โปรแกรมสร้าง แฟ้มข้อมูล ในการแลกเปลี่ยน Objectในระบบ Directory

The Development of LDAP Generator

โดย

เอกฤทธิ์ ธรรมสถิต

รหัส 45061614

อาจารย์ที่ปรึกษา

ผศ.ดร. โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2548

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	โปรแกรมสร้าง แฟ้มข้อมูล ในการแลกเปลี่ยน ObjectในระบบDirectory
นักศึกษา	นายเอกฤทธิ์ ธรรมสถิต
อาจารย์ที่ปรึกษา	ผศ.ดร. โชติพัชร์ ภรณวลัย
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2548

บทคัดย่อ

ในช่วงหลายปีที่ผ่านมาบริษัทต่างๆได้นำเอาระบบโครงสร้างบัญชีรายชื่อ Active Directory ในระบบปฏิบัติการ Windows Server มาใช้ในการควบคุมการเข้าใช้ทรัพยากรแต่เนื่องจากการจัดการระบบ Directory ค่อนข้างใช้เวลาถ้ามีการสร้างObjectจำนวนมากหรือต้องจัดการObjectในเครื่องที่อยู่ต่างสถานที่กันและต้องใช้ผู้ที่รู้จักโครงสร้างรายชื่อแบบ Directory ดังนั้น การจัดการ ด้วย VBScriptหรือ LDIF file จึงน่าจะเป็นเรื่องที่เหมาะในการจัดการเรื่องดังกล่าว โครงงานนี้เป็นโปรแกรมที่ใช้สร้าง VBScriptหรือ LDIF file เพื่อช่วยลดเวลาในการศึกษาและสร้าง VBScriptหรือ LDIF fileมาใช้เอง

Title	The Development of LDAP Generator
Student	Mr. Akerit Thamsatit
Advisor	Asst.Prof. Dr. Chotipat Pornavalai
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2005

ABSTRACT

In Window Server operating system, there is Active Directory that is directory service store information about users, resources and other network entities. In Addition to, most companies use the Active Directory Service to control resource accessing but they still have some problems, if there are lots of object were created or we have to manage the object that be in the different location, it will take a long time to manage the active directory service and we will need to have a specialist as well. Therefore it will be good to manage the active directory service by VBScript or LDIF File to solve the problem. In this study we will develop the program to generate VBScript or LDIF File in order to reduce the time.

กิตติกรรมประกาศ

โครงการพัฒนาโปรแกรมสร้าง แฟ้มข้อมูล ในการแลกเปลี่ยน Objectในระบบ Directory นี้ได้รับการสนันสนุนและให้คำแนะนำปรึกษาเป็นอย่างดีจากหลายฝ่ายซึ่งท่านเหล่านั้นยินดีที่จะเสียสละเวลาอันมีค่าเพื่อนำพาโครงการนี้บรรลุผลตามเป้าหมายที่ว่าไว้ผู้จัดทำใคร่ขอขอบพระคุณ

1. บิดา มารดา ที่ให้ความช่วยเหลือ ให้กำลังใจในการศึกษาและทำงาน
2. ผศ.ดร โชติพัต อาจารย์ที่ปรึกษาโครงการ ที่ได้ประสทธิประสาทวิชาความรู้แก่ข้าพเจ้า และให้คำแนะนำ คำปรึกษาในการจัทำโครงงาน
3. อาจารย์ทุกท่านที่ได้สั่งสอนให้ข้าพเจ้าคิดเป็นปฏิบัติเป็นและตัดสินใจในการแก้ไขปัญหาต่างๆจากองค์ที่มีอยู่ได้เป็น
4. เพื่อนๆทุกคนที่ให้กำลังใจและความช่วยเหลือมาโดยตลอด

เอกฤทธิ์ ธรรมสถิต

ผู้จัดทำ

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูป

หน้า

รูปที่

สารบัญรูป(ต่อ)

หน้า

สารบัญรูป(ต่อ)

หน้า

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

ระบบเครือข่ายถูกจัดเป็นส่วนประกอบที่มีความสำคัญ และมีความจำเป็น ในการดำเนินธุรกรรมต่อหน่วยงาน, สถาบันและองค์กรต่างๆ ในการดำเนินธรุกรรมประจำวัน และการแสดงตัวตนของผู้ใช้ทรัพยากรในเครือข่าย จึงมีความจำเป็นอย่างมาก ในการกำหนดสิทธิ์ และการเข้าถึงทรัพยากรนั้น

บัญชีรายชื่อสำหรับการเข้าใช้ที่ได้รับความนิยมมากอันหนึ่งในปัจุบัน คือ Active Directory ซึ่งเป็น ระบบรายชื่อที่ทำงาน บนระบบปฏิบัตการ Windows 2000 และ Windows 2003 Server ซึ่งเป็นไปตามมาตราฐาน X 500 ซึ่งมีโครงสร้าง ของระบบรายชื่อที่มีการแบ่งออกเป็นลำดับชั้นตั้งแต่ระดับ Forests , Domain ,Organization Unit และเก็บข้อมูลแบบ object โดย แต่ละobject มีอิสระจากกันแต่การสร้างโครงสร้างโดยใช้ Graphical User Interface นั้นเป็นไปได้อย่างล่าช้า การใช้ Script จึงเข้ามาเป็นทางเลือกที่ดีในการจัดการ ซึ่งการใช้ชุดคำสั่ง ออกจะเป็นเรื่องยากสำหรับผู้ที่พึ่งเริ่มรู้จะหรือแม้แต่ผู้ที่มีความชำนาญเองก็คงไม่สามารถจำชุดคำสั่งได้ทั้งหมด จึงเกิดแนวคิดในการใช้โปรแกรม Generate Script เพื่อช่วยในการจัดการโครงสร้างของ Active Directory

โปรแกรม Generate Script จะทำหน้าที่สร้าง Script (Script ก็คือ Fileที่รวมชุดของคำสั่งที่เป็น Command Line ที่ใช้ parametersในการกำหนดค่าต่างๆหรือ ชุดคำสั่งที่ถูกสร้างโดย VB เราอาจเรียนว่า VBScript) จากการที่ผู้ใช้ทำการออกแบบ Active Directory ออกมาเป็น File Script ที่อ้างอิงการจัดการ Active Directory ในรูปแบบ LDAP Data Interchange Format (LDIF : RFC 2849) และสามารถนำไป ใช้กับเครื่องที่ใช้ บนระบบปฏิบัตการ Windows 2000 และ Windows 2003 Server เพื่อสร้างโครงสร้างได้อย่างรวดเร็ว และใช้ในการเรียนรู้วิธีการเขียน Script สำหรับผู้ที่หัดเขียน รวมทั้งช่วยผู้ที่ชำนาญให้ลดเวลาในการสร้าง Scriptอีกด้วย โครงการพัฒนาระบบงานนี้ จึงเป็นการออกแบบและพัฒนาระบบการจัดการในการสร้างโครงสร้างบัญชีรายชื่อของ Active Directory ผ่าน Script File ที่ถูกสร้างขึ้นจากโปรแกรม เพื่อเพิ่มความสามารถในการทำงาน ของผู้บริหารและดูแลระบบ Active Directory ให้ทำงานได้เร็วขึ้นและสะดวกมากขึ้น นอกจากนี่โปรแกรมยังนำเสนอในรูปแบบที่เป็นรูปภาพ ที่สามารถที่เข้าใจได้ง่ายและสามารถทำแก้ไขหรือ

เพิ่มเติมค่าในตัว Script File ได้ตลอดการออกแบบ ที่มากไปกว่านั้นยังสามารถดึงค่าที่ได้มีการConfiguration ไว้ในเครื่องมานำเสนอ เป็นรูปโครงสร้าง และมีการแก้ไข ได้อีกด้วย

1.2 เป้าหมายของการพัฒนาระบบงาน

พัฒนาความสามารถในการสร้าง Script File ให้สะดวกและง่าย โดยนำเสนอในรูปแบบของ Graphic โดยใช้โปรแกรม AD Script Generator ซึ่งเป็นโปรแกรมที่ถูกพัฒนาขึ้นในโครงงานการพัฒนาโปรแกรม AD Script Generator สำหรับสร้าง Script เพื่อบริหารงาน Active Directory ให้สามารถทำงานได้ง่ายเพียงเรียกใช้ Script ก็จะสามารถจัดการกับ Active Directoryได้ โดยอาจไม่มีความรู้ในเรื่องคำสั่งในการจัดการ Active Directory ในแบบต่างๆมาก่อนเลย (Graphical User Interface: GUI และCommand Line Interface: CLI) โดยโปรแกรม AD Script Generator มีความสามารถต่างๆดังนี้

- สามารถดึงค่าConfiguration ที่มีอยู่ในเครื่อง Domain controller มาแสดงเป็น Graphic ที่เข้าใจง่าย
- สามารถ สร้าง Script ในการสร้าง Object ประเภทต่างๆได้โดยการจาก Graphic
- สามารถ สร้าง Script ในการแก้ไข Object ประเภทต่างๆได้ โดยการจาก Graphic
- สามารถ สร้าง Script ในการลบ Object ประเภทต่างๆได้ โดยการจาก Graphic
- สามารถสร้างScriptในการบริหารงานObjectประเภทต่างๆได้โดยการจาก Graphic
- สามารถใช้ในการออกแบบ Active Directory

1.3 วัตถุประสงค์ของการพัฒนาระบบงาน

- เพื่อศึกษา Active Directory, LDAP Data Interchange Formatและการเขียน Script โดยการใช้ Command Line Interface ในการบริหารงาน Active Directory
- ศึกษาการนำเสนอและการสร้าง Active Directory ในแบบ Graphic
- ทำการออกแบบและพัฒนาโปรแกรม สร้าง Script File จาก Graphic

1.4 ขอบเขตการพัฒนาระบบงาน

นำโปรแกรม AD Script Generator มาเพื่อพัฒนาวิธีการสร้างScriptในการสร้างและบริหารงาน Active Directory ซึ่งแต่เดิมการจะสร้างScript ได้นั้นต้อง มีความรู้พื้นฐานหลายอย่างและใช้เวลามากพอควร และยังต้องใช้ Command Line Interface ที่ มีParametersหลายตัวเข้ามาเกี่ยวข้องซึ่งไม่สะดวกและไม่เหมาะกับผู้บริหารงานระบบมือใหม่

1.5 ประโยชน์ที่คาดว่าจะได้รับ

โปรแกรมสร้าง Script ที่มีความสามารถในการสร้าง Script ในการสร้างและบริหารงาน Active Directory ในการสร้าง, ลบและแก้ไขค่าต่างๆ ของ object นั้นๆ

1.6 ขั้นตอนในการพัฒนาระบบงาน

- ศึกษาระบบบัญชีรายชื่อแบบ Active Directory
- ศึกษา LDAP Data Interchange Format ในการจัดการกับโครงสร้างของ Active Directory
- ศึกษา Command Line Interface ในการบริหารงาน Active Directory
- ทำการออกแบบโปรแกรม AD Script Generator
- ศึกษาเครื่องมือต่างๆที่จำเป็นต้องใช้ในการพัฒนาโครงงาน
- ทำการพัฒนาโครงงาน โปรแกรม AD Script Generator
- ทำการทดสอบโปรแกรม AD Script Generator ที่ได้พัฒนาขึ้น รวมทั้งปรับปรุงข้อบกพร่องต่างๆที่อาจเกิดขึ้น
- สรุปผลการทดสอบและทดลองใช้งานโปรแกรม
- จัดทำเอกสารประกอบโครงงาน

1.7 รายละเอียดของแต่ละบท

- บทที่ 2 ทฤษฎีการจัดการระบบบัญชีรายชื่อ แบบ Active Directory

อธิบายทฤษฎีโครงสร้าง แบบ Active Directory ซึ่งมีเนื้อหาครอบคลุมตั้งแต่ หลักการเบื้องต้น ของ Active Directory โปรโตคอล ที่ใช้ในการเข้าใช้งาน Active Directory รูปแบบการการจัดการโดยใช้ LDAP Data Interchange Format และรวมถึงการใช้ Command Line Interface บนระบบปฏิบัติการ Windows 2000 server และ Windows 2003 server

- บทที่ 3การออกแบบและพัฒนาระบบงาน

อธิบาย การออกแบบโปรแกรม ซึ่งจะมีการอธิบายหลักการทำงานของส่วน ประกอบต่างๆของโปรแกรม

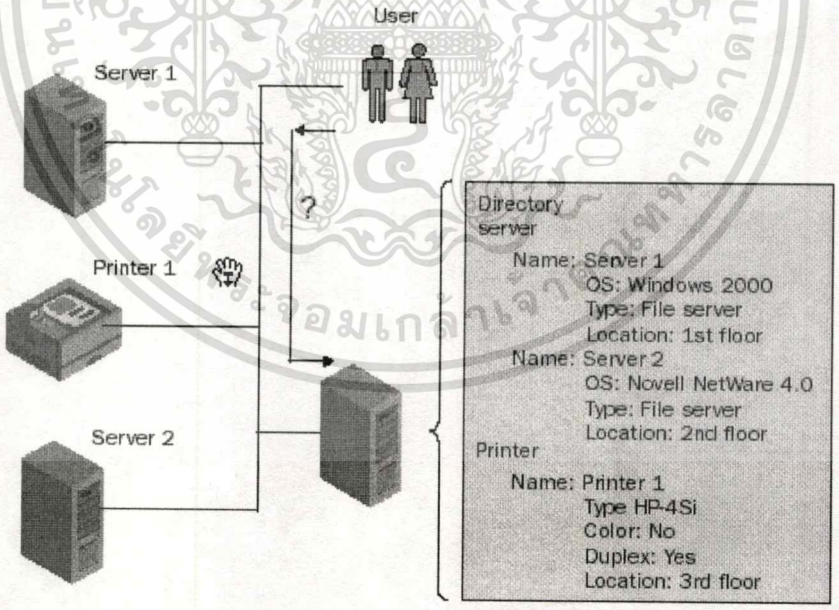
- บทที่4สรุปผลและข้อเสนอแนะโครงการพัฒนาระบบงาน

สรุปผลผลการทดลองใช้โปรแกรม,ข้อเสนอและรวมถึงข้อควรระวังในการใช้

บทที่ 2
ทฤษฎีการจัดการระบบบัญชีรายชื่อ แบบ Active Directory

2.1 Directory Services

Directory เป็นที่เก็บข้อมูลของออปเจค ตัวอย่างเช่น e-mail address book ที่เก็บของ User หรือที่อยู่กับผู้ติดต่อทาง e-mail ในระบบ Directory Services มีกลไกการกระจาย ในเครือข่ายสาธารณะ เช่น อินเตอร์เน็ตซึ่งมีหลายออปเจคที่เก็บใน Directory เช่น File Servers, Printers, Fax Server, Application, Databases และ Users ผู้ใช้สามารถที่หาตำแหน่งและเรียกใช้ออปเจคได้ ส่วน Administrators สามารถที่จะจัดการออปเจคต่างๆที่เก็บไว้ที่ส่วนกลาง Directory service เหมือนสวิตช์บอร์ดหลักของ Network Operating System ซึ่งเก็บการรับผิดชอบไว้ที่ส่วนกลาง และมีตัวแทนกระจายความสัมพันธ์ระหว่างทรัพยากรต่างๆ ซึ่งอนุญาตให้ทำงานร่วมกัน



รูปที่ 2.1 ตัวอย่างส่วนประกอบใน Directory Service

Directory Service รองรับการจัดการที่ง่าย และมีโครงสร้างของการเข้าใช้ทรัพยากรในระบบเครือข่ายคอมพิวเตอร์ ผู้ใช้ และผู้บริหารระบบที่ไม่รู้คุณลักษณะที่แท้จริงของออปเจค แต่

สามารถที่ค้นหาได้โดยกำหนดคุณสมบัติบางอย่างในการค้นหา เช่น หาออปเจคที่เป็นเครื่องพิมพ์ที่ตั้งอยู่ที่ชั้น 3 ดังรูปที่ 2.1

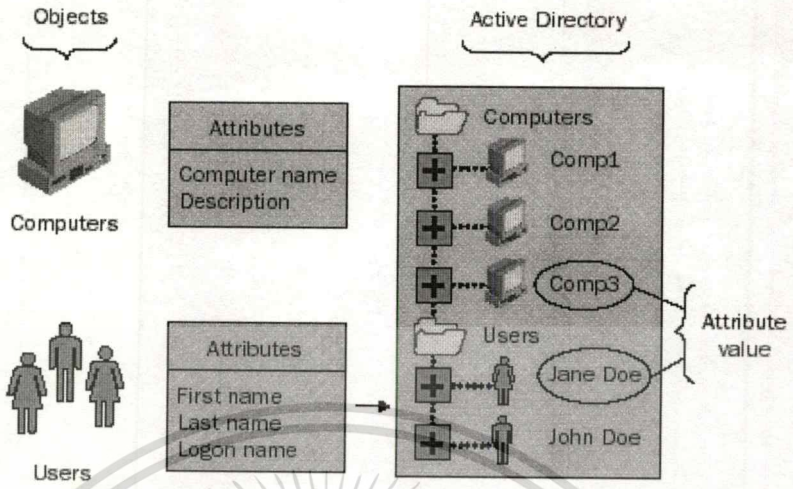
2.2 Windows Server 2003 Directory Service

เป็นระบบบัญชีรายชื่อที่เรียกว่า Active Directory ซึ่งเก็บข้อมูลต่างๆของทรัพยากร ซึ่งสามารถเรียกใช้ และรองรับใน Windows 2000 ด้วยฟีเจอร์ Active Directory ของ Windows Server 2003 ที่มีความสามารถเพิ่มขึ้นจาก Windows NT Domain เดิม

- การจัดเก็บส่วนกลาง
- รองรับองค์กรขนาดเล็ก ถึงขนาดใหญ่
- มีโครงสร้างที่เพิ่มเติมได้
- จัดการได้เป็นลำดับชั้น
- รองรับการทำงานกับ Domain Name System (DNS)
- รองรับการจัดการจากเครื่องลูกข่าย
- บริหารงานผ่าน Policy-based
- มีการเรพพลิเคตข้อมูล
- ยืดหยุ่น, การรับรอง และการอนุญาตอย่างปลอดภัย
- การใช้งานร่วมกับความปลอดภัย
- รองรับแอพพลิเคชั่นกับ Directory และโครงสร้าง Directory
- ใช้งานร่วมกับ Directory Services ระบบอื่นๆได้อย่างดี
- รองรับลายซื่ออิเล็กทรอนิกส์ และการเข้ารหัสของ LDAP

2.3 ออปเจคของ Active Directory

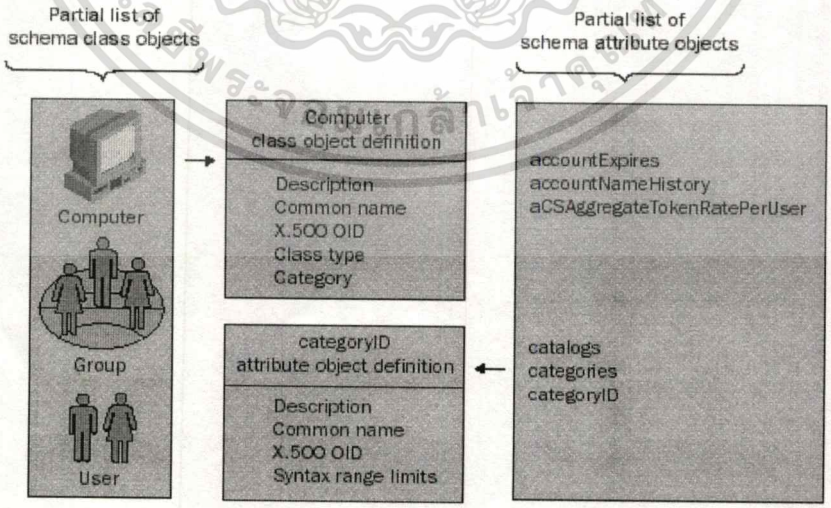
ข้อมูลถูกเก็บใน Active Directory เช่น Users, Printers, Servers, Databases, Groups, Computers, และ Security Policies ซึ่งมีการจัดการโครงสร้างที่ออปเจคแต่ละแบบมีคุณสมบัติที่แตกต่างกัน (Active Directory Schema) ออปเจคที่เป็นที่จัดเก็บเรียกว่า Organizational Unit (OU) ส่วนออปเจคอื่นๆก็จะเก็บในที่จัดเก็บ หรือโฟลเดอร์



รูปที่ 2.2 ออปเจคใน Active Directory

2.4 Active Directory Schema

ประกอบด้วย Schema classes กับ Schema attribute Schema Class เป็นกลุ่มของ Schema attribute ต่างๆสร้างเป็นออปเจคขึ้นSchema attribute เป็นคุณสมบัติของออปเจคในแต่ละอย่าง ซึ่งในคุณสมบัตินี้อาจอยู่ในหลายออปเจคได้ ซึ่งทั้ง Schema classes และ Schema attributes นี้รวมเรียกว่า Schema objects หรือ Metadata

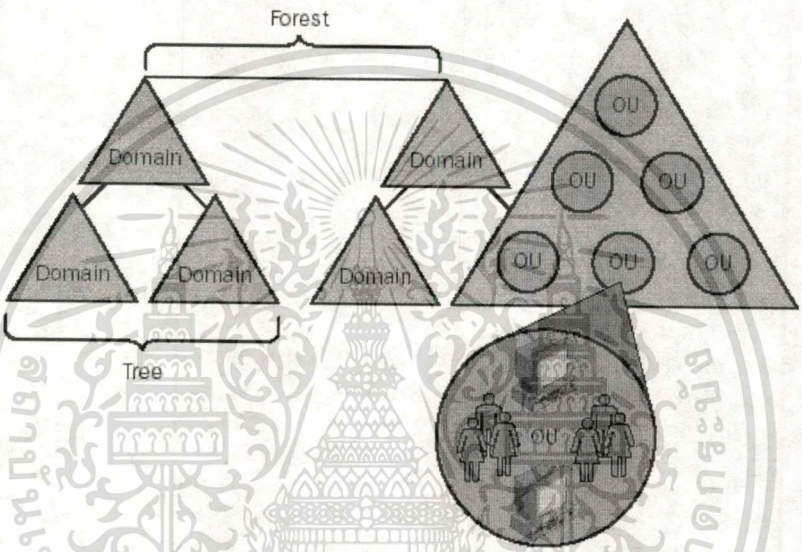


รูปที่ 2.3 Active Directory Schema

2.5 ส่วนประกอบ Active Directory

เป็นส่วนประกอบให้เกิดโครงสร้างรายชื่อ ซึ่งตรงกับความต้องการองค์กร โดยส่วนประกอบ แบ่งโครงสร้างการออกแบบเป็น Logical Structure กับ Physical Structure

- **Logical Structure**

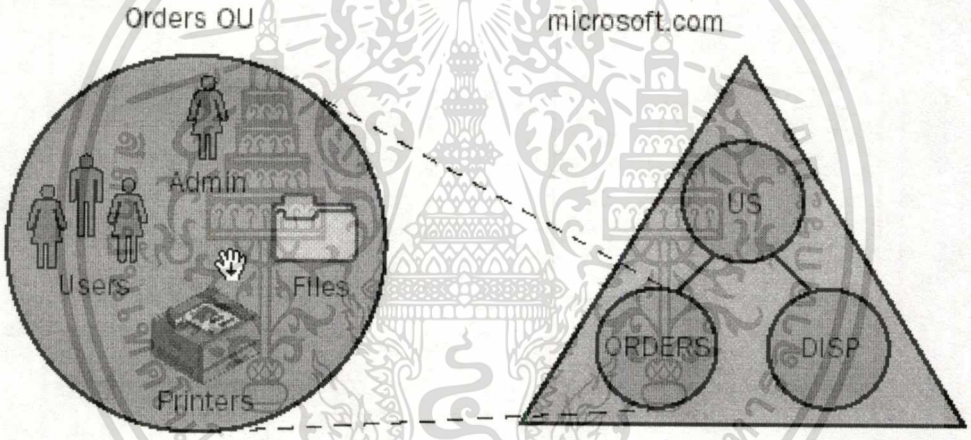


รูปที่ 2.4 Logical Structure

เป็นการออกแบบตามหลักการณ์ที่ต้องการในการจัดให้สอดคล้องกับโครงสร้างองค์กร ให้เข้าใช้ หรือจัดกลุ่มการเข้าใช้ได้ง่าย แบ่งการออกแบบเป็น

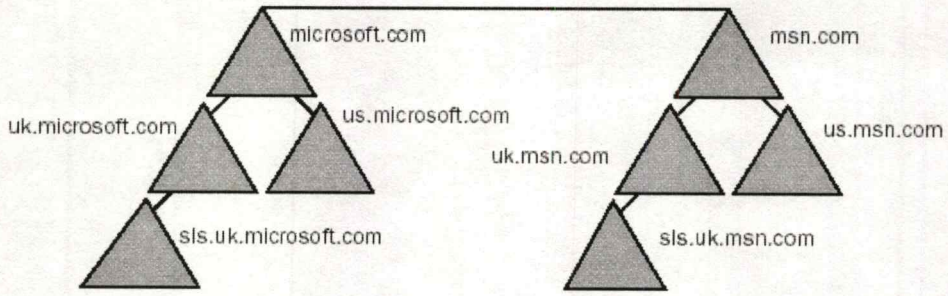
- Domains เป็นโครงสร้าง Logical ที่กำหนดกลุ่มขึ้นมาเพื่อให้สื่อสารในเครือข่าย โดยภายในจะประกอบด้วยเครื่องที่ดูแลโดเมนเรียกว่า Domain Controller และเป็นการเก็บข้อมูล และควบคุมการเข้าใช้ทรัพยากรในขอบเขตที่กำหนดเรียกว่า Access Control List (ACLs) ซึ่งถูกออกแบบมาใน Windows NT Domain จน Windows 2000 และ Windows Server 2003 ซึ่งโหมดของโดเมนแบ่งเป็น 4 โหมด คือ Windows 2000 (mixed), Windows 2000 native, Windows Server 2003 Interim, และ Windows 2003
- Windows 2000 (Mixed) เป็นค่าดีฟอลท์ที่กำหนด ซึ่งสามารถทำงานร่วมกับ Windows NT Domain, Windows 2000, หรือตระกูล Windows Server 2003 ได้ในโดเมนเดียวกัน

- Windows 2000 Native เป็นการทำงานร่วมกันระหว่าง Windows 2000 กับ Windows Server 2003
- Windows Server 2003 Interim เป็นการทำงานร่วมกับ Windows NT หรือ Windows Server 2003
- Windows Server 2003 เป็นบทบาทที่เครื่อง Domain controller ทำงานเฉพาะตระกูล Windows Server 2003
- OUs เป็นหน่วยเก็บย่อยในโดเมนที่สามารถบรรจุออปเจค และใช้ในการจัดโครงสร้างออปเจค หรือแบ่งแผนกได้ รวมถึงการมอบหมายงานในการบริหารในแต่ละที่บรรจุที่กำหนดไว้ ให้เป็นลำดับชั้น



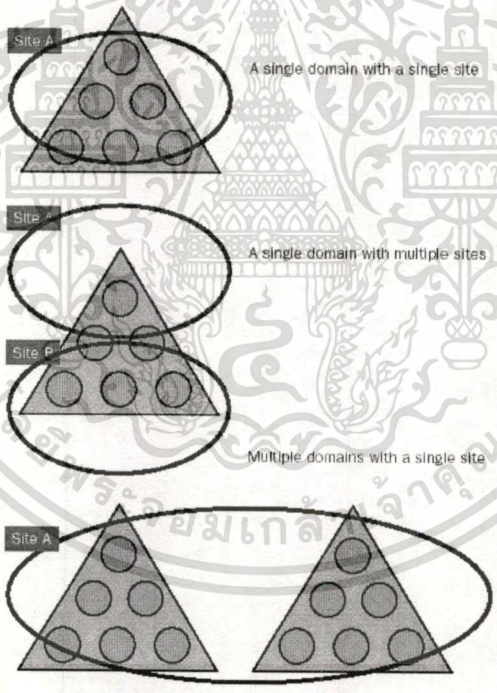
รูปที่ 2.5 แสดงส่วนประกอบภายใน OUs

- Trees เป็นกลุ่ม หรือลำดับชั้นของโดเมนใน Windows Server 2003 โดยทั้งหมดจะมีโครงสร้างต่อเนื่องในชื่อที่กำหนดเดียวกัน
- Forests เป็นกลุ่มลำดับชั้นที่ใช้จัดแย่ง ชื่อที่กำหนด หรือ Domain trees ออกจากัน โดยมีคุณลักษณะดังนี้
  - ทุกโดเมนใน Forest แชร์ Schema ร่วมกัน
  - ทุกโดเมนใน Forest แชร์ Global Catalog กัน
  - ทุกโดเมนใน Forest มีการทรัสต์แบบ Implicit two-way transitive
  - ทรีในฟอเรสต์จะมีโครงสร้างชื่อที่แตกต่างกัน
  - โดเมนในฟอเรสต์จะทำงานอิสระจากกัน แต่จะมีการสื่อสารข้ามกันได้ในองค์กร



รูปที่ 2.6 แสดงการ trust กันของโดเมนในแบบต่าง ๆ

– **Physical Structure**



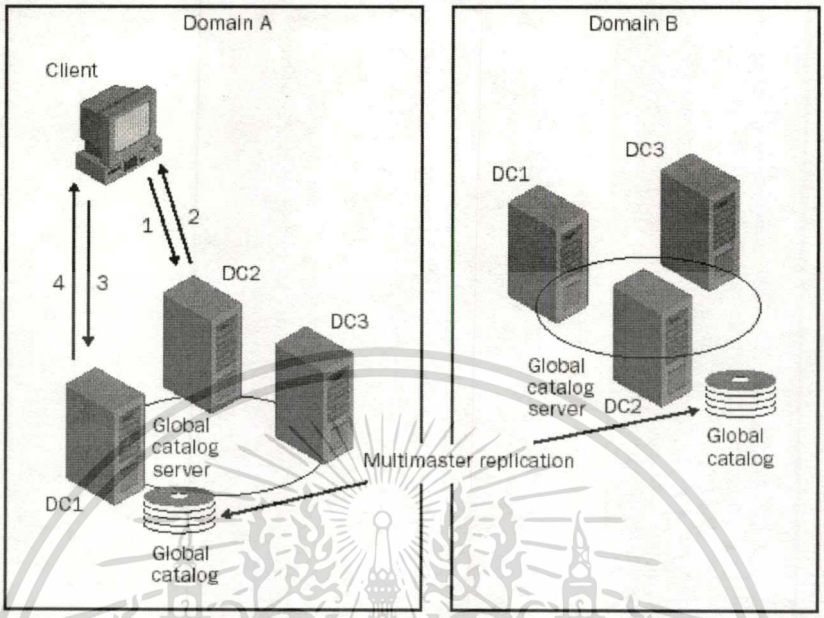
รูปที่ 2.7 Physical Structure

เป็นการออกแบบ Active Directory โดยพิจารณาด้านกายภาพ การเชื่อมต่อจริง ซึ่งจะแบ่งการออกแบบตาม Site และ Domain Controller

- Sites เป็นส่วนประกอบของเครือข่ายที่แบ่งตาม IP Subnet ซึ่งการติดต่อระหว่างไซต์จะต้องมีความน่าเชื่อถือ และการทำงานที่มีความเร็วที่สูง และดี ซึ่งความเร็วสูงที่กล่าวคือ 512 Kbps ซึ่งถ้าความเร็ว 128 Kbps ก็เพียงพอในการติดต่อไซต์เช่นกัน โดยไซต์นี้จะไม่พิจารณาตามชื่อโดเมน จะพิจารณาตามภูมิประเทศ และเครือข่าย
- Domain Controllers เป็นเครื่องคอมพิวเตอร์ที่ทำงานบน Windows Server 2003 มีการจัดเก็บฐานข้อมูลของโดเมน ซึ่งในแต่ละเครื่องมีกลไกในการเรพพลิเคต และมีความสามารถในการรองรับการทำงานในโดเมนได้ ซึ่งทุกโดเมนจะต้องมีเครื่อง Domain Controller อย่างน้อยหนึ่งเครื่อง สิ่งต่างๆของ Domain Controller มีดังนี้
  - ทุก Domain Controller จะเก็บข้อมูลอย่างสมบูรณ์ในโดเมนหนึ่งๆของ Active Directory Information
  - Domain controller จะมีการเรพพลิเคตข้อมูลถึงกันและกันโดยอัตโนมัติ
  - Domain Controller จะมีการเรพพลิเคตข้อมูลทันทีถ้าเป็นข้อมูลสำคัญ เช่นการ Disable ผู้ใช้
  - Active Directory ใช้การเรพพลิเคตเป็นแบบ Multimaster คือไม่มีเครื่อง Domain controllers ใดเป็น Master
  - แม้ว่า Active Directory จะรองรับ Multimaster แต่จะมีการกำหนดบทบาทของเครื่อง Domain controller ที่เป็น Operation master roles ที่ทำหน้าที่เฉพาะในบทบาทบางอย่าง
  - Domain controllers มีการตรวจสอบการชนกันข้อมูล ซึ่งถ้าพบว่าข้อมูลที่อัพเดตมีการส่งจากแหล่งที่แก้ไขสองแห่งจะมีการปรับเปลี่ยนเพิ่มหมายเลขเวอร์ชั่น
  - ถ้ามี Domain controller มากกว่าสองเครื่องจะรองรับ Fault tolerant
  - Domain controllers จัดการข้อมูลของผู้ใช้ได้ทันที เช่น การหาตำแหน่งที่เก็บออปเจค และการตรวจสอบผู้ใช้ที่ล็อกออน

2.6 Catalog Services

- **หน้าที่ของ Global Catalog**
  - รองรับผู้ใช้ที่ล็อกออนเข้าเครือข่ายในสมาชิกของ Universal
  - รองรับการค้นหาข้อมูลโดยไม่คำนึงถึงโดเมน
  - กระบวนการค้นหา



รูปที่ 2.8 กระบวนการค้นหา Global Catalog

ตรวจสอบจาก DNS เพื่อหา Global CatalogDNS ส่งกลับเป็น IP Address และระบุเรื่อง Domain Controllerลูกข่ายค้นหาโดยใช้หมายเลข IP Address ที่ได้รับที่ Port 3269 บน Domain Controller และ Active Directory จะส่งคำค้นที่พอร์ต 389 Global catalog server จะทำการค้นหาและส่งข้อมูลที่เก็บ

2.7 แนวคิด Active Directory

แนวคิดของ Active Directory ประกอบไปด้วย Replication, Trust Relationships, การบริหารงาน และการจัดการ, Group Policies, DNS, งานบริหารงาน Active Directory

– Replication

ข้อมูลที่ต้องทำการ Replication ประกอบด้วยอะไรบ้าง

– Schema Partition เป็นส่วนที่เก็บคุณสมบัติออปเจค และข้อมูลจะเหมือนกันทั้งโดเมน

– Configuration Partition เป็นที่เก็บโครงสร้าง logical ของโดเมนหรือ Replication topology ซึ่งทุกโดเมนในฟอเรสต์เหมือนกัน และถูกส่งไปยังทุก Domain controller ใน Forest

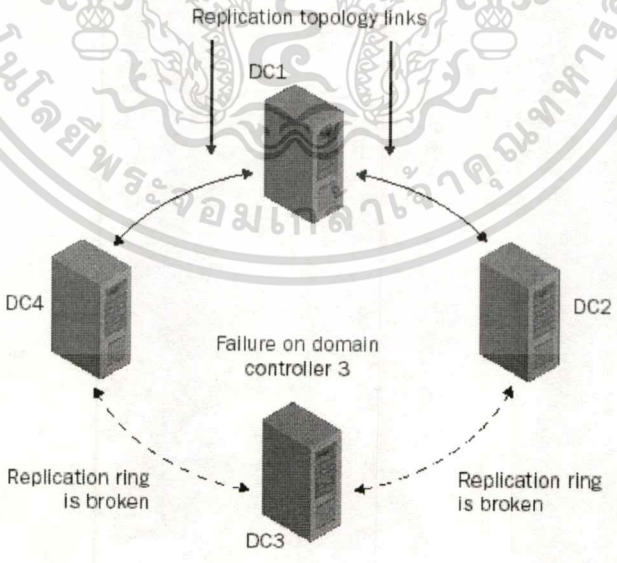
– Domain Partition เป็นการระบุการแบ่งข้อมูลออปเจค ที่ไม่มีการ replicated ไปยังโดเมนเอนๆ จะมีข้อมูลเรพพลิเคตเฉพาะในโดเมน ทุก Domain controllers

– Application Directory Partition เป็นส่วนที่แอพพลิเคชั่นที่มีระบุข้อมูลใน Active Directory ซึ่งจะไม่กวนประสิทธิภาพระบบ โดยมีการจัดเก็บชนิดออปเจค ยกเว้น Security principals (Users, Groups, และ Computer)

2.8 วิธีการ Replicate ข้อมูล

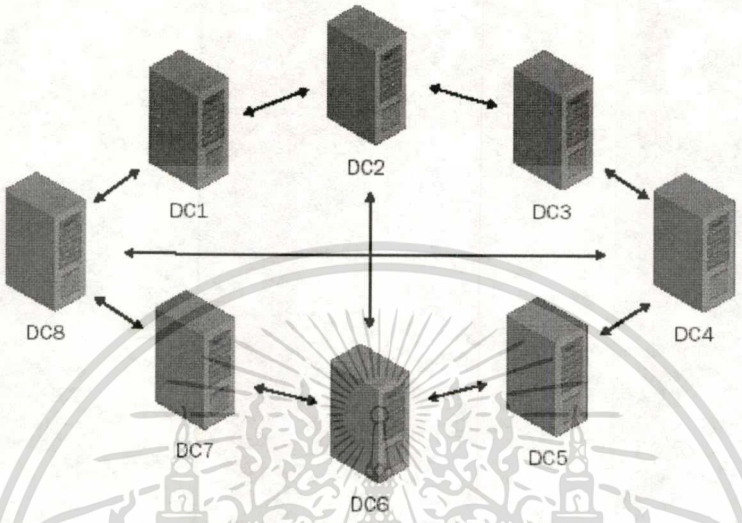
– Intrasite Replication

ใน Windows Server 2003 มีบริการที่เรียกว่า Knowledge consistency Checker (KCC) ที่สร้างโทโปโลยี่ในการเรพพลิเคต ซึ่งเป็นการสร้างระหว่างที่มีการเรพพลิเคตในกลุ่มเครื่อง Domain Controller ซึ่งจะมีการรับข้อมูลในการอัพเดต มีการแต่งตั้ง และเก็บประวัตที่มีการส่ง ซึ่ง Domain Controllers หนึ่งสามารถมีคู่ที่เรพพลิเคตได้มากกว่าหนึ่ง การจัดโครงสร้างเป็นรูปแบบวงดังรูปที่ 2.9



รูปที่ 2.9 Replication topology links

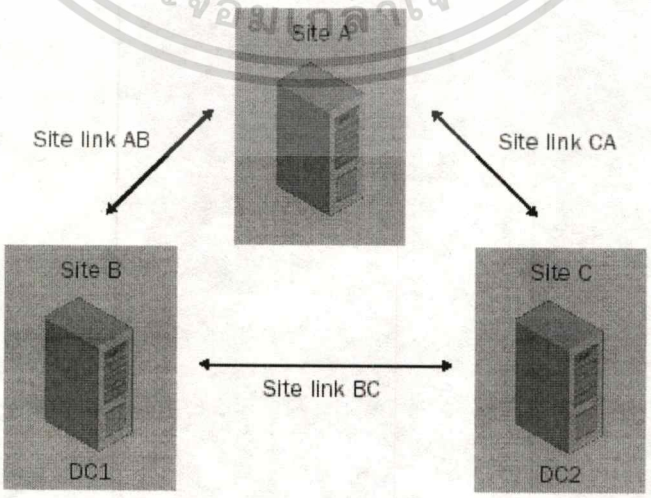
ในการสร้างกลไกการเรพพลิเคตของเครื่อง Domain controllers จะกำหนดไม่เกิน 3 การกระโดด ระหว่างที่มีการเชื่อมต่อออปเจคใน KCC



รูปที่ 2.10 Replication process

– Intersite Replication

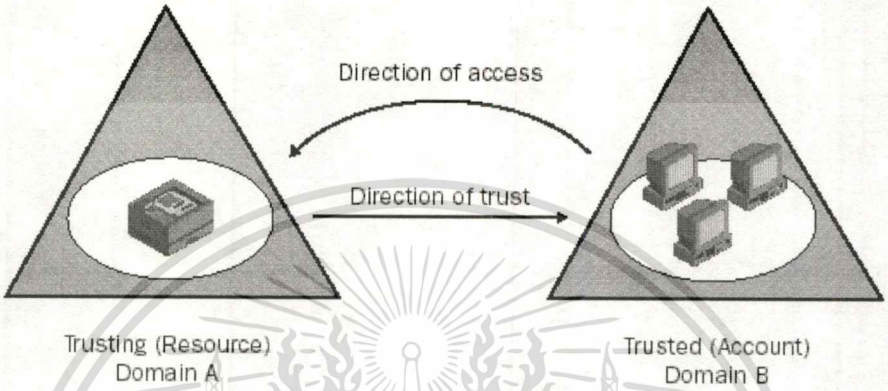
เป็นการเรพพลิเคตข้อมูลระหว่างไซต์ ซึ่งมีการเชื่อมต่อ โดยจะมีหนึ่ง KCC ต่อหนึ่งไซต์ รองรับการกำหนด Transport, Cost of a site link, times และดูลิงค์ที่ใช้ว่างหรือไม่



รูปที่ 2.11 Site link

– Trust Relationships

เป็นการเชื่อมต่อโดเมนระหว่างสองโดเมน ซึ่งในตระกูล Windows Server 2003 รองรับโปรโตคอลในการทรัสต์สองแบบคือ Kerberos version 5.0 หรือ NT LAN Manager (NTLM)



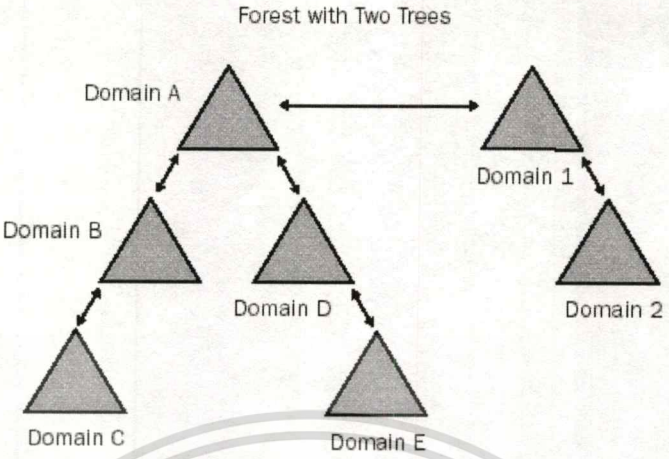
รูปที่ 2.12 Trust Relationships

การทรัสต์มีคุณลักษณะดังนี้

– วิธีการสร้าง ด้วยมือ หรืออัตโนมัติ (ที่เกิดจากผลการทรัสต์ระหว่างโดเมน)
– การส่งผ่าน ซึ่งจะเป็นการสร้างความสัมพันธ์ระหว่างโดเมนหนึ่ง กับอีกโดเมนหนึ่ง แต่โดเมนที่ถูกสัมพันธ์จะได้รับการทรัสต์ด้วย
– ทิศทาง เป็นการกำหนดว่าเป็นทิศทางเดียว หรือสองทิศทาง

2.9 รูปแบบของ Windows Server 2003

การเชื่อมต่อใน Tree เป็นการทรัสต์ระหว่างรูทของโดเมนในฟอเรสต์เดียวกัน การทรัสต์ใน Parent-Child เป็นการทรัสต์ที่มี Parent และ Child โดยโดเมนลูกจะมีชื่อต่อจากโดเมนแม่ เช่น Microsoft.com เป็น UK.microsoft.com



รูปที่ 2.13 Forest Trust

- Shortcut trust เป็นการทรัสต์ที่กำหนดเองโดยผู้บริหารระบบ เพื่อเพิ่มประสิทธิภาพระหว่างโดเมนในฟอเรสต์ เพื่อลดทิศทางระหว่างโครงสร้างทรี หรือฟอเรสต์ สามารถกำหนดได้หนึ่ง หรือสองทิศทาง
- External trust เป็นการกำหนดทรัสต์โดยผู้บริหารระบบ ใน Windows Server 2003 Domain ที่ต่างฟอเรสต์กัน หรือกับ Domain ใน Windows NT Server 4.0 หรือสูงกว่า โดยทั้งหมดจะแยกจากฟอเรสต์กัน ไม่สามารถที่เชื่อมต่อฟอเรสต์กันได้ ไม่เป็น Transitive และสามารถกำหนดหนึ่ง หรือสองทิศทางได้
- Forest trust เป็นการกำหนดด้วยผู้บริหารระบบที่ทำระหว่างสองฟอเรสต์ของรูท ซึ่งทุกโดเมนในหนึ่งฟอเรสต์สามารถที่ทรัสต์กับอีกฟอเรสต์ได้ เป็นสิ่งที่ทำได้ในเฉพาะ Windows Server 2003 ที่กำหนดโหมดโดเมนเป็น Windows Server 2003 functional level
- Realm trust เป็นการทรัสต์กับ non-Windows Kerberos realm กับ Windows Server 2003 domain ซึ่งทำให้สามารถใช้งานร่วมกันได้ใน Kerberos version 5 ไม่เป็น Transitive และทำได้ในหนึ่ง หรือสองทิศทาง

2.10 Active Directory Naming object

Active Directory รองรับในบริการรายชื่อกับมาตรฐาน LDAP ซึ่งสามารถที่ค้นหา LDAP จาก Active Directory Database ได้ซึ่งการกำหนดชื่อมีสิ่งที่ควรทราบดังนี้

- Distinguished Name (DN) เป็นชื่อที่กำหนดไม่ซ้ำกันในออปเจค เช่น Scott Cooper ทำงานที่โดเมน Microsoft.com จะมี DN เป็น CN=Scott Cooper, OU=Promotions, OU=Marketing, DC=Microsoft, DC=Com
- Relative Distinguished Name (RDN) เป็นการค้นหาคุณสมบัติที่กำหนดซึ่งผู้ใช้ไม่แน่ใจใน DN ที่ค้นหา เรียกว่า RDN เช่นเราค้นหา Scott จาก OU=Promotions เป็นต้น
- Globally Unique Identifier (GUID) เป็นเลขฐาน 16 ทั้งหมด 128 บิต ซึ่งรับประกันการไม่ซ้ำกันของชื่อโดย GUID จะไม่เปลี่ยน ใน Windows NT มีระบบการใช้เช่น Security Identifier (SID) ซึ่งเป็นการรับประกันในโดเมน แต่ GUID รับประกันในทุกโดเมน เมื่อมีการย้ายข้ามโดเมนหนึ่งไปยังอีกโดเมนหนึ่ง
- User Principle Name (UPN) เป็นการตั้งชื่อให้ง่ายต่อการใช้งาน เช่น ScottC@microsoft.com

2.11 การพิจารณาชื่อ Domain

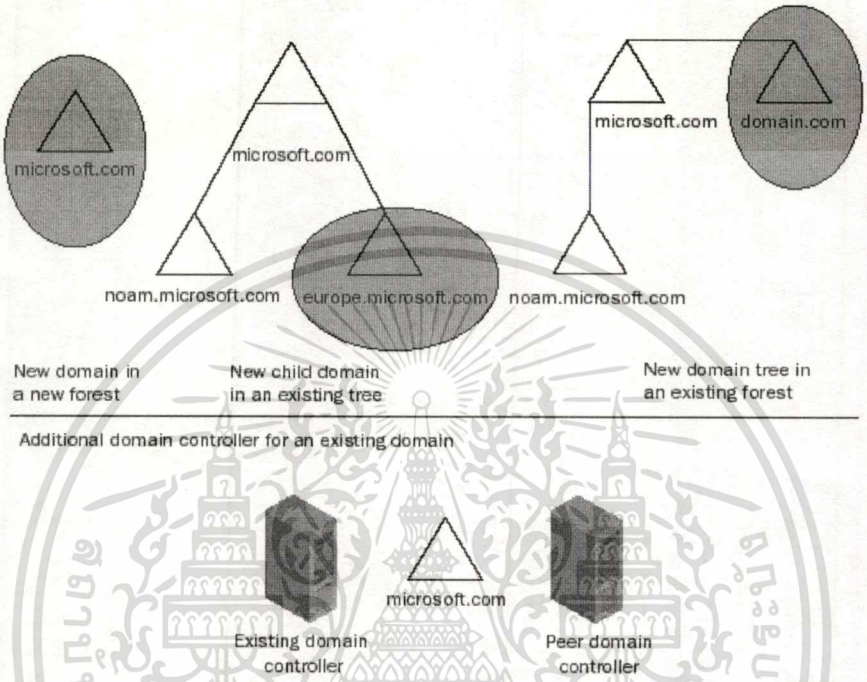
- กำหนดชื่อที่ใช้อักขระมาตรฐาน เช่น A-Z, a-z, 0-9 และ -
- กำหนดชื่อที่ใช้ภายใน และภายนอกที่แตกต่างกัน
- การวางชื่อ DNS ภายในบน DNS อินเตอร์เน็ต
- ไม่ใช้ชื่อโดเมนซ้ำกันสองครั้ง
- ใช้ชื่อที่ถูกลงทะเบียน โดยกำหนดลงทะเบียนในลำดับที่สอง
- ใช้ชื่อที่สั้น, ชัดเจน, และมีความหมาย
- ใช้ชื่อที่รองรับอินเตอร์เนชั่นแนล
- ใช้มาตรฐาน ISO ในการกำหนดชื่อ

2.12 การพิจารณาตำแหน่งที่เก็บไฟล์ฐานข้อมูล

- ดีฟอลท์กำหนดที่ %Systemroot%\Ntds
- ซึ่งกำหนดไว้ในไดร์ฟ NTFS แนะนำให้มีขนาดมากกว่า 1 Gbytes จำนวนที่น้อยที่สุด 250 Mbytes
- ไฟล์ที่เก็บคือ ntds.dit
- ข้อมูลที่เก็บ
- Schema
- Global catalog

– Objects ใน domain controller

2.13 ประเภท Domain Controller



รูปที่ 2.14 Type of Domain Controller

2.14 การพิจารณาการกำหนดค่า DNS

– กำหนดค่าเป็น IP Address ที่ถาวร

– ตรวจสอบเรคคอร์ด _ldap._tcp.dc._msdcs.DNSDomainName service (SRV)

– ตรวจสอบเรคคอร์ด A ที่มีการระบุที่ _ldap._tcp.dc._msdcs.DNSDomainName service (SRV)

2.15 การใช้เครื่องมือบริหารงาน Active Directory

คือ Active Directory administrative consoles เป็นเครื่องมือที่ติดตั้งอัตโนมัติเมื่อมีการประกาศเครื่องเป็น Domain Controllers โดยในชุดเครื่องมือมีดังนี้

– Active Directory Domains and Trusts

เป็นเครื่องมือที่ใช้ในการบริหาร และตรวจสอบการทรัสต์กันระหว่างโดเมน ซึ่งรองรับการจัดการใน Windows Server 2003 Domain, Windows 2000 Domain, Windows NT, รวมถึง Kerberos version 5 เราสามารถที่ปรับเปลี่ยนลำดับโดเมนได้จากที่นี่ และเปลี่ยนชื่อ UPN เพื่อสร้างผู้ใช้

ในลำดับ Domain Functional Levels กำหนดสิ่งต่างๆได้ดังนี้

– Windows 2000 mixed

– Windows 2000 Native

– Windows Server 2003 interim

– Windows Server 2003

ในลำดับฟอเรสต์ กำหนดสิ่งต่างๆได้ดังนี้

– Windows 2000 Native

– Windows Server 2003 interim

– Windows Server 2003

– Active Directory Sites and Services

เป็นเครื่องมือที่ให้ข้อมูลเกี่ยวกับโครงสร้าง Physical ซึ่งกำหนดในการบริการ Sites และกำหนดการเรพพลิเคต

– Active Directory Users and Computers

เป็นเครื่องมือที่ใช้ในการเพิ่ม แก้ไข และลบออปเจค เพื่อจัดโครงสร้างใน Windows Server 2003 ในหนึ่งโดเมน ซึ่งการบริหารงานโครงสร้างจะใช้ออปเจคที่เป็น Organizational Units (OUs)

– Active Directory Schema Snap-in

เป็นเครื่องมือที่ใช้ดู และแก้ไข Active Directory Schema โดยดีฟอลท์จะไม่สร้างเป็นเครื่องมือ หรือติดตั้งใน Snap-in ผู้บริหารต้องเลือกติดตั้งเพิ่มเอง

2.16 การติดตั้ง และการจัดการโดเมน, โดเมนทรี, และฟอเรสต์

– การสร้างหลายโดเมน, โดเมนทรี, และฟอเรสต์

– การสร้างหลายโดเมน ต้องพิจารณาจำนวนโดเมนที่ต้องการในแต่ละฟอเรสต์ขององค์กร ซึ่งต้องดูความสลับซับซ้อน และดูว่าหนึ่งโดเมนเพียงพอต่อการทำงานหรือไม่ การกำหนดโดเมนเพิ่มจะมีค่าใช้จ่าย และงานบริหารเพิ่ม

2.17 เหตุผลในการสร้างหลายโดเมน

การสร้างโดเมนให้ตรงกับความต้องการด้านความปลอดภัย มีการพิจารณาในเรื่องการกำหนด Security Policy ดังนี้

- Password Policy
- Account Lockout policy
- Kerberos policy

การสร้างโดเมนเพื่อให้ตรงกับงานบริหาร อาจจะดูความสามารถของ OUs ก่อนว่าสามารถทำให้โครงสร้างองค์กรทำงานได้หรือไม่ หรือถ้าไม่ได้ในหนึ่งโดเมนต้องมี Domain Admins ซึ่งเป็นผู้ดูแลแต่ละโดเมน และดูการควบคุมไฟล์ต่างๆในโดเมน

การสร้างโดเมนเพื่อลดการจราจร เราสามารถบริหารการจราจรระหว่างไซต์ได้โดยพิจารณา

- ความสามารถของลิงค์
- การควบคุมเวลาในการจราจร
- การดูลิงค์ กับค่าใช้จ่าย
- การดูความจำกัดในลิงค์ว่าใช้เป็น Simple Mail Transport Protocol ได้หรือไม่

การสร้างโดเมนเพื่อให้คงอยู่ใน Windows NT Domain เป็นการพิจารณาผู้บริหาร Windows NT Domain และเรื่องของความปลอดภัยในโดเมนที่ทำการทรัสต์กัน

2.18 ความหมายของการสร้างหลายโดเมน

สิ่งที่เกิดขึ้นตามมาในการสร้างหลายโดเมนคืองานที่ดำเนินเพิ่ม และค่าใช้จ่าย ซึ่งสิ่งที่พิจารณามีดังนี้

Domain Administrators กลุ่มการบริหารเพิ่มในแต่ละโดเมน

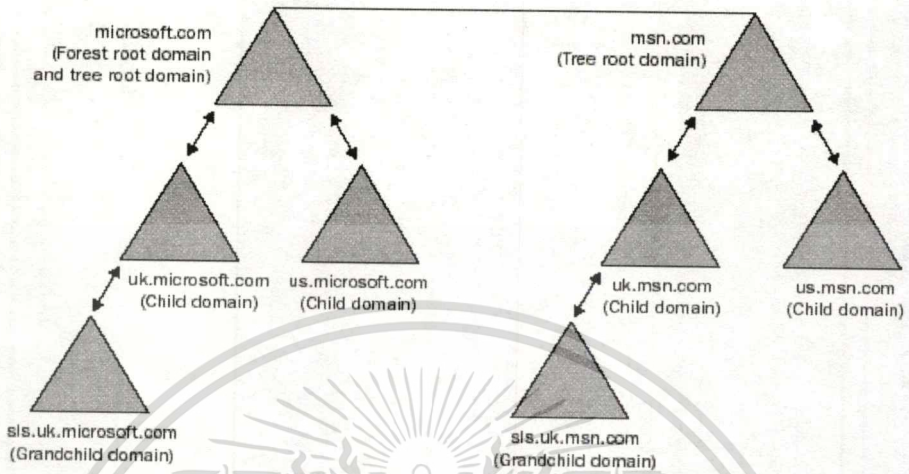
Security principals การกำหนดนโยบายของความปลอดภัยระหว่างโดเมน

Group policy and access control การควบคุมโดยกำหนดในระดับโดเมน ไม่ใช่ OUs

Domain Controller hardware and security facilities เครื่อง Domain Controller ที่ดูแลแต่ละโดเมน ถ้าต้องการรองรับ Fault-tolerance ต้องมีอีกหนึ่งเครื่องเป็นอย่างน้อย

Trust links ต้องพิจารณาผู้ใช้ที่ล็อกออนเข้าใช้ระบบ และถ้าลิงค์มีปัญหาจะต้องดูแล หรือบำรุงรักษาอย่างไร

– การสร้างหลายทรี



รูปที่ 2.15 ตัวอย่างแสดงการสร้างหลายทรี

– การสร้างหลายฟอเรสต์
  – เหตุผลการสร้างหลายฟอเรสต์
  – ความปลอดภัยข้อมูล
  – การแยกระบบการเรพพลิเคตรายชื่อ
  – เพื่อสะดวกในการพัฒนา และการทดสอบแล็บ

– การจัดการบทบาท Operations Master

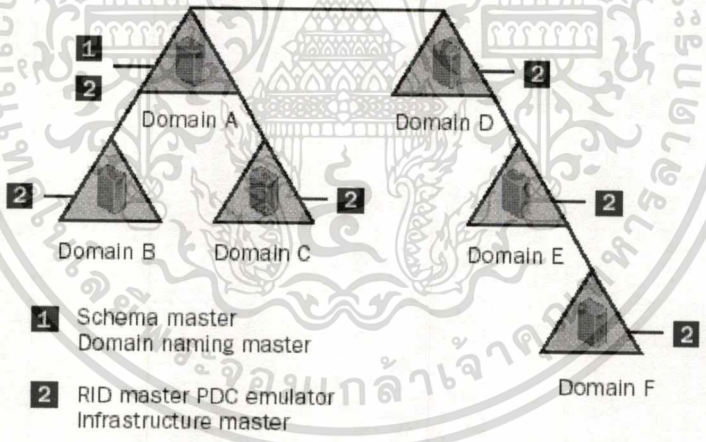
บทบาทของ Operations Master มีหลายบทบาท บางบทบาทมีได้เพียงหนึ่งเดียวเท่านั้นในฟอเรสต์ บางบทบาทมีได้หนึ่งเดียวในโดเมน

บทบาทของ Forest-Wide Operations Master

– Schema master หน้าที่คือทำการอัพเดต Schema ซึ่งจะมีเพียงหนึ่งเครื่องเป็น Master ในฟอเรสต์
– Domain Naming master หน้าที่คือจัดการเกี่ยวกับการเพิ่ม และนำโดเมนออก จะมีหนึ่งเครื่องเป็น Masterในฟอเรสต์

บทบาทของ Domain-Wide Operations Master

- Relative identifier (RID), หรือ Relative ID ทำหน้าที่ในการจัดลำดับ IDs ที่สัมพันธ์กันระหว่าง Domain controllers ต่างๆในโดเมน ซึ่งจะมีเครื่องเดียวที่เป็น Master
- Primary Domain Controller (PDC) emulator ถ้าโดเมนไม่มีเครื่อง Windows Server 2003 client software หรือมี Windows NT backup domain controllers เครื่องนี้จะเป็น PDC emulator role ที่เป็น Windows NT PDC ซึ่งกระบวนการเปลี่ยนรหัสจากเครื่องลูกข่ายจะมีการเรพพลิเคตกับ BDCs ซึ่งจะมีหนึ่งเครื่องที่เป็น Master ใน Domain ถ้าเป็น Windows Server 2003 อย่างเดียวหน้าที่ PDC emulator จะรับเรพพลิเคตรหัสผ่านไปยัง Domain controller อื่นๆในโดเมน
- Infrastructure master รับผิดชอบในการอัพเดตความสัมพันธ์ของกลุ่ม และสมาชิกในกลุ่ม เมื่อมีการเปลี่ยนชื่อในหนึ่งโดเมนจะมีหนึ่งเครื่องเท่านั้นที่เป็น Master เมื่อมีการเปลี่ยนชื่อ หรือย้ายสมาชิก Infrastructure master จะรับผิดชอบในกาอัพเดตค่าข้อมูลให้



รูปที่ 2.16 ตัวอย่างบทบาท Operations Master

การจัดการบทบาท Operations Master

- การโอนถ่ายบทบาท
- สามารถเรียกคำสั่ง Transfer ในชุดเครื่องมือ Active Directory
- การยึดบทบาท Operations Master

- ในกรณีที่เครื่อง Operations Master ไม่ทำงาน และต้องการให้เครื่องหนึ่งเป็น Operation Master ใช้คำสั่ง NTDSutil

การยึดบทบาทจะขึ้นอยู่กับปัญหาต่างๆเหล่านี้

- Schema Master มีปัญหา
- Domain Naming Master มีปัญหา
- RID Master มีปัญหา
- PDC Emulator มีปัญหา
- Infrastructure มีปัญหา

คำสั่งที่ใช้ในการตรวจสอบสถานในการยึดคือ Repadmin

รูปแบบมีดังนี้ Repadmin /showutdvec server2.microsoft.com dc-microsoft,dc=com และ Repadmin /showutdvec server2.microsoft.com dc-microsoft,dc=com

การยึดบทบาทจะใช้คำสั่งใน Ntdsutil

การวางแผนตำแหน่งของ Operations master

- ออกแบบให้มีการแบ่งโหลดการทำงาน
- คอยอัพเกรด และบำรุงรักษาฮาร์ดแวร์อยู่เสมอ
- ในกรณีที่มีโดเมนเดียว Domain Controller หนึ่งจะเป็นทุกบทบาท
- ถ้ามีมากกว่าหนึ่งโดเมน และมีหลาย Domain Controller สามารถเลือกที่กำหนดบทบาทใน Domain กระจายใน Domain Controller ได้
- ในกรณีที่เป็น Forest ต้องตรวจสอบเรื่องของ Schema และการอัพเดพ Schema
- ตรวจสอบการเติบโตของเครือข่าย เพื่อพิจารณา Operation Master

- การจัดการความสัมพันธ์ระหว่างโดเมน (Trust Relationship)
  - เป็นการสร้างความสัมพันธ์ระหว่างโดเมน โดยมีการรับรอง
  - คุณลักษณะมีสามแบบคือ
  - การสร้างด้วยมือ
  - การเป็น Transitive Trusts หรือ Non-Transitive Trusts
  - การกำหนดทิศทางเดียว หรือสองทิศทาง
  - Trust Protocols จะรองรับ Kerberos หรือ NTLM

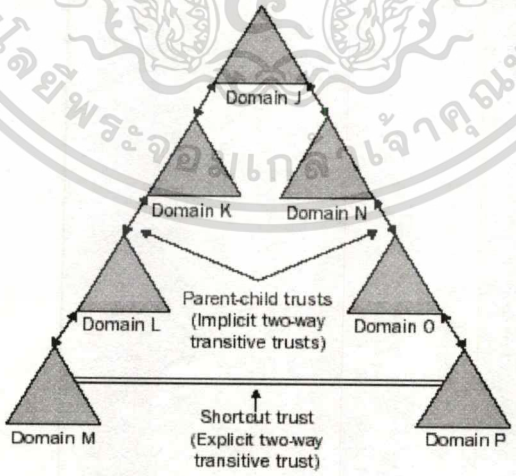
ชนิดของ Trust มี 6 ชนิด คือ Tree-root trust, Parent-child trust, Shortcut trust, Realm trust, External trust, Forest trust

เข้าใจเกี่ยวกับ Forest Trusts

- ทำให้การจัดการง่าย
- เป็นการทำ Trust แบบสองทิศทางในทุกโดเมนในสอง Forests
- UPN authentications สามารถข้ามระหว่างสองฟอเรสต์
- ทั้ง Kerberos และ NTLM authentication protocols สามารถที่ใช้ได้
- ทำให้การบริหารงานนั้นยืดหยุ่น

การวางแผน Trust Relationship มี Trust อยู่ 4 ประเภทที่ต้องการจัดการ

- Shortcut trusts
- Realm trusts
- External trusts
- Forest trusts



รูปที่ 2.17 Shortcut Trust

ผู้บริหารระบบสามารถกำหนด One-way Shortcut Trusts หรือ Two-way Shortcut Trusts

การกำหนด Shortcut จะทำให้การวิ่งระหว่าง Domain M กับ Domain P สั้นลง และลดเวลาในการร้องขอลงระหว่งโดเมน

การเข้าใช้ทรัพยากรข้ามโดเมนของ Shortcut Trust จะใช้ Active Directory Domains and Trusts ซึ่งจะมีการพิจารณาระหว่างสองโดเมน โดยดูที่ Selective Authentication ว่าเป็น Outgoing และ Incoming shortcut trusts ซึ่งต้องพิจารณาทั้งสองโดเมน เครื่องมือที่ใช้ในการสร้างคือ New Trust Wizard

การทำ Realm Trust

- เป็นการเชื่อมต่อระหว่างโดเมนที่ไม่รองรับ Windows Kerberos version 5 realm และ Windows Server 2003 domain ตัวอย่างเช่น UNIX หรือ MIT Realm
- สิ่งที่จำเป็น
- ต้องเป็น Enterprise Admins หรือ Domain Admins

การสร้าง External Trust

- เป็นการกำหนด One-way หรือ Two-way
- อยู่นอกขอบเขต Forest
- ใช้การดึงทรัพยากร Windows NT 4.0 หรือโดเมนของฟอเรสต์อื่นๆ
- สิ่งที่จำเป็น

ต้องเป็น Enterprise Admins หรือ Domain Admins

กำหนดรหัสผ่านที่รู้กันทั้งสองฝั่ง

การสร้าง Forest Trust

สิ่งที่ต้องพิจารณามี

- One-way Forest Trusts
- Two-Way Forest Trusts
- การเข้าใช้ทรัพยากรข้ามโดเมนโดย External Trust

- สิ่งที่ต้องการ
    - เป็นสมาชิกกลุ่ม Enterprise Admins ในทั้งสองโดเมน
    - กำหนดรหัสผ่านที่รู้กันทั้งสองฟอเรสต์

การสร้าง Trust Relationship

- ใช้คำสั่ง Active Directory Domains and Trusts
- ใช้คำสั่ง New Trust Wizard กำหนดตามขั้นตอน
- การใช้คำสั่ง Netdom เพื่อทำการ Trust โดยใช้คำสั่ง

2.19 การกำหนดค่าไซต์ และการจัดการเรพพลิเคต

ไซต์ที่กำหนดจะพิจารณาบน Internet Protocol (IP) Subnets ซึ่งต้องพิจารณาลิงค์ ว่ามีความน่าเชื่อถือ และความเร็ว ซึ่งโดยส่วนใหญ่จะเป็น Local Area Network (LAN) และใช้ IP Subnet ในการพิจารณา โดยความเร็วต้องสูงกว่า 128 Kbps และถ้าสูงกว่า 512 Kbps ถือว่ามีลิงค์ความเร็วสูง

2.20 ข้อมูลที่มีการเรพพลิเคต

- Schema Partition
- Configuration Partition
- Domain partition

ในกรณีที่มีชนิดของ Directory partition ใหม่ Application directory partition ที่ใช้ได้ใน Domain controllers ใน Windows Server 2003 operating system พาร์ติดชั่นที่ถูกใช้โดยแอพพลิเคชั่น และบริการที่เก็บข้อมูลที่ระบุ รวมถึงชนิดของออปเจคยกเว้น security principals (Users, groups, และ Computers) Application partition สามารถที่ถูกเรพพลิเคตได้ในกลุ่มของ Domain Controllers บนฟอเรสต์ ไม่จำเป็นต้องอยู่ในโดเมนเดียวกัน เช่น RAS, RADIUS, DHCP, Common Open Policy Service (COPS) เป็นต้อง

บาง Domain controllers ที่เป็น Global Catalog servers จะมีการจัดเก็บบางส่วนของ Directory partition objects จากโดเมนอื่น เพื่อใช้ในการค้นหา ซึ่งบางส่วนนี้จะกำหนดเป็น Read-only ที่เก็บในเครื่องที่รับการเรพพลิเคตโดยแอตทริบิ่วคือ isMemberOfPartialAttributeSet ค่าของ AttributeSchema objects กำหนดเป็น True

2.21 Site Link

- ในการติดต่อข้ามโดเมนจะมีการกำหนดค่า Site links โดยกำหนดเป็น Logical ซึ่งกำหนดระหว่างสองไซต์ หรือมากกว่า โดยการสร้างจะทำให้มีการสร้าง Replication Topology ซึ่งการกำหนนี้ต้องเป็นแบบด้วยมือ
- สรุปการกำหนด Site Link ดังนี้
- เป็นลิงค์ข้ามไซต์
- เป็นการกำหนดทาง Logical ซึ่งกำหนดการเชื่อมต่อ Transitive ระหว่างไซต์
- กำหนดค่าลิงค์ได้เป็น IP หรือ SMTP

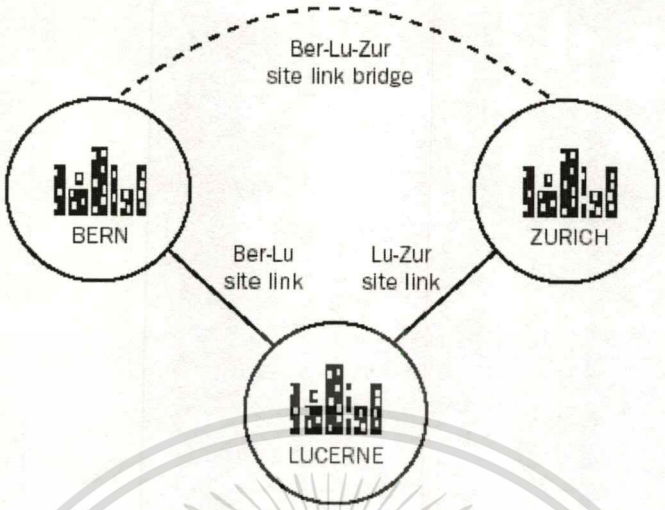
2.22 Site Link Transitivity

- โดยดีฟอลท์จะเป็น Transitive คือเมื่อ Site A-> Site B, Site B-> Site C แล้ว Site A-> Site C
- สาเหตุที่ยกเลิก Transitive
- ต้องการควบคุมการจราจร
- หลีกเลี่ยง Path ที่กำหนดในการเรพพลิเคตเป็นส่วนๆ
- IP network ไม่กำหนดเส้นทางสมบูรณ์

2.23 Site Link Bridges

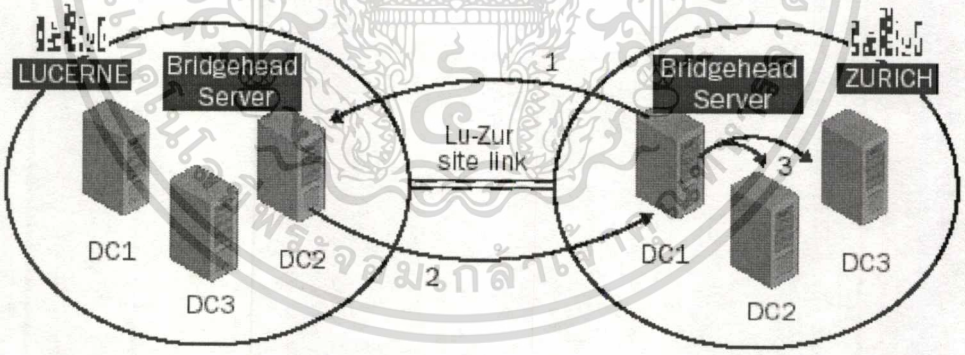
เป็นการลิงค์บน Transport ที่มีการกำหนด Transitive ซึ่งจะสามารถที่ไม่อนุญาต โดยสร้างการกำหนดใน Site link ที่ต้องการ

- เป็นการเชื่อมต่อสองไซต์ หรือมากกว่า
- กำหนดเพื่อสร้าง Transitive และ Logical link ระหว่างไซต์



รูปที่ 2.18 Site Link Bridges

2.24 Bridgehead servers



รูปที่ 2.19 Site Bridgehead servers

เป็นเครื่องที่อยู่ในโดเมนกำหนดให้เรพพลิเคต หรืออัพเดตจากไซต์อื่นๆ กำหนดโดยอัตโนมัติด้วย KCC

2.25 การทำงานของ Intersite Replication

- รอบเวลาที่กำหนด Bridgehead server ใน Zurich จะดึงข้อมูล Bridgehead server ใน Lucerne site เพื่ออัพเดตข้อมู
- ถ้า Bridgehead server ใน Lucerne site มีการอัพเดตข้อมูล Active Directory ที่มีการลดขนาดที่ส่งจาก Zurich Site
- เมื่อ Bridgehead server ใน Zurich site ได้รับข้อมูล ก็จะเรพพลิเคตต่อไปที่ Domain Controllers ต่างๆในไซต์

2.26 Global Catalog Servers

Global Catalog เป็นที่เก็บที่เก็บข้อมูลต่างๆของออปเจคในทรี หรือฟอเรสต์ ซึ่งโดยดีฟอลท์ Global Catalog จะสร้างขึ้นมาบนเครื่องแรกที่เป็น Domain Controller ซึ่งจะมีการเก็ฐออปเจคทั้งหมดในโดเมนที่อยู่ และข้อมูลบางส่วนของตามโดเมน

- มีคีย์หลักสามข้อคือ
  - อนุญาตให้ผู้ใช้ล็อกออนเครือข่ายรองรับสมาชิกใน Universal Group
  - อนุญาตให้ค้นหาข้อมูลรายชื่อ โดยเข้าไปโดเมนในฟอเรสต์
  - แก้ปัญหา User principal names (UPNs) เมื่อมีการตรวจสอบผู้ใช้
- ฟีเจอร์ Universal Group membership Caching

ระหว่างเครือข่ายแบนวิดช์ และ Server ที่มีข้อจำกัดฮาร์ดแวร์ อาจจะไม่มี Global Catalog ในออฟฟิศที่อยู่ทางไกล สามารถใช้ฟีเจอร์ของ Universal Group membership caching ความสามารถนี้เป็นความสามารถใหม่ใน Windows Server 2003 คือไม่ต้องเป็น Global Catalog server แต่เป็น Universal Group membership caching ที่สามารถที่ใช้ล็อกออนโดยไม่มี Global Catalog

โดยทั่วไป Universal Group membership จะมีการเก็บแคชแต่ละ Domain Controller ทุก 8 ชั่วโมง ซึ่งทำได้เฉพาะเครื่องที่เป็น Windows Server 2003 โดยจะส่ง Universal group membership ที่ยืนยันไปที่เครื่อง Global Catalog ซึ่งมีได้ถึง 500 Universal group memberships ในการอัพเดตต่อครั้ง

ข้อดีของการใช้ Universal group membership ในออฟฟิศที่อยู่ไกล

- ล็อกออนได้เร็ว เพราะว่าเครื่อง Domain Controllers จะไม่ต้องไปหา Global Catalog
- ไม่จำเป็นต้องอัพเกรดฮาร์ดแวร์ ใช้ Domain Controllers ที่มีอยู่เดิมในการรับความต้องการระบบเพิ่มสำหรับ Hosting a global catalog

– ลดการใช้แบนวิดช์ของเครือข่ายลง

2.27 OUs

Organizational Unit หรือที่เรียกว่า OU เป็นที่เก็บข้ออปเจค ในการจัดโครงสร้างออปเจค ซึ่งมีการจัดกลุ่มเพื่อบริหารงานเชิง Logical

– เหตุผลในการกำหนด OU

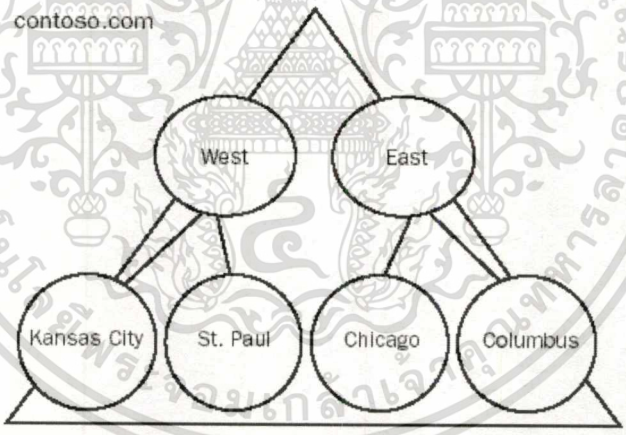
– การกำหนด OUs เพื่อแต่งตั้งผู้บริหารระบบ

– การกำหนด OUs เพื่อบริการ Group Policy

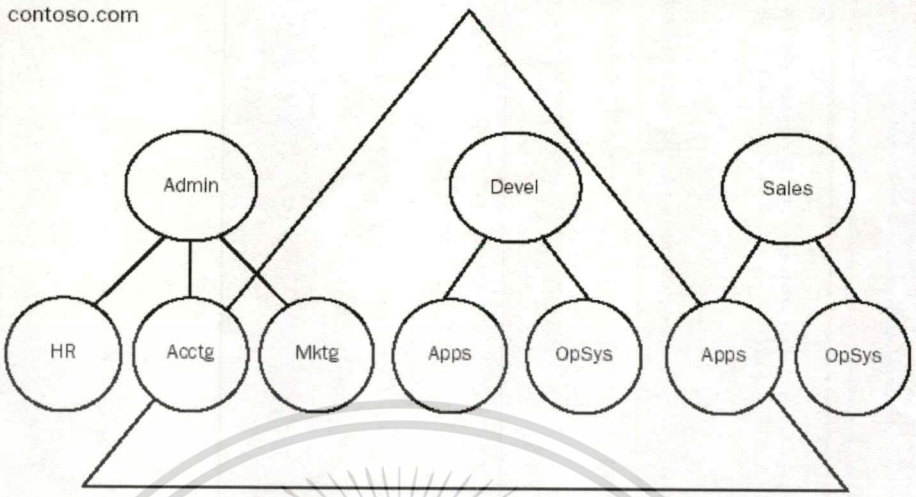
– การกำหนดเพื่อซ่อนออปเจค

– การกำหนด OUs เพื่อแต่งตั้งผู้บริหารระบบ

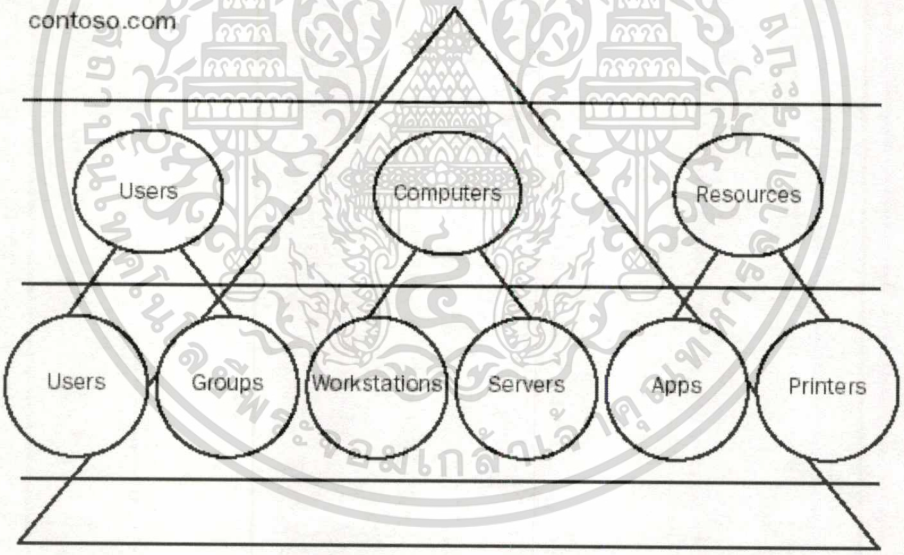
ผู้กำหนดสามารถที่กำหนด Access Control List ในแต่ละออปเจคของ OUs ได้ทำให้เกิดรูปแบบการบริหารงานเป็นลำดับชั้น โดยรูปแบบมีดังนี้



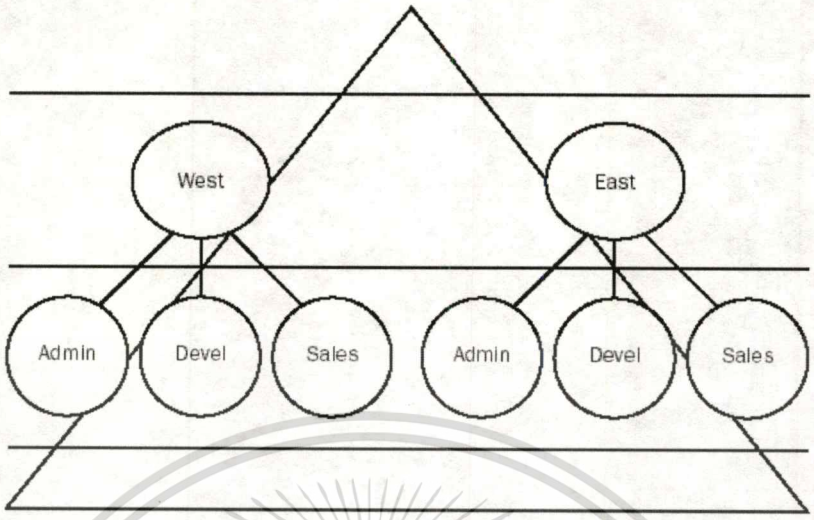
รูปที่ 2.20 การออกแบบOUs ตาม Location



รูปที่ 2.21 การออกแบบOUs ตาม Business Function



รูปที่ 2.22 การออกแบบOUs ตาม Object Type



รูปที่ 2.23 การออกแบบOUs แบบรวมกัน

– การกำหนด OUs เพื่อบริการ Group Policy

Group Policies เป็นที่เก็บค่าติดตั้งของผู้ใช้ และเครื่องคอมพิวเตอร์ ซึ่งจะสามารถลิงค์กับ Computers, Sites, Domains, และ OU เพื่อกำหนดค่าผู้ใช้ หรือเครื่องผู้ใช้ โดยจัดเก็บ Group Policy Objects

– การกำหนดเพื่อซ่อนออปเจค

ในองค์กรอาจจะมีออปเจคบางอย่างที่ต้องการซ่อนระหว่าง OUs ซึ่งไม่ต้องการให้ผู้ใช้เห็นที่เก็บที่อยู่ใน OU ที่สูงกว่า หรือระดับเดียวกัน การกำหนดนี้ต้องมีการพิจารณา Permissions ด้วย

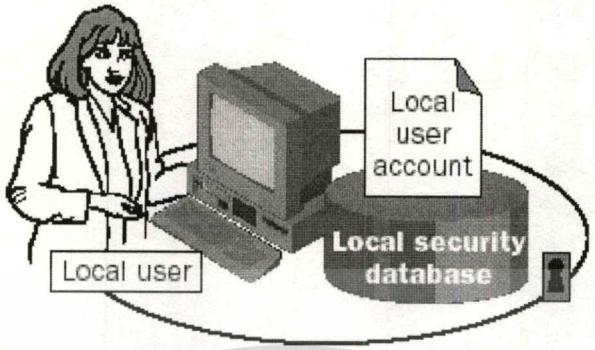
2.28 สิ่งที่ควรเข้าใจใน User accounts

User Account เป็นเรคคอร์ดที่ประกอบด้วยข้อมูลต่างๆที่กำหนดเป็นผู้ใช้ ร่วมถึง User Name, Password ที่กำหนดในการล็อกออน สมาชิกของกลุ่ม และ Permissions ต่างๆ ซึ่งเมื่อผู้ใช้มีการตรวจสอบจะได้รับสิทธิในการเข้าใช้ทรัพยากร การตรวจสอบเรียกว่า Authentication การใช้งาน ใน Windows Server 2003 ที่มีการจัดโครงสร้างเป็นลำดับชั้นทำให้ใช้ทรัพยากรต่างๆในโดเมนอื่นๆได้ เป็นผลให้ผู้ใช้ล็อกออนเพียงครั้งเดียว

ชนิดของ User Account

– Local User accounts

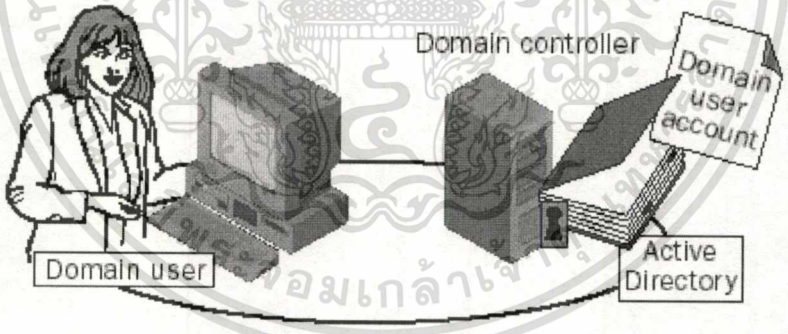
เป็นผู้ใช้ที่ล็อกออนบนเครื่อง และใช้ทรัพยากรในเครื่องที่ใช้นั้นๆ ฐานข้อมูลถูกจัดเก็บไว้ในเครื่องนั้น ๆ ผู้ใช้ที่สร้างในเครื่องนั้นๆจะไม่มีผลต่อการใช้งานทรัพยากรในโดเมน



รูปที่ 2.24 Local User accounts

– Domain User accounts

เป็นผู้ใช้ที่ล็อกออนในเครื่อง Domain Controller และได้รับสิทธิในทรัพยากรของโดเมนที่กำหนด โดยรองรับตั้งแต่ Windows NT Domain, Windows 2000, และ Windows Server 2003 โดยใน Windows Server 2000 และ Windows Server 2003 เรียกว่า Active Directory



รูปที่ 2.25 Domain User accounts

– Built-in User account

เป็นผู้ใช้ที่ระบบสร้างขึ้นมาในการติดตั้ง Windows Server 2003 เช่น Administrator และ Guest

Administrator เป็นผู้ใช้ที่สามารถจัดการเครื่อง และทรัพยากรต่างๆในโดเมนได้หมด ไม่ว่าจะเป็นการสร้าง แก้ไข ลบ หรือกำหนดนโยบายต่างๆ ซึ่งการใช้งานแนะนำให้เปลี่ยนชื่อ Administrator เพื่อป้องกันการเดารายชื่อในการล็อกออน ถ้าเป็นไปได้ควรแยก User ทั่วไปกับ

Administrator ออกจากกัน เพื่อความปลอดภัย โดยงานที่ไม่เกี่ยวกับงานบริหารให้ใช้ User ทั่วไปที่สร้างขึ้น

Guest เป็นชื่อที่สร้างในโดเมนไม่มีสิทธิในการล็อกออน โดยทั่วไปจะถูกกำหนดไม่ให้ใช้ Guest account ไม่ต้องกำหนดรหัสผ่านในการเข้าใช้ถ้ามีการ Enable

Administrator กับ Guest ไม่สามารถลบได้

- ชื่อที่กำหนดใน Domain User account
  - พิจารณาว่า User account ที่สร้างเป็น Local หรือ Domain
  - เลือกผู้ใช้ว่าจะใช้ชื่อล็อกออนอย่างไร โดยกำหนด DN ไม่ซ้ำกัน และข้อมูลกำหนดที่ใช้ในการค้นหา (RDN) ได้อย่างดี
  - พิจารณาอักขระที่ใช้ในชื่อล็อกออน กำหนดได้ถึง 20 อักขระ ถ้ายาวกว่านี้ก็จะใช้เพียง 20 อักขระ อักขระที่ใช้ไม่ได้เช่น / \ [ ] : ; | = , + * ? < > @ ในชื่อที่ล็อกออนไม่ Case Sensitive แต่จะรักษาตัวเล็กตัวใหญ่ไว้ให้
  - พิจารณาอักขระที่ใช้งานได้การป้องกันชื่อที่ซ้ำซ้อน โดยอาจจะใช้นามสกุลตัวอักขระแรก หรือหมายเลข เป็นต้น
  - ระบุชนิดของ User เช่นพนักงานประจำใช้ชื่อปกติ พนักงานชั่วคราวขึ้นต้นด้วย T-เป็นต้น
  - กำหนดให้รองรับกับ e-mail system
- การสร้าง และการจัดการผู้ใช้

Active Directory ต้องการตรวจสอบแยกผู้ใช้แต่ละคน ซึ่งกระบวนการนี้เรียกว่าการรับรองการเข้าใช้ (Authentication) โดยสิ่งที่ใช้ในการตรวจสอบคือชื่อผู้ใช้ รหัสผ่าน ซึ่งค่าที่ตรวจสอบจะพิจารณา Security Identifier (SID) ซึ่งมีเพียงหนึ่งเดียวเท่านั้น ระหว่างการล็อกออกระบบจะมีการสร้างโทเก็นที่เข้าใช้เป็นตัวแทนผู้ใช้ ซึ่งโทเก็นที่เข้าใช้นี้จะเก็บค่า SID ของผู้ใช้ หรือเป็นตัวแทนผู้ใช้ และจะสามารถใช้ยืนยันสิทธิที่กำหนด รวมถึงสิทธิที่ล็อกออนบนเครื่องที่ใช้ ไปถึงระบบ และการรับรองในทรัพยากรที่ตรวจสอบใน Access Control Lists (ACLs)

ผู้ใช้ที่ใช้กับ Active Directory user object จะไม่เพียงแต่มีชื่อผู้ใช้ รหัสผ่าน และ SID แต่ยังมีข้อมูลอื่นๆอีกเช่น หมายเลขโทรศัพท์ การรายงาน หรือสมาชิกของกลุ่ม, Roaming profiles, Terminal services, remote access, และค่าติดตั้งระบบอื่นๆ

เครื่องมือที่ใช้ในการสร้างผู้ใช้ใน Active Directory คือ Active Directory Users and Computers snap-in ซึ่งจะเป็นการสร้างออปเจคผู้ใช้ในโดเมน และจะมีโครงสร้างออปเจค และที่

จัดเก็บตามดีฟอลท์อยู่แล้ว ซึ่งสิ่งที่แนะนำหลังจากนี้คือการสร้างที่จัดเก็บเองเรียกว่า Organizational Unit ซึ่งสิ่งนี้สามารถที่แต่งตั้งผู้ดูแล และกำหนด Group Policy Objects (GPOs) เพื่อควบคุมระดับนโยบายได้

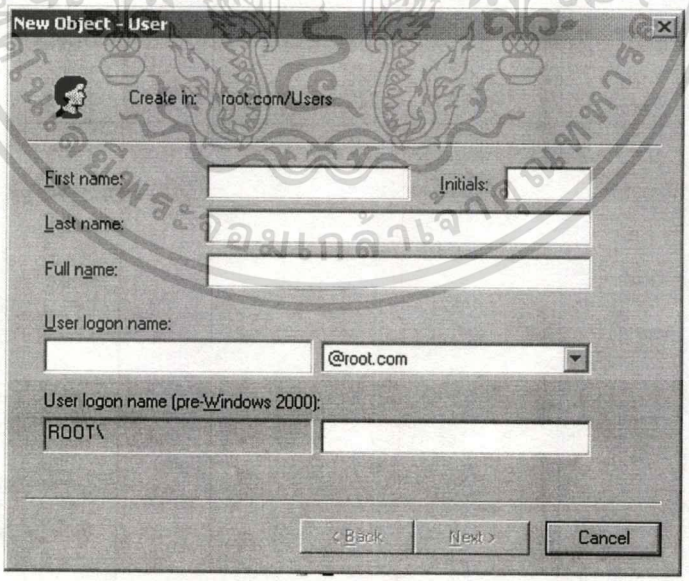
2.29 การสร้างออปเจค

สามารถทำได้ด้วยกันทั้งจาก Action Menu, Shortcut menu, หรือ Toolbar โดยการสร้างออปเจคผู้ใช้ได้นี้ผู้สร้างต้องเป็นสมาชิกกลุ่ม Enterprise Admins, Domain Admins, หรือ Account Operators หรือผู้ใช้/กลุ่มที่ได้รับการแต่งตั้งขึ้นมากเพื่อให้บริหารในที่เก็บนั้นๆ ซึ่งถ้าผู้สร้างไม่มีสิทธิในการสร้างออปเจคใดๆก็จะเห็นเป็นคำสั่งลางๆ หรือปุ่มสีเทา

เมื่อมีการเรียกคำสั่ง New -> User ก็จะปรากฏรายการไดอะล็อกบ็อกซ์ที่ให้ใส่ข้อมูลอยู่สองขั้นตอนใหญ่ๆคือ

- User Properties
- Password Properties

เมื่อกำหนดรายละเอียดใน User Properties เรียบร้อยแล้วคลิกที่ Next ก็จะที่รายละเอียดรหัสผ่าน

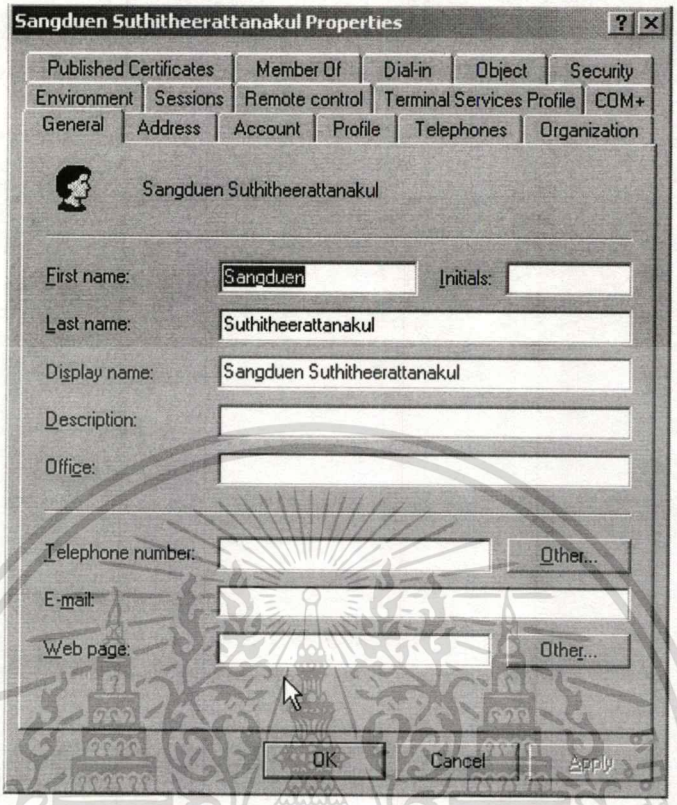


รูปที่ 2.26 การสร้างออปเจค

ตารางที่ 2.1 แสดงรายละเอียด User Properties

คุณสมบัติ	คำอธิบาย
First Name	เป็นชื่อของผู้ใช้ ไม่ต้องใส่ก็ได้
Initials	เป็นชื่อกลางผู้ใช้ ไม่ต้องใส่ก็ได้
Last Name	เป็นนามสกุลผู้ใช้ ไม่ต้องใส่ก็ได้
Full Name	เป็นชื่อเต็มผู้ใช้ ถ้ามีค่าที่กำหนดสำหรับ First หรือ Last name ก็จะปรากฏใน Full name โดยอัตโนมัติ สามารถแก้ไขปรับเปลี่ยนค่าได้ ชื่อที่ใส่จะเป็นค่าส่วนหนึ่งของ CN (Common name), DN (Distinguished name), ชื่อ, และชื่อที่แสดง เพราะว่า CN ต้องมีหนึ่งเดียวในที่จัดเก็บ ชื่อต้องหนึ่งเดียวในทุกออปเจคใน OU (หรือที่จัดเก็บอื่นๆ) เมื่อมีการสร้างออปเจคขึ้น
User Logon Name	เป็นชื่อที่ใช้ในการล็อกออนตาม User Principal Name (UPN) ซึ่งจะมีการต่อท้าย UPN โดยชื่อ DNS ที่กำหนดจะสร้างออปเจคนี้ขึ้นรูปแบบคือ logon-name@UPN-suffix
User Logon Name (Pre-Windows 2000)	เป็นชื่อที่ใช้ล็อกออนบนเครื่องลูกข่ายที่ต่ำกว่าเช่น Microsoft Windows 95, Windows 98, Windows ME, Windows NT 4, 3.51 ซึ่งจะมีเพียงหนึ่งเดียวในโดเมน

การจัดการออปเจคด้วย Active Directory Users and Computers



รูปที่ 2.27 การจัดการออปเจคด้วย Active Directory Users and Computers

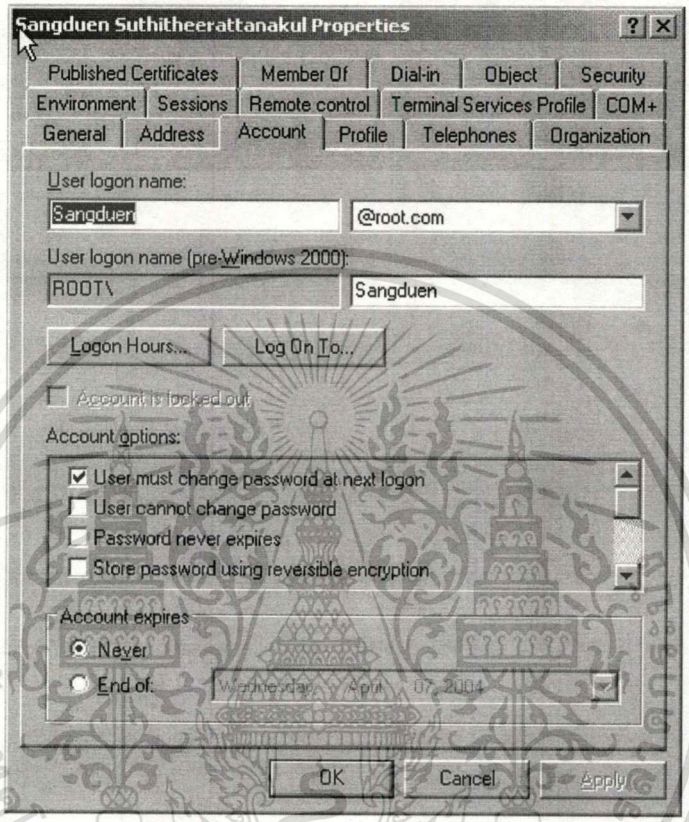
เมื่อสร้างผู้ใช้เรียบร้อยแล้ว เราสามารถที่ปรับเปลี่ยนค่าต่างๆที่กำหนดได้โดยใช้ Active Directory Users and Computers เพื่อกำหนดคุณสมบัติออปเจค โดยคลิกเลือกออปเจคที่ต้องการ-> คลิก Action menu -> Properties หรือจะคลิกขวาที่ออปเจค และเลือก Properties ใน Shortcut menu ก็ได้

- รายละเอียดต่างๆที่กำหนดแบ่งหน้าที่ได้ดังนี้
- รายละเอียดข้อมูลทั่วไป เพื่อใช้ในการค้นหา เช่นที่อยู่ หมายเลขโทรศัพท์ที่ติดต่อ เป็นต้น
- รายละเอียดของ User Account เช่น User Profiles หรือออปชั่นของผู้ใช้กับรหัสผ่าน
- รายละเอียด Dial-up เป็นการกำหนดอนุญาต หรือไม่อนุญาตให้ใช้งานเป็นต้น
- รายละเอียดเกี่ยวกับสมาชิก เพื่อใส่สมาชิกในกลุ่ม
- รายละเอียดแอพพลิเคชั่น เช่น Terminal Service, Remote Desktop และอื่นๆ

ตารางที่ 2.2 รายการที่กำหนดจะเป็นแท็บต่างๆดังนี้

แท็บ	คำอธิบาย
General	เป็นรายละเอียดข้อมูลทั่วไปเกี่ยวกับผู้ใช้
Address	เป็นรายละเอียดที่อยู่ซึ่งจะมีที่อยู่ และหมายเลขโทรศัพท์ที่ใช้ติดต่อ
Account	เป็นค่าที่กำหนดเกี่ยวกับระบบเช่น ชื่อที่ล็อกออน เครื่องที่ล็อกออน เวลาที่ล็อกออน วันหมดอายุ และออปชั่นในรหัสผ่าน
Profile	ใช้กำหนดค่า Roaming Profile, Home directory, และการอ่าน Logon script
Telephones	เป็นรายละเอียดเกี่ยวกับหมายเลขโทรศัพท์ที่ใช้ติดต่อ
Organization	เป็นรายละเอียดของโครงสร้างหน่วยงาน
Remote Control	เป็นการกำหนดค่าควบคุมกับแอพพลิเคชั่นที่ใช้ในการควบคุมจากทางไกล
Terminal Services Profile	เป็นตำแหน่งโฟลเดอร์ที่ให้ใช้เมื่อมีการล็อกออนผ่าน Terminal Service ที่เครื่องลูกข่าย
COM+	เป็นรายละเอียดของแอพพลิเคชั่นที่ให้รองรับกับผู้ใช้ที่ระบุนี้
Member Of	ใช้กำหนดกลุ่มสมาชิกในองค์กร
Dial-in	ใช้ระบุการติดต่อหมุนผ่านโทรศัพท์เข้ามาใช้งาน
Environment	เป็นการควบคุมค่าที่เข้าใช้เมื่อล็อกออนเข้ามาใช้ในระบบ
Sessions	เป็นการกำหนดเซสชั่นค่าต่างๆที่เข้ามาใช้ในระบบ

รายละเอียดของ Account มีดังนี้



รูปที่ 2.28 รายละเอียดของ Account

ในรายการคุณสมบัติของผู้ใช้ในแท็บ Account จะมีค่าที่กำหนดคุณสมบัติเพิ่มเติมในผู้ใช้ที่ระบุ ซึ่งจะมีรายการดังนี้

ตารางที่ 2.3 รายการคุณสมบัติของผู้ใช้ในแท็บ Account

คุณสมบัติ	คำอธิบาย
User logon name	ชื่อที่ใช้ในการล็อกออนในระบบปฏิบัติการ Windows Server 2003
User logon name (Pre-windows 2000)	ชื่อที่ล็อกออนสำหรับลูกข่ายเก่า เช่น Windows 9x, Windows NT
Logon Hours	เป็นการกำหนดชั่วโมงในการล็อกออน ที่อนุญาตให้ใช้ในเครือข่าย

คุณสมบัติ	คำอธิบาย
Log On To	เป็นการจำกัดเครื่องที่ผู้ใช้ล็อกออน โดยเครื่องที่ใช้ต้องรองรับ NetBIOS over TCP/IP
Store Password using reversible encryption	เป็นออปชั่นที่เก็บรหัสผ่านใน Active directory โดยปราศจากการใช้ความสามารถที่ดีของ Active Directory , nonreversible encryption hashing algorithm, ที่มีอยู่สำหรับแอพพลิเคชั่นที่รองรับโดยต้องการรู้เกี่ยวกับรหัสผ่าน ถ้าไม่ต้องการอย่างแท้จริง ไม่อนุญาตออปชั่นนี้เพราะจะทำให้รหัสผ่านอ่อนแอ รหัสผ่านที่เก็บโดยใช้การเข้ารหัส Reversible จะเก็บการจัดเก็บเป็น Plaintext ลูกข่าย Macintosh ใช้ AppleTalk protocol ที่ต้องการรู้รหัสผ่านผู้ใช้ ถ้ามีผู้ใช้ล็อกออนบน Macintosh จะต้องเลือกออปชั่นนี้
Smart card is required for Interactive logon	เป็นการนำระบบฮาร์ดแวร์เข้าไปประกอบกับข้อมูลของผู้ใช้ ซึ่งจะต้องแทรกส่วนประกอบที่เป็นกายภาพในการรับรองผู้ใช้ที่ต้องการ
Account is trusted for delegation	ออปชั่นนี้อนุญาตให้ service account ปอลมเป็นผู้ใช้เข้าใช้ทรัพยากรในเครือข่ายเป็นผู้ใช้ ซึ่งออปชั่นนี้ไม่ถูกเลือก เพราะไม่แน่ใจว่าออปเจคผู้ใช้นั้นเป็นคนนั้นหรือไม่ นิยมใช้กับ three-tier (หรือ Multi-tier) application infrastructure
Account expires	ใช้ควบคุมผู้ใช้ที่มีการระบุวันหมดอายุ

การจัดการคุณสมบัติของผู้ใช้หลายคนพร้อมกัน

Windows Server 2003 อนุญาตให้มีการแก้ไขผู้ใช้หลายคนได้พร้อมๆกัน โดยให้ใช้คีย์ CTRL เลือกผู้ใช้แต่ละคนที่ต้องการกำหนดออปชั่นร่วมกัน เมื่อเลือกแล้วให้คลิกที่ Action menu -> Properties ซึ่งค่าที่กำหนดได้จะมีดังนี้

ตารางที่ 2.4 คุณสมบัติของผู้ใช้หลายคนพร้อมกัน

แท็บ	คำอธิบาย
General	Description, Office, Telephone Number, Fax, Web Page, E-mail
Account	UPN suffix, Logon hours, Computer Restrction (logon workstations), all account Options, Account expires
Address	ถนน, PO Box, City, State/Province, ZIP/Postal Code, Country/Region

แท็บ	คำอธิบาย
Profile	Profile Path, Logon Script, และ Home Folder
Organzation	Title, Department, Company, Manager

– การย้ายผู้ใช้

ถ้ามีการโอนถ่ายระหว่างองค์กร อาจจะจำเป็นที่ต้องมีการย้ายออปเจคผู้ใช้ ซึ่งส่งผลให้การบริหารงาน และมีผลต่อค่ากำหนดคุณสมบัติออปเจคได้ เครื่องมือที่ใช้คือ Active Directory Users and Computers ซึ่งรองรับการย้ายได้ทั้ง Drag and Drop, คำสั่ง Move ใน Action menu หรือใน Shortcut menu

– การสร้าง และการจัดการผู้ใช้หลายคน

บางครั้งเราต้องการสร้างผู้ใช้หลายคนอย่างรวดเร็ว เนื่องจากมีพนักงาน หรือนักเรียนเข้ามามากในองค์กร จึงต้องทราบถึงวิธีการสร้างผู้ใช้โดยอัตโนมัติ และมีประสิทธิภาพที่สุด ซึ่งเครื่องมือที่เราสร้างผู้ใช้คือ Active Directory Users and Computers ในครั้งนี้เราจะให้ผู้สร้างใช้เครื่องมือในการสร้างเหมือนเดิม แต่จะให้สร้างเป็น Template ขึ้น นอกจากนี้ยังให้รู้จักเครื่องมือในการนำข้อมูลเข้า และการใช้สคริปต์เพื่อจัดการออปเจค

– การสร้างผู้ใช้จาก Templates

ถ้าเรามีการสร้างออปเจคที่มีคุณสมบัติคล้ายๆกัน เราสามารถที่จะสร้างออปเจคทั่วไปก่อน และใช้ออปเจคนี้เป็นต้นแบบหรือ Template ซึ่งใช้หลักการก๊อปปี้ข้อมูลจาก Template นี้ไปเป็นผู้ใช้ใหม่ แต่ก่อนที่จะสร้าง User template ผู้สร้างต้องทำการกำหนดข้อมูลที่ใช้บ่อยๆก่อน และกำหนดกลุ่มที่เหมาะสม

การสร้างผู้ใช้ Template ให้เลือกผู้ใช้ที่เป็นต้นแบบ และเลือกคำสั่ง Copy จาก Action menu หรือ Shortcut menu และกำหนดข้อมูลผู้ใช้ใหม่ได้แก่ ชื่อ นามสกุล ชื่อกลาง ชื่อล็อกออน รหัสผ่าน หรือออปชั่นผู้ใช้ ซึ่งค่าข้อมูลที่ก๊อปปี้มาได้มีดังนี้

ตารางที่ 2.5 คุณสมบัติของผู้ใช้ที่สร้างจาก Template

แท็บ	คำอธิบาย
General	ไม่มีข้อมูลก๊อปปี้มา
Address	ทุกคุณสมบัติยกเว้นถนน
Account	ทุกคุณสมบัติยกเว้น ชื่อล็อกออน, ซึ่งจะขึ้นให้ใส่ขณะที่ก๊อปปี้

แท็บ	คำอธิบาย
Profile	ทุกคุณสมบัติ และทำการกำหนดตำแหน่งที่แก้ไขตามชื่อผู้ใช้ที่กำหนดใหม่
Telephones	ไม่มีข้อมูลก๊อปปี้มา
Organization	ทุกคุณสมบัติยกเว้นตำแหน่ง
Member Of	ทุกคุณสมบัติ
Dial-in Environment, Sessions, Remove Control, Terminal Services Profile, COM+	ไม่มีข้อมูลก๊อปปี้มา

– คำสั่งที่ใช้นำออปเจคด้วย CSVDE

คำสั่ง CSVDE เป็นเครื่องมือที่ใช้ในการนำข้อมูลเข้า และข้อมูลออกใน Active Directory โดยใช้ "," ในการแยกข้อมูล ซึ่งทำให้เราสามารถที่ดู และแก้ไขข้อมูลได้ง่ายด้วย Notepad หรือ Excel ซึ่งรูปแบบคำสั่งมีดังนี้

Csvde [-i] [-f FileName] [-k]

-I : เป็นการระบุโหมดในการนำข้อมูลเข้า ถ้าไม่ระบุดีฟอลท์จะเป็นการนำข้อมูลออก

-f ชื่อไฟล์: เป็นการระบุชื่อไฟล์ที่ต้องการนำข้อมูลเข้า หรือนำข้อมูลออก

-k: เป็นการละเลยถ้าออปเจคมีอยู่แล้ว หรือมีปัญหาขึ้นระหว่างนำข้อมูลเข้า หรือมีคุณสมบัติที่กำหนอยู่แล้ว ระหว่างที่ดำเนินการนำข้อมูลเข้า โดยให้กระบวนการทำงานต่อไป

การนำไฟล์ที่มี , คั่น (*.csv หรือ *.txt) ในบรรทัดแรกจะมีรายการ Lightweight Directory Access Protocol (LDAP) ที่กำหนดในการนำเข้มูลเข้า ซึ่งในแต่ละออปเจคจะต้องมีค่ารายการนี้เสมอ ตัวอย่างเช่น

CN,FirstName,SurName,Description

FirstUserLogonName,1stUserFirstName,1stUserSurname,Manager

SecondUserLogonName,2ndUserFirstName,2ndUserSurname,President

หรือ

DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName

"CN=Scott Bishop,OU=Employees, DC=Contoso,DC=com", user, sbishop, Bishop, Scott, scott.bishop@contoso.com

ซึ่งในไฟล์นี้จะนำข้อมูลออปเจคผู้ใช้นี้ไปอยู่ใน OU ที่ชื่อ Employees ชื่อ Scott Bishop โดยค่าต่างๆจะถูกกำหนด และให้ออปเจคนี้ถูก Disabled ในขณะที่รหัสผ่านจะรีเซต เมื่อมีการ Enable ผู้ใช้นี้

คำสั่ง CSVDE สามารถดูวิธีการใช้งานได้จากภาคผนวก หรือเข้าไปดูใน Windows Server 2003 Help and Support Center ซึ่งคำสั่งที่ใช้อีกคำสั่งที่น่าสนใจคือ LDIFDE ซึ่งเป็นการนำข้อมูลเข้า และออกในรูปแบบ LDAP โดยโครงสร้างเข้าใจได้โดยง่าย

– เครื่องมือที่ใช้ในการจัดการ Active directory

คำสั่งที่ใช้ในการจัดการ Windows Server 2003 ที่มีศักยภาพมีเครื่องมือที่น่าสนใจต่างๆดังนี้

ตารางที่ 2.6 คำสั่งที่ใช้ในการจัดการ Windows Server 2003

คำสั่ง	คำอธิบาย
DSADD	เป็นการเพิ่มผู้ใช้ใน Active Directory
DSGET	เป็นการแสดงข้อมูลคุณสมบัติของออปเจคใน Active Directory
DSMOD	เป็นการแก้ไขคุณสมบัติของออปเจคที่มีอยู่ในรายการ
DSMOVE	เป็นคำสั่งที่ใช้ย้ายที่เก็บใหม่
DSRM	เป็นการนำออปเจคออก หรือนำข้อมูลซับทรีออก หรือทั้งคู่
DSQUERY	เป็นการค้นหา Active directory สำหรับการกำหนดค่าที่ตรงกับเงื่อนไข โดยคำสั่งนี้จะใช้ร่วมกับการสร้างออปเจค ซึ่งใช้ Piped เพื่อใช้จัดการ หรือแก้ไขข้อมูล

– เครื่องมือต่างๆเหล่านี้จะมีส่วนประกอบหลักดังนี้

  – ชนิดออปเจคเป้าหมาย เป็นหนึ่งในค่าที่กำหนดเพื่อบอกกลุ่มออปเจคใน Active Directory ตัวอย่างเช่น Computer, User, OU, Group, Server (หมายถึง Domain Controller)
  – ระบุออปเจคเป้าหมาย กำหนดชื่อที่ไม่ซ้ำเรียกว่า DN ซึ่งจะใช้กำหนดออปเจคหรือตำแหน่งที่ต้องการใน Active Directory Forest ตัวอย่างเช่น CN=Dan Holme, OU=Employees, DC=Contos, DC=Com
  – Server เป็นการระบุเครื่อง Domain Controller ที่ต้องการสั่งงาน

– User เป็นการระบุผู้ใช้ และรหัสผ่าน ซึ่งจะใช้ในการรันกรณีที่ไม่ได้ล็อกออนด้วย Administrator

การสวิตช์ และพารามิตเตอร์จะไม่พิจารณาตัวอักษรเล็กใหย่ และสามารถที่ใส่ร่วมกับ "–" หรือ "/" ได้

รูปแบบคำสั่งต่างๆเหล่านี้เราสามารถที่ค้นหาได้จาก Windows Server 2003 Help and Support Center โดยใช้เครื่องมือ Search พิมพ์คำสั่งต้องการค้นหา และคลิก Search เมื่อพบหัวข้อที่ต้องการก็ดับเบิ้ลคลิกเข้าไปดูได้

– การใช้คำสั่ง DSQUERY

เป็นคำสั่งที่ใช้ค้นหา Active Directory สำหรับกรณีที่ตรงกับเงื่อนไขที่ต้องการ

รูปแบบคำสั่งมีดังนี้

dsquery user [{StartNode | forestroot | domainroot}] [-o {dn | rdn | upn | samid}] [-scope {subtree | onelevel | base}] [-name Name] [-desc Description] [-upn UPN] [-samid SAMName] [-inactive NumberOfWeeks] [-stalepwd NumberOfDays] [-disabled] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]

ตารางที่ 2.7 DSQUERY พารามิเตอร์

พารามิเตอร์	คำอธิบาย
สโคปที่ค้นหา	
Object_type	ต้องระบุ เป็นการนำเสนอชนิดของออปเจค ซึ่งใช้ในการค้นหา เช่น Computer, Contact, Group, OU, Server, User หรือ * ซึ่งผู้ระบุต้องเจาะจงชนิดที่ต้องการลงไป
[{StartNode | forestroot | domainroot}]	เผื่อเลือก เป็นการระบุโหนดที่ต้องการเริ่มต้นค้นหา เช่นจาก Forest root, Domain root หรือจากโหนดที่กำหนด DN (StartNode) ถ้ามีการกำหนดใน Forestroot จะค้นหาใน Global Catalog โดยทั่วไปจะค้นหาใน Domainroot

พารามิเตอร์	คำอธิบาย
-scope [subtree | onelevel | base]	เป็นการระบุสโคปที่ค้นหา ซึ่งค่าที่กำหนดซับทีในการค้นหาจากจุดเริ่ม ค่าที่กำหนดในหนึ่งจะหาในลูกจากจุดเริ่มเท่านั้น ซึ่งค่าที่ระบุจะลงไปหนึ่งจาก Start node ถ้าเป็น Forestroot ก็จะหาเพียงหนึ่งในสโคปที่ปรากฏ ซึ่งดีฟอล์ทจะหาในซับทรีที่ใช้
การแสดงผลที่ต้องการ	
-o {dn, rdn, samid}	เป็นการระบุรูปแบบซึ่งเป็นรายการที่ค้นหาพบ โดยนำเสนอออกมา ค่า dn จะเป็น Distinguished name ในรายการ rdn จะแสดงรูปแบบ Relative distinguished name ในแต่ละรายการ ถ้า samid จะแสดง Security Accounts Manager ในรายการ โดยทั่วไปจะเป็นรูปแบบ dn
เงื่อนไขในการค้นหา	
-name Name	เป็นการค้นหาผู้ใช้ที่มีคุณสมบัติตรงกับชื่อที่กำหนด สามารถใช้ * ได้ ตัวอย่างเช่น “Jon*” หรือ “*ith” หรือ “j*th”
-desc Description	เป็นการค้นค่าผู้ใช้ที่มีคุณสมบัติตรงกับ Description โดยสามารถใช้ร่วมกับ * ได้
-upn UPN	เป็นการค้นหาค่าคุณสมบัติที่ตรงกับ UPN
-samid SAMName	เป็นการค้นหา SAM account name ที่ตรงกับ SAMName สามารถใช้กับ * ได้
-inactive NumberOfWeeks	เป็นการค้นหาคนที่ไม่มีการใช้งานเป็นจำนวนกี่สัปดาห์
-stalepwd NumberOfDays	เป็นการค้นหารหัสผ่านที่ไม่มีการเปลี่ยนมาแล้วกี่วัน
-disabled	เป็นการค้นหาผู้ใช้ที่ถูกห้ามใช้
คำสั่งที่ใช้ระบุเครื่อง Domain Controller และผู้ใช้ที่ตรวจสอบ	
{-s Server | -d Domain}	เป็นการต่อเชื่อมกับ Remote server หรือ Domain
-u UserName	เป็นการระบุชื่อผู้ใช้ที่ล็อกออนจากเครื่องอื่น โดยดีฟอลท์ –u ใช้กับชื่อผู้ใช้ที่ล็อกออก ซึ่งมีรูปแบบในการระบุชื่อได้ดังนี้ - User Name ตัวอย่างเช่น Akerit - Domain\User name ตัวอย่างเช่น Root\Akerit - UPN ตัวอย่างเช่น Akerit@root.com

พารามิเตอร์	คำอธิบาย
-p {Password | *}	เป็นการระบุรหัสผ่านที่ใช้ หรือใช้ * สำหรับการที่ให้ขึ้นรหัสผ่านขณะที่เรียกใช้คำสั่ง

ตัวอย่างการใช้งานร่วมกับคำสั่งอื่นๆเช่น DSMOD สามารถที่กำหนดได้ดังนี้

Dsquery user –name Dan* | Dsmod user –disabled yes

ซึ่งเป็นการกำหนดให้ผู้ใช้ที่ขึ้นต้นด้วย Dan ห้ามใช้งาน

– การใช้คำสั่ง DSADD

เป็นคำสั่งที่ใช้ในการสร้างออปเจคใน Active Directory ซึ่งถ้าใช้ DSADD USER จะเป็นการระบุชนิดของออปเจคที่ต้องการคือ User ซึ่งเราสามารถที่ดูรูปแบบคำสั่งได้จาก Windows Server 2003 Help and Support Center ซึ่งจะมีการอธิบายถึงพารามิตเรอีต่างๆที่มากกว่านี้

ตัวอย่างคำสั่ง

Dsadd user UserDN…

พารามิเตอร์ UserDN… สามารถที่ใส่หนึ่ง หรือมากกว่าได้ ซึ่ง DN นี้จะรวมกับช่องว่างและทั้ง DN จะใช้เครื่องหมาย ‘ ‘ ใน UserDN… นี้จะใส่ได้หนึ่งในวิธีดังนี้

– ใช้ piping “|” ในรายการ DNs กับคำสั่งอื่นๆเช่น DSQUERY
– ใช้ piping “|” ในแต่ละคำสั่ง โดยแยกด้วยช่องว่าง
– ปล่อยว่างไว้ และพิมพ์ DN ในแต่ละครั้งโดยคีย์บอร์ด และเคาะ Enter เพื่อใส่ DN กดคีย์ Ctrl+Z และ Enter ถ้าต้องการออกจาก DN สุดท้าย

– รูปแบบคำสั่ง DSADD

dsadd user UserDN [-samid SAMName] [-upn UPN] [-fn FirstName] [-mi Initial] [-ln LastName] [-display DisplayName] [-empid EmployeeID] [-pwd {Password | *}] [-desc Description] [-memberof Group;...] [-office Office] [-tel PhoneNumber] [-email Email] [-hometel HomePhoneNumber] [-pager PagerNumber] [-mobile CellPhoneNumber] [-fax FaxNumber] [-iptel IPPhoneNumber] [-webpg WebPage] [-title Title] [-dept Department] [-company Company] [-mgr Manager] [-hmdir HomeDirectory] [-hmdrv DriveLetter:] [-profile ProfilePath] [-loscr ScriptPath] [-mustchpwd {yes | no}] [-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-

pwdneverexpires {yes | no}] [-acctexpires NumberOfDays] [-disabled {yes | no}] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]

คำสั่ง DSADD USER สามารถที่กำหนดพารามิเตอร์ตามหลังได้ดังนี้

ตารางที่ 2.8 DSADD USER กำหนดพารามิเตอร์

พารามิเตอร์	คำอธิบาย
UserDN	จำเป็น ต้องระบุ Distinguished name ของผู้ใช้ที่เพิ่มลงไป และกำหนดในรูปแบบมาตรฐาน (stdin)
-samid SAMName	เป็นการระบุชื่อ SAM name ที่ไม่ซ้ำกันใน SAM account name ตัวอย่างเช่น Linda ซึ่งค่าที่สร้างจะนำ 20 อักขระแรกจาก Common Name (CN) ของ UserDN มาใช้
-upn UPN	เป็นการระบุชื่อ User Principal name ของผู้ใช้ที่ต้องการเพิ่ม ตัวอย่างเช่น Linda@widgets.microsoft.com
-fn FirstName	ระบุชื่อแรกของผู้ใช้ที่ต้องการเพิ่ม
-mi Initial	ระบุชื่อกลางของผู้ใช้ที่ต้องการเพิ่ม
-ln LastName	ระบุนามสกุลของผู้ใช้ที่ต้องการเพิ่ม
-display DisplayName	ระบุชื่อที่แสดงที่ต้องการเพิ่ม
-empid EmployeeID	ระบุหมายเลขพนักงานที่ต้องการ
-pwd {Password | *}	ระบุรหัสผ่านที่กำหนด ถ้าใช้ * จะเป็นการให้ขึ้นพรอมต์เพื่อใส่รหัสผ่าน
-desc Description	ระบุคำอธิบายของผู้ใช้
-memberof GroupDN …	ระบุ DN ของ Group ที่ต้องการให้ผู้ใช้เป็นสมาชิก
-office office	ระบุตำแหน่งที่อยู่ของออฟฟิศ
-tel PhoneNumber	ระบุหมายเลขโทรศัพท์ผู้ใช้
-email Email	ระบุ E-mail ที่ส่งของผู้ใช้
-hometel HomePhoneNumber	ระบุหมายเลขติดต่อทางบ้านของผู้ใช้
-pager PagerNumber	ระบุหมายเลขเพจเจอร์ของผู้ใช้
-mobile CellPhoneNumber	ระบุหมายเลขโทรศัพท์มือถือของผู้ใช้
-fax FaxNumber	ระบุหมายเลขแฟกซ์ของผู้ใช้
-iptel IPPHoneNumber	ระบุหมายเลขโทรศัพท์ IP ของผู้ใช้

พารามิเตอร์	คำอธิบาย
-webpg WebPage	ระบุเว็บเพจของผู้ใช้
-title Title	ระบุตำแหน่งของผู้ใช้
-dept Department	ระบุแผนกของผู้ใช้
-company Company	ระบุชื่อบริษัทของผู้ใช้
-mgr ManagerDN	ระบุ DN ของผู้จัดการที่ต้องการเพิ่ม
-hmdir HomeDirectory	ระบุตำแหน่ง Home directory ซึ่งจะใช้ Universal Naming Convention (UNC) path ที่ระบุต้องใช้ร่วมกับ –hmdrv ที่กำหนดไดร์ฟด้วย
-hmdrv DriveLetter:	ระบุไดร์ฟที่ใช้ ตัวอย่างเช่น E: ที่ต้องการของผู้ใช้
-profile ProfilePath	ระบุตำแหน่ง Profile ที่ต้องการเพิ่ม
-loscr ScriptPath	ระบุตำแหน่ง Logon script ที่ต้องการเพิ่ม
-mustchpwd {yes | no}	กำหนดให้ผู้ใช้เปลี่ยนรหัสผ่านเมื่อล็อกออนครั้งหน้า ถ้าเลือกเป็น Yes โดยดีฟอลท์ค่าที่กำหนดเป็น No
-canchpwd {yes | no}	ระบุให้ผู้ใช้เปลี่ยนรหัสผ่านได้ตลอดเวลาถ้าเป็น Yes โดยทั่วไปผู้ใช้จะเปลี่ยนรหัสผ่านได้เป็น Yes ค่านี้กำหนดเป็น Yes ถ้าค่าพารามิเตอร์ –mustchpwd กำหนดเป็น Yes
-reversiblepwd {yes | no}	ระบุถ้าผู้ใช้เก็บรหสผ่าน Reversible encryption Yes ถ้าไม่กำหนดเป็น No โดยดีฟอลท์กำหนดให้เป็น No
- pwdneverexpires {yes | no}	ระบุถ้าผู้ใช้ไม่หมดอายุให้เป็น Yes ถ้าไม่เป็น No โดยดีฟอลท์กำหนดเป็น No
-acctexpires NumberOfDays	ระบุจำนวนวันจากปัจจุบัน ถ้าต้องการให้มีวันหมดอายุ ค่าที่กำหนดเป็น 0 หมายถึงหมดอายุในวันนี้ ซึ่งค่าเป็นบวกจะหมดอายุในอนาคต และเป็นลบถ้าค่าที่กำหนดผ่านมาแล้ว ค่าไม่ได้กำหนดจะไม่เคยหมดอายุ ตัวอย่างเช่นค่าที่กำหนดเป็น 0 จะหมดอายุวันนี้ ค่า -5 หมดอายุเมื่อ 5 วันที่ผ่านมา ค่าที่เป็น 5 หมดอายุในอีก 5 วันข้างหน้า
-disabled {yes | no}	ระบุเพื่อให้ผู้ใช้ห้ามใช้งาน ซึ่งถ้าเป็น yes ห้ามใช้ No ไม่ ซึ่งถ้าต้องการให้ Enable ต้องกำหนดเป็น No

พารามิเตอร์	คำอธิบาย
{-s server | -d Domain}	ระบุการต่อเชื่อมกับเครื่อง Server หรือ Domain โดยทั่วไปเครื่องจะถูกกำหนดให้ไปที่ Domain Controller ที่ล็อกออน
-u UserName	เป็นการระบุผู้ใช้ที่ล็อกออนจากเครื่องอื่น โดยทั่วไปจะใช้ผู้ใช้ที่ล็อกออนอยู่ ซึ่งรูปแบบที่กำหนดมีดังนี้ - User Name ตัวอย่างเช่น Akerit - Domain\User name ตัวอย่างเช่น Root\Akerit - UPN ตัวอย่างเช่น Akerit@root.com
-p {Password | *}	เป็นการระบุรหัสผ่านที่ใช้ หรือใช้ * สำหรับการที่ให้ขึ้นรหัสผ่านขณะที่เรียกใช้คำสั่ง
-q	เป็นการไม่แสดงผลออกมา หรือเรียกว่า Quiet mode
{-uc | -uco | -uci }	เป็นการระบุข้อมูลที่นำเสนอเป็น Unicode ซึ่งจะมีการกำหนดรูปแบบดังนี้ - uc เป็นการระบุรูปแบบคำสั่งสำหรับการนำเข้า หรือนำออก ไปที่ Pipe (|) - uco เป็นการระบุรูปแบบคำสั่งสำหรับการนำออก ไปที่ Pipe (|) - uci เป็นการระบุรูปแบบคำสั่งสำหรับการนำเข้า ไปที่ Pipe (|)
/?	เป็นการแสดงความช่วยเหลือใน Command Prompt

ถ้าไม่กำหนดออปเจคเป้าหมายในคำสั่ง จากมาตรฐาน (stdin) ก็จะให้ใส่ค่าจากคีย์บอร์ด ซึ่งให้ใส่รูปแบบมาตรฐานไปเรื่อยๆ ถ้าต้องการยุติให้ใช้ CTRL+Z และเคาะ Enter

ตัวอย่างเช่น "CN=Mike Danseglio,CN=Users,DC=Microsoft,DC=Com"

ถ้าพารามิเตอร์มีหลายค่าให้ใช้เว้นวรรคแยกในรายการ

การระบุ $Username$ (ตัวเล็กใหญ่ไม่สำคัญ) อาจเป็นการแทนที่ด้วยชื่อ SAM account ที่ค่า - email, -hmdir, -profile, and -webpg parameters.

ตัวอย่างเช่น ถ้าชื่อ SAM account เป็น "Denise," พารามิเตอร์ –hmdir สามารถที่เขียนในรูปแบบตามนี้ได้

hmdir\users\Denise\home หรือ hmdir\users\$username$\home

การใช้รหัสผ่านที่แข็งแรงจะช่วยลดความเสี่ยงในเรื่องความปลอดภัย

– การใช้คำสั่ง DSMOD

คำสั่งนี้ใช้แก้ไขคุณสมบัติของออปเจค หนึ่งหรือมากกว่า มีตัวอย่างรูปแบบดังนี้

Dsmod user UserDN … พารามิเตอร์

– รูปแบบคำสั่ง

dsmod user UserDN ... [-upn UPN] [-fn FirstName] [-mi Initial] [-ln LastName] [-display DisplayName] [-empid EmployeeID] [-pwd (Password | *)] [-desc Description] [-office Office] [-tel PhoneNumber] [-email E-mailAddress] [-hometel HomePhoneNumber] [-pager PagerNumber] [-mobile CellPhoneNumber] [-fax FaxNumber] [-iptel IPPhoneNumber] [-webpg WebPage] [-title Title] [-dept Department] [-company Company] [-mgr Manager] [-hmdir HomeDirectory] [-hmdrv DriveLetter:] [-profile ProfilePath] [-loscr ScriptPath] [-mustchpwd {yes | no}] [-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}] [-acctexpires NumberOfDays] [-disabled {yes | no}] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-c] [-q] [{-uc | -uco | -uci}]

ซึ่งคำสั่งพารามิเตอร์ UserDN… จะใช้เหมือนกับ DSADD และมีพารามิเตอร์ที่ใช้เหมือนกัน แต่เปลี่ยนจากการเพิ่มเป็นการแก้ไขออปเจค ซึ่งค่าที่แก้ไขไม่ได้มีดังนี้

– SAMName (-samid)

– Group membership (-memberof) ให้ใช้คำสั่ง DSMOD GROUP แทน

DSMOD ที่ใช้ตามด้วย –c จะเป็นการทำงานต่อเนื่อง เมื่อมีปัญหาในการแก้ไขข้อมูลก็จะดำเนินต่อไป ถ้าไม่ใส่พารามิเตอร์ –c ก็จะหยุดเมื่อมีปัญหาเกิดขึ้น

– การใช้คำสั่ง DSGET

เป็นคำสั่งที่ใช้ในการนำข้อมูลออกมานำเสนอ ซึ่งสามารถระบุได้มากกว่าหนึ่งออปเจค

ตัวอย่างการใช้งาน

Dsget user UserDN… พารามิเตอร์

– รูปแบบคำสั่ง

dsget user UserDN ... [-dn] [-samid] [-sid] [-upn] [-fn] [-mi] [-ln] [-display] [-empid] [-desc] [-office] [-tel] [-email] [-hometel] [-pager] [-mobile] [-fax] [-iptel] [-webpg] [-title] [-dept]

[-company] [-mgr] [-hmdir] [-hmdrv] [-profile] [-loscr] [-mustchpwd] [-canchpwd] [-pwdneverexpires] [-disabled] [-acctexpires] [-reversiblepwd] [{-uc | -uco | -uci}] [-part PartitionDN [-qlimit] [-qused]]

ซึ่งคำสั่งพารามิเตอร์ UserDN... จะใช้เหมือนกับ DSADD และมีพารามิเตอร์ที่ใช้เหมือนกันเพียงแต่ DSGET ใช้เฉพาะพารามิเตอร์ไม่เกี่ยวข้องกับค่าของพารามิเตอร์ที่ต้องการ ตัวอย่างเช่น DSGET นำพารามิเตอร์ –samid ใช้ไม่ใช้ –samid SAMName มาใช้ ซึ่งเพราะการดึงข้อมูลต้องการแสดงไม่ได้เป็นการเพิ่มเติม หรือแก้ไขคุณสมบัติ ใน DSGET ไม่รองรับพารามิเตอร์ –password เพราะว่าไม่สามารถแสดงรหัสผ่านได้ GSGET เพิ่ม –dn และ –sid เพื่อแสดงข้อมูลของ Distinguished name และ SID

– การใช้คำสั่ง DSMOVE

คำสั่งนี้ใช้ในการย้าย หรือเปลี่ยนชื่อออปเจคในโดเมน ไม่สามารถทำข้ามโดเมนได้ ซึ่งตัวอย่างรูปแบบคำสั่งมีดังนี้

Dsmove ObjectDN [-newname NewName] [-newparent ParentDN]

– รูปแบบคำสั่ง

dsmove ObjectDN [-newname NewName] [-newparent ParentDN] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]

DSMOVE รองรับ –s, -u, และ –p ซึ่งอยู่ในเรื่องของ DSQUERY

ออปเจคที่มีการระบุ DN ใน ObjectDN จะเปลี่ยนชื่อ หรือกำหนดชื่อใหม่ด้วยพารามิเตอร์ NewName ซึ่งระบุใน DN ของที่เก็บในพารามิตเรอ์ ParentDN จะเป็นการย้ายออปเจคในที่เก็บ

– ตัวอย่างการใช้งาน

ถ้าต้องการเปลี่ยนชื่อจาก Kim Akers เป็น Kim Ralls ใช้

dsmove "CN=Kim Akers,OU=Sales,DC=Microsoft,DC=Com" -newname "Kim Ralls"

การย้าย Kim Akers จาก Sales organization ไปที่ Marketing organization, พิมพ์ว่า

dsmove "CN=Kim Akers,OU=Sales,DC=Microsoft,DC=Com" -newparent OU=Marketing,DC=Microsoft,DC=Com

เป็นการใช้การเปลี่ยนชื่อ ร่วมกับการย้าย

dsmove "CN=Kim Akers,OU=Sales,DC=Microsoft,DC=Com" -newparent OU=Marketing,DC=Microsoft,DC=Com -newname "Kim Ralls"

– การใช้คำสั่ง DSRM

เป็นการย้ายออปเจค ซับทรี หรือทั้งคู่ ตัวอย่างรูปแบบคำสั่งมีดังนี้

Dsrm ObjectDN … [-subtree [-exclude]] [-noprompt] [-c]

– รูปแบบคำสั่ง

dsrm ObjectDN ... [-subtree [-exclude]] [-noprompt] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-c] [-q] [{-uc | -uco | -uci}]

DSRM รองรับ –s, -u, และ –p ซึ่งอยู่ในเรื่องของ DSQUERY

ออปเจคที่ระบุโดย DN ใส่ในพารามิเตอร์ ObjectDN ซึ่ง –subtree เป็นการสวิตช์ตรงไปที่ DSRM เพื่อนำออปเจคที่เก็บ ถ้าออปเจคบรรจุออปเจค

-exclude switch เป็นการยกเว้นออปเจคนั้นเอง

สามารถใช้เพียงการต่อเชื่อมกับ –subtree

ระบุทั้ง –subtree และ –exclude

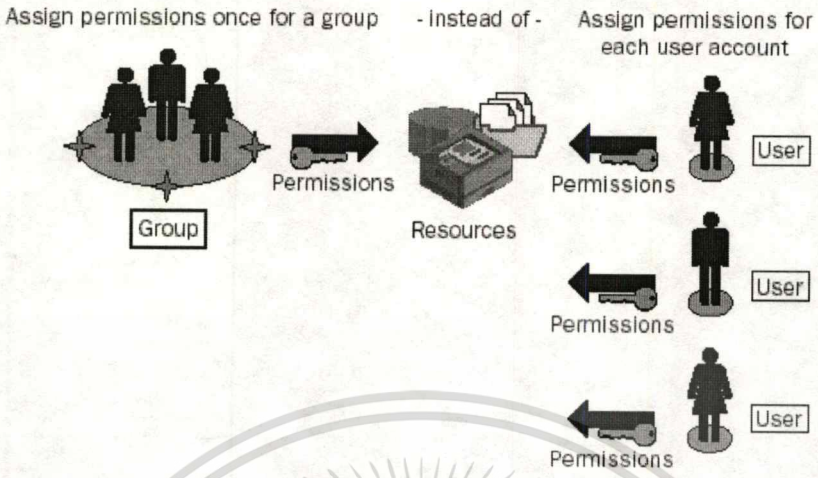
ตัวอย่างเช่น ถ้าต้องการลบ OU และ Subtree แต่เหลือ OU คงอยู่เดิม โดยดีฟอลท์ไม่ใส่ –subtree หรือ –exclude เพียงเท่านี้ออปเจคก็ถูกลบ

เราสามารถที่ให้ขึ้นพรอมต์ระหว่างที่ลบออปเจคได้โดยใช้พารามิเตอร์ –noprompt และใช้ –c เพื่อให้การทำงานต่อเนื่องเมื่อมีปัญหาให้ทำต่อไป ถ้าไม่ใส่ –c ก็จะหยุดทันทีที่มีปัญหาเกิดขึ้น

ตารางที่ 2.9 กลุ่มรหัสผ่านที่แข็งแกร่ง

กลุ่ม	ตัวอย่าง
ตัวใหญ่	A, B, C, …
ตัวเล็ก	a, b, c, …
เลข	0, 1, 2, …
สัญลักษณ์	‘ ~ ! @ # $ % ^ & * ( ) _ + - = [ ] { } | \ : “ ; < > ? , . /

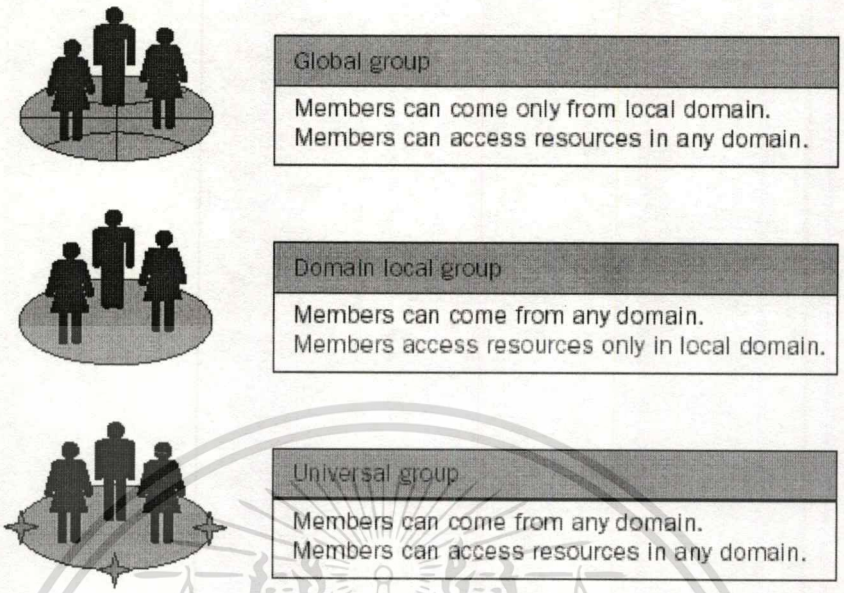
– Group



รูปที่ 2.29 แสดงการใช้งาน Group

การกำหนดกลุ่มเพื่อให้งานการบริหารงานนั้นง่ายลง โดยกำหนดเพียงรายการเดียวแทนการกำหนดผู้ใช้ทีละคนได้หมด

- ชนิดของ Group
- Security Group เป็นกลุ่มที่ใช้กำหนด Permissions ในการเข้าใช้ทรัพยากร ซึ่งโปรแกรมจะใช้กลุ่มนี้ในทั้ง Security Group และ Non-Security Group
- Distribution Group เป็นกลุ่มที่ใช้ในหน้าที่ Non-Security Group ซึ่งจะกำหนดใช้ในการส่ง E-mail ไม่สามารถกำหนดใน Permissions ของทรัพยากรได้ ตัวอย่างเช่น Distribution Group ใน Exchange Server



รูปที่ 2.30 scope Group

Global Groups

เป็นกลุ่มที่ใช้ในการเก็บสมาชิก

คุณลักษณะ

- กำหนดสมาชิก ที่ผู้ใช้
- กำหนดการเข้าใช้ทรัพยากรในโดเมนใดๆในฟอเรสต์

Domain Local Groups

เป็นกลุ่มที่ใช้ในการกำหนด Permissions ในทรัพยการ

- คุณลักษณะ
  - กลุ่มเปิดในการบรรจุสมาชิก สามารถนำผู้ใช้จากโดเมนอื่น หรือ Global Group มาใส่เป็นสมาชิกได้
  - กำหนดการเข้าใช้ทรัพยกรในโดเมนที่อยู่

- Universal Groups

เป็นกลุ่มที่เพิ่มมาใน Windows Server 2003 ขึ้นไป ใช้ในการกำหนด Permissions ในหลายโดเมน ซึ่งมีคุณลักษณะดังนี้

- เป็นกลุ่มเปิด สามารถใส่สมาชิกเป็น User และ Global Group
- เข้าใช้กำหนดทรัพยากรในโดเมนใดๆได้
- รองรับเฉพาะโดเมน ที่ Domain funcational level set ของ Windows 2000 Native หรือ Windows Server 2003

การกำหนด Universal นี้จะมีผลต่อการเรพพลิเคต ข้อมูลต่างๆที่เป็นสมาชิกของ Universal จะถูก Replicate ใน Global catalog Server

- สมาชิกของ Group
  - Global Group
  - Domain Local Group
  - Universal Group
- Local Groups

แนวทางการใช้ Local Group

- ใช้ Local groups เฉพาะที่ต้องการใช้ในเครื่องนั้นๆเท่านั้น
- ใช้ Local groups บนเครื่องที่ทำงานบน Windows XP Professional หรือ Windows Server 2003 ที่เป็น member server
- ใช้ Local groups เฉพาะเครื่องที่ไม่เป็นทรัพยากรของโดเมน
- กฎของการกำหนดสมาชิก
- Local groups สามารถที่บรรจุ Local user account จากเครื่องคอมพิวเตอร์ที่สร้าง
- Local groups ไม่สามารถเป็นสมาชิกกลุ่มอื่นๆได้

- Built-in Local Groups
  - Default Groups
  - โฟลเดอร์ที่อยู่ใน Built-in
  - โฟลเดอร์ที่อยู่ใน Users
  - กลุ่มที่ระบุพิเศษ
  - การใช้ Anonymous User เพื่อเพิ่มความปลอดภัย

- การใช้ LDIFDE

Lightweight Directory Access Protocol (LDAP) Data Interachange Formant (LDIF) คือ มาตรฐานในการเปลี่ยนรูปแบบไฟล์ที่ต้องการกำหนดให้ทำงานแบบแบต์ชต่อรายชื่อที่อยู่ใน มาตรฐาน LDAP ซึ่ง LDIF สามารถที่นำข้อมูลเข้า และออก โดยอนุญาตให้ทำงานตามแบต์ชที่ Add, Create, Modify ต่อ Active Directory ซึ่งเครื่องมือนี้รองรับในระบบปฏิบัติการ Windows Server 2003 ซึ่งการทำงานตามมาตรฐาน LDIF file format

LDIFDE เป็นคำสั่งใน Command Prompt ซึ่งสามารถเรียกความช่วยเหลือโดยพิมพ์ Ldifde /?

รูปแบบคำสั่ง

ldifde [-i] [-f FileName] [-s ServerName] [-c String1 String2] [-v] [-j Path] [-t PortNumber] [-d BaseDN] [-r LDAPFilter] [-p Scope] [-l LDAPAttributeList] [-o LDAPAttributeList] [-g] [-m] [-n] [-k] [-a UserDistinguishedName Password] [-b UserName Domain Password] [-?]

ตารางที่ 2.10 คำสั่งการใช้ LDIFDE

คำสั่ง	การใช้งาน
พารามิเตอร์ทั่วไป	
-i	เป็นการเปิดโหมดนำเข้า โดยดีฟอลท์คือนำออก
-f filename	เป็นการระบุชื่อไฟล์ที่นำเข้า หรือนำออก
-s servername	เป็นการระบุเครื่องที่ผูกติดไว้
-c FromDN toDN	เป็นการแทนสิ่งที่เกิดของ FromDN ไป ToDN
-v	เป็นการเปิดโหมดบันทึกเต็มที่ หรือ Verbose
-j path	ตำแหน่งล็อกไฟล์
-t port	กำหนดพอร์ตซึ่งดีฟอลท์คือ 386
-?	ขอความช่วยเหลือ
พารามิเตอร์การนำออก	

คำสั่ง	การใช้งาน
-d RootDN	กำหนดตำแหน่งรูทของ LDAP ที่ค้นหา โดยดีฟอลท์ไปที่ Naming Context
-r filter	LDAP search filter โดยดีฟอลท์ไปที่ “(objectClass=*)”)
-p SearchScope	กำหนดสโคปที่ค้นหา (Base/OneLevel/Subtree)
-l list	กำหนดรายการคุณสมบัติ (ใช้คอมม่าคั่น) เพื่อดูจาก LDAP ที่ค้นหา
-o list	กำหนดรายการคุณสมบัติ (ใช้คอมม่าคั่น) เพื่ออนญาตจากการนำเข้า
-g	เป็นการห้ามค้นหาในหน้า
-m	อนุญาตให้ Security Accounts Manager (SAM) logic บนการนำออก
-n	ไม่นำค่าไบนารี่ออก
พารามิเตอร์การนำเข้า	
-k	นำเข้าโดยไม่สนใจว่ามี Error กับค่าคงที่มีปัญหา และออปเจคที่มีอยู่
พารามิเตอร์การตรวจสอบ	
-a UserDN	ชุดคำสั่งที่ทำงานใน User distinguished name และ Password ตัวอย่างเช่น “Cn=administrator,dc=contoso,dc=com”
-b UserName Domain	กำหนดชุดคำสั่งที่ผู้ใช้ และรหัสผ่านในโดเมน โดยทั่วไปจะใช้ผู้ใช้ที่ล็อกออนอยู่

คำสั่ง LDIFDE ใน Windows Server 2003 สามารถถูกก๊อปปี้ด้วย Windows 2000 Professional หรือ Windows XP ได้โดยใช้จากทางไกล

วิธีการสร้างกลุ่มด้วย DSADD

Dsadd เป็นคำสั่งที่ใช้ในการเพิ่มผู้ใช้ในกลุ่ม

ตัวอย่างคำสั่ง

Dsadd group GroupDN…

รูปแบบคำสั่ง

dsadd group GroupDN [-secgrp {yes | no}] [-scope {l | g | u}] [-samid SAMName] [-desc Description] [-memberof Group ...] [-members Member ...] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]

ค่าพารามิเตอร์ GroupDN… สามารถใส่ DN ได้มากกว่าหนึ่ง สำหรับออปเจคผู้ใช้ใหม่ ถ้า DN มีการเว้นวรรค และใช้ DN แยกด้วย ‘ ‘ โดยพารามิเตอร์ที่ใส่ทำได้หนึ่งในนี้

- ใช้ piping "|" ในรายการ DNs กับคำสั่งอื่นๆเช่น DSQUERY
- ใช้ piping "|" ในแต่ละคำสั่ง โดยแยกด้วยช่องว่าง
- ปล่อยว่างไว้ และพิมพ์ DN ในแต่ละครั้งโดยคีย์บอร์ด และเคาะ Enter เพื่อใส่ DN กดคีย์ Ctrl+Z และ Enter ถ้าต้องการออกจาก DN สุดท้าย
- คำสั่ง DSADD GROUP สามารถที่มีพารามิเตอร์เพิ่มดังนี้
- Secgrp {yes | no} เป็นการพิจารณาว่าเป็น Security Group (yes) หรือเป็น Distribution group (no) โดยดีฟอลท์คือ Yes
- Scope {l | g | u} เป็นการพิจารณาว่ากลุ่มที่ใช้เป็น Domain Local (l), Global (g เป็นดีฟอลท์) หรือ Universal (u)
- Samid SAMName
- Desc Description
- Memberof GroupDN… ซึ่งสามารถระบุกลุ่มที่ต้องการเพิ่มในกลุ่มใหม่
- Members MemberDN… ระบุสมาชิกที่เพิ่มในกลุ่ม

นอกจากนี้ยังสามารถที่กำหนดการตรวจสอบกับ Server, User, และใส่รหัสผ่านด้วยพารามิเตอร์ดังนี้

ตารางที่ 2.11 พารามิเตอร์คำสั่ง DSADD GROUP

พารามิเตอร์	คำอธิบาย
{-s Server | -d Domain}	เป็นการต่อเชื่อมกับ Remote server หรือ Domain
-u UserName	เป็นการระบุชื่อผู้ใช้ที่ล็อกออนจากเครื่องอื่น โดยดีฟอลท์ –u ใช้กับชื่อผู้ใช้ที่ล็อกออก ซึ่งมีรูปแบบในการระบุชื่อได้ดังนี้ - User Name ตัวอย่างเช่น Akerit - Domain\User name ตัวอย่างเช่น Root\Akerit - UPN ตัวอย่างเช่น Akerit@root.com
-p {Password | *}	เป็นการระบุรหัสผ่านที่ใช้ หรือใช้ * สำหรับการที่ให้ขึ้นรหัสผ่านขณะที่เรียกใช้คำสั่ง

การแก้ไขกลุ่มด้วย DSMOD

DSMOD เป็นคำสั่งที่ใช้ในการแก้ไขสมาชิกใน Active Directory

ตัวอย่างการใช้

Dsmod group GroupDN…

รูปแบบคำสั่ง

dsmod group GroupDN ... [-samid SAMName] [-desc Description] [-secgrp {yes | no}] [-scope {l | g | u}] [{-addmbr | -rmmbr | -chmbr} MemberDN ...] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-c] [-q] [{-uc | -uco | -uci}]

คำสั่งที่ใช้มีความคล้ายกับ DSADD รวมถึง –samid, -desc, -secgrp, และ –scope ซึ่งการกำหนดนี้ไม่มีการเปลี่ยนคุณสมบัติในกลุ่มที่มีอยู่ แต่จะใช้ในการแก้ไขปัญหาสมาชิก

– addmbr Member… เป็นการเพิ่มสมาชิกในกลุ่มที่ระบุ

– rmmbr Member… เป็นการลบสมาชิกจากกลุ่มที่ระบุ

คำสั่งในรายชื่อ DN กำหนดเต็ม DN ของ Active Directory object อื่นๆ, และใช้ ‘ ‘ ล้อมรอบ ถ้ามีมากกว่าหนึ่งให้ใช้เว้นวรรคใน DN

การใช้พารามิเตอร์ –addmbr กับ rmmbr ใช้พร้อมกันไม่ได้

ตัวอย่างคำสั่ง

เพื่อเพิ่มผู้ใช้ Mike Danseglio ไปในทุกกลุ่ม Administrators ที่เป็น Distribution พิมพ์

dsquery group "OU=Distribution Lists,DC=microsoft,DC=com" -name adm* | dsmod group -addmbr "CN=Mike Danseglio,CN=Users,DC=microsoft,DC=com"

เพื่อเพิ่มสมาชิกของ US info group ไปใน Canada Info group พิมพ์

dsget group "CN=US INFO,OU=Distribution Lists,DC=microsoft,DC=com" -members | dsmod group "CN=CANADA INFO,OU=Distribution Lists,DC=microsoft,DC=com" -addmbr

เพื่อแปลงชนิดกลุ่มของ Serveral groups จาก Security เป็น Non-secuirty พิมพ์ซ

dsmod group "CN=US Info,OU=Distribution Lists,DC=Microsoft,DC=Com" "CN=Canada Info,OU=Distribution Lists,DC=Microsoft,DC=Com" "CN=Mexico Info,OU=Distribution Lists,DC=Microsoft,DC=Com" -secgrp no

เพื่อเพิ่มสมาชิกใหม่ในกลุ่ม "CN=US Info,OU=Distribution Lists,DC=Microsoft,DC=Com", พิมพ์

dsmod group "CN=US Info,OU=Distribution Lists,DC=Microsoft,DC=Com" -addmbr "CN=Mike Danseglio,CN=Users,DC=Microsoft,DC=Com" "CN=Legal,OU=Distribution Lists,DC=Microsoft,DC=Com" "CN=Denise Smith,CN=Users,DC=Microsoft,DC=Com"

เพื่อเพิ่มผู้ใช้ทั้งหมดจาก Marketing organization unit ไปเป็นกลุ่ม Marketing Staff, พิมพ์

dsquery user OU=Marketing,DC=Microsoft,DC=Com | dsmod group "CN=Marketing Staff,OU=Marketing,DC=Microsoft,DC=Com" -addmbr

เพื่อลบสมาชิกสองรายการจาก กลุ่ม"CN=USInfo,OU=DistributionLists,DC=Microsoft,DC=Com", พิมพ์

dsmod group "CN=US Info,OU=Distribution Lists,DC=Microsoft,DC=Com" -rmmbr "CN=Mike Danseglio,CN=Users,DC=Microsoft,DC=Com""CN=Legal,OU=DistributionLists,DC=Microsoft, DC=Com"

– Computer Accounts

การนำเครื่องเข้ายังโดเมน

เมื่อติดตั้ง Windows Server 2003 โดยดีฟอลท์เครื่องต่างๆจะอยู่ในกลุ่ม Workgroup ซึ่งความสามารถของ Windows NT-Based Computer จนถึง Windows Server 2003 (Windows NT 4.0, Windows 2000, Windows XP, Windows 2003) สามารถที่รับรองการเข้าใช้ใน Local Security Accounts Manager (SAM) database ในเครื่อง Stand-alone system ซึ่งการกำหนดสมาชิกในกลุ่มเป็นเพียงบทบาทย่อยๆ ในการใช้บริการบราวข้อมูลดู ผู้ใช้ทุกคนสามารถที่เข้าใช้แชร์ในกลุ่ม หรือในโดเมน ซึ่งอาจจะไม่เคยล็อกออนเข้าในเครื่องกับ Domain account ก็ได้

ก่อนที่ล็อกออนคอมพิวเตอร์ด้วย Domain user account เครื่องคอมพิวเตอร์ต้องอยู่ในโดเมน ซึ่งมีอยู่สองขั้นตอนในการเชื่อมต่อเครื่องในโดเมน ลำดับแรกคือการสร้าง Account สำหรับคอมพิวเตอร์ ลำดับที่สองให้กำหนดเครื่องคอมพิวเตอร์เชื่อมต่อในโดเมนโดยใช้ Account ดังกล่าว

Computers ที่บำรุงรักษา accounts จะทำโดยให้ระบุชื่อผู้ใช้ รหัสผ่าน และ Security identiifer (SID) ซึ่งเป็นการกำหนดคุณสมบัติของเครื่องเข้ายังโดเมน โดยกระบวนการนี้คล้ายกับการเตรียมผู้ใช้ในโดเมน ที่ต้องสร้างเครื่องคอมพิวเตอร์ใน Active Directory

– การสร้าง Computer Accounts

ผู้ที่สร้างได้จะต้องอยู่ในกลุ่ม Administrators หรือ Account Operators groups บน Domain controllers ที่สร้างออปเจคคอมพิวเตอร์เข้าไปใน Active Directory

ซึ่งโดยทั่วไป Domain Admins และ Enterprise Admins จะเป็นสมาชิกใน Administrators group ซึ่งเราอาจจะแต่งตั้งผู้บริหารระบบที่ทำการสร้างออปเจคคอมพิวเตอร์เองได้

ใน Domain Users สามารถที่สร้างออปเจคคอมพิวเตอร์โดยอ้อม เมื่อคอมพิวเตอร์เข้ามาเชื่อมต่อโดเมน และไม่มี Account Active Directory สร้างออปเจคของคอมพิวเตอร์อัตโนมัติ โดยดีฟอลท์ในโฟลเดอร์ Computers ซึ่งผู้ใช้ที่อยู่ใน Authenticated User group (ผู้ใช้ที่ล็อกออนทุกคน) อนุญาตให้ต่อเชื่อมเครื่องได้ 10 เครื่องในโดเมน และสามารถที่สร้างได้ 10 ออปเจคในชนิดนั้นๆ

การสร้างออปเจค Computer โดยใช้ Active Directory Users and Computers

เพื่อสร้างออปเจค Computer, หรือ "Account" ต้องเปิด Active Directory Users and Computer และเลือกที่เก็บ OU ที่ต้องการสร้างคลิกขวาเลือก Shortcut menu, เลือกคำสั่ง New Computer ซึ่งจะมีข้อมูลให้กรอก และกำหนดชื่อเครื่องที่ต้องการ และคลิก Next ซึ่งจะมีการร้องขอ GUID และผ่านขั้นตอน Computer account สำหรับ Remote Installation Services (RIS)

deployment กับสโคปที่ได้ถกเถียงกัน ซึ่งไม่จำเป็นต้องใส่ GUID เมื่อสร้างComputer account ที่เชื่อมต่อโดเมนด้วยวิธีอื่นๆ และคลิก Next, คลิก Finish

– การสร้างออปเจค Computer ด้วย DSADD

Windows Server 2003 มีเครื่องมือที่ชื่อ DSADD ในการที่สร้างเครื่องคอมพิวเตอร์ใน Command Prompt หรือในไฟล์แบตช์ โดยการสร้างออปเจคคอมพิวเตอร์จะใช้ DSADD computer Computer DN ซึ่งการกำหนด ComputerDN กำหนดเป็น CN=Desktop123,OU=Desktops,DC=Contoso,DC=com

รูปแบบคำสั่ง

dsadd computer ComputerDN [-samid SAMName] [-desc Description] [-loc Location] [-memberof GroupDN ...] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]

ถ้ามีการกำหนด DN เว้นวรรคไว้ก็สามารถใส่ DN ที่มีเครื่องหมาย '' โดยพารามิเตอร์ ComputerDN สามารถมีได้มากกว่า 1 DN ต่อหนึ่งครั้ง พารามิเตอร์ที่ใส่ได้หนึ่งในรายการนี้

– ใช้ piping "|" ในรายการ DNs กับคำสั่งอื่นๆเช่น DSQUERY
– ใช้ piping "|" ในแต่ละคำสั่ง โดยแยกด้วยช่องว่าง
– ปล่อยว่างไว้ และพิมพ์ DN ในแต่ละครั้งโดยคีย์บอร์ด และเคาะ Enter เพื่อใส่ DN กดคีย์ Ctrl+Z และ Enter ถ้าต้องการออกจาก DN สุดท้าย

ในคำสั่ง DSADD Computer สามารถที่ใส่พารามิเตอร์ตามหลัง DN ได้ดังนี้

– samid SAMName
– desc Description
– loc Location

การสร้าง Computer Account ด้วย NetDOM

เป็นคำสั่งที่อยู่ใน Support Tools ซึ่งต้องติดตั้ง SupTools.msi ในซีดีรอมของ Windows Server 2003 ที่ Support\Tools โดยการติดตั้งนี้สามารถทำได้บน Windows XP และ Windows 2000 CD ด้วย โดยเวอร์ชั่นขึ้นอยู่กับแพลตฟอร์ม Netdom อนุญาตให้แสดง Domain account และงานความปลอดภัยจากคำสั่ง

ในการสร้าง Computer account ในโดเมนใช้คำสั่งดังนี้

Netdom add Computername /domain:DomainName /userd:User /PasswordD:UserPassword [/ou:OUDN]

ในการสร้าง ComputerName ในโดเมน DomainName จะต้องมีการระบุ User และ Password โดย /OU อาจจะต้องการระบุที่เก็บในออปเจคที่สร่าง ซึ่งต้องระบุ OUDN ถ้า OUDN ไม่กำหนดจะอยู่ในโฟลเดอร์ Computers โดยดีฟอลท์ ซึ่งผู้ใช้ที่ระบุต้องได้รับอนุญาตให้สร้างออปเจคคอมพิวเตอร์ด้วย

– การเชื่อมต่อเครื่องคอมพิวเตอร์เข้ายังโดเมน

เป็นการสร้างความสัมพันธ์ความปลอดภัยที่ต้องการระหว่างโดเมนกับคอมพิวเตอร์ โดยการกำหนดจะใช้ System ใน Control Panel ในการระบุ และกำหนดผู้ใช้รหัสผ่านที่มี Permissions ในการเข้าใช้

ตำแหน่งโดยดีฟอลท์ที่เก็บอยู่ในโฟลเดอร์ Computers โดยเมื่อสร้างจะมีการกำหนดตำแหน่ง และทำความสัมพันธ์ทรัสต์ระหว่างโดเมน ซึ่งเปลี่ยน SID เพื่อตรงกับ Account ในการแก้ไขและการจัดสมาชิกในกลุ่ม เครื่องต้องทำการรีสตาร์ทเมื่อกำหนเรียบร้อยแล้ว

คำสั่ง Netdom Join เป็นการเชื่อมต่อเครื่องเข้ายังโดเมน โดยระบุตำแหน่งที่ต้องการใน OU ที่ออปเจคต้องการอยู่ได้

– ที่เก็บ Computers กับ Ous

ที่เก็บ Computer ใน Active Directory หลังจากที่เครื่อง Windows NT 4 อัพเกรดไปเป็น Windows 2000 ทุกเครื่องที่พบจะอยู่ในที่เก็บ ซึ่งอยู่ที่ Computers Container หรือที่เก็บ Computers

แม้ว่าใน Computers container เป็นตำแหน่งดีฟอลท์ที่อยู่ในออปเจค จะไม่ใช่ OUs คือไม่สามารถกำหนดนโยบาย หรือจำกัดการดูข้อมูลได้ ดังนั้นถ้าต้องการควบคุมแนะนำให้ผู้บริหารระบบทำการสร้างเป็น Ous สำหรับคอมพิวเตอร์ต่างๆ และแบ่งเป็นแผนก พื้นที่ หรือแยกการบริหารกลุ่มโน้ตบุ๊ค, เครื่องตั้งโต๊ะ, หรือเครื่องแม่ข่าย และเครื่องที่รองรับแอพพลิเคชั่น

ตัวอย่างเช่นกลุ่มเครื่อง Domain Controllers ที่ถูกกำหนดเป็น Ous แยกออกไปเพื่อให้กำหนดนโยบาย และควบคุมการกำหนดค่าได้ดียิ่งขึ้น

ถ้าองค์กรมีกลุ่ม Ous สำหรับเครื่องมากก็ให้ระบุการสร้าง Computers Container ให้เหมาะกับ OU โดยใช้คำสั่งย้ายไปยังไว้ในตำแหน่งที่ต้องการ หรือใช้การลาก แล้วปล่อย

– คำสั่งที่ใช้ในการย้ายคอมพิวเตอร์คือ DSMOVE

Dsmove ObjectDN [-newname NewName] [-newparent ParentDN]

พารามิเตอร์ -newname เป็นการเปลี่ยนชื่อออปเจค พารามิเตอร์ –newparent เป็นการอนุญาตให้ย้ายออปเจค เพื่อย้าย Computer และเปลี่ยนชื่อ และที่เก็บไปใน Desktops สามารถทำได้ดังนี้

Dsmove?CN=DesktopABC,CN=Computers,DC=Contoso,DC=com?–newparent ?OU=Desktops,DC=Contoso,DC=com?

ในคำสั่งจะมีการระบุระหว่าง Computers container (CN) และ Desktops Organizational unit (OU)

ผู้ที่มีสิทธิในการย้ายออปเจคใน Active Directory โดยดีฟอลท์คือ Account Operators ที่ใช้ย้ายตำแหน่งเครื่องคอมพิวเตอร์ ยกเว้น Domain Controllers OU

Administrators รวมถึง Domain Admins, Enterprise Admins สามารถที่ย้ายออปเจคคอมพิวเตอร์ระหว่างที่เก็บ รวมถึง Domain Controllers Ous ที่ต่างๆได้ด้วย

– การจัดการเครื่องคอมพิวเตอร์

หลังจากที่เราได้ทำการกำหนดความสัมพันธ์เครื่องคอมพิวเตอร์กับโดเมนแล้ว โดยการเชื่อมต่อกับโดเมน เราสามารถที่จะจัดการเกี่ยวกับคุณสมบัติของออปเจคได้ด้วย

– การจัดการ Permissions ในออปเจคคอมพิวเตอร์

เราพบว่าการเชื่อมต่อเครื่องยังโดเมนจะต้องระบุผู้ที่มี Permissions ในการเข้าเชื่อมต่อด้วย ซึ่งนั่นคือระบบความปลอดภัย โดยทั่วไปเราใช้ Domain Admins แต่จริงแล้วใน Active Directory สามารถที่จะระบุกำหนดกลุ่มอื่นๆได้เช่น Installers เพื่อเชื่อมต่อเครื่องในโดเมน โดยการกำหนด Permissions ในออปเจคคอมพิวเตอร์ใน Active Directory ให้สามารถที่ Modify ได้

ซึ่งการกำหนดนี้ในคอมพิวเตอร์ใหม่จะมี Globally unique identifier (GUID) ของเครื่องที่ติดตั้งโดยการใช้ Remote Installation Services (RIS) ซึ่งต้องไปดูเพิ่มใน RIS จากเว็บ http://support.microsoft.com

ถ้าเครื่องที่กำหนดรันเก่ากว่า Windows 2000 ให้เลือกเช็กบ็อกซ์ Assign this Computer account as a Pre-Windows 2000 computer ถ้าเป็น Windows NT Backup Domain Controller ให้คลิกที่ Assign this computer account as a Backup Domain Controller

– การกำหนดคุณสมบัติของเครื่อง

ออปเจค Computer ที่มีคุณสมบัติบางอย่างที่มองไม่เห็นในการสร้างขึ้น เมื่อเปิดเข้าไปในคุณสมบัติของออปเจค Computer จะกำหนดตำแหน่ง และคำอธิบาย กำหนดสมาชิกในกลุ่ม และ

Dial-in permissions ซึ่งมีการลิงค์กับออปเจคผู้ใช้ด้วย โดยการกำหนดคุณสมบัติ Operating System ให้ Read-only ข้อมูลต่างๆจะประกาศใน Active Directory โดยอัตโนมัติ ซึ่งจะว่างไว้จนกระทั่งมีเครื่องเข้ามาเชื่อมต่อในโดเมนด้วย Account ดังกล่าว

ในกลุ่มออปเจคยางอย่างใน Active directory รองรับ Manager ที่แสดงขึ้นมาซึ่งมีการเชื่อมต่อกับออปเจคผู้ใช้ และทุกคุณสมบัติก็จะมีการดึงมาจากออปเจคผู้ใช้ ซึ่งไม่ได้เก็บไว้ใน Computer เอง

คำสั่ง DSMOD สามารถที่กำหนดปรับเปลี่ยนคุณสมบัติข้อมูลได้

– การค้นหาออปเจค และการติดต่อออปเจคใน Active Directory

เมื่อผู้ใช้เรียกดูปัญหาในระบบปฏิบัติการ หรือ Service Pack ที่ติดตั้งในระบบ เราสามารถเรียนรู้ได้จากคุณสมบัติของออปเจคคอมพิวเตอร์ ซึ่งในตำแหน่งออปเจคคอมพิวเตอร์ที่ค้นหาอาจจะยากต่อการเรียกดูเนื่องจากอาจจะมีหลายโดเมน หรือหลาย Ous ดังนั้นคำสั่งที่ใช้ในการเรียกหาคือ Find ซึ่งสามารถที่แสดงชนิดที่ต้องการค้นหาได้จากเครื่องมือ Active Directory Users and Computers

– การแก้ปัญหาเครื่องคอมพิวเตอร์

Active directory domains จะยึดถือการกำหนดหลักการความปลอดภัย โดยเหมือนกับ User account ที่กำหนดโดยมีการกำหนดชื่อ รหัสผ่าน และ SID ซึ่งการแก้ปัญหาจะต้องมีความเข้าใจเกี่ยวกับออปเจคคอมพิวเตอร์ด้วย

– การลบ และการไม่อนุญาต และรีเซต Computer Accounts

Computer accounts จะเหมือนกับ User account ที่มี SID เดียว ซึ่งอนุญาตให้ Administrator กำหนด Permissions ได้โดยกำหนดผ่านกลุ่ม สิ่งที่ต้องเข้าใจในการลบ Computer account ก็จะมีเรื่องของ SID และสมาชิกที่ลบออกไป ถ้ามีการลบด้วยอุบัติเหตุ และมีเครื่องอื่นๆสร้างชื่อเหมือนกัน ก็จะมีหมายเลข SID ที่แตกต่างกัน และสมาชิกต้องกำหนดสร้างขึ้นใหม่ และ Permissions ที่กำหนดในออปเจคนั้นๆก็จะต้องกำหนดใหม่ ดังนั้นการลบออปเจคคอมพิวเตอร์ต้องมีความมั่นใจในคุณสมบัติต่างๆของออปเจคนั้นที่สัมพันธ์กัน

เครื่องมือที่ใช้ในการลบ Computer account ใช้ Active Directory Users and Computers ซึ่งเรียกได้จากเลือกที่ออปเจคเครื่อง คลิกที่ Action menu หรือคลิกขวาเรียก Shortcut -> เลือกคำสั่ง Delete -> จะมีการกำหนดยืนยันโดยดีฟอลท์กำหนด No ถ้าต้องการลบคลิกที่ Yes

คำสั่ง DSRM เป็นคำสั่งที่ใช้ในการลบออปเจค

วิธีใช้คือ

DSRM ObjectDN

ObjectDN ที่กำหนดเป็น Distinguished name ของเครื่องเช่น "CN=Desktop15, OU=Desktops,DC=contoso,DC=com" ซึ่งจะมีพรอมต์ขึ้นมายืนยันในการลบ

ในการยกเลิกการเชื่อมต่อโดเมนถ้าเครื่องทำงานอยู่จะลบออปเจคใน Active Directory ไปด้วย ถ้าไม่ทำงานจะไม่ทำการนำออกถ้าเครื่องที่ปฏิบัติอยู่ในภาวะออฟไลน์ หรือไม่ใช้ในระหว่างเวลาที่กำหนด เราอาจจะทำการไม่อนุญาตให้ใช้ได้ ตามหลักความปลอดภัย ซึ่งการระบุต้องกำหนดจำนวนผู้ใช้ที่ต้องการให้กำหนดตามเป้าหมายขององค์กร การไม่อนุญาตจะไม่มีผลต่อ SID หรือสมาชิกในกลุ่ม ซึ่งเมื่อเครื่องกลับมาปกติเราก็สามารถที่กำหนดให้อนุญาตได้ เครื่องที่กำหนดไม่อนุญาตจะมีสัญลักษณ์เป็นรูปกากบาท ในขณะที่ไม่อนุญาตให้ใช้เครื่องไม่สามารถที่จะเข้าใช้ช่องความปลอดภัยในโดเมนได้ ซึ่งส่งผลให้ไม่มีผู้ใช้ล็อกออนในโดเมนได้ รวมถึงผู้ใช้ที่ไม่มีอยู่ในแคชที่ล็อกออนบนเครื่อ จะไม่สามารถที่ใช้ได้จนกว่าจะมีการอนุญาตให้ใช้ การอนุญาตก็เพียงแต่เลือกเครื่องคอมพิวเตอร์ และเรียกคำสั่ง Enable จาก Action menu หรือ Shortcut menu

คำสั่งที่ไม่อนุญาต หรืออนุญาตให้เครื่องใช้งานได้สามารถใช้ผ่าน Command Prompt ได้ คือคำสั่ง DSMOD ซึ่งรูปแบบคำสั่งมีดังนี้

DSMOD Computer ComputerDN –disabled Yes

DSMOD Computer ComputerDN –disabled No

ถ้าเครื่องเป็นสมาชิกในกลุ่ม หรือ SID ที่กำหนดต้องการให้ทำงานในโดเมน ไม่ต้องการลบออก เพื่อว่าจะได้นำเครื่องใหม่มาแทน หรืออัพเกรดฮาร์ดแวร์ สามารถใช้คำสั่ Reset เครื่องคอมพิวเตอร์ได้

คำสั่ง Reset ใน Computer account เป็นการรีเซตรหัสผ่าน แต่ยังคงคุณสมบัติต่างๆเหมือเดิม ซึ่งจะส่งผลให้ "Available" สำหรับการใช้ เครื่องคอมพิวเตอร์อื่นๆสามารถที่เชื่อมต่อกับโดเมนโดยใช้ Account รวมถึงการอัพเกรดระบบ

การรีเซตสามารถใช้คำสั่ง DSMOD ได้ดังนี้

Dsmod computer ComputerDN –reset

คำสั่ง NETDOM ที่อยู่ใน Windows Server 2003 Support Tools สามารถที่อนุญาตให้รีเซต Computer account ได้

ปัญหาในการจัด Computer Account ใหม่

Computer Account จะมีความสัมพันธ์กับโดเมนซึ่งมีความแข็งแกร่ง ดังนั้นเมื่อมีการยุติ Secure channel หรือมีปัญหาที่เด่นชั่น การกำหนดจะขึ้นข้อความว่าไม่สามารถที่ติดต่อกับ Domain Controller ได้ซึ่งเมื่อได้รับข้อความนี้ก็จะสูญเสียการติดต่อระหว่างโดเมน

- โดยข้อความที่ขึ้นนี้จะเป็นเครื่องบ่งบอกถึงปัญหา พร้อมแนะนำวิธีการแก้ไข เช่น รหัสผ่าน, การทรัสต์, ช่องความปลอดภัย, ความสัมพันธ์กับโดเมน หรือ Domain Controller
- เครื่องคอมพิวเตอร์ที่มีปัญหากับ Active Directory
- หนึ่งในปัญหาที่เกิดขึ้นต้องได้รับการแก้ไขโดยรู้จักกับการลบ, การไม่อนุญาต, การรีเซส Computer account และการเริ่มต้นในการเชื่อมต่อโดเมน

ซึ่งกฎการแก้ปัญหามีดังนี้

- ถ้า Computer Account ยังมีอยู่ใน Active Directory ให้ใช้ Reset
- ถ้า Computer Account ผิดพลาดจาก Active Directory ให้กำหนด Computer account ใหม่
- ถ้าเครื่องยังคงอยู่ในโดเมน ให้นำออกจากโดเมน และเปลี่ยนเป็น Workgroup และเลือก Workgroup ที่ไม่ได้ใช้
- ทำการเชื่อมต่อใหม่เข้ากับโดเมน โดยกำหนดเป็นเครื่องใหม่ ชื่อเดิมใน Computer account

ปัญหาของเครื่องคอมพิวเตอร์จะมีเพียง 4 กฎนี้เท่านั้นซึ่งสามารถที่กำหนดตั้งแต่แรกจนถึงขั้นสุดท้าย

ในสถานการณ์แรก ผู้ใช้บ่นว่าเมื่อพยายามล็อกออกได้รับข้อความบอกว่า Missing

กำหนดในกฎแรกแล้วเปิด Active Directory Users and Computers พบว่ามีเครื่องอยู่ จึงทำการรีเซต ในข้อสองจึงไม่ได้ดำเนินการเพราะมี Computer account อยู่ เมื่อถึงข้อสามก็ทำการนำออกจากระบบ และข้อสี่ก็เชื่อมต่อใหม่

ในสถานการณ์ที่ 2 ถ้าเครื่องที่รีเซตเกิดปัญหาในเงื่อนไขข้อหนึ่ง ยังคงรีเซตได้ต่อไป โดยข้อที่สองไม่ทำเนื่องจากมีเครื่องอยู่ในโดเมน และข้อที่สามถ้ายังมีการเชื่อมต่อยังโดเมน ก็ต้องนำออก และทำการเชื่อมต่อใหม่

ซึ่งกฎทั้งสี่ข้อนี้ใช้ในการแก้ปัญหาเกี่ยวกับ Computer Account ที่เสียหาย

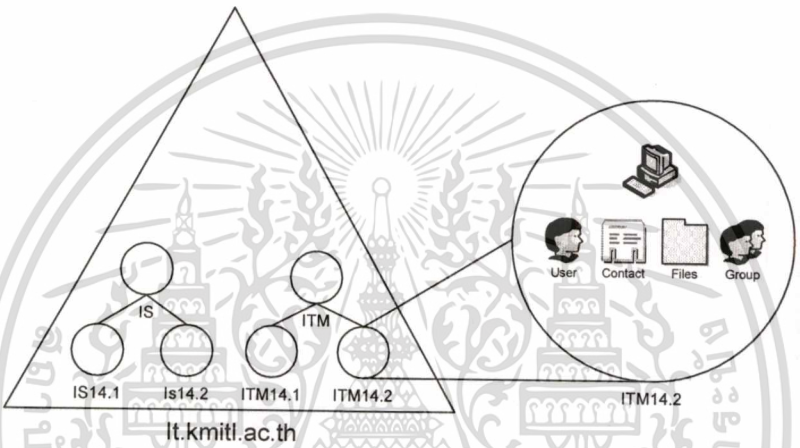
บทที่ 3

การออกแบบและพัฒนาระบบงาน

3.1 ความต้องการของระบบ

การที่เราได้ใช้กรณีศึกษาจากรูปแบบการบริหารงาน Active Directory ของคณะเราเองซึ่งมีแบ่งเป็น 2 ส่วน

– โครงสร้างแบบ Logical

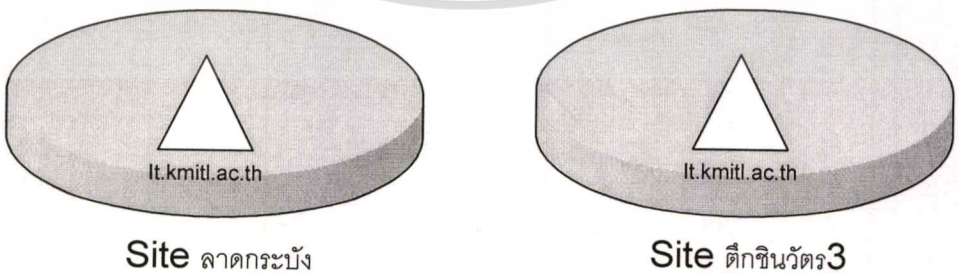


รูปที่ 3.1 ลักษณะโครงสร้างแบบ Logical

Domain ตามโครงสร้างคือ it.kmitl.ac.th และมีการแบ่ง Organizational Unit โดยแยกตามภาควิชา เช่น IS,ITM และภายในก็มีรายชื่อนักศึกษา และอื่นๆ

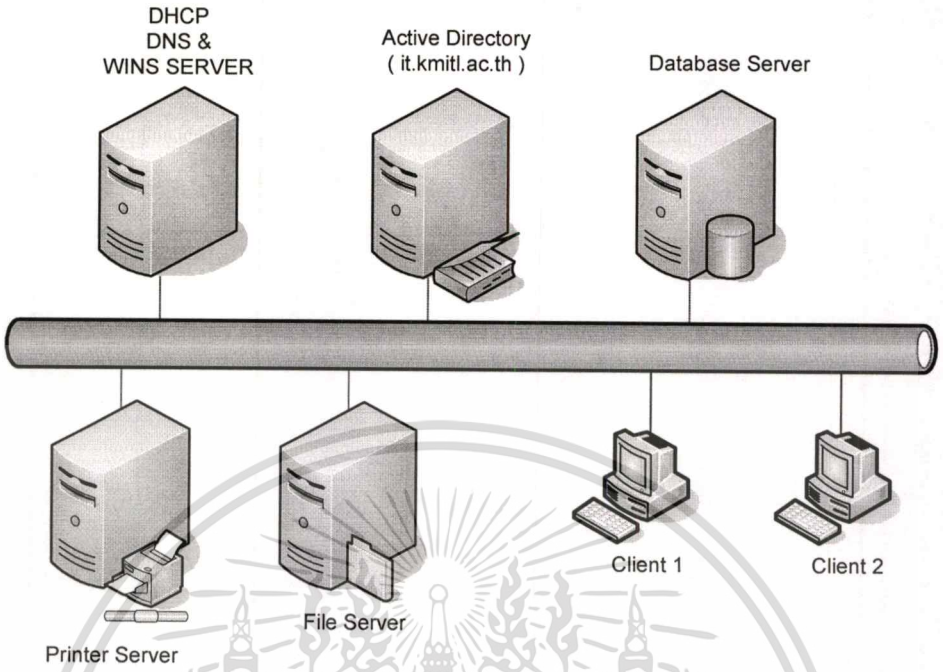
– โครงสร้างแบบ Physical

ที่คณะเราได้ จัดโครงสร้าง Active Directory ทาง Logical และPhysical เหมือนกัน แต่แยกกันอยู่โดยไม่ได้มีการReplication กัน



รูปที่ 3.2 โครงสร้างActive Directoryทางกายภาพของคณะ

จากโครงสร้างที่ได้นำมาคิดให้การออกแบบโปรแกรมคือเมื่อคณะรับนักศึกษาใหม่ก็จะต้องทำการ เพิ่มรายชื่อนักศึกษาในระบบ เพื่อให้นักศึกษาสามารถที่จะใช้คอมพิวเตอร์ได้รวามทั้งจะได้นำรายชื่อมาควบคุมการพิมพ์เอกสารให้พิมพ์เอกสารได้ตามจะตามจำนวนที่คณะกำหนดด้วย



รูปที่ 3.3 แสดงNetwork Diagramในโครงสร้าง Active Directory

Microsoft Windows 2000 Pro : ระบบปฏิบัติการClient

Microsoft Windows XP : ระบบปฏิบัติการClient

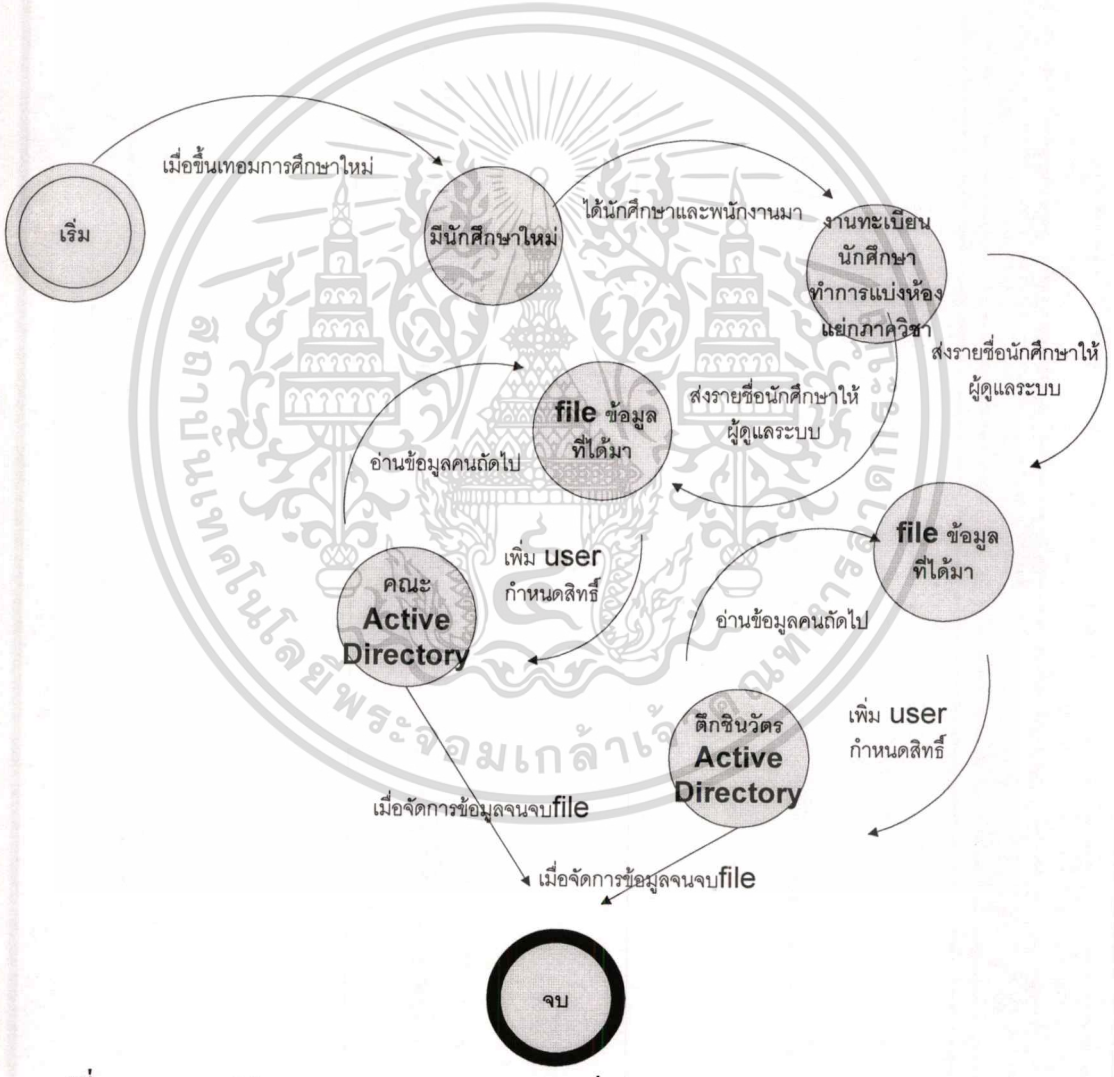
Microsoft Window 2003 Server : ระบบปฏิบัติการที่ใช้โดเมน

Microsoft .NET Framwork v1.1 : ในการเรียกใช้โปรแกรม LDIF Gennerator

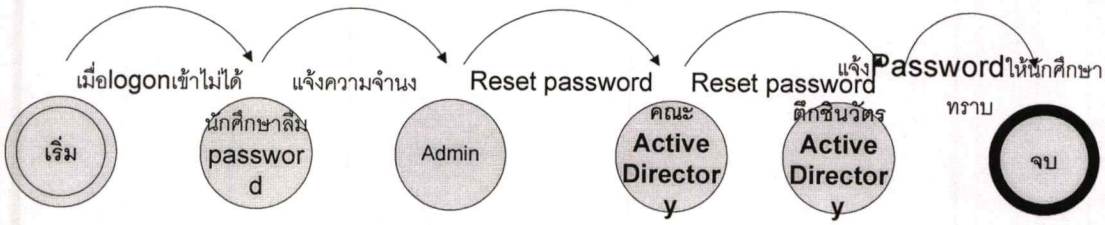
ระบบควรมี โครงสร้างโดเมนอยู่ก่อนแล้ว Run ldifde commandเพื่อใช้สร้างLDIF Fileที่จะนำมาใช้ในสร้างTreeของโปรแกรม

– **ระบบเดิม**

เมื่อขึ้นเทอมใหม่คณะก็รับนักศึกษาใหม่เข้ามาและจำเป็นต้องเพิ่มรายชื่อผู้ใช้งานของระบบซึ่งงานทะเบียนนักศึกษาก็จะจัดส่งFile ข้อมูลที่เป็น Excel ซึ่งAdminก็จะทำการเพิ่มรายชื่อและกำหนดสิทธิเข้าไปโดยตรงที่ละคนจะครบและต้องทำทั้งสองที่คือที่คณะและที่ ตึกชินวัตรด้วยในกรณีที่นักศึกษากลุ่มนั้นเป็นภาคสมทบเช่นเดียวกันในกรณีที่มีนักศึกษาลืมPassword ก็จะเป็นดังรูปที่3.4 และก็ต้องทำทั้งที่คณะและที่ตึกชินวัตรเช่นกันถ้าเป็นนักศึกษาสมทบ



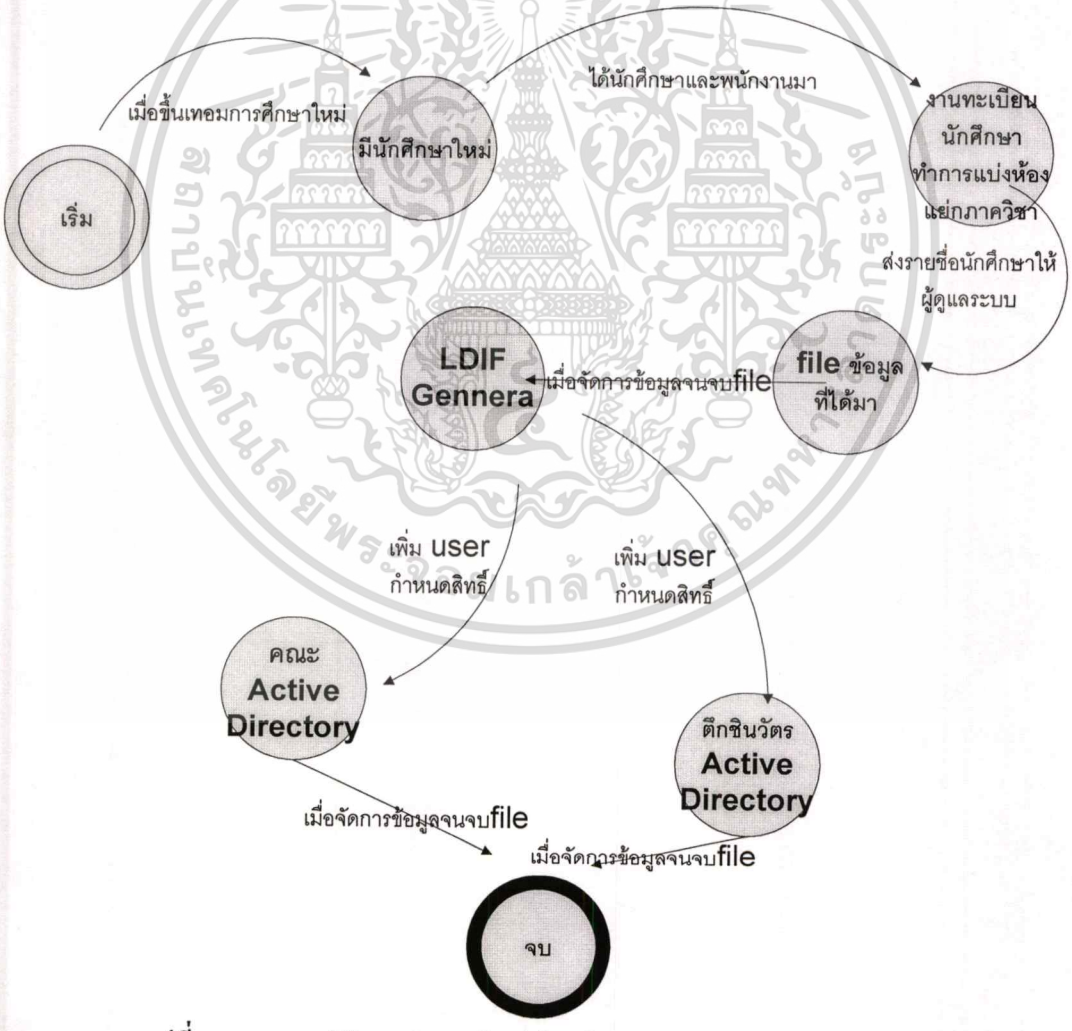
รูปที่ 3.4 แสดงวิธีการจัดการActive Directory เมื่อมีการรับนักศึกษาใหม่ในรูปแบบเดิม



รูปที่ 3.5 แสดงสิ่งที่เกิดขึ้นเมื่อมีนักศึกษาคนหนึ่งลืมPasswordในรูปแบบเดิม

– ระบบใหม่

จากระบบเดิมที่ต้องทำสองครั้งและอยู่คนละสถาณที่กันทำให้การจัดการทำได้ลำบากเราจึงได้ทำการออกแบบระบบใหม่ให้โดยใช้ โปรแกรม Genera script เข้ามาช่วยทำให้การสามารถลดงานและระยะเวลาได้มาก โดยมีรูปแบบดังรูปที่3.5



รูปที่ 3.6 แสดงวิธีการทำงานใหม่ โดยใช่ Ldif Gennerator เข้าไปช่วย

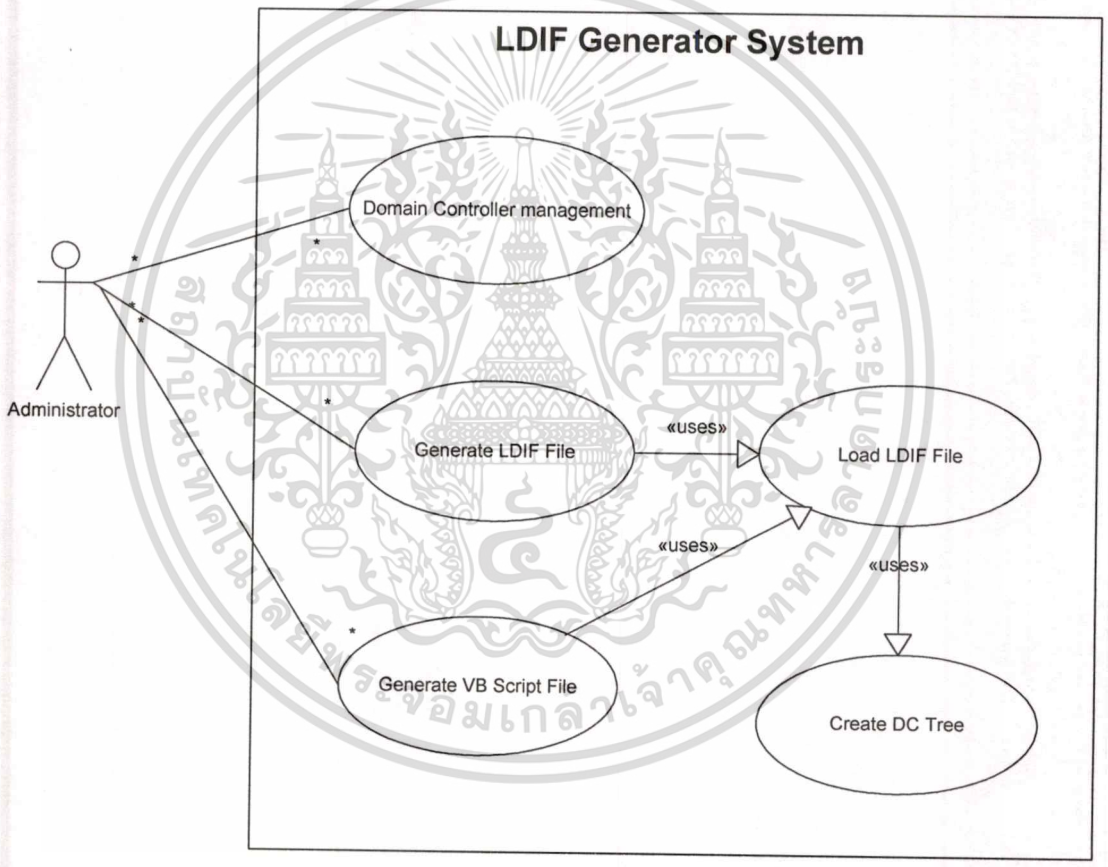
3.2 ภาพรวมโครงงานที่ได้ทำการพัฒนา

โครงงานมีระบบการจัดการหลักอยู่สามส่วน

Domain Controller Management ใช้Promo Domain ,ย้าย FSMO,รวมทั้งย้ายDomainไปsite

Generate LDIF File ใช้จัดการโครงสร้าง Objectของโดเมน

Generate VB Script File ใช้ กำหนด ค่าOptions ต่างๆของ Objects



รูปที่ 3.7 Use case Diagram

Use case discition

Use case : Domain Controller Management

Actor : Admin

Precondition : Admin request to manage Domain

Post Condition : Domain Change Option

สรุป :การบริหารงาน โดเมน

Use case : Load LDIF File

Actor : Admin

Precondition : มี LDIF file อยู่ก่อน

Post Condition : อ่านค่าLDIF File

สรุป :เก็บค่า Attribute ของ LDIF file เพื่อเตรียมเรียก Create Tree

Use case : Create Tree

Actor : Admin

Precondition : มีการLoad LDIF แล้ว

Post Condition : Treeที่เป็น โครงสร้างที่เคยมีอยู่

สรุป : นำค่า LDIF File มาอ่านค่าที่ละบรรทัดและนำมาสร้างTree

Use case : LDIF Gennerator

Actor : Admin

Precondition : Admin request to add,delete,modified and Gennera LDIF file
Load LDIF File and Create Tree เรียบร้อยแล้ว

Post Condition : ได้ LDIF File ที่มีโครงสร้างและ Attributes ที่เปลี่ยนไป

สรุป :สร้าง LDIF file ที่เกี่ยวกับ Object ตัวที่เลือกที่ได้ทำการแก้ไขไป

Use case : VB Script Gennerator

Actor : Admin

Precondition : Load LDIF File and Create Tree เรียบร้อยและต้องการจะเปลี่ยนOptionของObject

Post Condition : ได้Vb Script ที่จะนำไปใช้เปลี่ยน Option

สรุป : ใช้สร้าง Vb Script เพื่อ Set Option ของ

3.3 โครงสร้าง LDIF File

Distinguished name.....

Change type.....

Object Class.....

Attributes.....

Attributes.....

Attributes.....

บรรทัดที่1 ต้องระบุ Distinguished name (dn)

บรรทัดที่2 ประกอบไปด้วยchangetype ที่ซึ่งสามารถระบุได้สามอย่างคือ

- Add

ใช้เมื่อต้องการจะเพิ่มobject ซึ่งจะต้องระบุAttribute ต่างๆที่ใช้ในการกำหนดค่าเริ่มต้น โดยกำหนดAttributeละหนึ่งบรรทัด

เช่น dn: cn=Akerit,cn=user,dc=rallencorp,dc=com

Changetype : add

Objectclass : user

Samaccountname: Akerit

Sn: Akerit

- Delete

ใช้ในการลบ object ซึ่งไม่จำเป็นต้องระบุบค่าของAttributeใดๆ

เช่น dn: cn=Akerit,cn=user,dc=rallencorp,dc=com

Changetype : delete

- Modify

ใช้เพื่อทำการแก้ไขซึ่งมีความจำเป็นต้องระบุบวิธีการแก้ไขซึ่งก็ทำได้อีกสามวิธีคือ add replacec และ delete

เช่น dn: cn=Akerit,cn=user,dc=rallencorp,dc=com

Changetype : modify(ระบุว่าเป็นการแก้ไขobjectที่มีอยู่แล้ว)

Objectclass : user (ที่เป็น user)

Add: givenname(โดยการเพิ่มค่าgivename)

Givenneme: ken(ให้เป็นken)

Replace: sn (และเปลี่ยนค่า sn)

Sn: Thamsatit(ให้เป็นThamsatit)

– โครงสร้าง รูปแบบการเขียนVB script ในการกำหนดค่า ต่างๆ

เนื่องจาก Active Directory จัดเก็บข้อมูลทุกอย่างในรูป object การเขียนโปรแกรมเพื่อเข้าไปจัดการ ก็เพียงแต่ call object ตัวนั้นๆแล้วแล้วเรียก method และตามด้วยค่าที่ต้องการจะกำหนดให้เท่านั้น ดังตัวอย่าง

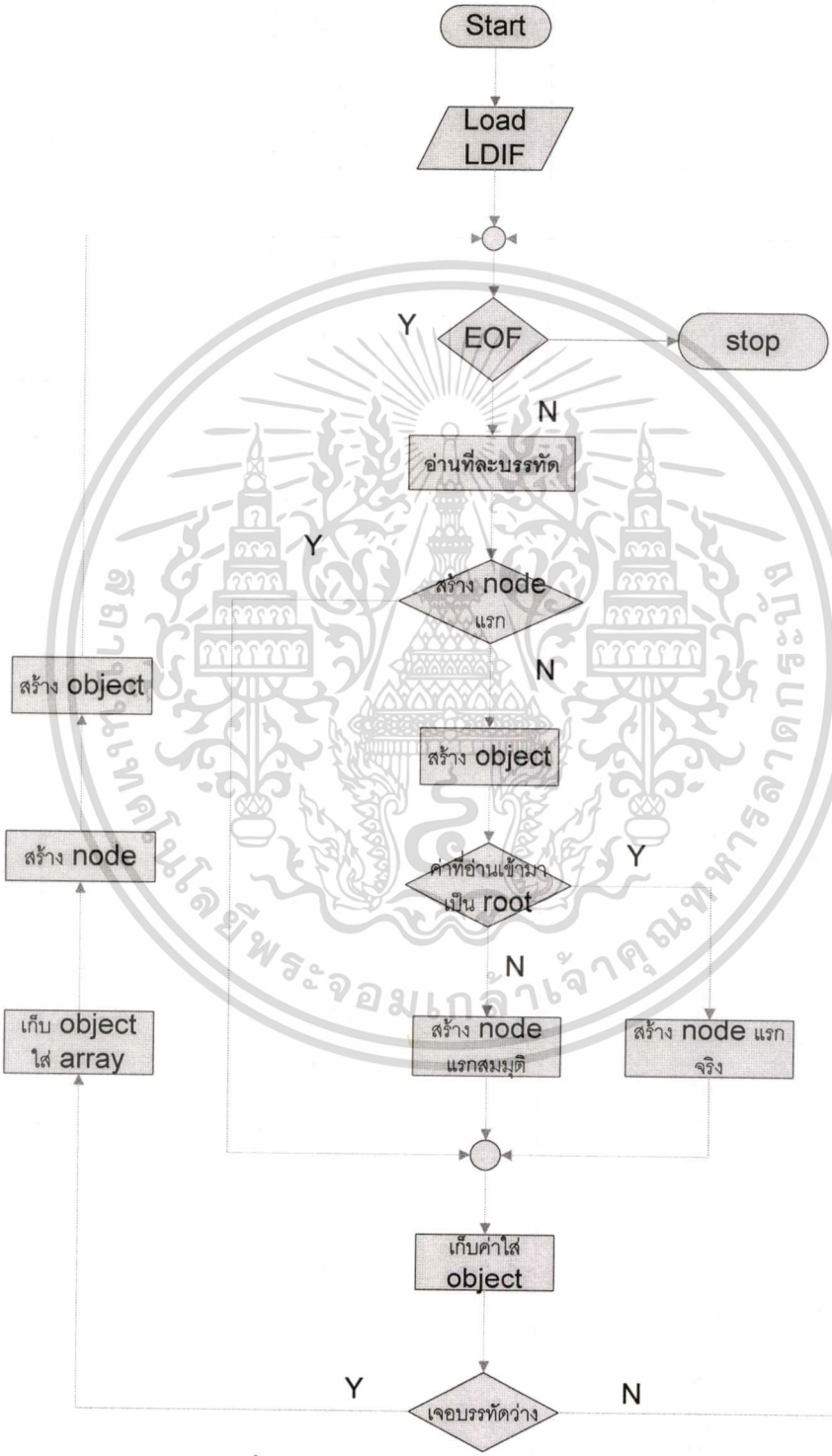
```
'------SCRIPT CONFIGURATION---
strUserDN = "<userDN>"
'CN=IS45061614 ,OU= IT ,DC=IT,DC=KMITL,DC=AC,DC=TH
strNewPasswd = "Newpassword"  'P@SSWORD
'------END CONFIGURATION-------
set objUser = GetObject("LDAP://" & strUserDN )
objUser.Setpassword(strNewPasswd)
Wscript.echo " Password set "objUser.get("cn")
```

3.4 การออกแบบระบบงาน

เมื่อได้ศึกษาถึงโครงสร้าง LDIF และรูปแบบของ VB Script แล้วนำมาออกแบบส่วนต่าง ๆ ของโปรแกรม เพื่อใช้ในการสร้าง script และ LDIF File เพื่อจะนำไปใช้และพิจารณาใช้ LDIF ในการกำหนดค่าให้ Attributes ต่าง ๆ ของ Object และใช้ VB Script ในการเรียกใช้ Method ของ Object เพื่อให้ได้ Script ที่ทำงานได้ครอบคลุมในการบริหารงาน Object มากที่สุด โดยแบ่งเป็นส่วนต่าง ๆ ของโปรแกรมได้ดังนี้

– Load LDIF File and Tree Generate

เป็นส่วนแรกของโปรแกรมที่เราจะทำการเรียกใช้ในกรณีที่เรามีโครงสร้างเดิมอยู่แล้วและต้องการที่จะทำการสร้างObjectเพิ่มในโครงสร้างเดิมจึงมีความจะเป็นต้องรู้ว่าโครงสร้างเดิมเป็นอย่างไร



รูปที่ 3.8 FlowChart แสดงวิธีการสร้าง Tree

- Add , Modify , Delete Object by LDIF

ในส่วนนี้มีการเรียกใช้ 2เงื่อนไขคือ ในกรณีที่ได้ Load โครงสร้างจากLDIF Fileหรือต้องการสร้างObject แบบ ไม่ได้ Load โครงสร้าง เดิม

- Manage by VB Script

3.5 ซอฟต์แวร์ที่ใช้ในการพัฒนาโปรแกรม

Microsoft Windows XP	:	ระบบปฏิบัติการที่ใช้ในการพัฒนาโปรแกรม
Microsoft Window 2003 Server	:	ระบบปฏิบัติการที่ใช้ในการติดตั้งโดเมนเพื่อทำการทดสอบ
Microsoft Visual Basic.NET	:	ซอฟต์แวร์ที่ใช้ในการพัฒนาโปรแกรม
Notepad	:	Text Editor ที่ใช้ในการพัฒนา

3.6 การออกแบบหน้าจอการทำงานของโครงงานการพัฒนาระบบงาน

หน้าจอหลักของโครงงานการพัฒนาระบบงาน

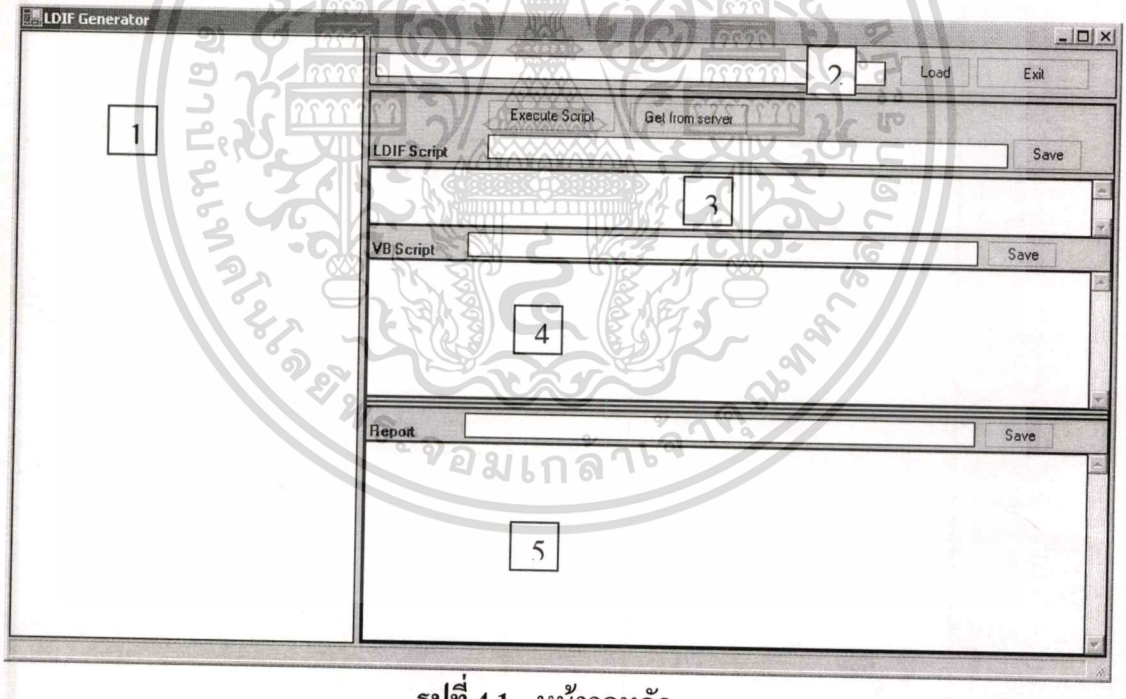
เริ่มต้นการใช้งานโปรแกรมซึ่งสามารถเรียกใช้ที่เครื่องใดๆก็ได้แสดงผลดังรูปที่3.9โดยโปรแกรมแบ่งออกเป็น4ส่วนดังนี้

- ส่วนการแสดงผลของ Tree ซึ่งแสดงรูปแบบของ Active Directory
- LDIF Script แสดง LDIF File ที่มีการเปลี่ยนแปลงที่เกิดจากการใช้งานโปรแกรมในการเพิ่ม ,แก้ไข,ลบ object
- VB Script แสดง Script File ที่มีเกิดขึ้นจากการกำหนดค่าที่ต้องเรียนใช้ method ของ object ที่ไม่สามารถกำหนดค่าได้โดยใช้LDIF
- Report แสดงผลว่าถ้านำเอา file ที่ได้ทั้งสองส่วนไปใช้งานแล้วจะเกิดผลอย่างไรบ้าง

บทที่ 4
การใช้งานโปรแกรม

4.1 หน้าจอหลักแสดงเมื่อ Run Program LDIF Generator มีองประกอบอยู่ด้วยกัน5ส่วน

- ส่วนที่หนึ่งส่วนแสดงผลโครงสร้าง Tree
- ส่วนที่สองส่วนที่ใช้ load ldif file
- ส่วนที่สามเป็นส่วน ldif file ที่เป็น output ที่จะนำไปใช้
- ส่วนที่สี่เป็นส่วนที่ vb script ที่เป็น output ที่จะนำไปใช้
- ส่วนที่ห้าเป็นส่วนที่ แสดงผลว่าได้ทำการแก้ส่วนใดในโครงสร้างไปบ้าง

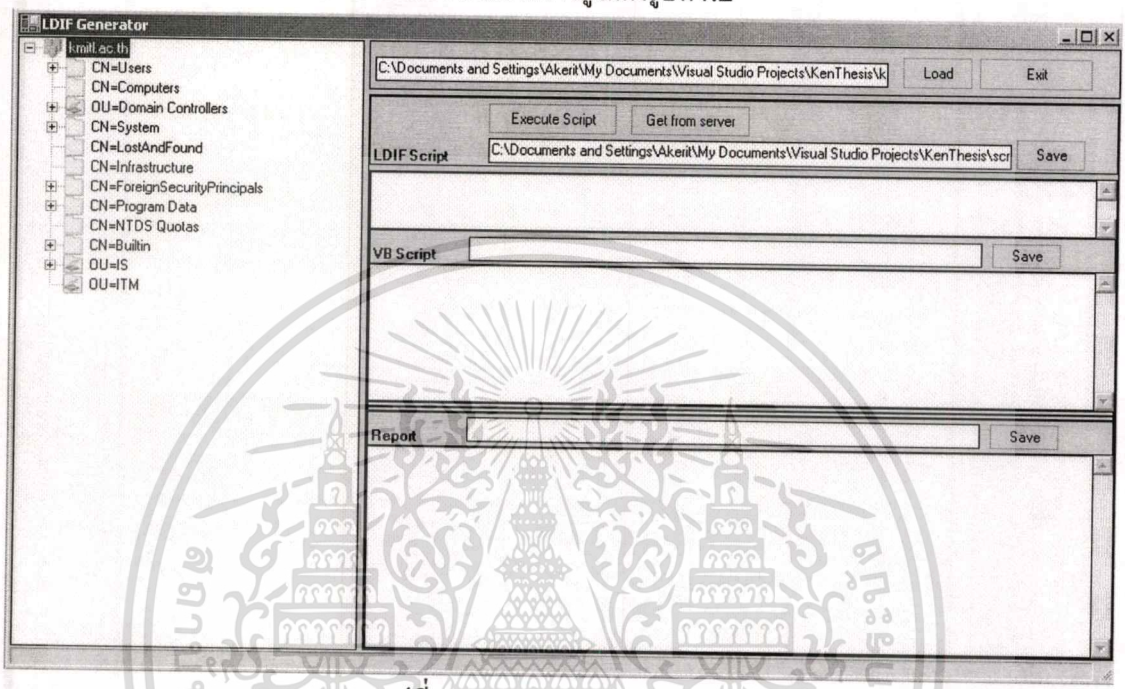


รูปที่ 4.1 หน้าจอหลัก

4.2 ขั้นตอนการสร้าง LDIF File เพื่อใช้ในการจัดการโครงสร้าง

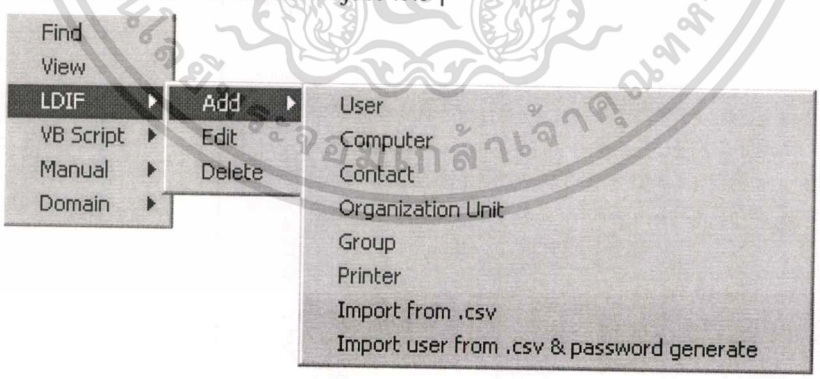
- RUN Ldifde - f output.ldf ที่เครื่อง โดเมน
- เรียกใช้โปรแกรม LDIF Generator
- คลิกที่ปุ่มLoad และเลือก file Output.ldf
- รอจนกว่าโปรแกรมจะสร้างโครงสร้าง

ทั้งนี้ขึ้นอยู่กับว่าโครงสร้างประกอบด้วย Object มากน้องเท่าใดจะใช้เวลานานไม่เท่ากันหลังจากได้โครงสร้าง สามารถกดที่เครื่องหมาย + เพื่อทำการกระจายโครงสร้างดูได้ดังรูปที่4.2

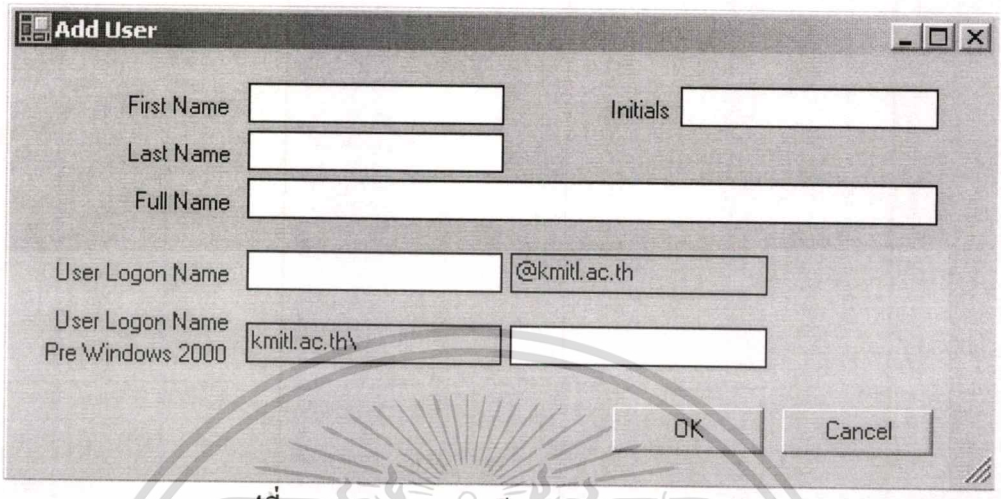


รูปที่ 4.2 ผลจากGenera Tree

- คลิกเม้าขวาที่ Object เพื่อ เรียกใช้Menu : add,edit,delete
- ใส่รายละเอียด ของแต่ละ Object นั้นๆ

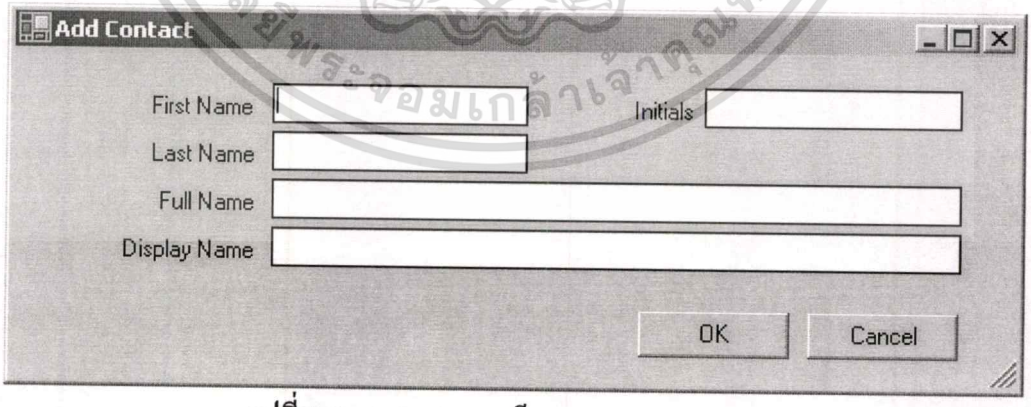


รูปที่ 4.3 Main Menu

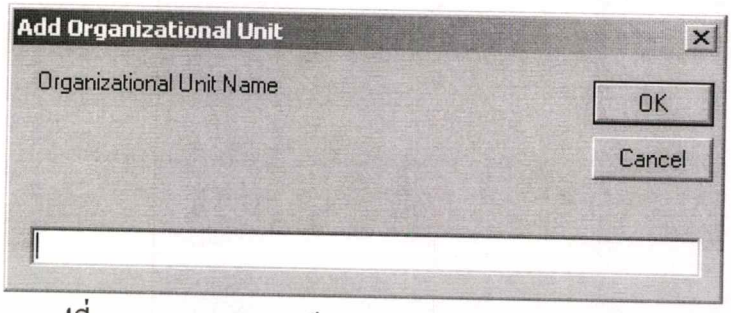


รูปที่ 4.4 แสดงรายละเอียดของการAdd User

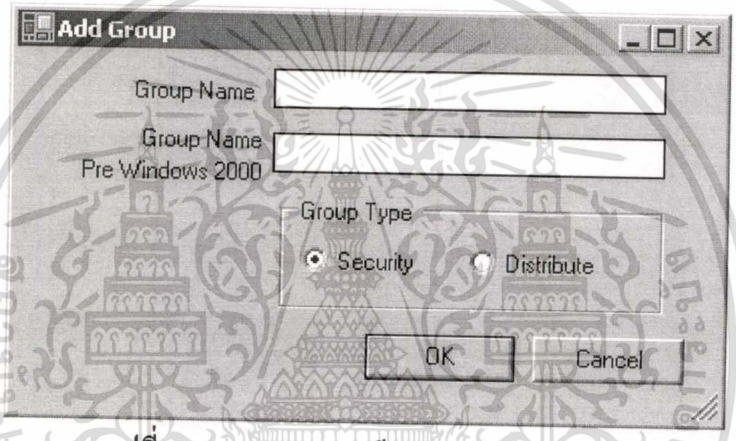
รูปที่ 4.5 แสดงรายละเอียดการ Add Computer



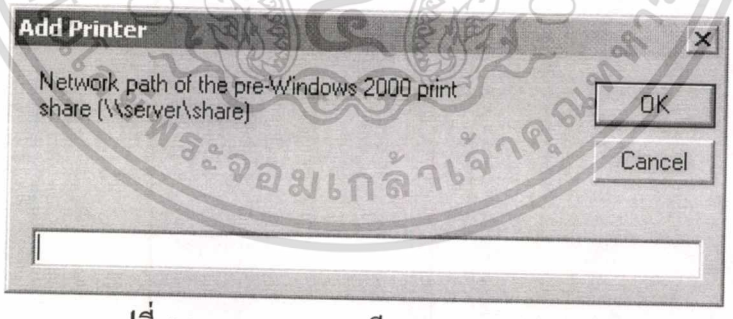
รูปที่ 4.6 แสดงรายละเอียดการ Add Contact



รูปที่ 4.7 แสดงรายละเอียดการ Add Organization Unit



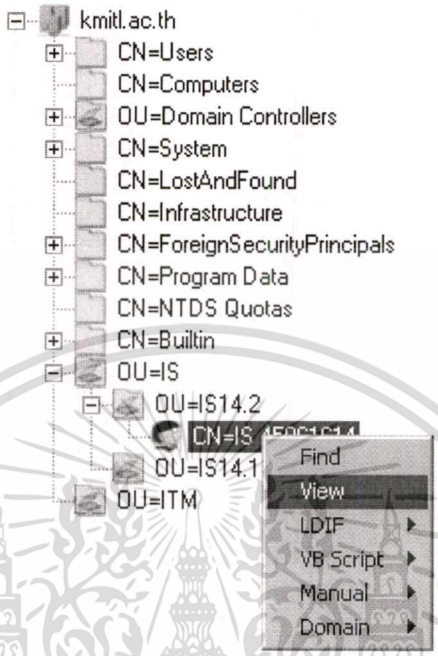
รูปที่ 4.8 แสดงรายละเอียดการ Add Group



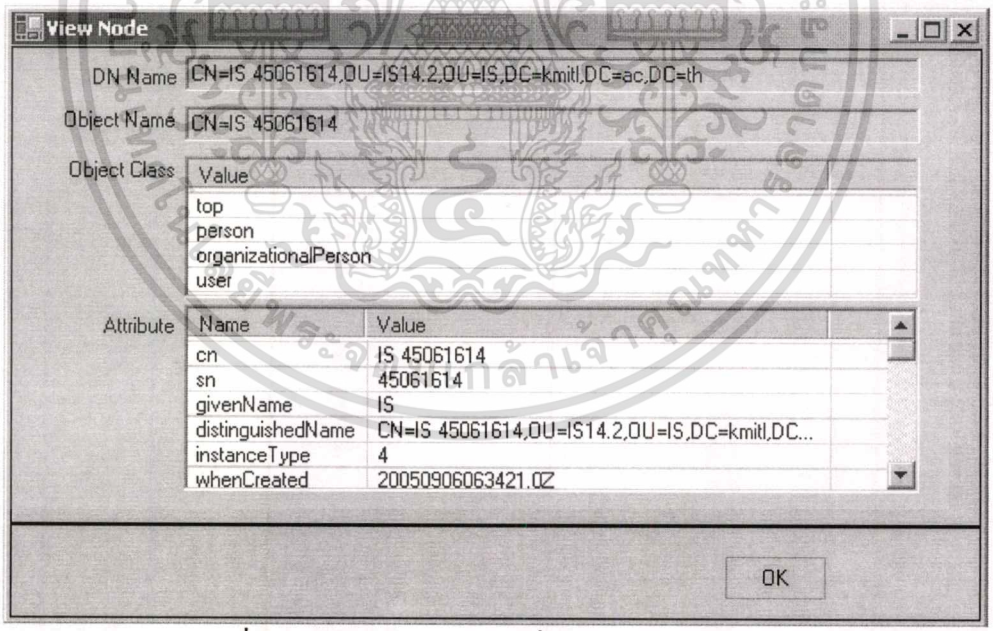
รูปที่ 4.9 แสดงรายละเอียดการ Add Printer

4.3 วิธีการเรียกดูค่ารายละเอียดของObject

- เลือกObject ที่ต้องการ
- คลิกเม้าขวาโปรแกรมจะแสดงMenu
- เลือก Menu View
- โปรแกรมก็จะแสดงรายละเอียดของObject



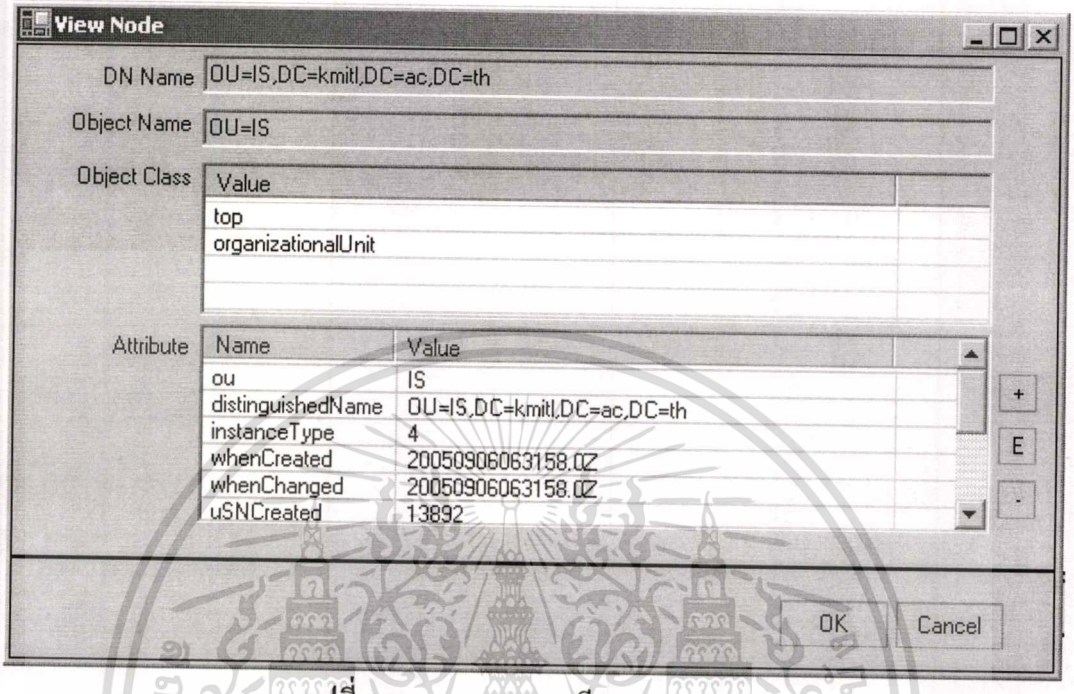
รูปที่ 4.10 การเลือก Object เพื่อต้องการจะดูรายละเอียด



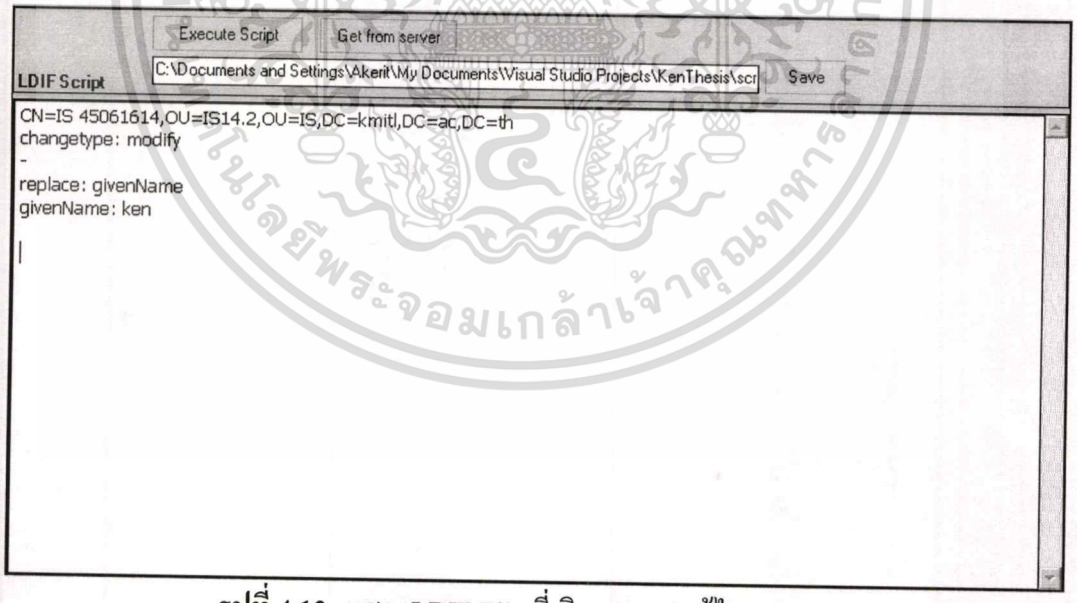
รูปที่ 4.11 แสดงรายละเอียดเมื่อเลือก Menu View

4.4 วิธีแก้ไขข้อมูลภายในObject

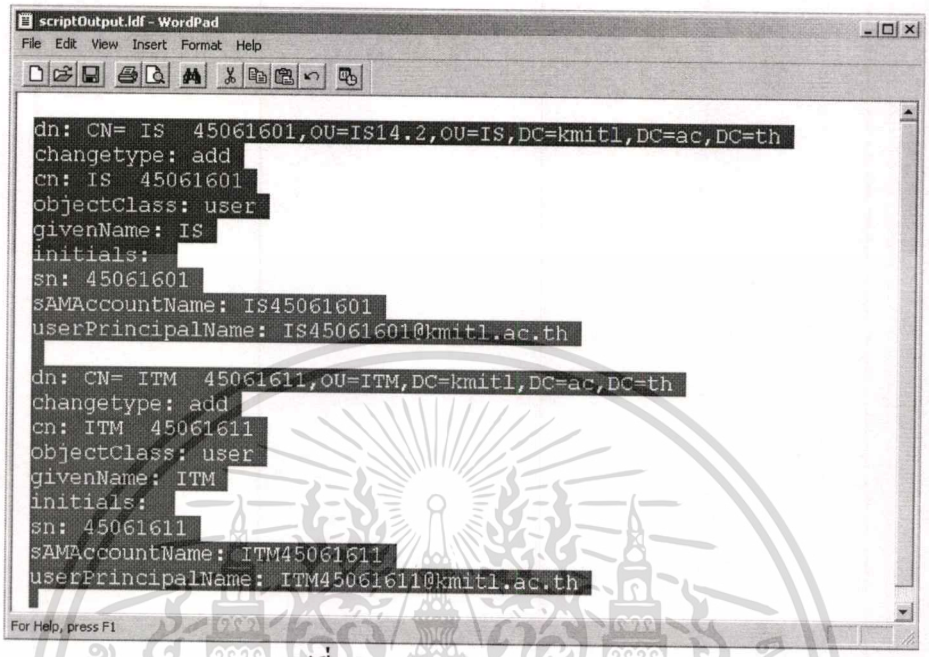
- เลือกObject ที่ต้องการ
- คลิกเม้าขวาโปรแกรมจะแสดงMenu
- เลือก LDIF และเลือกedit



รูปที่ 4.12 แสดงรายละเอียดการ Edit



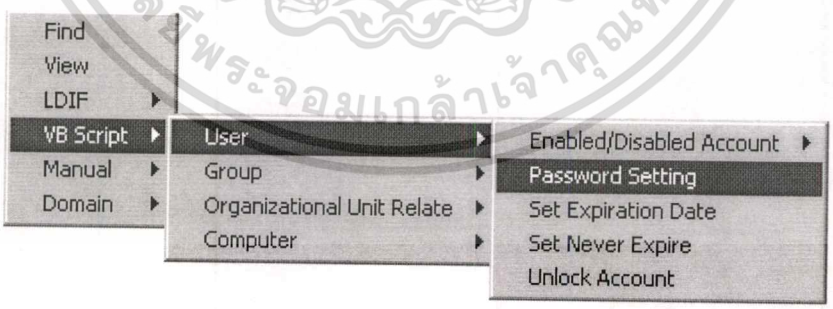
รูปที่ 4.13 แสดงLDIF File ที่เกิดจากการแก้ไขObject



รูปที่ 4.14 ตัวอย่าง LDIF file

4.5 วิธีการสร้าง VB Script

- เลือกObject ที่ต้องการ
- คลิกเม้าขวาโปรแกรมจะแสดงMenu
- เลือก VB Script เลือก ชนิด Object ที่ต้องการ
- ใส่ค่าที่สิ่งที่ต้องการจะกำหนด



รูปที่ 4.15 แสดงการใช้โปรแกรมสร้าง VB Script

บทที่ 5
สรุปผลและข้อเสนอแนะโครงการพัฒนาระบบงาน

5.1 สรุปผลโครงการพัฒนาระบบงาน

จากผลการทดสอบการนำFile LDIF และ VB Script ไปใช้ในการกำหนดค่าให้กับserver ที่มีระบบActive Directory พบว่าทำงานได้ดีแล้วสามารถช่วยให้การจัดการserver ที่อยู่ห่างไกลได้โดยการส่ง file ให้นำไปเรียกใช้งานทำให้หน่วยงานที่มี ผู้จัดการระบบน้อยแต่มีserver กระจายอยู่หลายที่ทำงานได้ละดวกมากขึ้นรวมทั้งยังได้ไปทดลองใช้ในการสร้างUser จำนวนมากในการแค่เรียนใช้ Script file เพียงครั้งเดียวรวมถึงการ Join to Domain ของเครื่องคอมพิวเตอร์ซึ่งทำโดยuser ทำให้งานของ ผู้ดูแลระบบทำงานในการSupportน้อยลง และที่สำคัญที่สุด LDIF เป็นมาตรฐานกลางที่สามารถจัดการ Object ใน ระบบโครงสร้าง แบบ Directory ไม่ได้ใช้กันในระบบปฏิบัติการ Windowsเพรียงอย่างเดียวเท่านั้นยังลองรับใน Netwarec และ Linux อีกด้วย

5.2 ข้อเสนอแนะโครงการพัฒาระบบงาน

- ก่อนนำLDIF file และ VB Script ไปใช้งานควรทดสอบก่อนนำไปใช้จริงทุกครั้ง เนื่องจากถ้าได้ทำการ เรียกใช้ LDIF file และ VB Script จะไม่สามารถเรียกคืนได้ยกเว้นได้มีการBackupไว้
- การใช้งานโปรแกรมผู้ใช้จะต้องรู้จักระบบรายชื่อแบบ Directory อยู่บ้างและทำการจัดการกับobjectตามลำดับ
- ในการสร้างโครงสร้างTree ที่ใช้แสดงระบบรายชื่อของ Active Directoryใช้เวลามากถ้ามีโครงสร้างใหญ่
- การบริหารงานWindows ด้วย Script เป็นวิธีการใหม่และจะเป็นแนวทางที่คาดว่าจะได้รับความสนใจมากขึ้นในระยะเวลาอันใกล้

บรรณานุกรม

Oram, Andy. 2003. **Active Directory Cookbook for Windows Server 2003 & Windows 2000.** California : O'Reilly & Associates.

Reynolds, Matthew and Blair, Richard. 2002. **คัมภีร์การใช้ Visual Basic.NET ฉบับสมบูรณ์.** แปลโดย ชัชวาล ศุภเกษม. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

Seitsonen, Mika and Kouti, Sakari. 2005. **Inside Active Directory Second Edition.** Boston : Pearson Education.

ประวัติผู้เขียน

ชื่อผู้เขียน	นายเอกฤทธิ์ ธรรมสถิต
วันเกิด	1 มิถุนายน 2521
สถานที่เกิด	ฉะเชิงเทรา
วุฒิการศึกษา	วิทยาศาสตร์บัณฑิต คณะวิทยาศาสตร์ สาขาสถิติ มหาวิทยาลัยศรีนครินทรวิโรฒ
ตำแหน่งหน้าที่	
สถานที่ทำงาน	