าต่าง Manage Your Server ซึ่งจะเป็นตัวอำนวยความ สะดวกและช่วยเหลือในการจัดการวินโดวส์เซิร์ฟเวอร์ 2003 ในด้านต่างๆ เช่น Adding Roles to Your Server ซึ่งจะ อำนวยความสะดวกในการเพิ่มหน้าที่ให้กับวินโดวส์เซิร์ฟเวอร์ และ Managing Your Server Roles ซึ่งจะอำนวย ความสะดวกในการจัดการการทำงานต่างๆ ของเซิร์ฟเวอร์

ขั้นตอนการติดตั้ง Domain Controller และ Active Directory

ในตัวอย่างนี้ จะแสดงถึงขั้นตอนการติดตั้ง Active Directory โดยการติดตั้งวินโดวส์เซิร์ฟเวอร์ 2003 เป็นโดเมน กอนโทรลเลอร์ใน New Domain และ New Forest ซึ่งมีขั้นตอนดังนี้

การ Active Directory แบบ New Domain และ New Forest นั้นมีวิธีการทำดังนี้

 ทำการถือกออนเข้าเครื่องเซิร์ฟเวอร์ด้วยยูสเซอร์ที่เป็นโลคอลแอดมิน จากนั้นในหน้า Manage Your Server ให้คลิกที่ Add or remove a role จะได้หน้าไดอะล็อกบ็อกซ์ Preliminary Steps



Manage Your Server

- 2. ในหน้าต่าง Preliminary Steps ให้คลิก Next
- 3. ในหน้าใดอะล็อกบ็อกซ์ Configuration Options ให้กลิกเลือก Custom Configuration เสร็จแล้วกลิก

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

Next

select a role. If the role has not been add emove it. If the role you want to add or	fed, you can add it. remove is not listed,	I it has already been added, you can open <u>Add or Remove Programs</u> .	
Server Role File server	Configured No	Domain Controller (Active Directory)	
rint server oplication server (IIS, ASP.NET) fail server (POP3, SMIP) ferminal server	No No No	Domain controllers store directory data and manage user logon processes and directory searches.	
Remote access / VPN server	No	Read about domain controllers	
DNS server DHOP server Streaming media server WINS server	No No No No		

Server Role

- 5. ในหน้าใดอะถือกบ็อกซ์ Summary of Selections ให้คลิก Next
- 6. ในหน้าใดอะลีอกบ็อกซ์ Active Directory Installation Wizard ให้คลิก Next
- 7. ในหน้าใดอะล็อกบ็อกซ์ Operating System Compatibility ให้กลิก Next

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

Sp	ecity the role you want this server to have.
Do ad	you want this server to become a domain controller for a new domain or an ditional domain controller for an existing domain?
(•	Domain controller for a new domain
	Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
С	Additional domain controller for an existing domain
	Proceeding with this option will delete all local accounts on this server.
	All cryptographic keys will be deleted and should be exported before continuing.
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

Domain Controller Type

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

Active Dir	ectory Installation Wizard	×
Create Se	e New Domain lect which type of domain to create.	
Cre	sale a new.	
G	Domain in a new forest	
	Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.	
C	Child domain in an existing domain tree	
	If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters example microsoft.com as a child domain of the domain example microsoft.com.	
С	Domain tree in an existing forest	
	If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.	
	< <u>B</u> ack <u>N</u> ext> Cancel]

Create New Domain

หมายเหตุ:

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

2. หากต้องการการติดตั้งวิน โดวส์เซิร์ฟเวอร์ 2003 เป็นโดเมนคอนโทรลเลอร์ใน Child Domain ให้เลือก

เป็น Child domain in an existing domain

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

You can configure or install Do	main Naming Service (DNS) on this computer.	S
Domain Naming Service (DNS running on this network?) is not configured on this computer. Is DNS already	
C Yes, I will configure the DN	IS client	
No. just install and configured in the second se	e DNS on this computed	

Install or configure DNS

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

Active Directory Installation Wizard	×
New Domain Name Specity a name for the new domain.	X
Type the full DNS name for the new domain (for example: headquarters example microsoft.com).	
Eul DNS name for new domain:	
xper.com	
(Back Next)	Cancel

New Domain Name

12. ในหน้าใดอะลีอกบ็อกซ์ NetBIOS Domain Name ให้กลิก Next

13. ในหน้าใดอะล็อกบ็อกซ์ Database and Log Folders ในช่อง Database folder ให้ใช้ค่าที่ระบบกำหนดให้โดย อัตโนมัติ ส่วนในช่อง Log folder นั้นหากเครื่องเซิร์ฟเวอร์มี partition เดียวก็ให้ใช้ค่าที่กำหนดให้อัตโนมัติ แต่หาก มี partition อื่นก็ให้เลือกเป็น partition อื่นก็ได้ เสร็จแล้วคลิก Next

14. ในหน้าไดอะล็อกบ็อกซ์ Shared System Volume ให้ใช้ก่าที่กำหนดให้อัตโนมัติ เสร็จแล้วให้กลิก Next

15. ในหน้าใดอะล็อกบ็อกซ์ Permissions ให้คลิกเลือก Permission ที่ต้องการ เสร็จแล้วคลิก Next

16. ในหน้าใดอะล็อกบ็อกซ์ Directory Services Restore Mode Administrator Password ให้ใส่พาสเวิร์คที่ต้องการ

ในช่อง Restore Mode Password และ ในช่อง Confirm password เสร็จแล้วคลิก Next

17. ในหน้าไดอะล็อกบ็อกซ์ Summary ให้คลิก Next แล้วรอให้ระบบจะทำการติดตั้ง Active Directory

18. ในหน้าใดอะถือกบื้อกซ์ Completing the Active Directory Installation Wizard ให้คลิก Finish

19. ทำการรีสตาร์ทเครื่องโดยคลิก Restart Now

20. เมื่อเซิร์ฟเวอร์พร้อมใช้งาน ให้ทำการล็อกออนด้วยยูสเซอร์โดเมนแอดมิน

21. ในหน้าไดอะล็อกบ็อกซ์ Configure Your Server Wizard จะแจ้งว่า ขณะนี้เครื่องเซิร์ฟเวอร์ทำหน้าที่เป็นโดเมน กอนโทรลเลอร์ ให้คลิก Finish