Active Directory (AD)

Active Directory ทำหน้าที่จัดเก็บข้อมูลเกี่ยวกับ object ต่างๆ เช่น ยูสเซอร์ (User) กลุ่ม (Group) คอมพิวเตอร์ (Computer) หรือ นโยบายรักษาความปลอดภัย (Security Policy) เป็นต้น โดย Active Directory นั้นจะเก็บ object ต่างๆ เหล่านี้ไว้ใน Active Directory Database และมีเซิร์ฟเวอร์ที่ทำหน้าที่เป็น Domain Controller (DC) เป็นตัวจัดการอีกทีหนึ่ง

ส่วนประกอบของ Active Directory

Active Directory นั้น จะมีส่วนประกอบอยู่ 2 ส่วนด้วยกัน คือ

1. Active Directory Service ซึ่งเป็นส่วนประกอบที่ทำหน้าที่ให้บริการแก่ยูสเซอร์และผู้บริหารระบบ
2. Active Directory Database เป็นฐานข้อมูลสำหรับใช้ในการเก็บ Directory Object ต่างๆ เช่น User Account, Group Account, Shared Folder, Organizational Unit (OU), System Configuration, Group Policy Object (GPO) เป็นต้น

โครงสร้างของ Active Directory

การใช้งาน Windows Server เป็น Domain Controller (DC) ในสภาพแวดล้อมแบบ Domain นั้น โดยจะไม่มีบทบาท (Role) แบบ Primary Domain Controller (PDC) หรือ Backup Domain Controller (BDC) แต่เครื่องเซิร์ฟเวอร์ทุกๆ ตัวรับบทบาทเป็น Domain Controller (DC) ซึ่งระดับการทำงานเท่ากัน นั้นคือ DC แต่ละเครื่องสามารถที่จะเปลี่ยนแปลงฐานข้อมูลของ Active Directory ได้ และเมื่อมีการเปลี่ยนแปลงที่เครื่อง DC เครื่องใดเครื่องหนึ่ง Active Directory ก็จะทำการถ่ายโอน (Replication) ฐานข้อมูลที่เปลี่ยนแปลงนั้น ไปยัง DCอื่นๆ ทุกตัว ทั้งนี้เพื่อให้ DC ทุกตัวมีฐานข้อมูลที่ทันสมัยเสมอ ทั้งนี้ในแต่ละ Domain นั้นสามารถมีเซิร์ฟเวอร์ที่มีบทบาทเป็นDC ได้หลายเครื่อง

โดเมน (Domain)

โดเมน (Domain) นั้นคงเป็นที่คุ้นเคยกันดีการใช้งานระบบอินเทอร์เน็ต เช่น โดเมน .co.th, .ac.th, .net, .com เป็นต้น ซึ่งโดเมนที่กล่าวมานั้นจะเป็นโดเมนในรูปแบบของ Domain Naming Service (DNS) ซึ่งให้บริการโดย Domain Naming Service Server (DNS Server) โดยความหมายของโดเมนในระบบ DNS นั้น จะหมายถึง treeหรือ sub-tree ที่อยู่ภายใน DNS namespace เดียวกัน

ตัวอย่างเช่น ftp.abc.com และ mail.abc.com จะอยู่ในโดเมนเดียวกันคือ abc.com เป็นต้น

สำหรับใน Active Directory นั้น โดเมน (Domain) จะมีหมายถึง กลุ่มของทรัพยากรต่างๆ (Resources) เช่น Computer, User, Group, Shared Folder, Printer ที่อยู่ภายใต้ Directory Database เดียวกัน มีSecurity Policy เดียวกัน และมีความสัมพันธ์ด้าน Security กับ Domain อื่นๆ แต่ เช่น xyz.com เป็นต้น

Domain Controller

Domain Controller (DC) คือ เครื่องเซิร์ฟเวอร์ Windows Server ที่ทำหน้าที่เก็บรักษา Active Directory database ให้บริการและดูแลการให้บริการของ Active Directory Service จัดการการสื่อสาร ระหว่าง User กับ Domain ให้การบริการและตรวจสอบการ Logon (Authentication) เข้า Domain ของเครื่องลูกข่าย (Client) และ ยูสเซอร์ (User) โดยในแต่ละ Domain นั้น จะต้องมีเซิร์ฟเวอร์ที่มีบทบาทเป็น DC อย่างน้อย 1เครื่อง

Root Domain

Root Domain คือ โดเมน (Domain) แรกที่ทำการสร้างขึ้นในสภาพแวดล้อมแบบ Active Directory ตัวอย่างเช่นxyz.com หรือ เป็นต้น โดยมีข้อสังเกตคือ Root Domain นั้น จะไม่มีโดเมนอื่นอยู่ระดับที่สูงกว่า

Child Domain

Child Domain คือโดเมน (Domain) ย่อยที่สร้างอยู่ภายใต้ Root Domain อีกทีหนึ่ง

Domain Tree

Domain Tree คือ โครงสร้างโดเมน (Domain) ที่เกิดจากการรวมกันของ Root Domain และ Child Domain เป็นการจัดเรียงตามลำดับชั้น คล้ายกับระบบชื่อใน DNS

Domain Forest

Domain Forest คือ โครงสร้างของโดเมน (Domain) ที่เกิดจากการรวมกันของ Domain Tree ตั้งแต่สองโดเมน (Domain) ขึ้นไป โดยแต่ละ โดเมน (Domain) จะมีการเชื่อมโยงกันผ่านทาง Trust Relationship แบบสองทาง (2 way trust)

Class

Class คือตัวแบ่งประเภทของ Object

Object

Object ชื่อของทรัพยากรต่างๆ ที่ใน Active Directory เช่น User, Computer, Printer, Shared Folder เป็นต้น

Attributes

Attributes เป็นค่าที่ใช้บอกคุณลักษณะของ Object เช่น password และ username เป็น attribute ของ object user โดย Object ที่อยู่ใน Class เดียวกันจะมี attribute เหมือนกัน

Schema

Schema เป็นข้อกำหนดต่างๆ ที่กำหนดว่า object แต่ละประเภทจะมี attribute อะไรบ้าง
เช่น object ประเภท userมี attribute คือ password, email เป็นต้น

Containers

Containers คล้ายกับโฟลเดอร์ (Folder) โดยจะใช้เก็บ containers และ objects ต่างๆ ไว้ภายใน โดย container ใน Active Directory จะมีอยู่ 3 ประเภท คือ 1. Domains, 2.Sites, 3. Organizational Units (OU)

Site

Site คือ เครือข่ายย่อย ที่การเชื่อมต่อมีความน่าเชื่อถือสูง มีความเร็วสูงและเชื่อมต่อถึงกันตลอดเวลา

Organizational Units (OU)

Organizational Units (OU) เป็น container ที่สามารถใช้เก็บ Object ต่างๆ ของโดเมน (Domain) ที่ตัวมันอยู่ เช่น Computer, User, Printer หรือ OU ย่อยก็ได้ แต่ไม่สามารถใส่ object จาก domain อื่นได้

Domain User Computer and Group

User Account

User Account คือ object ที่เก็บข้อมูลต่างๆ ของ User คือ user name, password, member ซึ่งถ้าเป็น Domain User Account นั้นจะเก็บและจัดการโดย Active Directory โดยจะเก็บอยู่ในฐานข้อมูลของโดเมนในไฟล์ชื่อ NTDS.DIT ซึ่งไฟล์นี้จะถูกจัดเก็บอยู่ในโดเมนคอนโทรลเลอร์ทุกตัวของโดเมน

สำหรับ Local User Account เช่น User Account ของ Member Server หรือ Client Computerแต่ละตัวนั้นก็จะเก็บและจัดการแบบ Local โดย Member Server หรือ Client Computer ที่ User Account นั้นอยู่ในระบบ โดยจะเก็บในเครื่องใครเครื่องมันอยู่ในฐานข้อมูลของระบบวินโดวส์ในไฟล์ชื่อ SAM (Security Account Manager) ซึ่งไฟล์นี้จะถูกจัดเก็บอยู่ในโฟลเดอร์ %System root%\Windows\System30\config\
การจัดการ User Account นั้น ถ้าเป็น Domain User Account จะใช้เครื่องมือที่ชื่อ Active Directory Users and Computers แต่ถ้าเป็น Local User Account จะใช้เครื่องมือที่ชื่อ Computers Management

Computer Account

Computer Account คือ object ที่เก็บข้อมูลต่างๆ ของเครื่องคอมพิวเตอร์ที่เป็นสมาชิกของโดเมน โดยหลังจากทำการเพิ่ม (Join) เครื่องคอมพิวเตอร์เข้าเป็นสมาชิกของโดเมน (Domain) แล้ว คอมพิวเตอร์แต่ละเครื่องก็จะได้รับ Account เพื่อใช้ในการระบุตัวตนของเครื่องนั้นๆ โดยที่ Account ที่ได้นั้นจะเป็นชื่อเดียวกันกับชื่อเครื่อง (Computer name) และต้องไม่ซ้ำกับเครื่องอื่น โดย Computer Account จะเก็บและจัดการโดย Active Directory แบบเดียวกันกับ User Account คุณสมบัติต่างๆ ของ Computer accounts จะมีลักษณะเหมือนกันกับ User account คือ สามารถ add, disable, reset และ delete ได้โดยใช้เครื่องมือที่ชื่อ Active Directory Users and Computers

Group

Group คือ Object ที่สามารถมีสมาชิกเป็น ยูสเซอร์ (Users) เครื่องคอมพิวเตอร์ (Computer) หรือกลุ่ม (Groups)อื่นๆ โดย Group นั้น มีวัตถุประสงค์เพื่อให้การการกำหนดสิทธิ์ (Right) ให้แก่ยูสเซอร์และ การรับ-ส่ง email ทำได้สะดวกขึ้น โดยในสภาพแวดล้อมแบบ Domain นั้น จะ Group อยู่ 2 ประเภทด้วยกัน
คือ Distribution Group และSecurity Group

Group type มีอยู่ 2 ประเภท ด้วยกันคือ
- Distribution Group เป็นกลุ่ม (Group) ที่ใช้ได้เฉพาะกับ email application เพื่อใช้สำหรับการรับ-ส่ง email เท่านั้น
- Security Group เป็นกลุ่ม (Group) ที่ใช้สำหรับการกำหนดสิทธิ์ (Right) ในการกระทำต่างให้กับกลุ่ม (Group)และใช้สำหรับการกำหนด Permission ในการใช้งาน Shared Resources ต่างๆ

Tips:
ประเภทของกรุ๊ป หรือ Group type นั้น สามารถทำการเปลี่ยนแปลงได้ ถ้าหากว่า domain functional level เป็นแบบ Windows

Group Scope

Group Scope คือ ขอบเขตของกลุ่ม ซึ่งมีอยู่ 3 แบบ ด้วยกันคือ Universal Group, Global Group และ Domain local Group โดยค่าดีฟอลท์ (Default) สำหรับการสร้าง New Group ขึ้นมานั้น จะกำหนดให้เป็นกลุ่มแบบ Security Group - Global Scope โดยที่ Group Scope นั้นสามารถเปลี่ยนแปลงได้ ถ้าหากว่าdomain functional level เป็นแบบ Windows

คุณลักษณะของ Group Scope

- สมาชิกของกลุ่ม Universal Group นั้น สามารถเป็น กลุ่ม (Group) อื่นๆ และ account จากโดเมน (Domain)ใดๆ ที่อยู่ในโดเมนทรี (Domain Tree) หรือ ฟอเรสต์ (Forest) สามารถใช้ Universal Group ในการกำหนดPermission ในโดเมน (Domain) ใดๆ ที่อยู่ในโดเมนทรี (Domain Tree) หรือฟอเรสต์ (Forest)
- สมาชิกกลุ่ม Global Group สามารถเป็นกลุ่ม (Group) อื่นๆ และ account เฉพาะจากโดเมน (Domain) ที่Global Group นั้นอยู่ สามารถใช้ Global Group ในการกำหนด Permission ในโดเมน (Domain) ใดๆ ที่อยู่ในโดเมนทรี (Domain Tree) หรือ ฟอเรสต์ (Forest)
- สมาชิกกลุ่ม Domain local Group สามารถเป็นกลุ่ม (Group) อื่นๆ และ account จาก Windows Server สามารถใช้ Domain local Group ในการกำหนด Permission เฉพาะในโดเมน (Domain) เท่านั้น

ข้อกำหนดในการเปลี่ยน Group Scope

ในการเปลี่ยนแปลง Group Scope นั้น มีข้อกำหนดดังต่อไปนี้

- Global to universal จะทำได้ถ้ากลุ่ม (Group) ที่ต้องการเปลี่ยนนั้นไม่ได้เป็นสมาชิกของ global scope group อื่นๆ
- Domain local to universal จะทำได้ถ้ากลุ่ม (Group) ที่ต้องการเปลี่ยนนั้นไม่มี domain local groupอื่นเป็นสมาชิก
- Universal to global จะทำได้ถ้ากลุ่ม (Group) ที่ต้องการเปลี่ยนนั้นไม่มี universal group อื่นเป็นสมาชิก
- Universal to domain local ทำการเปลี่ยนได้โดยไม่มีข้อจำกัด