การบริหารจัดการ internet/intranet service แบบกึ่งรวมศูนย์

วิภัทร ศรุติพรหม*

บทคัดย่อ

ได้ออกแบบระบบบริหารจัดการ internet/intranet แบบกึ่งรวมศูนย์ ที่เหมาะสมกับองค์กรแบบสถาบันการศึกษา มีคุณสมบัติคือทุก host/service ที่ให้บริการในระบบ ยังคงใช้ชื่อบัญชีผู้ใช้และรหัสผ่านเดียวกันซึ่งรวมกันอยู่ที่ศูนย์กลาง โดยที่ผู้ดูแลระบบเจ้าของ host/service สามารถบริหารจัดการทรัพยากรของตนเองแยกเป็นอิสระจากศูนย์กลาง ได้วิเคราะห์เปรียบเทียบผลกระทบต่าง ๆของการบริหารจัดการแบบกึ่งรวมศูนย์กับอีก 2 แบบคือแบบรวมศูนย์กลางและแบบแยกอิสระ ใช้กรณีศึกษาเป็นสภาพแวดล้อมของมหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ สร้างต้นแบบด้วยซอฟต์แวร์แบบโอเพนซอร์สระบบปฏิบัติการลินุกซ์

Keywords: internet/intranet,host,service,manage

---

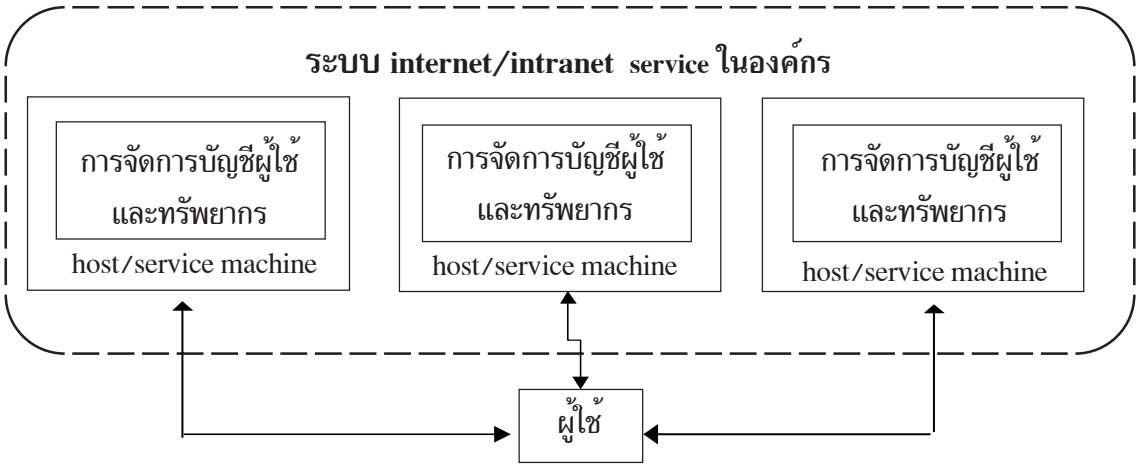
* นักวิชาการคอมพิวเตอร์ ชำนาญการ
ศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

1. บทนำ

ปัจจุบันได้มีการใช้งานระบบเครือข่ายอินเทอร์เนตกัน อย่างแพร่หลายกว้างขวาง สถาบันการศึกษาต่าง ๆมีระบบเครือข่ายคอมพิวเตอร์น้อย อินเทอร์เนตและบริการระบบงานต่าง ๆเชื่อมต่อกันผ่านเครือข่ายภายใน (intranet) ของสถาบัน และเชื่อมต่อเข้ากับเครือข่ายภายนอก (internet) ด้วย เมื่อการขยายตัวของระบบบริการผ่านเครือข่าย (internet/intranet service) มีจำนวนมากขึ้น ก่อให้เกิดปัญหาทั้งต่อผู้รับบริการ (user) และเจ้าของผู้ดูแลระบบ (admin)

การบริหารจัดการระบบแบบเดิมทั่ว ๆไปมีลักษณะแต่ละhost/service เป็นอิสระจากกัน ดังนั้นเมื่อมีจำนวน host/serviceมากขึ้น ก็ทำให้เกิดปัญหาความยุ่งยากในการบริหารจัดการบัญชีผู้ใช้ รวมทั้งก่อปัญหาให้แก่ผู้ใช้บริการที่ต้องจำชื่อบัญชีผู้ใช้รหัสผ่านหลาย ๆอันที่เป็นของแต่ละ host/service

ในปัจจุบันนิยมการบริหารจัดการแบบศูนย์กลาง (directory service) ที่อนุญาตผู้ใช้สามารถใช้บริการทุกระบบโดยการป้อนชื่อผู้ใช้และรหัสผ่านเพียงครั้งเดียว (single sign-on) ระบบนี้เหมาะสมกับองค์กรทางธุรกิจที่มีระบบงานเฉพาะทางและผู้ใช้ต้องมีความรับผิดชอบสูง เนื่องจากระบบมีการตรวจสอบเพียงครั้งเดียว ระบบนี้ไม่เหมาะกับองค์กรที่มีจำนวนเครื่องคอมมีผู้ใช้หลาย ๆคนจำเป็นต้องร่วมกันใช้คอมพิวเตอร์เครื่องเดียวกัน



รูปที่ 1. วิธีบริหารจัดการแบบแยกอิสระจากกัน

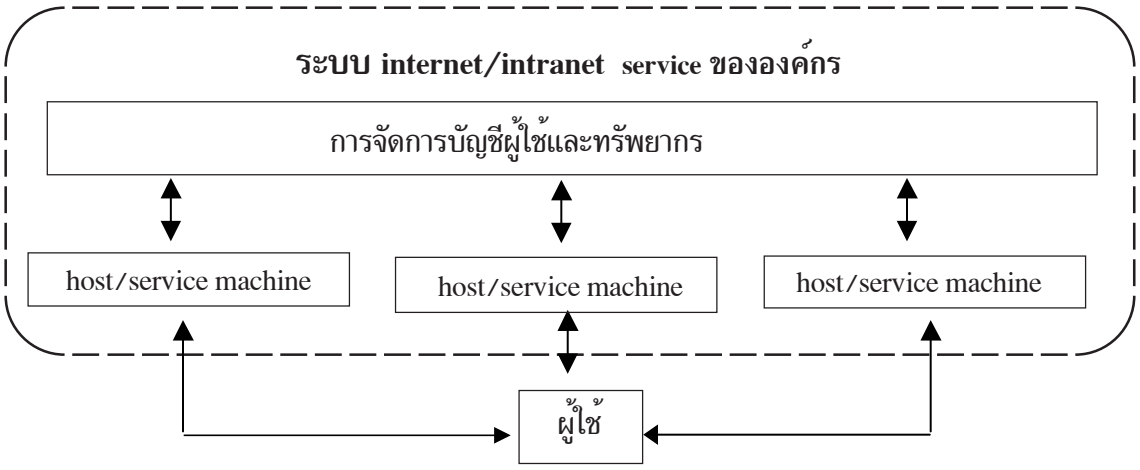
2. วิธีบริหารจัดการ host/service

วิธีบริหารจัดการ host/service ที่นิยมใช้กันแพร่หลายมี 2 แบบคือ

2.1 วิธีบริหารจัดการแบบแยกอิสระจากกัน

จากรูปที่ 1. การบริหารจัดการระบบแบบนี้เป็นแบบพื้นฐาน มีลักษณะแต่ละ host/service ทั้งหมดในระบบแยกเป็นอิสระจากกัน มีการบริหารจัดการบัญชีผู้ใช้และทรัพยากรต่าง ๆแยกจากกันไปตาม host/service เป็นภาพของระบบบริการย่อย ๆ ที่ไม่มีความกลมกลืนเป็นเนื้อเดียวกันข้อดีของรูปแบบนี้ก็คือ จัดสร้างระบบง่าย เพราะไม่ต้องเชื่อมต่อเข้ากับ host/service อื่น ข้อเสียของรูปแบบนี้คือ ต้องดูแลบริหารจัดการบัญชีผู้และใช้และทรัพยากรต่าง ๆของทุก ๆ host/service ก่อปัญหาให้แก่ผู้ใช้บริการที่ต้องจำชื่อบัญชีผู้ใช้/รหัสผ่านหลาย ๆอันที่เป็นของแต่ละhost/service

2.2 วิธีบริหารจัดการแบบรวมศูนย์กลาง



รูปที่ 2. วิธีบริหารจัดการแบบรวมศูนย์กลาง

จากรูปที่ 2 การบริหารจัดการระบบแบบนี้มีลักษณะHost/service ทั้งหมดในระบบเชื่อมต่อรวมเป็นระบบเดียวกัน

มีการบริหารจัดการบัญชีผู้ใช้และทรัพยากรของHost/service ทั้งหมดในระบบอยู่ที่ศูนย์กลาง เหมาะสำหรับการใช้งานในองค์กรที่มีรูปแบบใช้งานชัดเจนแน่นอน

ข้อดีของรูปแบบนี้คือ ระบบบริการได้รับการจัดทำให้มีความกลมกลืนกันเป็นเนื้อเดียว ผู้รับบริการใช้ชื่อบัญชีผู้ใช้และรหัสผ่านเพียงอันเดียวและเพียงครั้งเดียว สามารถเข้าไปใช้ได้ทุกบริการ (single sign-on)

ข้อเสียของรูปแบบนี้คือ ต้องดำเนินการบริหารจัดการทรัพยากรของแต่ละ host/service ซอฟต์แวร์ที่ใช้ในระบบต้องเป็นมาตรฐานข้อกำหนดในการเชื่อมต่อ host/service ด้วย

3. เทคโนโลยีที่เกี่ยวข้องกับการบริหารจัดการ internet/intranet service

3.1 ระบบปฏิบัติการลินุกซ์

เป็นระบบปฏิบัติการแบบยูนิกซ์ที่ใช้กับเครื่องไมโครคอมพิวเตอร์ได้ เป็นซอฟต์แวร์แบบโอเพนซอร์ส ที่เพื่อการศึกษาทั้งในเชิงวิศวกรรมย้อนรอยและต่อยอดได้ ระบบปฏิบัติการลินุกซ์ได้รับการพัฒนาอย่างต่อเนื่อง จนถึงปัจจุบัน สามารถเลือกใช้งานบริหารจัดการได้ทั้งรูปแบบที่แยกอิสระจากกันรวมศูนย์กลาง

3.2 UNIX POSIX account

เป็นฐานข้อมูลบริหารจัดการทรัพยากรรักษาความปลอดภัยเป็นแบบ Standard UNIX password ที่เป็นพื้นฐานดั้งเดิมใช้กันในระบบปฏิบัติการแบบยูนิกซ์ ระบบจัดเก็บข้อมูลสำหรับการจัดการทรัพยากรไว้ใน host ของตนเอง เมื่อผู้ใช้ติดต่อเข้ามาเพื่อขอใช้ทรัพยากร ระบบจะทำการพิสูจน์ตัวตนและตรวจสอบอนุญาติสิทธิการใช้ทรัพยากรใน host ของตนเองนี้ ตามข้อมูลที่ได้บันทึกไว้

3.3 Directory Services

เป็นฐานข้อมูลใช้จัดเก็บข้อมูลทรัพยากรต่าง ๆ ของสมาชิก เช่นข้อมูลส่วนบุคคล อุปกรณ์คอมพิวเตอร์ และสิทธิการใช้งานต่าง ๆ เป็นต้น ใช้ประโยชน์สำหรับการค้นหาข้อมูลผู้ใช้ระบบรักษาความปลอดภัย ตลอดจนการบริหารจัดการทรัพยากรแบบรวมศูนย์กลาง

3.4 X.500 Directory

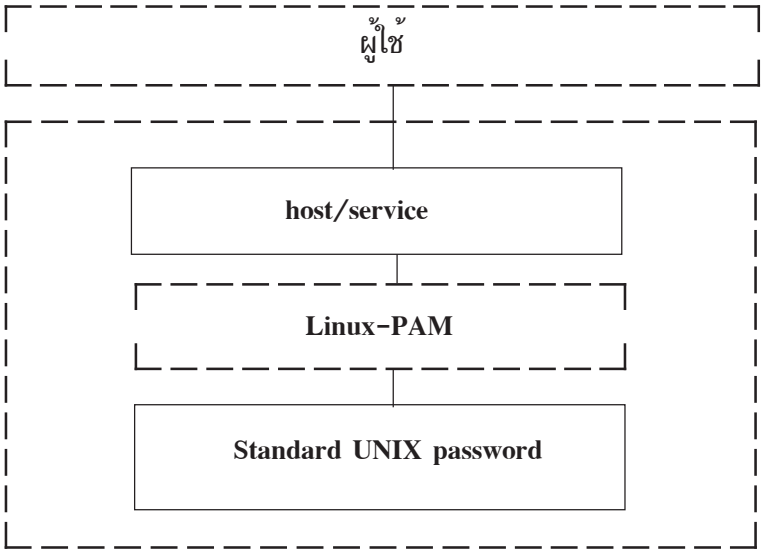
เป็นมาตรฐานข้อกำหนดเกี่ยวกับ DirectoryServices ใช้เป็นต้นแบบสำหรับอุตสาหกรรมที่เกี่ยวข้องกับDirectory Services เป็นระบบที่มีประสิทธิภาพสูงสามารถจัดเก็บข้อมูลได้หลากหลาย ใช้โปรโตคอลคือ Directory AccessProtocal (DAP) ในการเชื่อมต่อเข้าถึงข้อมูลของ X.500Directory ต้องมีเครื่องบริการแม่ข่าย (server) ที่ใช้ในการจัดเก็บข้อมูล

3.5 Lightweight Directory Access Protocol (LDAP)

โปรโตคอลใช้สำหรับเชื่อมต่อเข้าถึงข้อมูล X.500Directory แทนโปรโตคอล DAP ที่มีความซับซ้อนมาก ทำให้สิ้นเปลืองทรัพยากร ระบบทำงานล่าช้า การทำงานแบ่งออกเป็น 2ระดับ คือระดับที่เป็น LDAP server ทำหน้าที่เป็นเครื่องบริการแม่ข่ายของฐานข้อมูล และระดับที่เป็น LDAP client ทำหน้าที่เชื่อมต่อเข้ากับข้อมูล LDAP server ระบบงานหรือซอฟต์แวร์ที่ใช้เชื่อมต่อทำงานกับ LDAP server ต้องมีคุณสมบัติเป็นไปตามข้อกำหนด

3.6 Pluggable Authentication Modules for Linux (Linux-PAM)

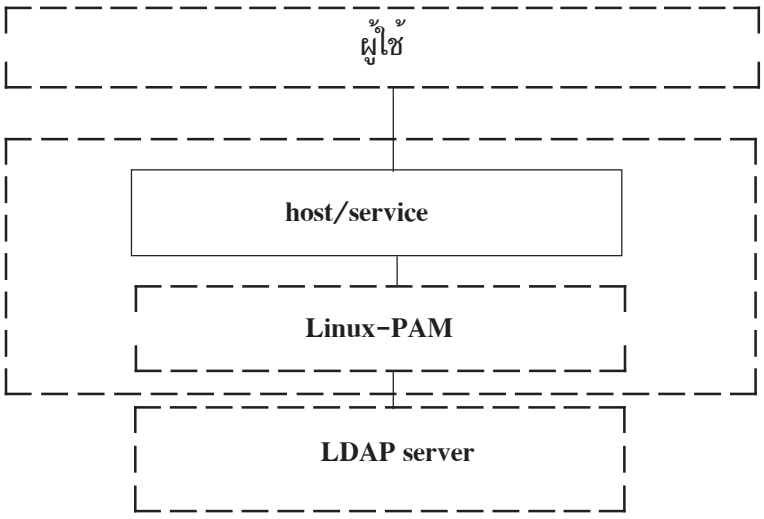
เป็นเครื่องมือระบบรักษาความปลอดภัยของระบบปฏิบัติการลินุกซ์ ในขั้นตอนพิสูจน์ตัวตนของผู้ร้องขอใช้ทรัพยากรของระบบ เป็นเครื่องมือที่มีความยืดหยุ่นสูง สามารถใช้เป็นตัวกลางเชื่อมต่อกับระบบรักษาความปลอดภัยแบบต่าง ๆ ได้รับความนิยมใช้ในระบบปฏิบัติการลินุกซ์



รูปที่ 3 แสดงขั้นตอนทำงานของระบบบริหารจัดการแบบแยกอิสระจากกัน

3.7 ขั้นตอนทำงานของระบบการบริหารจัดการแบบแยกอิสระจากกัน

การบริหารจัดการแบบแยกอิสระใช้ฐานข้อมูลทรัพยากรแบบ UNIX POSIX account และระบบรักษาความปลอดภัยแบบ Standard UNIX password (รูปที่ 3.) เมื่อมีสมาชิกขอใช้ทรัพยากร ระบบบริการดำเนินการตั้งแต่ขั้นตอนพิสูจน์ตัวตนและตรวจสอบข้อมูลภายใน host ของตนเอง จนกระทั่งถึงขั้นตอนให้บริการ ในปัจจุบันมีการใช้ Linux-PAMเป็นตัวกลางเชื่อมต่อเข้ากับระบบรักษาความปลอดภัยแบบ Standard UNIX password



รูปที่ 4 แสดงขั้นตอนทำงานของระบบบริหารจัดการแบบรวมศูนย์กลาง

3.8 ขั้นตอนทำงานของระบบการบริหารจัดการแบบรวมกลาง

การบริหารจัดการแบบแยกรวมศูนย์กลางใช้ฐานข้อมูลทรัพยากรและระบบรักษาความปลอดภัยเป็นแบบ DirectoryServices ระบบนี้ (รูปที่ 4.)มีเครื่องบริการแม่ข่าย LDAP serverเพื่อเป็นศูนย์กลางข้อมูล เมื่อ host/service ได้รับการร้องขอใช้บริการจากผู้ใช้ host/service นั้นเริ่มดำเนินการขั้นตอนพิสูจน์ตัวตนและสิทธิการใช้การทรัพยากรไปยัง LDAP server ที่ทำหน้าที่ศูนย์กลางฐานข้อมูลที่กำหนด เมื่อผ่านขั้นตอนระบบรักษาความปลอดภัยแล้ว host/service จึงเริ่มให้บริการแก่ผู้ขอใช้บริการ

ซอฟต์แวร์ระบบบริการสามารถเชื่อมต่อกับ LDAPServer ได้ 2 วิธีคือวิธีแรก ซอฟต์แวร์ระบบบริการต้องเชื่อมต่อเป็นส่วนหนึ่งของระบบโดยตรง ซอฟต์แวร์ต้องมีคุณสมบัติตามข้อกำหนดของ LDAP server (LDAP support) ทำให้มีความยุ่งยากในการจัดหาซอฟต์แวร์และขาดความยืดหยุ่น ส่วนวิธีที่สองเป็นการเชื่อมต่อกับ LDAP server ผ่าน Linux-PAM ซอฟต์แวร์ระบบบริการนี้ต้องมีคุณสมบัติเชื่อมต่อโดยตรงกับLinux-PAMส่วนขั้นตอนการเชื่อมต่อเข้ากับ LDAP server เป็นความสามารถของ Linux-PAM (PAM-LDAP support)

4. การออกแบบและจัดทำ

4.1 วัตถุประสงค์ของการออกแบบ

ออกแบบวิธีบริหารจัดการ internet/intranet แบบกึ่งรวมศูนย์ ที่มีความเหมาะสมสอดคล้องกับการใช้งานในองค์กรแบบสถาบันการศึกษา เป็นระบบที่มีการเชื่อมต่ออย่างกลมกลืนกัน แต่ยังคงมีความยืดหยุ่นและอิสระในการบริหารจัดการทรัพยากรของหน่วยงาน

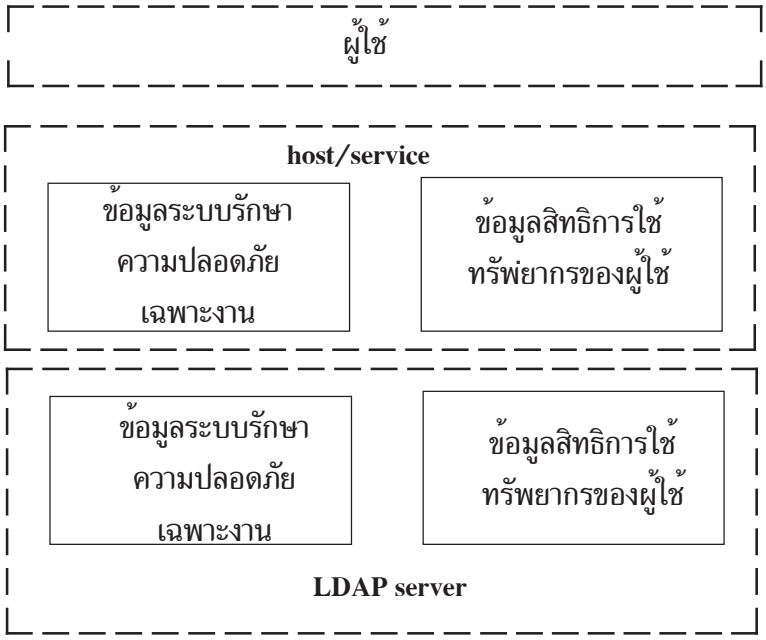
4.2 กำหนดเงื่อนไขสภาพแวดล้อม

ระบบบริการบนเครือข่าย host/service ที่ใช้การบริหารจัดการแบบกึ่งรวมศูนย์ตามเทคนิควิธีการจัดเก็บข้อมูลที่เหมาะสมด้วยระบบปฏิบัติการแบบลินุกซ์ ประกอบด้วย LDAP server,Mail service, Web mail service, Web hosting service,FTP Service, Computer Lab service, Computer Lab printingService ทั้งหมดนี้ใช้รวมเป็นระบบบริการบนเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ทุก host/service ต้องใช้บัญชีผู้ใช้และรหัสผ่านเดียวกันหมด แต่มีความยืดหยุ่นและอิสระ ทุก host/service ถูกบริหารจัดการทรัพยากรเฉพาะของหน่วยงานเอง ไม่จำเป็นต้องมาจัดการที่ศูนย์กลาง

4.3 ขั้นตอนวิธีออกแบบ

ได้ศึกษาระบบปฏิบัติการลินุกซ์ในส่วนของการจัดการทรัพยากรและระบบรักษาความปลอดภัยโดยละเอียด พบว่าสามารถประยุกต์จัดทำการบริหารจัดการแบบกึ่งรวมศูนย์ โดยให้มีระบบบริหารจัดการทรัพยากรและระบบรักษาความปลอดภัยไว้ ทั้งในส่วนที่เป็นศูนย์กลาง (LDAP server)

รูปแบบการบริหารจัดการแบบกึ่งรวมศูนย์นี้ ไม่ต้องพัฒนาซอฟต์แวร์ใหม่ ใช้เทคนิควิธีการจัดการระบบที่เหมาะสมคือเลือกจัดฐานข้อมูลของระบบบริการที่เกี่ยวข้องให้มีบางส่วนเป็นฐานข้อมูลรวมที่ศูนย์



รูปที่ 5 แสดงรูปแบบการบริหารจัดการแบบกึ่งรวมศูนย์กลางที่ออกแบบใหม่

กลาง (LDAP server)และและมีบางส่วนเป็นฐานข้อมูลเฉพาะที่หน่วยงาน(host/service) ดังรูปที่ 5

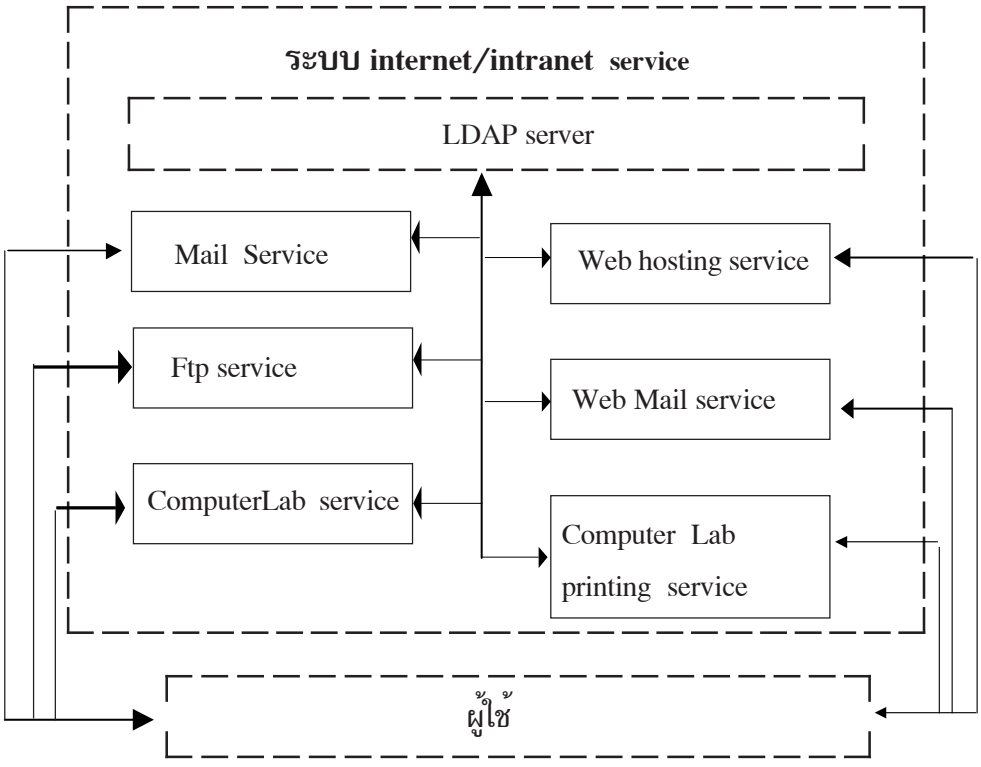
ข้อมูลระบบรักษาความปลอดภัยขั้นต้นที่ใช้สำหรับพิสูจน์ตัวตนชื่อผู้ใช้และรหัสผ่าน ถูกจัดเก็บเป็นแบบรวมศูนย์กลางไว้ที่ LDAP server

ข้อมูลระบบรักษาความปลอดภัยเฉพาะงาน(access list) ถูกจัดเก็บเป็นแบบแยกอิสระบน Host/service

ข้อมูลสภาพแวดล้อมทรัพยากรของผู้ใช้ ถูกจัดเก็บเป็นแบบรวมศูนย์กลางไว้ที่ LDAP server

ข้อมูลสิทธิการใช้ทรัพยากรของผู้ใช้ถูกจัดเก็บเป็นแบบแยกอิสระบน host/service

4.4 การจัดทำระบบตัวอย่างและทดสอบ



รูปที่ 6 แสดงต้นแบบระบบบริการรวมภายในองค์กรที่ออกแบบใหม่

ได้จัดทำต้นแบบระบบบริการรวมภายในองค์กร (รูปที่6) ที่ใช้การบริหารจัดการแบบกึ่งรวมศูนย์ด้วยระบบปฏิบัติการแบบลินุกซ์ ประกอบด้วย LDAP server, Mail Service, WebMail service, Web hosting service, Ftp service, ComputerLab service, Computer Lab printing service

5. สรุปผลการทดสอบและข้อเสนอแนะ

ได้ทดสอบใช้งานต้นแบบระบบบริการที่ออกแบบจัดทำไว้ พบว่าระบบบริการรวมภายในองค์กรมีคุณสมบัติผู้ใช้สามารถใช้ชื่อบัญชีผู้ใช้และรหัสผ่านเดียวกันในทุกบริการ มีชื่อบัญชีผู้ใช้ที่เป็นเฉพาะตนหนึ่งเดียวในทั้งระบบ การนำ host/service เข้าเชื่อมต่อกับระบบบริการรวมเป็นไปอย่างอิสระ ไม่จำเป็นต้องรับสิทธิอนุญาตจากศูนย์กลาง และยังมีสิทธิในการจัดการทรัพยากร host/service ของตนเองด้วย การบริหารจัดการระบบบริการไม่ได้ถูกจำกัดจากซอฟต์แวร์แต่เพียงอย่างเดียวสามารถจัดการได้ด้วยตนเอง ไม่จำเป็นต้องจัดหาซอฟต์แวร์ที่เป็นเฉพาะซึ่งจัดหายาก ทำให้ระบบมีความยืดหยุ่นสูงสามารถปรับขยายระบบได้ง่าย ดังสรุปไว้ในตาราง 1

แสดงข้อดีของการบริหารจัดการแบบกึ่งรวมศูนย์เปรียบเทียบกับแบบรวมศูนย์กลางและแบบแยกอิสระจากกัน

ข้อดีของการบริหารจัดการแบบกึ่งรวมศูนย์เปรียบเทียบกับแบบรวมศูนย์กลางและแบบแยกอิสระจากกัน	แบบกึ่งรวมศูนย์	แบบรวมศูนย์กลาง	แบบแยกอิสระจากกัน
ทุกบริการชื่อบัญชีผู้ใช้และรหัสผ่านอันเดียวกัน	ได้	ได้	ไม่ได้
ทั้งระบบบริการ ชื่อบัญชีผู้ใช้เฉพาะตนไม่ซ้ำกัน	ได้	ได้	ไม่ได้
การเชื่อม host service เข้ากับระบบบริการรวม	ด้วยตนเอง	ต้องได้รับสิทธิ์จากศูนย์กลาง	ด้วยตนเอง
สิทธิการจัดการทรัพยากรของ host service ของตนเอง	ด้วยตนเอง	ต้องได้รับสิทธิ์จากศูนย์กลาง	ด้วยตนเอง
วิธีการบริหารจัดการระบบบริการรวม	ด้วยตนเอง	ขึ้นกับซอฟต์แวร์	ด้วยตนเอง
การจัดหาซอฟต์แวร์ของ host service ที่มีคุณสมบัติเชื่อมต่อเข้ากับระบบบริการรวม	จำเป็นแต่จัดหาง่าย	จำเป็นและจัดหายาก	ไม่จำเป็น
การปรับลดหรือขยายระบบบริการรวม	ยืดหยุ่น	มีข้อจำกัด	ยืดหยุ่น

การบริหารจัดการแบบกึ่งรวมศูนย์นี้ ทำให้องค์กรสามารถขยายขีดความสามารถในการให้บริการได้อย่างรวดเร็วเพราะผู้ให้บริการสามารถจัดทำได้อย่างอิสระและยืดหยุ่น ตัวอย่าง host/service ที่สามารถเพิ่มเติมเข้าไปในระบบได้อีกเช่น Host Compiler service, Web board service. Mailing list service และ File service เป็นต้น

เอกสารอ้างอิง

[1] A Linux-PAM page. [Online]. Available:http://www.kernel.org/pub/linux/libs/pam [2004,Apr 30]

[2] A Summary of the X.500(96) User Schema for usewith LDAPv3, RFC 2256. [Online]. Available : http://www.ieft.org [2004,Apr 30]

[3] Apache HTTP Server Version 2.0 Documentation-Apache HTTP Server.[Online].Available:http://httpd.apache.org/docs-2.0/[2004,Apr 30]

[4] Authentication Methods for LDAP, RFC 2829. [Online]. Available: http://www.ieft.org [2004,Apr 30]

[5] Deborah Russell, "Practical UNIX Security", O'Reilly & Associates, USA, June 1994

[6] Fedora project. [Online]. Available:http://fedora.redhat.com [2004,Apr 30]

[7] Gerald Carter, "LDAP System Administration",North, Sebastopol, CA 95472, April 2003O'Reilly & Associates, Inc.,1005 Gravenstein Highway

[8] Lightweight Directory Access Protocal (v3), RFC2251. [Online]. Available: http:// www.ieft.org [2004,Apr30]

[9] Lightweight Directory Access Protocol (v3): AttributeSyntax Definitions, RFC 2252. [Online].Available: http://www.ieft.org [2004,Apr 30]

[10] Linux LDAP Tutorial: Deploying OpenLDAP - Directory Installation and configuration (V1.2 and 2.x). [Online].Available: http://yolinux.com/TUTORIALS/ LinuxTutorialLDAP.htm 1 [2004,Apr 30]

[11] Norber Klasen. Directory Services for Linux in comparison with Novell NDS and Microsoft Active Directory. [Online] Available:http://www.daasi.de/staff/norbert/ thesis/thesis.pdf. [2004,Apr 30]

[12] OpenLDAP. [Online].Available: http://www.openldap.org [2004,Apr 30]

[13] pGina: Making the big boys play nice - Latest News.[Online].Available: http:// pgina.xpasystems.com [2004,Apr 30]

[14] Presentation. [Online]. Available: http://www.librelogiciel.com/presentation [2004,Apr 30]

[15] Red Hat. [Online].Available: http://www.redhat.com [2004,Apr 30]

[16] SquirrelMail. [Online]. Available: http://www.squirrelmail.org [2004,Apr 30]

[17] The LDAP URL Format, RFC 2255. [Online]. Available: http://www.ieft.org [2004,Apr 30]

[18] The Postfix Home page. [Online]. Available:http://www.postfix.org [2004,Apr 30]

[19] The String Representation of LDAP Search Filters,RFC 2254. [Online]. Available : http://www.ieft.org [2004,Apr 30]

[20] จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์ "เจาะระบบNetwork ฉบับสมบูรณ์" ,บริษัท ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด, นนทบุรี, ธันวาคม 2546

****