ระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย

MONITORING AND TROUBLESHOOTING SYSTEM FOR SYSTEMS AND AND NETWORKS

โดย

สุทธินี่ เตชะปรัชญา

SUTTHINEE TECHAPRACHYA

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ ๒

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ ๒ ปีการศึกษา ๒๕๕๘

ระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย

MONITORING AND TROUBLESHOOTING SYSTEM FOR SYSTEMS AND NETWORKS

โดย

สุทธินีย์ เตชะปรัชญา

SUTTHINEE TECHAPRACHYA

อาจารย์ที่ปรึกษา

ผศ.ดร. สุเมธ ประภาวัต

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2558

MONITORING AND TROUBLESHOOTING SYSTEM FOR SYSTEMS AND NETWORKS

SUTTHINEE TECHAPRACHYA

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT`S INSTITUTE OF TECHNOLOGY LADKRABANG

2/ 2015

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย

MONITORING AND TROUBLESHOOTING SYSTEM FOR SYSTEMS AND NETWORKS

นางสาวสุทธินีย์ เตชะปรัชญา

รหัสประจำตัว 55661025

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาการอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีเครือข่ายและระบบ)

ภาคเรียนที่ 2 ปีการศึกษา 2558

.....**อาจารย์ที่ปรึกษา**

(ผศ.ดร. สุเมธ ประภาวัต)

.....**กรรมการสอบ**

(รศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์)

.....**กรรมการสอบ**

(ผศ.ดร. กันต์พงษ์ วรรัตน์ปัญญา)

ชื่อหัวข้อ	ระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย
นักศึกษา	นางสาวสุทธินีย์ เตชะปรัชญา
รหัสนักศึกษา	55661025
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2556
อาจารย์ที่ปรึกษา	ผศ.ดร.สุเมธ ประภาวัต

บทคัดย่อ

สารนิพนธ์ฉบับนี้นำเสนอการพัฒนาระบบบริหารและจัดการเครือข่ายผ่านเว็บแอพพลิเคชั่น โดยการพัฒนาระบบให้สามารถใช้งานระบบได้ง่าย มีฟังก์ชั่นการทำงานที่ช่วยในการบริหารและจัดการเครือข่าย ที่ช่วยในการลดภาระงานของผู้ดูแลระบบ และปัญหาในการตรวจสอบระบบเมื่อมีการทำงานที่ผิดปกติ โดยมีระบบแจ้งเตือนสถานะเพื่อให้ผู้ดูแลระบบรับทราบถึงปัญหาที่เกิดขึ้นในระบบเครือข่าย และนำข้อมูลมาใช้ประโยชน์ในการวิเคราะห์สาเหตุและแก้ไขปัญหาได้เร็วขึ้น

การตรวจสอบการทำงานระบบเครือข่าย สามารถเข้าตรวจสอบได้ผ่านเว็บแอพพลิเคชั่น และสามารถที่จะเก็บรวบรวมข้อมูลไว้ ช่วยในการจัดการระบบเครือข่ายให้ทำงานอย่างมีประสิทธิภาพ ช่วยในการออกแบบและวิเคราะห์ปัญหา เพื่อสามารถป้องกัน ตรวจสอบและแก้ปัญหาต่างๆ ที่เกิดขึ้นบนระบบเครือข่ายได้

Title	Monitoring and Troubleshooting System for Systems and Networks
Student	Miss Sutthinee Techaprachya
Student ID.	55661025
Degree	Master of Science
Program	Information Technology
Major	Network and System Technologies
Academic Year	2015
Advisor	Asst. Prof. Dr. Sumet Prapawat

ABTRACT

This thesis proposed the implementation of network management system via Web application which increased the usability and reduced the burden of network monitoring. Furthermore, a novel networking system also has many beneficial functions such as detection and notification when abnormal network behaviors is occurred, analyzing/diagnosing network problems and giving useful information for instant network recovery, enabling network administrators to examine and monitor network traffic through web application, and storing analyzed information in order to design and build an efficient network infrastructure which helps to improve overall network performance.

กิตติกรรมประกาศ

การศึกษาอิสระในหัวข้อเรื่อง “ระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย” ฉบับนี้ สำเร็จได้ด้วยความกรุณาจากท่านอาจารย์ที่ปรึกษา ผศ.ดร.สุเมธ ประภาวัต ที่รับเป็นที่ปรึกษาให้กับข้าพเจ้า โดยให้คำแนะนำแนวทางที่ดี ตรวจสอบแก้ไขเพื่อความสมบูรณ์ตลอดจนให้ความช่วยเหลือและให้ความรู้ที่เป็นประโยชน์สำหรับการนำมาพัฒนาระบบเป็นอย่างยิ่ง ส่งผลให้การศึกษา วิเคราะห์ ออกแบบ และการพัฒนาระบบสำเร็จลุล่วงด้วยดี

ขอขอบพระคุณรุ่นพี่และเพื่อนคณะเทคโนโลยีสารสนเทศ และเพื่อนผู้ร่วมงานที่ช่วยสนับสนุนการทำโครงการ ช่วยให้คำแนะนำ ข้อเสนอแนะที่เป็นประโยชน์ยิ่งต่อการทำโครงการและให้การสนับสนุนทางด้านการศึกษาของข้าพเจ้าด้วยดีเสมอมา พร้อมทั้งให้กำลังใจในการดำเนินการครั้งนี้

ข้าพเจ้าขอขอบคุณ เจ้าหน้าที่และนักศึกษาปริญญาโท คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังที่ให้ความช่วยเหลือและให้กำลังใจในการทำรายงานการศึกษาอิสระฉบับนี้

สุดท้ายนี้ข้าพเจ้าขอบคุณบิดา มารดา รวมถึงญาติพี่น้องที่คอยสนับสนุนกำลังทรัพย์และเป็นกำลังใจ ที่ทำให้มีความพยายาม มุมานะในการศึกษาและพัฒนาโครงการ จนทำให้ข้าพเจ้าสามารถทำโครงการนี้ให้สำเร็จลุล่วงได้ด้วยดี สำหรับคุณงามความดีและประโยชน์อันพึงมาจากโครงการนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่านคะ

นางสาวสุทธินีย์ เตชะปรัชญา

สารบัญ

หน้า

บทคัดย่อภาษาไทย I

ABTRACT II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญ(ต่อ) V

สารบัญตาราง VI

สารบัญรูป VII

บทที่ 1 บทนำ

1.1 ความเป็นมาและที่มาของปัญหา 1

1.2 วัตถุประสงค์ของการศึกษา 1

1.3 ประโยชน์ที่คาดว่าจะได้รับ 1

1.4 ขอบเขตของระบบ 2

1.5 ขั้นตอนการดำเนินงาน 2

บทที่ 2 ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

2.1 งานวิจัยที่เกี่ยวข้อง 3

2.2 ระบบดูแลและบริหารเครือข่าย 4

2.3 เทคโนโลยีด้านการพิสูจน์ทราบตัวตน (Authentication) 5

2.4 Mail Server บริการไปรษณีย์อิเล็กทรอนิกส์ 8

2.5 Web server เว็บเซิร์ฟเวอร์ 10

บทที่ 3 การศึกษาและวิเคราะห์ระบบงานปัจจุบัน

3.1 ความต้องการของระบบ 11

3.2 การวิเคราะห์และออกแบบระบบ 11

บทที่ 4 การออกแบบหน้าจอการทำงาน

4.1 การออกแบบหน้าจอการทำงาน 28

บทที่ 5 สรุปผลการพัฒนา

5.1 ผลการพัฒนา 36

5.2 อุปสรรคในการพัฒนา 36

สารบัญ (ต่อ)

หน้า

5.3 ข้อเสนอแนะเพิ่มเติม 37
บรรณานุกรม..... 38
ประวัติผู้เขียน..... 39

สารบัญตาราง

ตารางที่		หน้า
3.1	รายละเอียดของการตรวจสอบข้อมูลมอนิเตอร์การทำงานระบบเครือข่าย.....	14
3.2	รายละเอียดของข้อมูลการแจ้งเตือนระบบ.....	15
3.3	รายละเอียดของการจัดการข้อมูลระบบเพื่อการมอนิเตอร์ระบบเครือข่าย.....	16
3.4	รายละเอียดของการเข้าสู่ระบบ.....	17
3.5	รายละเอียดของการจัดการนโยบายในการ Monitor ระบบ.....	18
3.6	รายละเอียดการปรับปรุงประสิทธิภาพการใช้ทรัพยากรเครือข่าย.....	19
3.7	ConfigCheck_Connect รายละเอียดการตั้งค่าการตรวจสอบการเชื่อมต่อ.....	22
3.8	ConfigCheck_Services รายละเอียดการตั้งค่าการตรวจสอบการ Service ให้บริกา....	22
3.9	ConfigCheck_TCP รายละเอียดการตั้งค่าการตรวจสอบโปโตคอล.....	22
3.10	CONFIGS รายละเอียดการตั้งค่าระบบ monitoring.....	23
3.11	CountConnectServer ข้อมูลรายละเอียดนับปัญหาส่วนการเชื่อมต่อระบบ.....	23
3.12	CountServices ข้อมูลรายละเอียด นับปัญหาส่วนของ Service.....	23
3.13	CountTCPServices ข้อมูลรายละเอียด การนับ TCP Service.....	24
3.14	LogConnectServer ข้อมูลรายละเอียด ประวัติการทำงานส่วนการเชื่อมต่อ.....	24
3.15	LogServices ข้อมูลรายละเอียดการจัดเก็บ log การตรวจสอบ Services.....	25
3.16	LogTCPServices ข้อมูลรายละเอียดการจัดเก็บ log ตรวจสอบโปรโตคอล.....	25
3.17	ServerClient ข้อมูลรายละเอียดเครื่อง Server ในระบบเครือข่าย.....	26
3.18	ServicesLocal ข้อมูลรายละเอียด Services ที่ใช้งาน.....	26
3.19	TransmissionControlProtocol ข้อมูลรายละเอียดเกี่ยวกับโปรโตคอล.....	26
3.20	USERS ข้อมูลรายละเอียดของผู้ใช้งานระบบ.....	26
3.21	ServerClient ข้อมูลรายละเอียดของเครื่องที่ติดต่อในระบบ.....	27

สารบัญรูป

รูปที่		หน้า
2.1	อุปกรณ์ Token.....	7
2.2	อุปกรณ์ Token OTP.....	8
3.1	ภาพรวมสถาปัตยกรรมระบบ.....	11
3.2	แผนภาพยูสเคสของระบบ	13
3.3	แอคทิวิตไดอะแกรม.....	20
3.4	แผนภาพความสัมพันธ์ของข้อมูล (ER-Diagram).....	21
4.1	แสดงหน้าจอการล็อกอินเข้าระบบ.....	28
4.2	แสดงหน้าจอการจัดการข้อมูลผู้ใช้.....	29
4.3	แสดงหน้าจอเมนูสิทธิ์ผู้ดูแลระบบส่วน Monitor.....	29
4.4	แสดงหน้าจอการจัดการเครื่องคอมพิวเตอร์.....	30
4.5	แสดงหน้าจอข้อมูลเครื่องคอมพิวเตอร์.....	30
4.6	แสดงหน้าจอการจัดการ Service Computer.....	31
4.7	แสดงหน้าจอการจัดการข้อมูลส่วนของพอร์ต และโปรโตคอล.....	31
4.8	แสดงหน้าจอการตั้งค่าในการตรวจสอบและการแจ้งเตือนการทำงาน Service.....	32
4.9	แแสดงหน้าจอจัดการการตั้งค่านโยบายการตรวจสอบข้อมูลระบบเครือข่าย.....	32
4.10	แสดงหน้าจอการมอนิเตอร์ระบบ.....	33
4.11	แสดงหน้าจอ Report การมอนิเตอร์.....	33
4.12	แสดงหน้าจอการแจ้งเตือนผ่านทางระบบ E-mail.....	34
4.13	แสดงหน้า Dashboard ระบบโดยรวม.....	34
4.14	แสดงหน้า Application Connect ที่เอเจนต์.....	35
4.15	แสดงการทำงานของการตรวจสอบเซอร์วิสที่เอเจนต์.....	36

บทที่ 1
บทนำ

1.1 ความเป็นมาและที่มาของปัญหา

การใช้งานระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร มักมีปัญหาเกิดขึ้น ซึ่งทำให้ผู้ดูแลระบบต้องทำการแก้ไขปัญหาที่เคยเกิดด้วยวิธีเดิมๆ เช่น ผู้ใช้งานเข้าใช้ระบบอีเมลไม่ได้ ก็จะแจ้งเจ้าหน้าที่ให้ช่วยแก้ปัญหาให้ ซึ่งการแก้ปัญหาเบื้องต้น อาจตรวจสอบว่า ระบบอีเมลขององค์กรสามารถใช้งานได้หรือไม่ โดยการตรวจสอบเบื้องต้น ตรวจสอบจากเซอร์วิสหรือโปรโตคอลของระบบอีเมล หากเซอร์วิสไม่ทำงาน ก็อาจจะทำการรีสตาร์ทเซอร์วิส การแก้ไขปัญหาดังกล่าวเป็นตัวอย่างขั้นตอนแก้ไขปัญหาเบื้องต้น

จึงต้องการพัฒนาระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย ซึ่งระบบดังกล่าวจะช่วยตรวจจับการทำงานของเซอร์วิสและโปรโตคอลของระบบที่ใช้งานภายในองค์กร เพื่อนำข้อมูลมาใช้ประโยชน์การวิเคราะห์สาเหตุ หรือตรวจสอบสถานะต่างๆในการใช้งานในระบบคอมพิวเตอร์ จากนั้นเมื่อพบปัญหาจะทำการแก้ไขปัญหาให้เบื้องต้นโดยอัตโนมัติ หากแก้ไขแล้วสามารถใช้งานได้ จะช่วยลดภาระของผู้ดูแลระบบและช่วยให้ไม่เกิด Downtime ของระบบต่างๆ เป็นเวลานาน และระบบจะทำการแจ้งเตือนผู้ดูแลระบบว่าเกิดปัญหาอะไรบ้าง แก้ปัญหาได้อย่างไร เมื่อเวลาใด และเหตุการณ์ที่เกิดขึ้นในแต่ละครั้งจะมีการรายงานให้ทางผู้ดูแลระบบทราบ

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาแนวทางการพัฒนาระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย
2. เพื่อวิเคราะห์ออกแบบระบบ ให้สามารถแสดงผลการตรวจสอบและแก้ปัญหาระบบเครือข่ายในลักษณะที่ใช้งานง่ายและมีประสิทธิภาพ
3. เพื่อศึกษาและวิเคราะห์ปัญหาที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่าย ให้สามารถลดเวลา downtime ที่เกิดขึ้นในระบบและเพิ่มประสิทธิภาพการใช้งานเครือข่ายได้

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ความรู้และความเข้าใจในระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย
2. ทำให้มีระบบตรวจสอบและเข้าไปช่วยผู้ดูและระบบบริหารจัดการเครือข่าย

3. ช่วยแบ่งเบาภาระของผู้ดูแลระบบ ในเรื่องของการตรวจสอบและแก้ไขการทำงานภายในระบบเครือข่าย

1.4 ขอบเขตของระบบ

1. สามารถตรวจสอบสถานการณ์ทำงาน และวิเคราะห์ปัญหาที่เกิดขึ้นในระบบเครือข่ายได้
2. สามารถแก้ไขปัญหาเบื้องต้นที่เกิดขึ้นในระบบเครือข่ายได้ เช่นปัญหาที่เกี่ยวกับ Mail Server Web Server และ Authentication Server
3. สามารถแจ้งปัญหาและการแก้ไขปัญหาที่เกิดขึ้นภายในเครือข่ายให้กับผู้ดูแลระบบได้
4. มีการเก็บ Monitoring Log บันทึกลงฐานข้อมูลเพื่อตรวจสอบข้อมูลย้อนหลังได้

1.5 ขั้นตอนการดำเนินงาน

1. ศึกษาหาความรู้พื้นฐานทำงานของเซอร์วิสและโปรโตคอลต่างๆ ปัญหา วิธีการแก้ไข เพื่อนำมาใช้ในการพัฒนาระบบ
2. ทำการออกแบบส่วนต่างๆ ของระบบ เช่นส่วนในการวิเคราะห์ปัญหา ส่วนที่ตรวจสอบข้อมูลในเครือข่าย และส่วนแสดงผลให้ผู้ที่เกี่ยวข้องในการดูแลระบบทราบ
3. ตรวจสอบการใช้งานระบบ สรุปผลการทำงานของระบบ

บทที่ 2
ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

2.1 งานวิจัยที่เกี่ยวข้อง

2554 พงศ์ธรณ์ กิตติศิริชัยกุล และศิกวัส ชีชนะ ระบบบริหารจัดการเครือข่ายที่ใช้ง่ายและมีประสิทธิภาพ [1] เป็นระบบที่ช่วยเหลือผู้ดูแลระบบเครือข่ายให้สามารถทำงานได้สะดวกขึ้น รวดเร็วขึ้นระบบบริหารจัดการเครือข่ายที่ง่ายและมีประสิทธิภาพสำหรับธุรกิจขนาดเล็กและขนาดกลาง เพื่อช่วยสนับสนุนการทำงานของผู้ดูแลระบบ โดยสามารถทำงานผ่านเว็บบราวเซอร์ ได้หรือใช้งานผ่านเว็บแอพพลิเคชั่นได้ และที่สำคัญเป็นระบบที่ใช้งานได้ง่ายเมื่อเปรียบเทียบกับระบบบริหารจัดการเครือข่ายที่มีใช้ทั่วไป มี UI ที่นำใช้งานและมีฟังชันที่อำนวยความสะดวกให้แก่ผู้ดูแลระบบ มีระบบจัดการข้อมูลอุปกรณ์ในการเพิ่ม การแก้ไข และการดึงข้อมูลอุปกรณ์มาใช้ตรวจสอบการทำงานและเรียกดูข้อมูลแบบ real-time มีระบบแจ้งเตือนโดย SNMP Protocol ผ่านทางเว็บบราวเซอร์ ผ่านทาง E-mail และการแจ้งเตือนจาก Network Device โดยอัตโนมัติ ระบบมีการดึงข้อมูลสำหรับการหาที่อยู่ของผู้ใช้งานในระบบ

ในส่วนของงานวิจัยดังกล่าว เป็นระบบที่ช่วยเหลือผู้ดูแลระบบเครือข่าย ซึ่งครอบคลุมในการตรวจสอบการทำงานในการจัดการส่วน Network Device เป็นหลัก ระบบที่พัฒนานี้ได้เสนอแนวทางในการนำแนวคิดมาพัฒนาต่อ ซึ่งมีฟังก์ชันการทำงานที่ปรับปรุงและเพิ่มเติมเพื่อให้มีความยืนหยุ่นในการตรวจสอบระบบคอมพิวเตอร์มากยิ่งขึ้น โดยเน้นการตรวจสอบเครื่องให้บริการเป็นหลัก ตัวอย่างเช่น การตรวจสอบเครื่องเซิฟเวอร์ให้บริการเกี่ยวกับเมล เครื่องเซิฟเวอร์ให้บริการเวบเกี่ยวกับไฟล์เซิฟเวอร์ เป็นต้น

ในการพัฒนาระบบตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่ายนี้ จะมีฟังก์ชันการทำงานที่ปรับปรุงเพิ่มเติมดังนี้

- ฟังก์ชันในการลำดับความสำคัญของปัญหาที่ตรวจสอบพบในระบบเครือข่าย
- ฟังก์ชันการตรวจสอบสถานะการทำงานเกี่ยวกับเซอร์วิสให้บริการ โปรโตคอล และตรวจสอบการเชื่อมต่อของเครื่องคอมพิวเตอร์ในระบบ
- ฟังก์ชันในการแก้ไขปัญหาเบื้องต้นที่ระบบสามารถแก้ไขปัญหาด้วยตัวเองได้ เช่น การสร้างนโยบายการตรวจสอบและการ Restart Service ที่ขัดข้องโดยอัตโนมัติ
- มีส่วนแสดงข้อมูลเครื่องคอมพิวเตอร์และทรัพยากรของเครื่อง เกี่ยวกับ ซีพียู หน่วยความจำ เป็นต้น

2553 สุรชัย ชัยสิริเจริญกุล ระบบมอนิเตอร์และวางแผนสำหรับความสามารถของเครื่องเซิร์ฟเวอร์ [2] เป็นการนำเอาหลักการทำงานด้านมอนิเตอร์ และการวางแผนปรับปรุง หรือ

เปลี่ยนแปลงความสามารถของเครื่องเซิร์ฟเวอร์มาใช้ มีข้อดีในส่วนของการวางแผนสำหรับความสามารถของเครื่องเซิร์ฟเวอร์ที่มีการใช้งานในปัจจุบัน และการคาดการณ์ในอนาคต ช่วยในด้านการใช้งบประมาณกับการลงทุนในการใช้ทรัพยากร ระบบนี้ยังรองรับในการตรวจสอบการทำงานของระบบปฏิบัติการวินโดว์เซิร์ฟเวอร์ ระบบปฏิบัติการลีนุกซ์ และระบบปฏิบัติการโซลาริส

สำหรับในส่วนระบบตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่ายที่จัดทำขึ้นนี้จะมีในส่วนตรวจสอบระบบและจัดการในส่วนของการแก้ปัญหา ซึ่งจะเป็นการสร้างประสิทธิภาพการทำงานระบบได้ในอีกลักษณะหนึ่ง

2557 สุดาพร ฮุยสูงเนิน ระบบการจัดการบัญชีผู้ใช้บนแอคทีฟไดเร็กทอรี่ผ่านเว็บ [3] โดยการเป็นการเอาหลักการทำงานของเทคโนโลยี PKI มาทำงานร่วมกับระบบจัดการแอคทีฟไดเร็กทอรี่ สามารถเข้าระบบได้จากทุกที่ ที่มีการเชื่อมต่อระบบอินเทอร์เน็ต มีการจัดการส่วนของความปลอดภัยในด้านการพิสูจน์ตัวตนในการเข้าใช้งานระบบผ่านการยืนยันตัวตนด้วย Token

ในส่วนนี้ระบบตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่าย ที่ได้จัดทำขึ้นจะมีการตรวจสอบการทำงานของระบบในส่วนของการพิสูจน์ทราบตัวตน (Authentication) ด้วยจะตรวจสอบการทำงานของระบบที่ทำงานร่วมกับเทคโนโลยี PKI เช่น มีการตรวจสอบเกี่ยวกับการเรื่องของ CRL และสถานะของการติดต่อระบบของผู้ใช้งาน การศึกษางานวิจัยนี้ ให้ประโยชน์เกี่ยวกับการทำงานของเครื่องให้บริการ ที่มีหน้าที่ในการให้บริการออกใบรับรองอิเล็กทรอนิกส์ ระบบสามารถตรวจสอบการทำงานของเซอร์วิสที่เกี่ยวกับการให้บริการในการออกใบรับรอง เช่น Active Directory Certificate Services เป็นต้น

2.2 ระบบดูแลและบริหารเครือข่าย (Network Management System : NMS)

การทำงานต่าง ๆ นั้นเพื่อที่จะทำให้เกิดประสิทธิภาพในการทำงาน จึงต้องมีการควบคุมดูแลการทำงานและผู้ที่ทำหน้าที่ในการควบคุมการทำงานในองค์กร ก็คือผู้บริหารจัดการ โดยเป็นผู้คอยตรวจสอบดูแล ระบบการทำงาน ว่ามีการดำเนินการอย่างไร มีเหตุให้ความเสี่ยง หรือความไม่ปลอดภัยกับระบบ มีข้อบกพร่องตรงส่วนไหนในระบบที่ควรจะได้รับการปรับปรุงแก้ไขเพื่อที่จะให้การทำงานเป็นไปอย่างมีประสิทธิภาพมากที่สุด ในระบบเครือข่ายก็เช่นกันโดยเฉพาะระบบเครือข่ายขนาดใหญ่อย่างอินเทอร์เน็ต หากไม่มีการบริหารที่ดีจะทำให้การสื่อสารข้อมูลเกิดความผิดพลาดขึ้นได้ ระบบบริหารเครือข่าย NMS เกิดขึ้นมามีวัตถุประสงค์ที่สำคัญก็คือ ทำหน้าที่ในการดูแลบริหารระบบเครือข่าย และการจัดการเครือข่ายขององค์กร ในการจัดการส่วนประกอบต่าง ๆ ในระบบ ทั้งเกี่ยวกับอุปกรณ์ ผังระบบ บัญชีผู้ใช้งาน รายการการตั้งค่า การบริหารจัดการที่ดีจะช่วยลดข้อผิดพลาดในการทำงาน หรือกรณีมีข้อผิดพลาด สามารถแก้ไขให้ทำงานได้ทัน และสร้างความต่อเนื่องในการดูแลระบบ และทำให้ผู้ใช้ได้รับประโยชน์สูงสุดจากระบบเครือข่าย

2.2.1 องค์ประกอบต่าง ๆ ภายในระบบบริหารเครือข่าย มีดังนี้

- Managed Devices อุปกรณ์เครือข่ายที่ต้องการจัดการ เป็นส่วนปลายทางที่ทำหน้าที่รวบรวมข้อมูลข่าวสาร การทำงานจากอุปกรณ์ เพื่อนำไปใช้ในการอ้างอิงการบริหารจัดการเครือข่าย
- เอเจนต์ (Agent) เป็นลักษณะการทำงานของซอฟต์แวร์ที่มีขนาดไม่มาก ติดตั้งอยู่บนอุปกรณ์ หรือ คอมพิวเตอร์ที่ต้องการตรวจสอบ ทำหน้าที่รายงานสถานะการทำงานของคอมพิวเตอร์
- ระบบบริหารจัดการเครือข่าย (Network management System หรือ NMS)ส่วนที่ทำหน้าควบคุมและจัดการการทำงานและความต้องการใช้ทรัพยากรของ Managed Devices

2.2.2 แนวทางในการระบบดูแลและบริหารเครือข่าย

1. การบริหารประสิทธิภาพ (Performance Management)

การทำงานของระบบเครือข่ายได้เต็มประสิทธิภาพ มีการจัดการต่อความต้องการของผู้ใช้ในการบริหารจัดการทรัพยากรของระบบ มีการมอนิเตอร์ เพื่อการประเมิน การปรับปรุงให้มีประสิทธิภาพตามมา

2. การบริหารการตั้งค่า (Configuration Management)

บริหารค่าต่างๆ ที่มีการตั้งค่าของอุปกรณ์ในระบบ เช่น ค่าการ Configuration ของอุปกรณ์เน็ตเวิค ค่า IP Address เป็นต้น

3. บริหารเกี่ยวกับข้อผิดพลาด (Fault Management)

ลักษณะของการบริหารจัดการในการบันทึก Log เหตุการณ์ และการเฝ้าระวังการเกิดข้อผิดพลาด มีการตรวจสอบ การแจ้งเตือนผู้ดูแล และการแก้ไขเหตุผิดพลาด ต่าง ๆ นั้นในระบบเครือข่ายได้ทันเวลา

4. การบริหารจัดการบัญชีผู้ใช้งาน (Account Management)

การบริหารจัดการทรัพยากรระบบของผู้ใช้งาน การยืนยันตัวตน การกำหนดสิทธิ์ในการใช้งาน ในการเข้าถึงทรัพยากรที่อนุญาต เป็นต้น

5. การบริหารจัดการด้านความปลอดภัยระบบ (Security Management)

เป็นสิ่งสำคัญในการสร้างความมั่นคงให้ระบบเครือข่าย ในการป้องกันระบบตามนโยบายที่วางไว้

2.3 เทคโนโลยีด้านการพิสูจน์ทราบตัวตน (Authentication)

ในด้านการรักษาความปลอดภัยคอมพิวเตอร์และเครือข่าย ส่วนหนึ่งที่สำคัญคือ การสร้างความเชื่อมั่นและการทำให้แน่ใจว่าเป็นตัวจริงในการใช้งานระบบ การพิสูจน์ทราบตัวตนหมายถึง การตรวจสอบตัวตนในรูปแบบดิจิตอลของผู้ที่กำลังสื่อสารกับระบบ ถือเป็นการจัดการส่วนแรก

สำหรับการควบคุมรักษาความปลอดภัยข้อมูลขององค์กร เชื่อมโยงไปสู่การอนุญาตใช้งานระบบ การตรวจสอบสิทธิ์ และการแก้ไขข้อมูลต่าง ๆ

การพิสูจน์ทราบตัวตนประกอบด้วย 2 ขั้นตอนในการทำงานคือ การยืนยันความถูกต้องของหลักฐานระบุว่าเป็นตัวตนที่แท้จริง (Identification) โดยแสดงหลักฐานที่มีอยู่ในระบบ ตัวอย่างในการระบุตัวตน เช่น การใช้ Username ในการระบุตัวตนเข้าระบบ, Fingerprint, Smart card, Token เป็นต้น และส่วนพิสูจน์ทราบตัวตน (Authentication) โดยการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง เช่น Password, Pass phase, Fingerprint, PIN เป็นต้น

2.3.1 ประเภทของการพิสูจน์ทราบตัวตน

- สิ่งที่คุณรู้ (Something you know) เป็นลักษณะการพิสูจน์ทราบตัวตน แบบ "One-Factor" ในการตรวจสอบตัวตนจากสิ่งที่ตัวจริงรู้ เช่น การกรอกชื่อผู้ใช้ และรหัสผ่าน หรือลักษณะการตอบคำถาม การใช้ชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบโดยทั่วไป ต้องมีล็อกอิน การพิสูจน์ทราบตัวตนในลักษณะนี้ ถือเป็นแบบที่ระดับความปลอดภัยอ่อนที่สุด เพราะถ้าใครรู้ชื่อผู้ใช้และรหัสผ่านก็สามารถเข้าใช้งานระบบได้ทันที นอกจากนี้ไม่สามารถตรวจสอบตัวตนของผู้ใช้ระบบว่าใครเป็นใครได้ การใช้รหัสผ่านอาจจะไม่ปลอดภัยในการป้องกันคอมพิมเตอร์และระบบเครือข่ายได้ เนื่องจากอาจมีการตั้งค่ารหัสผ่านที่ง่ายไป ทำให้บุคคลอื่นสามารถสุ่มเดาได้ และอาจเกิดการขโมยข้อมูลรหัสผ่านในระหว่างการสื่อสารข้อมูลด้วยวิธีต่าง ๆ ได้
- สิ่งที่คุณมี (Something you have) เป็นลักษณะการพิสูจน์ทราบตัวตน แบบ "Two-Factor" คือวิธีการล็อกอินเพื่อเข้าถึงระบบหรือบริการต่างๆโดยอาศัยปัจจัยสองอย่างที่นำมายืนยันร่วมกัน ซึ่งจะต้องไม่มีความสัมพันธ์เหมือนกัน เพื่อจุดประสงค์ในการสร้างความมั่นคงปลอดภัยให้มีประสิทธิภาพมากยิ่งขึ้นเช่น บัตร ATM, Token, Swipe card, Access card และ Smart Card เป็นต้น รูปแบบของการใช้ Smart Card ก็คือผู้ใช้งานจะต้องมีอุปกรณ์และรหัสผ่านเฉพาะเพื่อเข้าระบบ ผู้อื่นถึงแม้จะขโมย Smart Card ไปแต่ก็ไม่ทราบรหัสของอุปกรณ์ ทำให้ยากไปอีกขั้นหนึ่งในการเจาะเข้าสู่ระบบ

ระบบ Smart Card ควรมีการใช้งานร่วมกับระบบ PKI หรือ "Public-Key Infrastructures" ซึ่งผู้ใช้แต่ละคนจะได้รับ "Digital Certificate" ที่ได้รับรองจาก CA หรือ Certificate Authority ว่าผู้ใช้มีตัวตนจริง และ ใน Smart Card จะเก็บ "Private key" ของผู้ใช้ไว้ตลอดจนมีการเข้ารหัสลับเพื่อไม่ให้แฮกเกอร์สามารถนำ Private key ไปใช้ได้ง่าย ๆ

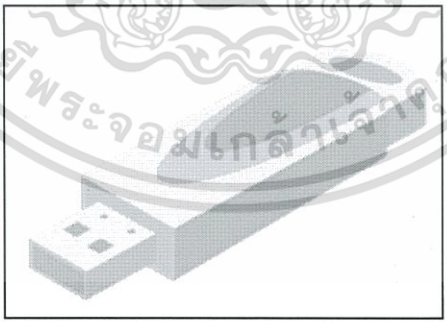
ระบบ One time password เป็นอีกระบบหนึ่งที่เป็นลักษณะ Two-factor Authentication เช่นกัน แต่ระบบนี้จะแตกต่างจากกันโดยจะมีการ generate ตัวเลขชุดหนึ่งออกมาเพื่อใช้ประกอบในการ Log in เข้าสู่ระบบโดยเราต้องติดตั้ง Radius Server เพื่อรองรับการ Log in จาก client ถ้าตรงกันก็จะให้ client เข้าสู่ระบบได้ ตัวเลขนี้จะใช้แค่เพียงครั้งเดียวเท่านั้น การใช้งาน

แบบนี้ต้องอาศัย hardware และ software เฉพาะ และต้องติดตั้งระบบในรูปแบบที่แต่ละผลิตภัณฑ์ได้กำหนดไว้

- สิ่งที่คุณเป็น(Something you are) เป็นการพิสูจน์ทราบตัวตนด้วยเทคโนโลยีไบโอเมตริกส์ โดยเอาลักษณะทางกายภาพของแต่ละบุคลที่ไม่ซ้ำกันมาตรวจสอบ อาศัยอวัยวะที่คนเรามีอยู่ และ มีลักษณะที่ไม่ซ้ำกัน ได้แก่ ลายนิ้วมือ ม่านตา เป็นต้น การใช้งาน Smart Card สามารถร่วมกับเทคโนโลยีไบโอเมตริกส์ ได้ กล่าวคือ เราสามารถเก็บลายนิ้วมือของคนลงไปใน Microchip ที่อยู่ใน Smart Card ได้ด้วย ซึ่งจะเพิ่มระดับของความปลอดภัยมากขึ้น แต่ค่าใช้จ่ายก็จะสูงขึ้นเช่นกันเช่น ม่ายตา ลายนิ้วมือ เสียง ตาดำ ฝ่ามือ เป็นต้น

2.3.2 เทคโนโลยี Token PKI

เป็นเทคโนโลยี USB Smartcard ใช้งานผ่านเครื่องคอมพิวเตอร์ที่มี Port USB สามารถรองรับการใช้งานใบรับรองอิเล็กทรอนิกส์ (PKI) โดยการสร้างและเก็บข้อมูลประจำตัว (Credential) ของผู้ใช้ เช่น คีย์ส่วนตัว (Private Key) รหัสผ่าน (Password) และใบรับรองอีเล็กทรอนิกส์ (Digital Certificate) ซึ่งจะปกป้องโดยชิพสมาร์ทการ์ด (Smart Card Chip) ในการยืนยันตัวบุคคล ผู้ใช้จะต้องมีทั้งอุปกรณ์ Token และรหัสผ่านของอุปกรณ์ จะช่วยให้เกิดความปลอดภัยแบบสองระดับ (Two factor authentication) ซึ่งช่วยปกป้องการเข้าถึงทรัพยากรภายในองค์กรได้เพื่อเข้าระบบขององค์กรที่มีความปลอดภัยสูง เช่น การเข้าระบบโดยผ่าน VPN, Network Logon การบริหารรหัสผ่าน (Password Management), ลายเซ็นอิเล็กทรอนิกส์ (Digital Signing), การเข้ารหัสข้อมูลการ เข้ารหัสและถอดรหัสจดหมายอิเล็กทรอนิกส์ (Email Encryption) เป็นต้น



รูปที่ 2.1 อุปกรณ์ Token

2.3.3 เทคโนโลยี OTP

One Time Password (OTP) หรือ Secure ID Solutions คือ เครื่องมือที่ใช้ในการสร้างรหัสผ่าน โดยจะสามารถใช้ได้ครั้งเดียวเท่านั้น และจะเปลี่ยน Random รหัสผ่านใหม่ในทุกระบบ One-Time Password (OTP) มีหลายรูปแบบ ทั้งอุปกรณ์ Hardware และ Software แต่ที่

นิยมเป็นการใช้อุปกรณ์พกพาหรือ Token ในการสร้างรหัสผ่าน และระบบส่งรหัสผ่านไปยังโทรศัพท์มือถือปลายทาง (Mobile Password)

One-Time Password (OTP) มีระยะเวลาหมดอายุ (Expire Time) ที่แน่นอน และไม่สามารถนำรหัสเดิมกลับมาใช้งานได้อีก สามารถใช้ร่วมกับระบบ Log In ได้หลากหลาย ทั้ง E-mail, VPN, Active Directory, Remote Service, Share Server, Web Applications ฯลฯ

2.3.4 ประโยชน์ในการพิสูจน์ตัวตน

- เพิ่มระดับความปลอดภัยให้กับระบบต่างๆ ที่ต้อง Log In
- หมดปัญหา Password รั่วหรือ User แปะรหัสไว้หน้าคอมพิวเตอร์
- หมดปัญหา User แจก Password ให้กับผู้ไม่เกี่ยวข้อง
- หมดปัญหา User ลืม Password

รูปที่ 2.2 อุปกรณ์ Token OTP

2.4 บริการไปรษณีย์อิเล็กทรอนิกส์ (Mail Server)

จดหมายอิเล็กทรอนิกส์ หรืออีเมล (Electronic Mail) [4] เป็นการสื่อสารที่สะดวกรวดเร็ว สิ่งสำคัญที่ผลักดันให้การรับส่งอีเมลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตเป็นไปอย่างง่ายดาย คือ Mail Server เพราะทำหน้าที่จัดการรับอีเมล ช่วยให้อีเมลของผู้ส่งสามารถเดินทางไปสู่ผู้รับภายในเวลาอันสั้น ส่วนผู้ใช้อีเมลต้องมีอีเมลแอดเดรส เป็นของตนเองและผู้ใช้ทุกคนจะมีเมลบ็อกซ์ หรือกล่องใส่จดหมายที่อยู่บน Mail Server ที่ตนเองเป็นสมาชิก

2.4.1 โปรโตคอลของอีเมล

การทำงานของระบบอีเมลจะทำงานอยู่ในระดับ Application layer จะอยู่ใน layer 7 ซึ่งจะมีโปรโตคอลที่เกี่ยวข้องกับการทำงานหลายตัว ในการส่ง Mail ที่สำคัญก็คือ SMTP โดยที่ application ที่ใช้ในการรับ ส่ง Mail จะเป็นโปรโตคอลคนละตัวกัน ในการรับจะใช้ POP, IMAP สามารถอธิบายรายละเอียดได้ดังนี้

SMTP (Simple Mail Transfer Protocol) เป็นโปรโตคอลที่ใช้ส่งอีเมลจากเครื่องคอมพิวเตอร์ของผู้ส่งไปยัง Mail Server และใช้ส่งอีเมลระหว่าง Mail Server ด้วยกันเอง หมายความว่าอีเมลฉบับหนึ่งอาจส่งผ่าน Mail Server มากกว่าหนึ่งเครื่องจนกว่าจะถึง Mail Server ปลายทาง โดยสอบถามไอพีแอดเดรสของ Mail Server ปลายทางจาก DNS Server สำหรับโปรโตคอล SMTP จะทำงานผ่านพอร์ตหมายเลข 25

POP3 (Post Office Protocol 3) เป็น Mail Server ใช้รับอีเมลที่มาจาก Mail Server เครื่องอื่นแล้วนำมาเก็บไว้ในเมลบ็อกซ์ของผู้รับ ซึ่งการทำงานตรงนี้เป็นหน้าที่ของ POP Server ส่วนผู้รับที่ใช้โปรแกรมอีเมลไคลเอนต์ดาวน์โหลดอีเมลมายังคอมพิวเตอร์ของตนเอง จะเป็นการทำงานของ POP Client (POP Client จะถูกฝังอยู่บนโปรแกรมอีเมลไคลเอนต์ต่างๆ) และเมื่ออีเมลทั้งหมดถูกส่งมายังเครื่องของผู้รับ อีเมลในเมลบ็อกบนเครื่องเซิร์ฟเวอร์จะถูกลบทิ้งไป ยกเว้นว่าจะกำหนดให้โปรแกรมอีเมลไคลเอนต์ทำสำเนาอีเมลเก็บไว้บนเซิร์ฟเวอร์ สำหรับโปรโตคอล POP 3 ได้พัฒนามาถึงเวอร์ชั่น 3 ซึ่งทำงานผ่านพอร์ตหมายเลข 110

IMAP 4 (Internet Message Access Protocol) IMAP เป็นโปรโตคอลหรือข้อตกลงทางการสื่อสารข้อมูลโดยมมาตรฐานเหมือนกับ SMTP โปรโตคอล IMAP ทำหน้าที่ติดต่อเข้าสู่อีเมลภายในเมลบ็อกซ์ของแต่ละผู้ใช้ที่Mail Server เปรียบเสมือนการเปิดอ่านข้อความในจดหมายแต่ละฉบับ ข้อดีของการใช้ IMAP คืออีเมลของแต่ละผู้ใช้จะถูกเก็บไว้ที่เครื่องเซิร์ฟเวอร์ ผู้ใช้สามารถเปิดดูอีเมลได้จากที่ต่างๆ ไม่ว่าจะเป็นที่ทำงาน ที่บ้าน หรือแม้แต่ส่วนใดของโลกที่อินเทอร์เน็ตสามารถไปถึง สำหรับผู้ ที่จะติดตั้งเว็บเมลไว้ใช้ จำเป็นต้องใช้ IMAP ในการเข้าถึงข้อมูล โปรแกรม IMAP ที่ใช้กันทั่วไปเป็นเวอร์ชัน 4 ซึ่งใช้พอร์ตหมายเลข 143

2.4.2 การเพิ่มความปลอดภัยอีเมล (Email Security Enhancements)

1. E-mail Message Confidentiality คือการรักษาความลับ สร้างความมั่นใจได้ว่าการส่ง อีเมลนั้นเป็นการส่งไปยังผู้รับอย่างปลอดภัย ผู้รับต้องเป็นผู้ที่ไดรับการอนุญาตเท่านั้น

2. E-mail Message Integrity เป็นความต้องการที่จะมั่นใจได้ว่า ข้อความที่ผู้ส่ง ส่งไปไม่มีการสูญหาย หรือถูกเปลี่ยนแปลงแก้ไขใดๆ ในระหว่างทาง เพราะบางครั้งข้อมูลที่ส่งไปจะเป็นข้อมูลที่เป็นความลับ หรือข้อมูลที่เป็นเรื่องเกี่ยวกับการเงิน ซึ่งการจัดการในการสร้างความมั่นใจตรงส่วนนี้ได้โดยวิธีการ คือ การทำ digital signature จะสามารถยืนยันตัวตนผู้ส่ง และสร้างความมั่นใจได้ว่าข้อความไม่ได้ถูกแก้ไข

3. Message sender Authentication คือ การทำให้สามารถพิสูจน์ตัวตนของผู้ส่งข้อมูลได้ เพื่อให้สามารถตรวจสอบได้ว่าใครคือผู้ส่งข้อมูล หรือในทางตรงกันข้าม ก็คือเพื่อป้องกันการแอบอ้างได้ คือการปฏิเสธไม่ได้ (Non-Repudiation)

2.5 เว็บเซิร์ฟเวอร์ (Web server)

หน้าที่ให้บริการข้อมูลแก่เครื่องลูกข่าย ที่ได้ขอรับบริการ เป็นลักษณะของข้อมูลที่เป็นสื่อผสม ผ่านระบบเครือข่าย โดยการแสดงผล ผ่านทางช่องโปรแกรมเว็บบราวเซอร์ หรืออาจจะกล่าวได้ว่า Web server คือโปรแกรมที่คอยให้บริการแก่ Client ที่ร้องขอข้อมูลเข้ามาโดยผ่าน web browser ที่ร้องขอข้อมูลผ่านโปรโตคอลเฮชทีทีพี HTTP (Hyper Text Transfer Protocol) เครื่องบริการจะส่งข้อมูลให้ผู้ร้องขอในรูปแบบสื่อผสมจะเป็นข้อความ ภาพ หรือในรูปแบบเสียง เครื่องบริการเว็บมักเปิดบริการพอร์ต 80 (HTTP Port) ให้ผู้ร้องขอได้เชื่อมต่อWeb server คือ เครื่องคอมพิวเตอร์ ที่ติดตั้งโปรแกรมคอมพิวเตอร์ ซึ่งทำและนำข้อมูลไปใช้ เช่น Internet Explorer หรือ Firefox Web Browser การเชื่อมต่อเริ่มด้วยการระบุที่อยู่เว็บเพจที่ร้องขอ Web Address หรือ URL โปรแกรมที่นิยมใช้เป็นเครื่องบริการเว็บ คือ อาปาเช่ (Apache Web Server) หรือไมโครซอฟท์ไอไอเอส (Microsoft IIS: Internet Information Server) สำหรับโปรแกรมที่นำมาทำเว็บเซิร์ฟเวอร์ที่ได้รับความนิยมมีดังนี้

- Internet Information Server (IIS) จากไมโครซอฟท์
- Apache HTTP Server จาก Apache Software Foundation
- Zeus Web Server จาก Zeus Technology
- Sun Java System Web Server จากซัน ไมโครซิสเต็มส์

บทที่ 3
การศึกษาและวิเคราะห์ระบบงานปัจจุบัน

การบริหารจัดการระบบเครือข่ายนั้นการติดตั้ง และใช้งาน จำเป็นต้องมีการตรวจสอบเฝ้าระวังประสิทธิภาพการทำงานเพื่อทำการบำรุงรักษาให้ระบบทำงานได้อย่างมีประสิทธิภาพและสร้างต่อเนื่อง เพื่อลดความเสียหายที่เกิดจากระบบเครือข่ายที่ขัดข้องให้มีการจัดการแก้ไขที่ทันถ่วงที ทันต่อเหตุการณ์และการพร้อมใช้งาน

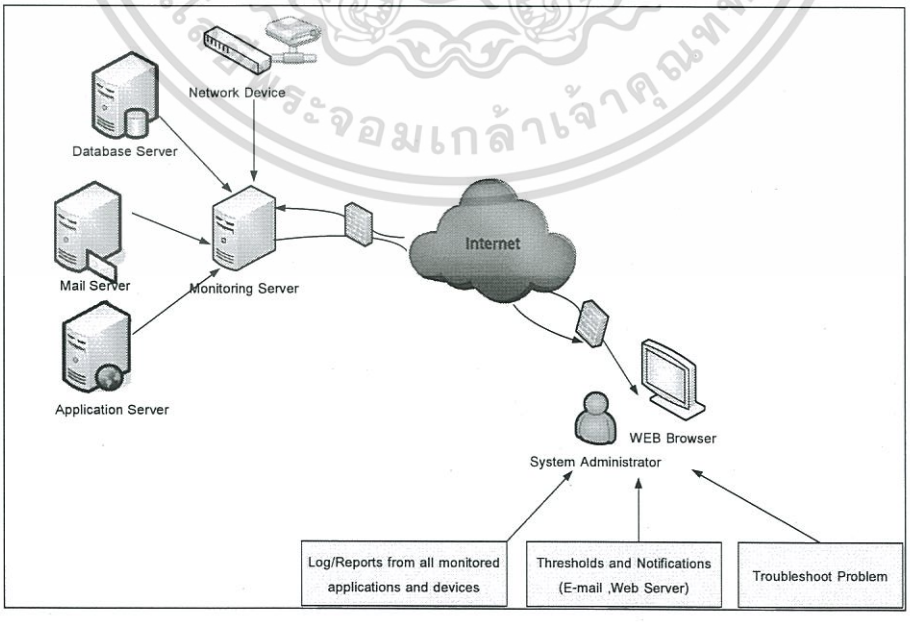
3.1 ความต้องการของระบบ

- ระบบสามารถเก็บบันทึกข้อมูลของอุปกรณ์เครือข่ายองค์กรได้
- ระบบทำการแจ้งเตือนเมื่อเกิดปัญหาผิดปกติหรือเหตุการณ์ไม่พึงประสงค์ได้ผ่านทางระบบและอีเมล์ผู้ดูแลระบบได้
- ระบบทำงานผ่าน Web application
- เป็นระบบที่ใช้งานได้ง่าย
- ระบบมีการตรวจสอบและจัดกลุ่มระดับปัญหาที่เกิดขึ้นเพื่อรายงานผลได้

3.2 การวิเคราะห์และออกแบบระบบ

ในการออกแบบฐานข้อมูล มีแบบจำลองที่เกี่ยวข้องกับระบบที่นำเสนอ ดังนี้

3.2.1 สถาปัตยกรรมระบบ



รูปที่ 3.1 ภาพรวมสถาปัตยกรรมระบบ

จากภาพที่ 3.1 อธิบายได้ดังนี้

1. มอนิเตอร์ริงเซิร์ฟเวอร์ (Monitoring Server)

คือ เซิร์ฟเวอร์ทำหน้าที่ในการรับส่งข้อมูลในเครือข่าย ดึงข้อมูลการตรวจสอบต่างๆในระบบเน็ตเวิร์ค เช่นจาก mail Server , File Server และ SQL Server และนำข้อมูลแสดงผลการมอนิเตอร์ริงให้ผู้ดูแลระบบสามารถตรวจสอบผ่านทาง Web Browser

2. ผู้ดูแลระบบ (System Administrator)

สามารถเรียกดูข้อมูลผ่านทางเว็บบราวเซอร์ เพื่อทำการตรวจสอบระบบเครือข่าย สามารถตรวจสอบการทำงาน ดูการแจ้งเตือนเมื่อระบบเครือข่ายมีปัญหา

3. อุปกรณ์เน็ตเวิร์ค (Network Device) คือ การจัดการส่วนอุปกรณ์เครื่องคอมพิวเตอร์อื่น ๆ ของระบบเครือข่ายที่ต้องการตรวจสอบ
4. ดาต้าเบสเซิร์ฟเวอร์ (Database server) ทำหน้าที่ให้บริการฐานข้อมูลในระบบเครือข่าย
5. เมลเซิร์ฟเวอร์ (mail Server) คือ เซิร์ฟเวอร์ซึ่งให้บริการรับส่งอีเมลในระบบเครือข่าย
6. Application Server คือ เซิร์ฟเวอร์ที่รันโปรแกรมประยุกต์ต่างๆ

3.2.2 แผนภาพยูสเคส (User Case Diagram)

รูปที่3.2 แผนภาพยูสเคสของระบบ

จากรูปที่ 3.2 แสดงยูสเคสไดอะแกรมการทำงานของระบบทั้งหมด โดยจะมีผู้เกี่ยวข้องกับระบบได้แก่ ผู้ดูแลระบบมีอำนาจหน้าที่สูงสุดในระบบ สามารถจัดการเกี่ยวกับการกำหนดนโยบายในการตรวจสอบ และจัดการเครื่องคอมพิวเตอร์ให้บริการที่ต้องการตรวจสอบ และเจ้าหน้าที่ Operator มีหน้าที่ในการตรวจสอบระบบมอนิเตอร์ ดูรายงานการทำงานของระบบ

คำอธิบายยูสเคสไดอะแกรม (Use Case Description)

จากยูสเคสไดอะแกรม มีคำอธิบายรายละเอียดของแต่ละยูสเคส ดังตารางที่ 3.1 ถึง 3.6

ตารางที่ 3.1 รายละเอียดของการตรวจสอบข้อมูลมอนิเตอร์การทำงานระบบเครือข่าย

Use Case Name :	Monitoring
Triggering Event : ผู้ดูแลระบบตรวจสอบระบบเครือข่ายคอมพิวเตอร์	
Brief Description : ฟังก์ชัน แสดงข้อมูลการทำงานของระบบ	
Actors : Administrator (ผู้ดูแลระบบ) , Operator	
Related Use Case :	
Stakeholder :	
Precondition :เพิ่มข้อมูล computer , service และ Protocol และตั้งค่าการจัดการ Policy ในการตรวจสอบระบบ	
Post Condition : แจ้งเตือนกรณีพบปัญหา	
Minimal guarantee :	
Success guarantee : ตรวจสอบการทำงานระบบมอนิเตอร์ได้	
Flow of Events : 1. ผู้ใช้งานระบบล็อกอินเข้าสู่ระบบและเลือกเมนูใช้งาน 2. ระบบแสดงหน้าจอมอนิเตอร์การทำงานของระบบ 3. ผู้ใช้ระบบสามารถระบุข้อมูลระบบที่ต้องการดูได้ 4. ระบบจะแสดงสถานะของอุปกรณ์ในเครือข่าย	
Sub Flows :	
Extension :	
Alternative/Exceptional : กรณีที่การทำงานของระบบมีความไม่ถูกต้อง ระบบจะแสดงข้อความเตือนให้ผู้ดูแลระบบทราบ	

ตารางที่ 3.2 รายละเอียดของข้อมูลการแจ้งเตือนระบบ

Use Case Name :	Notification Alerts
Triggering Event : ผู้ดูแลระบบดูการแจ้งเตือนของระบบ	
Brief Description : ฟังก์ชัน แสดงข้อมูลการแจ้งเตือนในระบบเมื่อเกิดความผิดปกติขึ้น	
Actors : Administrator (ผู้ดูแลระบบ) และ Operator	
Related Use Case :-	
Stakeholder :-	
Precondition :ทำเพิ่ม computer , service และ Protocol และตั้งค่าการจัดการ Policy ในการตรวจสอบระบบ	
Post Condition : -	
Minimal guarantee :-	
Success guarantee : ตรวจสอบการทำงานระบบมอนิเตอร์ได้	
Flow of Events : 1. ผู้ใช้งานระบบล็อกอินเข้าสู่ระบบและเลือกเมนูใช้งาน 2. ผู้ดูแลระบบดูการแจ้งเตือนในระบบหรือผ่าน E-mail 3. ระบบจะแสดงสถานะรายละเอียดของข้อขัดข้อง	
Sub Flows : 1. กรณีที่ข้อมูลการทำงานของระบบผิดปกติ ไม่ถูกต้อง ระบบจะแสดงข้อความเตือนต่อผู้ใช้งานระบบ	
Extension :	
Alternative/Exceptional :	

ตารางที่ 3.3 รายละเอียดของการจัดการข้อมูลระบบเพื่อการมอนิเตอร์ระบบเครือข่าย

Use Case Name :	Manage Server to monitoring
Triggering Event :	
Brief Description : ฟังก์ชันสำหรับจัดการข้อมูลระบบเครือข่าย เพื่อบันทึกข้อมูลที่จะทำการมอนิเตอร์ จัดการในส่วนการเพิ่มข้อมูล การแก้ไขข้อมูล และการลบข้อมูลในระบบ เพื่อจัดการกับการเปลี่ยนแปลงใน Computer , Network Services และ Protocol ในการตรวจสอบ	
Actors : Administrator (ผู้ดูแลระบบ)	
Related Use Case :-	
Stakeholder : System Administrator (ผู้ดูแลระบบ)	
Precondition : ต้องเข้าสู่ระบบก่อน	
Post Condition : -	
Minimal guarantee :-	
Success guarantee : จัดการในส่วนของข้อมูลระบบเครือข่าย	
Flow of Events : 1. ผู้ใช้งานระบบล็อกอินเข้าสู่ระบบและเลือกเมนูใช้งาน 2. ระบบแสดงหน้าจอมอนิเตอร์การทำงานของระบบ 3. ผู้ใช้ระบบสามารถระบุการจัดข้อมูลเครือข่ายได้ดังนี้ - เรียกดูข้อมูลพื้นฐาน ข้อมูลเกี่ยวกับ service computer เครื่อง Server ที่ทำงานในระบบ ข้อมูลการตั้งค่าต่าง ๆ ได้ - เพิ่มข้อมูล - แก้ไขข้อมูล - ลบข้อมูล 4. ระบบจะแสดงผลการทำงาน	
Sub Flows :	
Extension :	
Alternative/Exceptional กรณีที่ระบุข้อมูลไม่ถูกต้องตามเงื่อนไข หรือข้อมูลไม่ครบถ้วน ระบบจะแสดงข้อความเตือนให้ตรวจสอบความถูกต้อง	

ตารางที่ 3.4 รายละเอียดของการเข้าสู่ระบบ

Use Case Name :	Login to System
Triggering Event : -	
Brief Description : -	
Actors : Administrator (ผู้ดูแลระบบ) Operator (เจ้าหน้าที่ Monitor)	
Related Use Case :	
Stakeholder : Administrator (ผู้ดูแลระบบ) Operator (เจ้าหน้าที่ Monitor)	
Precondition :ต้องเข้าสู่ระบบก่อน	
Post Condition : -	
Minimal guarantee :	
Success guarantee : สามารถเข้าสู่ระบบได้และจัดการได้ตามกลุ่มผู้ใช้	
Flow of Events : 1. ผู้ดูแลระบบและOperator ต้องการเข้าสู่ระบบ - กรอกข้อมูล ชื่อผู้ใช้ และ รหัสผ่าน - คลิก เข้าสู่ระบบ 2. ระบบจะตรวจสอบสิทธิ์ผู้ใช้งาน 3. ระบบแสดงผลการ Login	
Sub Flows :	
Extension :	
Alternative/Exceptional	

ตารางที่ 3.5 รายละเอียดของการจัดการนโยบายในการ Monitor ระบบ

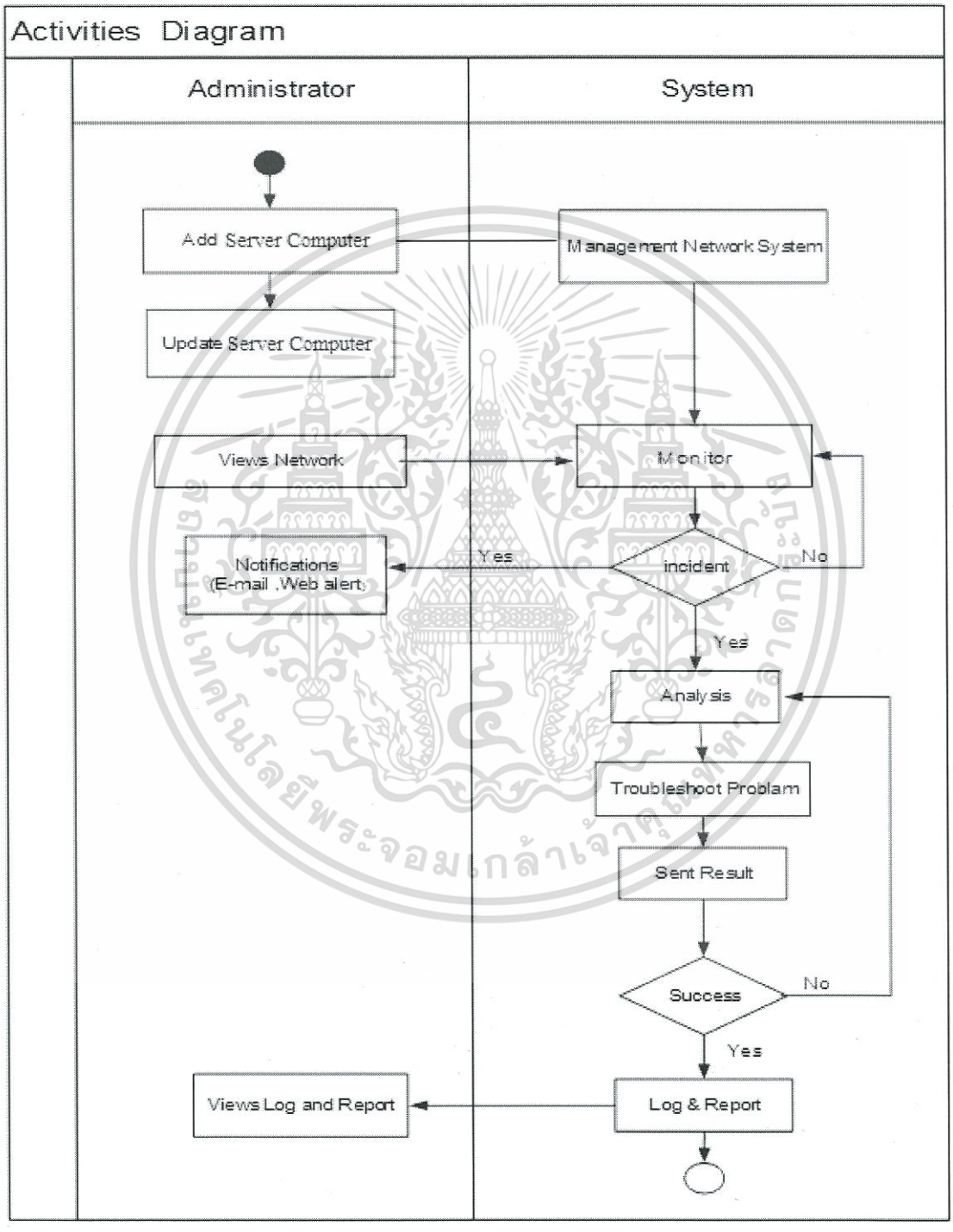
Use Case Name :	Manage Policy Monitor
Triggering Event : ผู้ดูแลระบบ กำหนดนโยบายการตรวจสอบระบบ	
Brief Description : ฟังก์ชันแสดงการตั้งค่าในการตรวจสอบระบบ	
Actors : Administrator (ผู้ดูแลระบบ)	
Related Use Case :	
Stakeholder :	
Precondition :ต้องเข้าสู่ระบบเพื่อตรวจสอบสิทธิ์ก่อน	
Post Condition : -	
Minimal guarantee :	
Success guarantee : ตรวจสอบการทำงานระบบมอนิเตอร์ได้	
Flow of Events : 1. ผู้ใช้งานระบบล็อกอินเข้าสู่ระบบและเลือกเมนูใช้งาน 2. ระบบแสดงหน้าการทำงานของระบบ 3. ผู้ใช้ระบบสามารถระบุการจัดข้อมูลเครือข่ายได้ดังนี้ 4. เพิ่มการตรวจสอบข้อมูลข้อมูลเกี่ยวกับ service computer เครื่อง Server ที่ทำงานในระบบ การตั้งค่าการตรวจโปโคคอลต่าง ๆ และตรวจสอบสถานะการเชื่อมต่อของเครื่องคอมพิวเตอร์ในระบบ 5. เพิ่มข้อมูล 6. แก้ไขข้อมูล 7. ลบข้อมูล 8. ระบบจะแสดงผลการทำงาน	
Sub Flows :	
Extension :	
Alternative/Exceptional : กรณีที่การทำงานของระบบมีความไม่ถูกต้อง ระบบจะแสดงข้อความเตือนให้ผู้ดูแลระบบทราบ	

ตารางที่ 3.6 รายละเอียดการปรับปรุงประสิทธิภาพการใช้ทรัพยากรเครือข่าย

Use Case Name :	Troubleshoot Problem
Triggering Event : -	
Brief Description : ฟังก์ชั่นสำหรับการแก้ปัญหาในระบบที่ตรวจสอบเจอให้การทำงานมีประสิทธิภาพมากขึ้น	
Actors : System Administrator (ผู้ดูแลระบบ)	
Related Use Case :-	
Stakeholder : System Administrator (ผู้ดูแลระบบ)	
Precondition :มีการจัดการ Policy ในการตรวจสอบการ monitor และกำหนดการแก้ไขเบื้องต้น	
Post Condition : ระบบจะมีการแก้ปัญหาเบื้องต้นที่ตรวจสอบ และแจ้งรายงานผลกับผู้ดูแลระบบ	
Minimal guarantee :	
Success guarantee : สามารถเข้าสู่ระบบได้	
Flow of Events : 1. ผู้ดูแลระบบเข้าสู่ระบบและเลือกเมนูใช้งาน 2. ระบบแสดงหน้าจอรายงานการทำงานในการแก้ปัญหาระบบที่เกิดขึ้น 3. ส่งผลการแก้ปัญหาให้ผู้ดูแลระบบผ่านทางระบบ	
Sub Flows :	
Extension :	
Alternative/Exceptional : -	

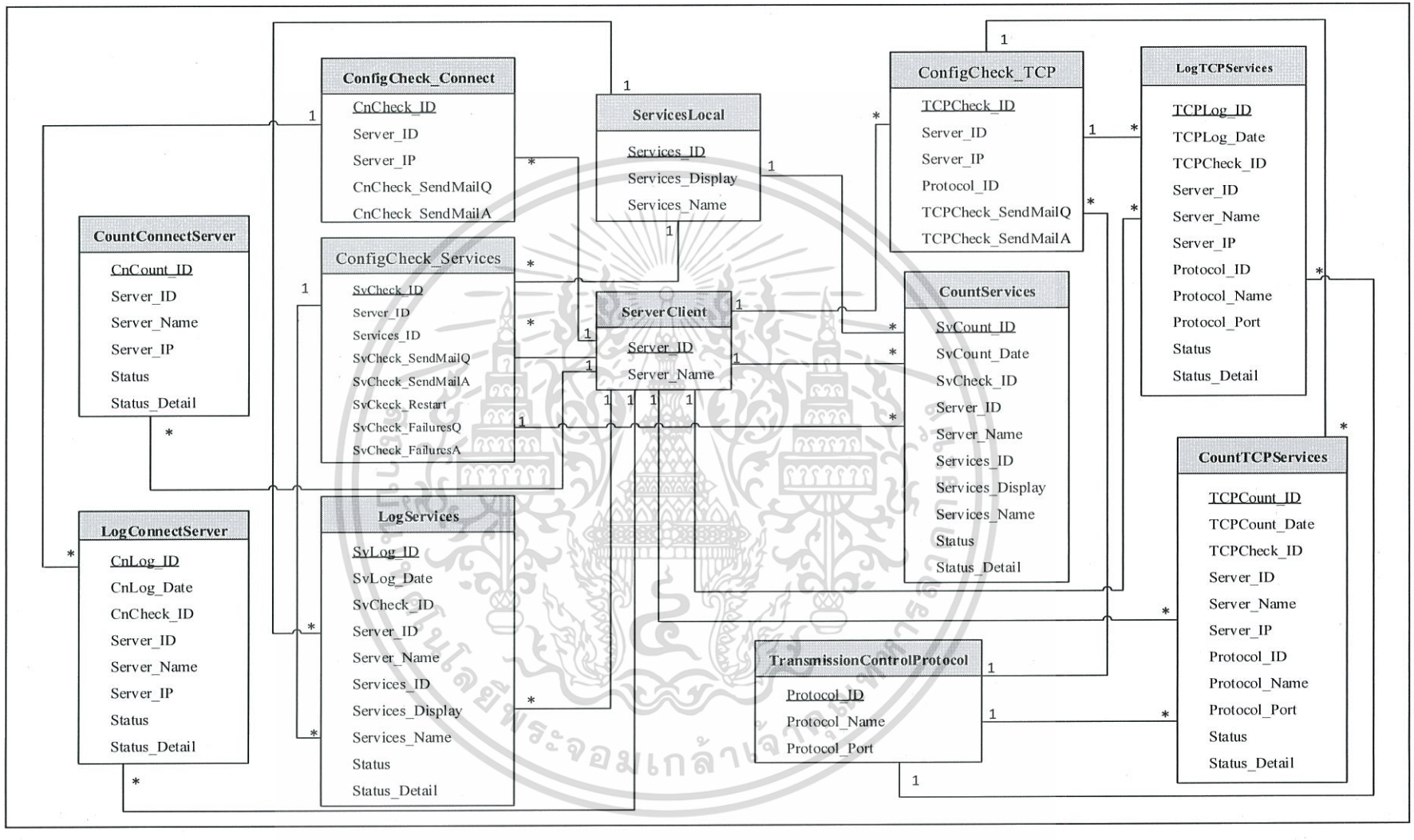
3.2.3 แอคทิวิตีไดอะแกรม (Activity Diagram)

แอคทิวิตีไดอะแกรม แสดงรายละเอียดที่ใช้อธิบายขั้นตอนการทำงานของระบบ แสดงให้เห็นถึงกระบวนการทำงานของแต่ละกิจกรรมของผู้ใช้งานที่เกิดขึ้นภายในระบบ สามารถแสดงการทำงานได้ดังนี้



รูปที่ 3.3 แสดงแอคทิวิตีไดอะแกรม

3.2.4 แผนภาพความสัมพันธ์ของข้อมูล (ER-Diagram)



รูปที่ 3.4 แผนภาพความสัมพันธ์ของข้อมูล (ER-Diagram)

3.2.5 พจนานุกรมข้อมูล (Data Dictionary)

พจนานุกรมข้อมูลระบบตรวจสอบและแก้ไขปัญหาระบบคอมพิวเตอร์และเครือข่าย เพื่อแสดงความสัมพันธ์ระหว่างข้อมูลของแต่ละตาราง องค์ประกอบที่สำคัญของระบบ ดังนี้

ตารางที่ 3.7 ConfigCheck_Connect ข้อมูลรายละเอียดการตั้งค่าการตรวจสอบการเชื่อมต่อ Server

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
CnCheck_ID	รหัสการตรวจสอบ	int	PK
Server_ID	รหัสเครื่อง Server	int	FK
Server_IP	หมายเลข IP เครื่อง Server	varchar (25)	
CnCheck_SendMailQ	การตั้งค่าการส่งเมล	bit	
CnCheck_SendMailA	จำนวนครั้งที่ตั้งค่าส่งเมล	int	

ตารางที่3.8 ConfigCheck_Services ข้อมูลรายละเอียดการตั้งค่าการตรวจสอบการService ให้บริการ

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
SvCheck_ID	รหัสการตรวจสอบ	int	PK
Server_ID	รหัสเครื่อง Server	int	FK
Services_ID	รหัส Service	varchar (25)	FK
SvCheck_SendMailQ	การตั้งค่าการส่งเมล	bit	
SvCheck_SendMailA	นับจำนวนการตรวจสอบเพื่อส่งเมล	int	
SvCkeck_Restart	การตั้งค่าการ Restart	bit	
SvCheck_FailuresQ	การตั้งค่า นับ failure	int	
SvCheck_FailuresA	นับจำนวนการตรวจสอบการ failure	int	

ตารางที่ 3.9 ConfigCheck_TCP ข้อมูลรายละเอียดการตั้งค่าการตรวจสอบโปรโตคอล

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
TCPCheck_ID	รหัสตรวจสอบ TCP	int	PK
Server_ID	รหัสเครื่อง Server	int	FK
Server_IP	หมายเลข IP	varchar (25)	
Protocol_ID	รหัส Protocal	int	FK
TCPCheck_SendMailQ	การตั้งค่าการส่งเมล	bit	
TCPCheck_SendMailA	จำนวนครั้งที่ตั้งค่าส่งเมล	int	

ตารางที่ 3.10 CONFIGS ข้อมูลรายละเอียด การตั้งค่าระบบ monitoring

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
CONFIG_SEQ	ลำดับ	int	PK
CONFIG_NAME	ชื่อการตั้งค่า	varchar (50)	
CONFIG_VALUE	ค่าในระบบ	varchar (150)	

ตารางที่ 3.11 CountConnectServer ข้อมูลรายละเอียด นับปัญหาส่วนการเชื่อมต่อ

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
CnCount_ID	รหัส	bigint	PK
CnCount_Date	วันที่เกิดปัญหา	datetime2	
CnCheck_ID	รหัสการตรวจสอบ	int	FK
Server_ID	รหัสเครื่อง Server	int	FK
Server_Name	ชื่อเครื่อง Server	Varchar (25)	
Server_IP	หมายเลข IP	Varchar (25)	
Status	สถานะ	Varchar (50)	
Status_Detail	รายละเอียด	Varchar (100)	

ตารางที่ 3.12 CountServices ข้อมูลรายละเอียด นับปัญหาส่วนของ Service

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
SvCount_ID	รหัส	bigint	PK
SvCount_Date	วันที่	datetime2	
SvCheck_ID	รหัสการตรวจสอบ	int	FK
Server_ID	รหัสเครื่อง Server	int	FK
Server_Name	ชื่อเครื่อง Server	Varchar (25)	
Services_ID	รหัสเครื่อง Server	int	FK
Services_Display	Display	Varchar (200)	
Services_Name	ชื่อ Service	Varchar (50)	
Status	สถานะ	Varchar (50)	
Status_Detail	รายละเอียด	varchar (100)	

ตารางที่ 3.13 CountTCPServices ข้อมูลรายละเอียด การนับ TCP Service

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
TCPCount_ID	รหัส	bigint	PK
TCPCount_Date	วันที่	datetime2	
TCPCheck_ID	รหัสการตรวจสอบ	int	FK
Server_ID	รหัสเครื่อง Server	int	
Server_Name	ชื่อเครื่อง Server	Varchar (25)	
Server_IP	หมายเลข IP	Varchar (25)	
Protocol_ID	รหัส Protocol	int	FK
Protocol_Name	ชื่อ Protocol	Varchar (200)	
Protocol_Port	พอร์ต	Varchar (5)	
Status	สถานะ	Varchar (50)	
Status_Detail	รายละเอียด	Varchar (100)	

ตารางที่ 3.14 LogConnectServer ข้อมูลรายละเอียด ประวัติการทำงานส่วนการเชื่อมต่อ

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
CnLog_ID	รหัส	bigint	PK
CnLog_Date	วันที่	datetime2	
CnCheck_ID	รหัสการตรวจสอบ	int	FK
Server_ID	รหัสเครื่อง Server	int	FK
Server_Name	ชื่อเครื่อง Server	Varchar (25)	
Server_IP	หมายเลข IP	Varchar (25)	
Status	สถานะ	Varchar (50)	
Status_Detail	รายละเอียด	Varchar (100)	

ตารางที่ 3.15 LogServices ข้อมูลรายละเอียด

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
SvLog_ID	Log Service ID	bigint	PK
SvLog_Date	วันที่	datetime2	
SvCheck_ID	รหัสการตรวจสอบ Service	int	FK
Server_ID	รหัส Server	int	FK

ตารางที่ 3.15 LogServices ข้อมูลรายละเอียด (ต่อ)

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
Server_Name	ชื่อเครื่อง	Varchar (25)	
Services_ID	รหัส Service	int	FK
Services_Display	ชื่อService ที่แสดง	Varchar (200)	
Services_Name	ชื่อ Service	Varchar (50)	
Status	สถานะการทำงานของ Service	Varchar (50)	
Status_Detail	รายละเอียด	Varchar (100)	

ตารางที่ 3.16 LogTCPServices ข้อมูลรายละเอียดการเก็บ log การตรวจสอบโปรโตคอล

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
TCPLog_ID	รหัส log	bigint	PK
TCPLog_Date	วันที่	datetime2	
TCPCheck_ID	รหัสตรวจสอบ TCP	int	FK
Server_ID	รหัสเครื่อง server	int	FK
Server_Name	ชื่อเครื่อง	Varchar (25)	
Server_IP	IP เครื่อง Server	Varchar (25)	
Protocol_ID	รหัสโปโตคอล	int	FK
Protocol_Name	ชื่อโปโตคอล	Varchar (200)	
Protocol_Port	พอร์ต	Varchar (5)	
Status	สถานะ	Varchar (50)	
Status_Detail	รายละเอียด	Varchar (100)	

ตารางที่ 3.17 Server Client ข้อมูลรายละเอียดเครื่อง Server ในระบบเครือข่าย

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
Server_ID	รหัส Server	int	PK
ServerName	ชื่อ Server	Varchar(25)	

ตารางที่ 3.18 ServicesLocal ข้อมูลรายละเอียด Services ที่ใช้งาน

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
Services_ID	รหัส Services	int	PK
Services_Display	ชื่อที่แสดง Services	Varchar(200)	
Services_Name	ชื่อ Services	Varchar(50)	

ตารางที่ 3.19 TransmissionControlProtocol ข้อมูลรายละเอียดเกี่ยวกับโปรโตคอล

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
Protocol_ID	รหัสโปโตคอล	int	PK
Protocol_Name	ชื่อโปโตคอล	Varchar(200)	
Protocol_Port	พอร์ตโปโตคอล	Varchar(5)	

ตารางที่ 3.20 USERS ข้อมูลรายละเอียดของผู้ใช้งานระบบ

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
USER_ID	รหัสผู้ใช้	int	PK
USER_NAME	ชื่อผู้ใช้	Varchar (100)	
USER_LOGIN	ชื่อในการเข้าระบบ	Varchar(50)	
USER_PASS	รหัสผ่านในการเข้าระบบ	Varchar (15)	
EMAIL	อีเมล	Varchar (50)	
PHONE	เบอร์โทรศัพท์	Varchar (25)	
POSITION	ตำแหน่ง	Varchar (70)	
GROUP_NAME	กลุ่มของผู้ใช้งาน	Varchar (20)	
USER_STATUS	สถานะผู้ใช้งาน	Varchar (10)	

ตารางที่ 3.21 ServerClient ข้อมูลรายละเอียดของเครื่องที่ติดต่อในระบบ

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
Server_ID	รหัส Server	int	PK
Server_Name	ชื่อเครื่อง	varchar(25)	
Server_OS	ระบบปฏิบัติการเครื่อง	varchar(200)	
Server_Version	เวอร์ชัน	varchar(50)	

ตารางที่ 3.21 ServerClient ข้อมูลรายละเอียดของเครื่องที่ติดต่อในระบบ (ต่อ)

ชื่อแอททริบิวต์	คำอธิบายข้อมูล	ชนิดข้อมูล	คีย์
Server_SP	เวอร์ชั่น Service pack	Varchar (100)	
Server_ProductID	รหัสสินค้า	Varchar (100)	PK
Server_CPU	CPU	Varchar (100)	
Server_RamTotal	จำนวน RAM	Varchar (50)	
Server_RamAvailable	Ram ที่ยังไม่ได้ใช้	Varchar (50)	
Server_BiosName	ชื่อ Bios	Varchar (150)	
Server_BiosID	รหัส Bios	Varchar (150)	
Server_Disk	หน่วยความจำ	Varchar (250)	

บทที่ 4
การออกแบบหน้าจอการทำงาน

4.1 การออกแบบหน้าจอ

ระบบตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่าย ถูกพัฒนาขึ้นในรูปแบบของเว็บแอพพลิเคชั่นให้มีการใช้งานง่ายและสะดวกขึ้น ระบบจะมีการแจ้งเตือนเมื่อระบบเครือข่ายมีปัญหา สามารถเรียกดูรายงานที่เกิดขึ้นได้

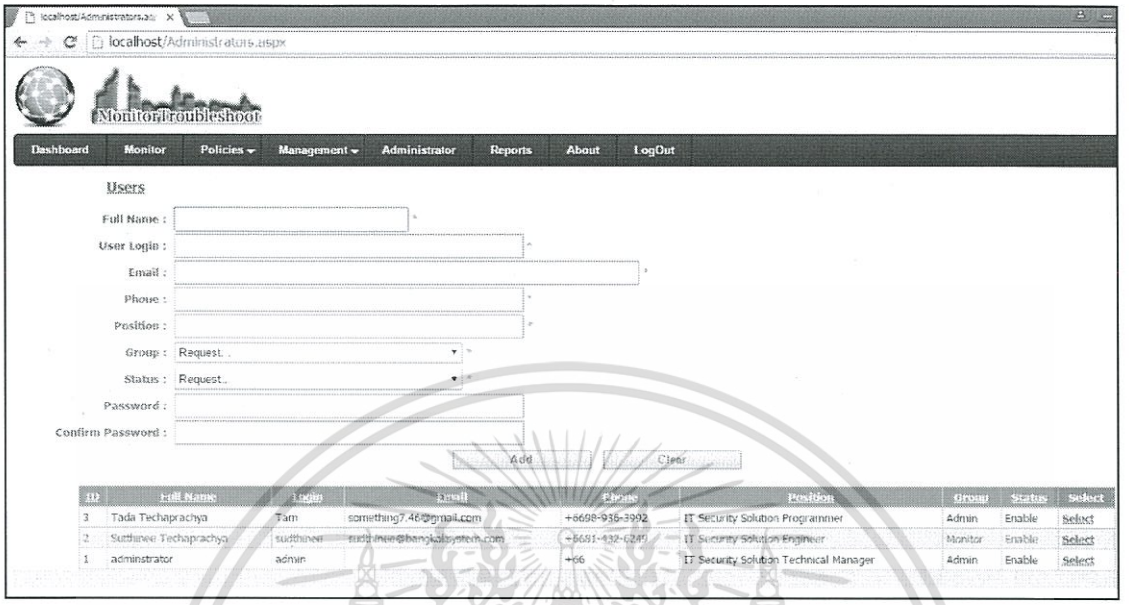
4.1.1 หน้าจอล็อกอินเข้าสู่ระบบและตรวจสอบสิทธิ์

การทำงานผ่าน Web Browser ผู้ใช้งานระบบทำการกรอกชื่อผู้ใช้และรหัสผ่านในการพิสูจน์ตัวตนใช้งานระบบตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่าย

รูปที่4.1 แสดงหน้าจอการล็อกอินเข้าระบบ

4.1.2 หน้าจอในการการจัดการข้อมูลผู้ดูแลระบบ

สามารถจัดการข้อมูลเกี่ยวกับผู้ใช้งานระบบได้มากกว่า 1 คนในการจัดการโดนทำการเพิ่ม ลบ แก้ไข ข้อมูลผู้ใช้งาน E mail ในการแจ้งเตือนจากระบบ



รูปที่4.2 แสดงหน้าจอการจัดการข้อมูลผู้ใช้

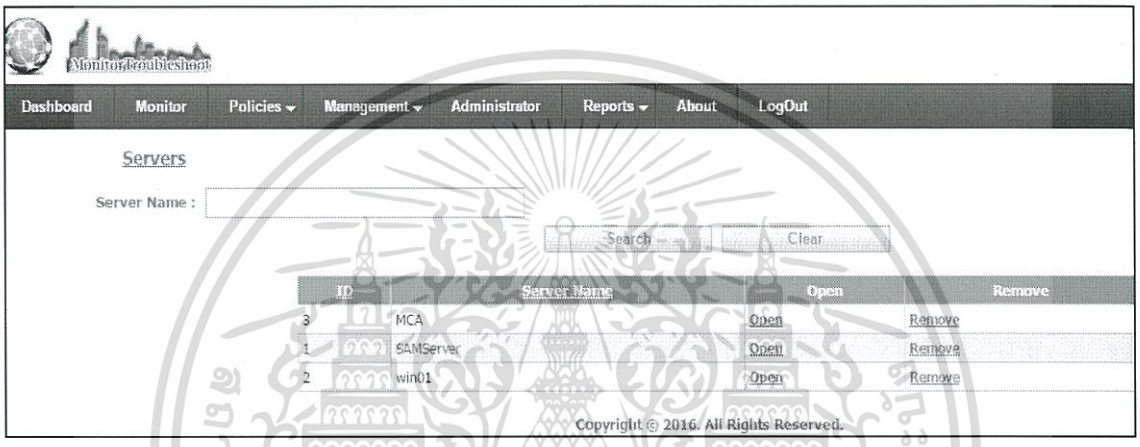
- การจัดการผู้ใช้จะมีสิทธิ์ในการจัดระดับผู้ดูแลระบบเป็น 2 ระดับ คือ ระดับ admin ระบบกับ Monitor ระบบซึ่งจะไม่มีสิทธิ์ในการจัดการ Policy และจัดการส่วน Management ต่าง ๆ ในระบบ จะทำได้แค่ในส่วนการ ดูหน้า Dashboard ดู Monitor ออกรายงาน ซึ่งแสดงดังหน้าจอด้านล่าง

รูปที่4.3 แสดงหน้าจอเมนูสิทธิ์ผู้ดูแลระบบส่วน Monitor

4.1.3 การจัดการข้อมูลระบบเครือข่าย

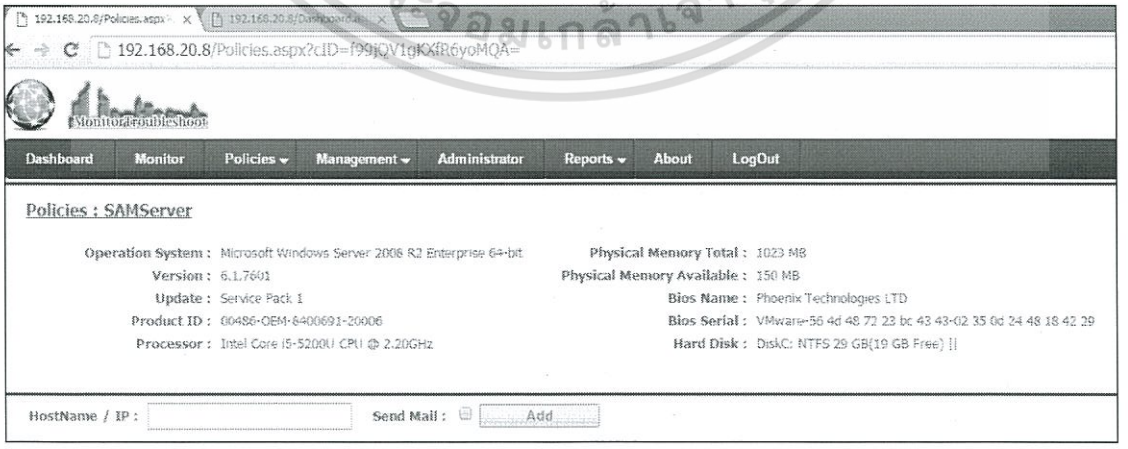
เป็นหน้าจอที่ผู้ดูแลระบบเข้าสู้ระบบเพื่อจัดการในส่วนการเพิ่ม ลบ และสามารถดึงข้อมูลมาทำการแก้ไขข้อมูลในระบบเครือข่ายคอมพิวเตอร์ และกำหนดการตั้งค่านโยบายในการตรวจสอบเครือข่ายได้ โดยผู้ดูแลระบบจะต้องใส่ข้อมูลที่จำเป็นสู่ระบบที่แทบเมนู Policies

ส่วนที่ 1 การจัดการเกี่ยวกับข้อมูลเครื่องคอมพิวเตอร์ในระบบที่ต้องการตรวจสอบการทำงาน เมื่อทำการติดตั้งตัวเอเจนต์ที่เครื่องคอมพิวเตอร์ที่ต้องการตรวจสอบ จะแสดงข้อมูลคอมพิวเตอร์ในระบบ



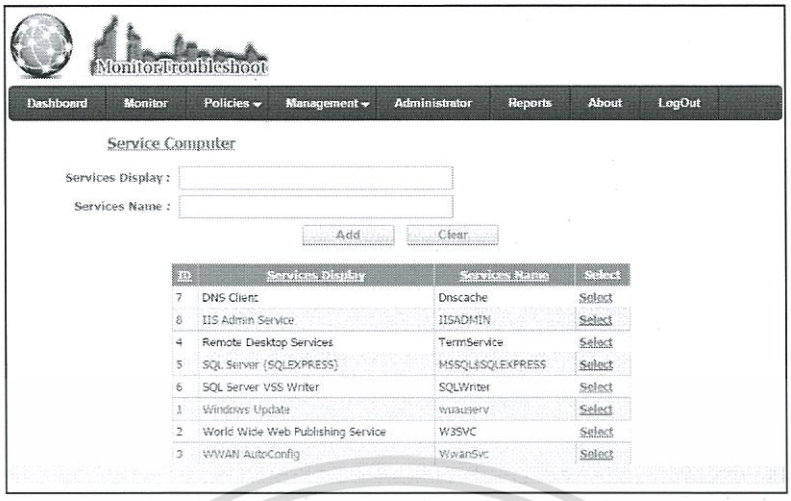
รูปที่4.4 แสดงหน้าจอการจัดการเครื่องคอมพิวเตอร์

การจัดการส่วนนี้สามารถเรียกดูข้อมูลทรัพยากรของเครื่องคอมพิวเตอร์ในระบบได้ โดยคลิกเลือกที่เครื่องที่ต้องการ ระบบจะแสดงข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์ ระบบปฏิบัติการเครื่อง เวอร์ชั่น และความหน่วยความจำ เป็นต้น



รูปที่4.5 แสดงหน้าจอข้อมูลเครื่องคอมพิวเตอร์

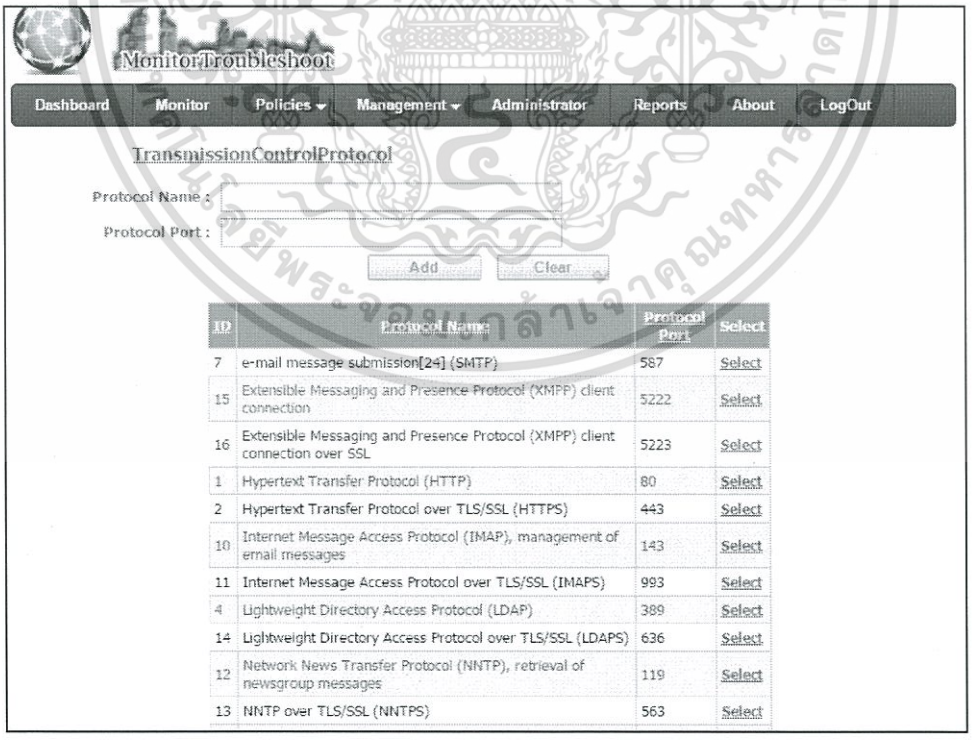
ส่วนที่ 2 การจัดการเกี่ยวกับ Service Computer ที่จะตรวจสอบการทำงาน



รูปที่4.6 แสดงหน้าจอการจัดการ Service Computer

ส่วนที่ 3 การจัดการข้อมูลส่วนของพอร์ต และโปรโตคอล ที่ต้องการตรวจสอบ

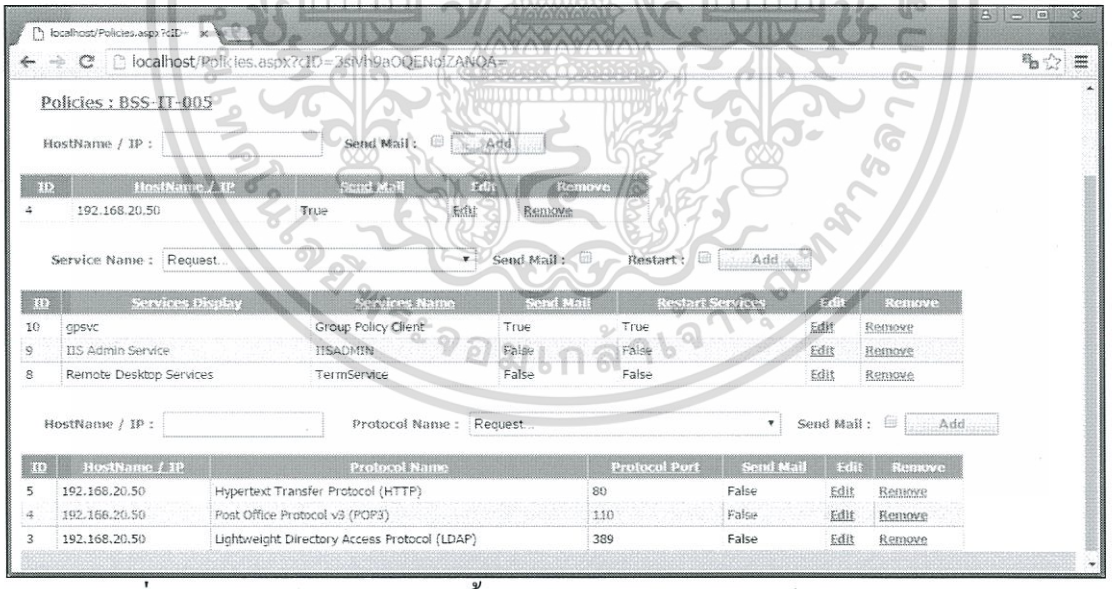
ผู้ดูแลระบบสามารถเพิ่มการตรวจสอบของพอร์ต และโปรโตคอลที่มีการใช้งานในเครื่องคอมพิวเตอร์ที่ให้บริการอยู่ เพื่อนำไปจัดตรวจสอบการทำงาน โดยการเพิ่มแล้วไปกำหนดที่ Policy ให้ตรวจสอบ



รูปที่4.7 แสดงหน้าจอการจัดการข้อมูลส่วนของพอร์ต และโปรโตคอล

ส่วนที่ 4 การตั้งค่าในการตรวจสอบและการแจ้งเตือน

รูปที่4.8 แสดงหน้าจอการตั้งค่าในการตรวจสอบและการแจ้งเตือนการทำงาน Service การตั้งค่าในการตรวจสอบและการแจ้งเตือน

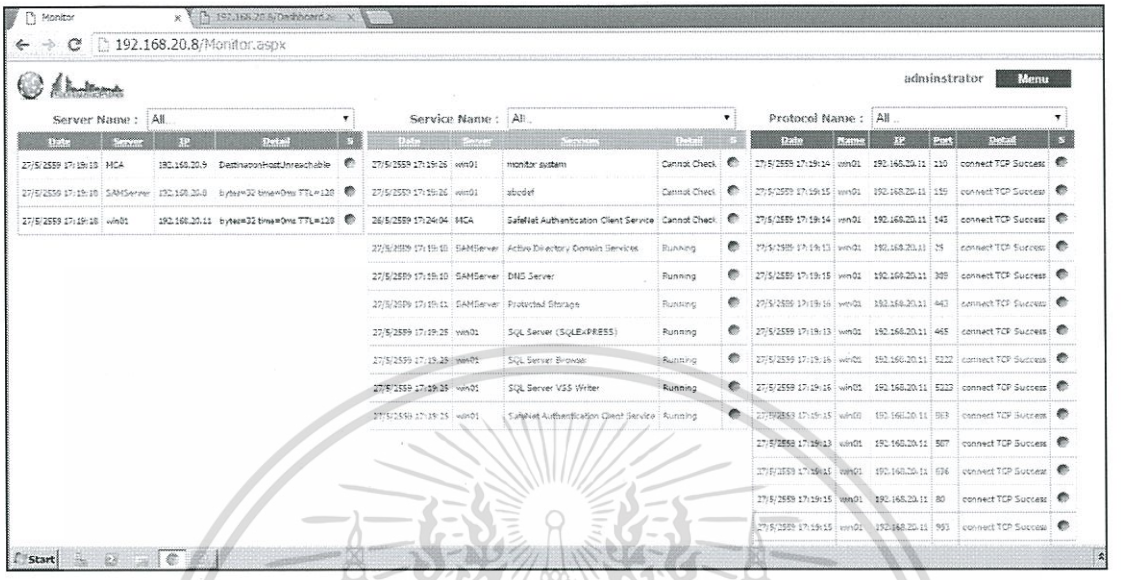


รูปที่4.9 แสดงหน้าจอจัดการการตั้งค่านโยบายการตรวจสอบข้อมูลระบบเครือข่าย

4.1.4 การทำงานของระบบในส่วนมอนิเตอร์

ทำงานในลักษณะการแสดงผลสถานะการตรวจสอบการทำงานของระบบตามนโยบายที่ผู้ดูแลระบบกำหนดในการตรวจสอบ โดยแสดงผลการตรวจสอบออกเป็น 3 ส่วนหลัก คือ

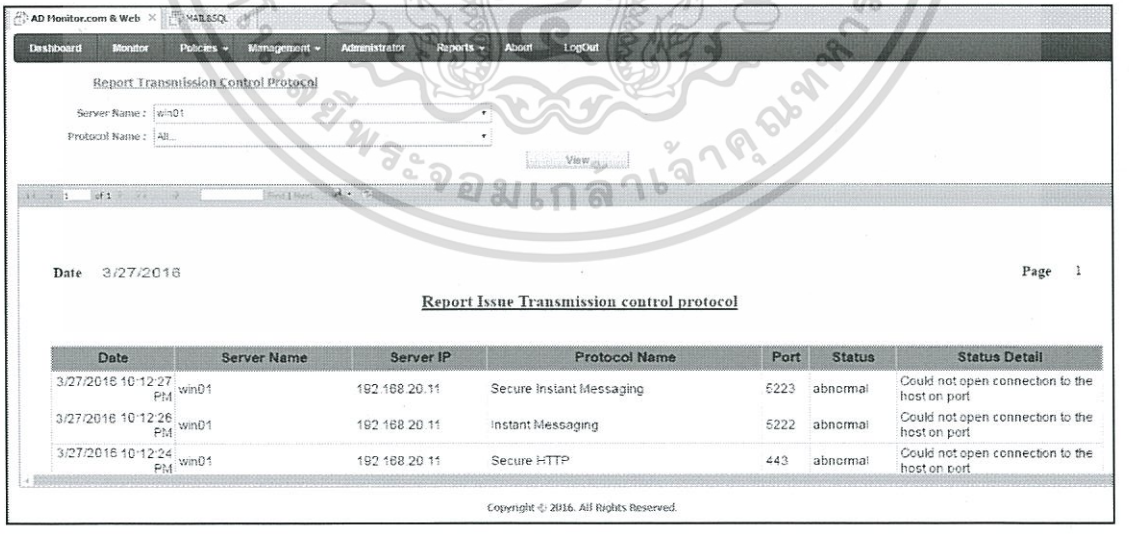
- ส่วนของ Server ตรวจสอบการเชื่อมต่อของเครื่องคอมพิวเตอร์
- ส่วนของ Service ตรวจสอบสถานะการทำงานของเซอร์วิสของเครื่องให้บริการ
- ส่วนของ Protocol ตรวจสอบสถานะการทำงานของโปรโตคอล



รูปที่4.10 แสดงหน้าจอการมอนิเตอร์ระบบ

4.1.5 หน้าจอในส่วนการแสดงรายงาน

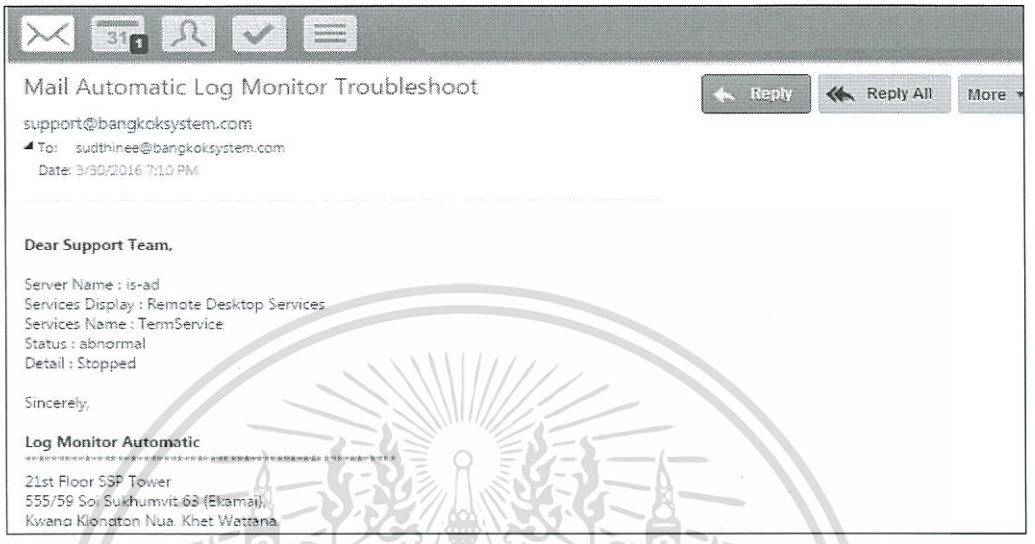
การทำงานระบบ โดยคลิกเลือกเมนูสำหรับแสดงรายงาน ระบบจะทำการแสดงผลหน้าจอรายงานเหตุการณ์และLogsที่เกิดขึ้น ตามวัน เวลา และเหตุการณ์ที่เกิดขึ้นในระบบ สามารถทำการบันทึกรายงานออกมาได้เป็นชนิดของไฟล์นามสกุลต่างๆ ได้



รูปที่4.11 แสดงหน้าจอ Report การมอนิเตอร์

4.1.6 การแจ้งเตือนผ่านทาง E-mail

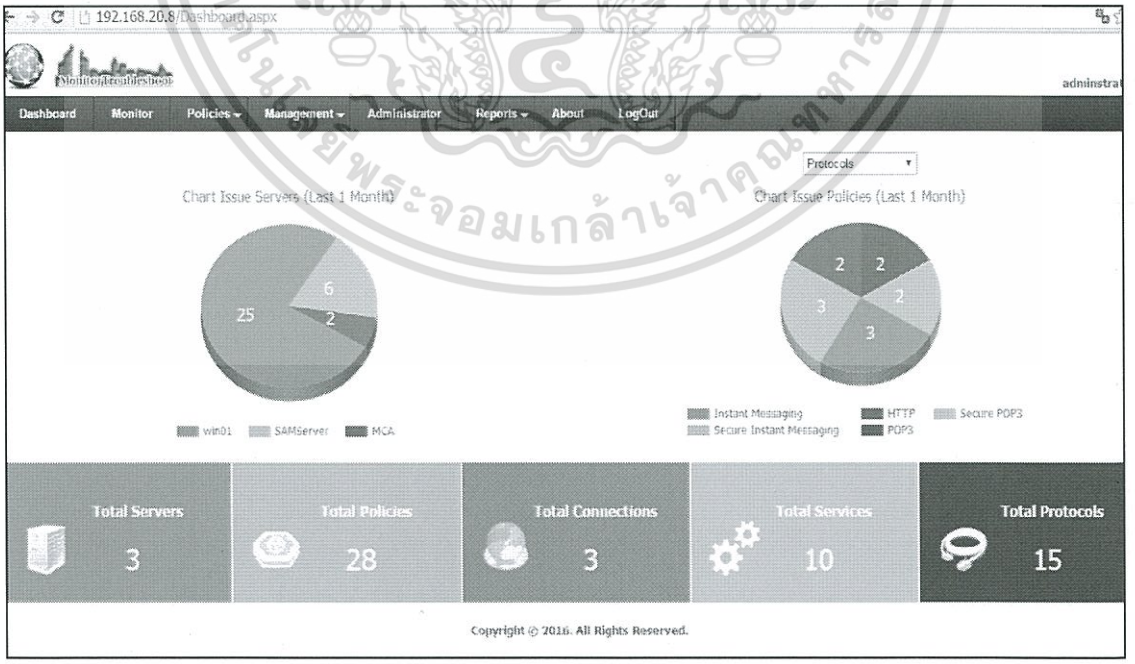
เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้นในระบบ หรือมีปัญหาไม่สามารถติดต่อได้ เพื่อแจ้งให้ผู้ดูแลระบบทราบโดยแจ้งผ่านทาง E-mail แจ้งเตือนเหตุการณ์และรายละเอียดต่างๆ กับผู้ดูแลระบบ



รูปที่ 4.12 แสดงหน้าจอการแจ้งเตือนผ่านทางระบบ E-mail

4.1.7 แสดงหน้า Dashboard ระบบ

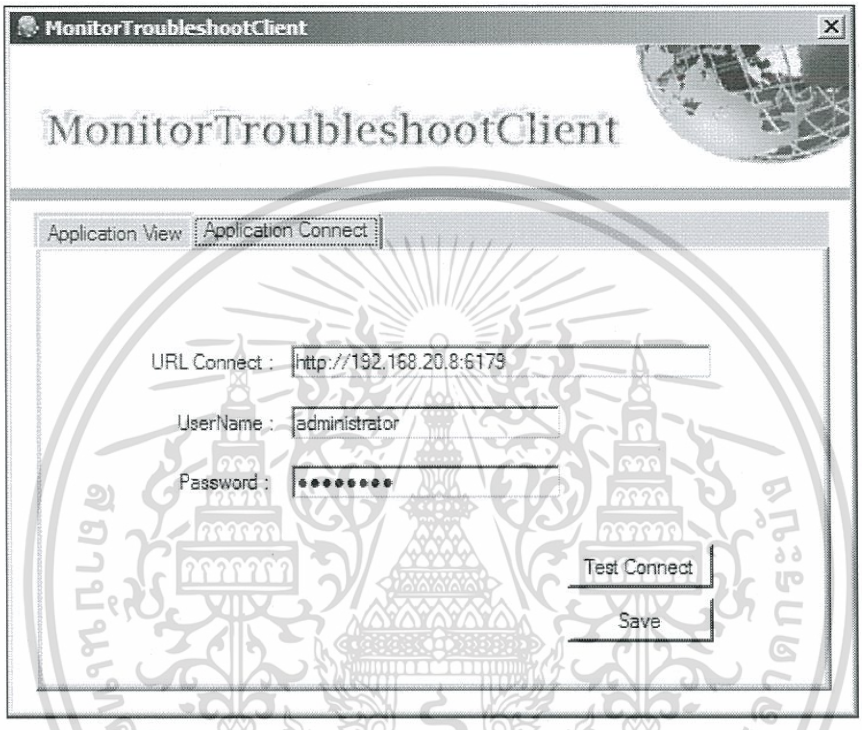
แสดงการทำงานภาพรวมของระบบในการมอนิเตอร์และการตรวจเจอปัญหา พร้อมทั้งแสดงภาพรวมของการกำหนดนโยบาย



รูปที่ 4.13 แสดงหน้า Dashboard ระบบโดยรวม

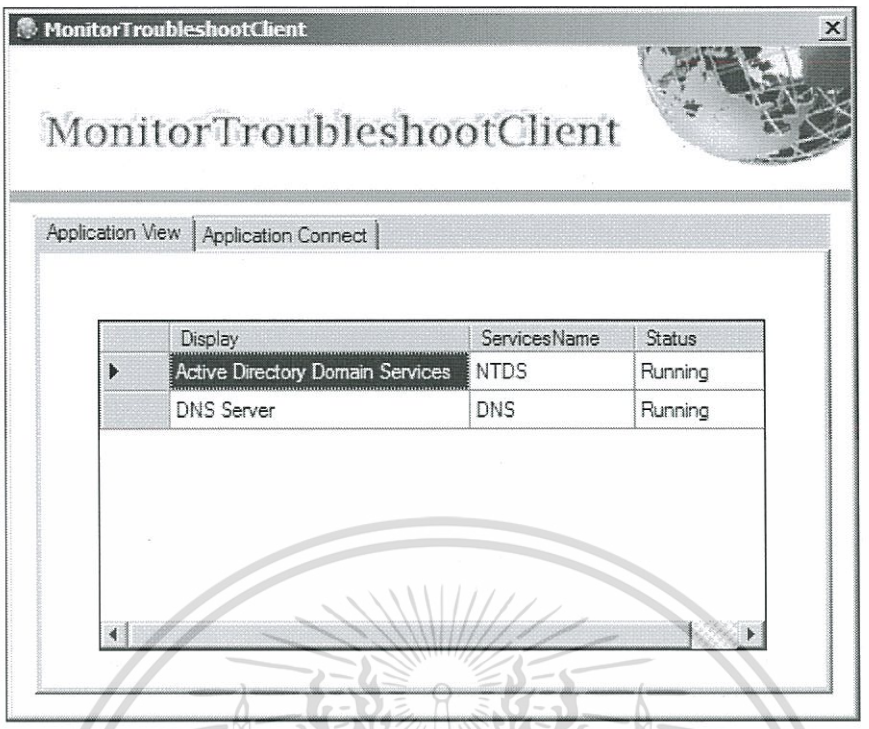
4.1.8 แสดงหน้าจอเอเจนต์ ในการตรวจสอบเซอร์วิสของเครื่องให้บริการ

ในการตรวจสอบการทำงานของเครื่องให้บริการที่ต้องการจะตรวจสอบและรายงานผลสถานะการทำงานผ่านหน้าเวบมอนิเตอร์นั้น จะมีการติดตั้งเอเจนต์เพื่อการตรวจสอบเซอร์วิสที่ทำงานที่เครื่องให้บริการ โดยการกำหนดการเชื่อมต่อการทำงานไปยังเวบเซอร์วิสและกำหนดชื่อผู้ใช้ รหัสผ่านในการตรวจโดยสามารถทดสอบการเชื่อมต่อได้ ที่ปุ่ม Test Connect



รูปที่ 4.14 แสดงหน้า Application Connect ที่เอเจนต์

- แสดงสถานะการทำงาน เมื่อมีการสร้าง Policy ในการตรวจสอบ เอเจนต์จะแสดงสถานะการทำงานของเซอร์วิสตาม Policy ที่สร้างจากหน้าเวบ



รูปที่ 4.15 แสดงการทำงานของการตรวจสอบเซอร์วิสที่เอเจนต์

บทที่ 5
สรุปผลการพัฒนาระบบ

5.1 ผลการพัฒนาระบบ

การพัฒนาระบบตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่ายได้มีการวิเคราะห์และออกแบบระบบการทำงานผ่านทางหน้าเวบ โดยส่วนนี้มีการออกแบบ ยูสเคส ไดอะแกรม อีอาร์ไดอะแกรม ทำให้สามารถพัฒนาระบบออกมาได้อย่างเป็นระบบ ซึ่งระบบที่พัฒนาขึ้นมานี้สามารถตรวจสอบและแก้ไขปัญหาระบบงานคอมพิวเตอร์และเครือข่าย ระบบดังกล่าวจะช่วยตรวจสอบการทำงานของเซอร์วิสและโปรโตคอลของระบบที่ใช้งานของเครื่องคอมพิวเตอร์ที่ให้บริการต่าง ๆ เพื่อนำข้อมูลมาใช้ประโยชน์การวิเคราะห์สาเหตุ หรือตรวจสอบสถานะต่างๆ ในการใช้งาน และตรวจสอบการเชื่อมต่อในระบบคอมพิวเตอร์ นอกจากนั้นเมื่อพบปัญหาจะทำการแก้ไขปัญหาให้เบื้องต้นโดยอัตโนมัติได้

ผู้จัดทำได้ทำการออกแบบและพัฒนาระบบโดยมีส่วนการทำงานใหญ่ ๆ ดังนี้

1. ส่วนแสดงหน้า Dashboard แสดงการทำงานระบบโดยภาพรวม แสดงในส่วนของเครื่องคอมพิวเตอร์ที่ให้บริการที่มีการเชื่อมต่อมายังระบบ แสดงส่วนของจำนวนการเกิดเหตุขัดข้องของแต่ละเงื่อนไขที่ระบบตรวจสอบ ซึ่งแบ่งออกเป็น เซอร์วิสให้บริการ โปรโตคอล และการเชื่อมของเครื่องให้บริการ
2. ระบบจัดการเกี่ยวกับเพิ่มข้อมูลเกี่ยวกับ Server ให้บริการหรือเซอร์วิสให้บริการโปรโตคอลที่ต้องการตรวจสอบได้
3. ระบบการมอนิเตอร์ เพื่อการตรวจสอบสถานะการทำงาน เกี่ยวกับเชื่อมต่อของเครื่องในระบบ การทำงานของ เซอร์วิสให้บริการในระบบได้
4. ระบบการแจ้งเตือน ผ่านทาง E-mail
5. ระบบการแจ้งเตือน ผ่านหน้าเว็บเบราว์เซอร์
6. ระบบการแสดงรายงาน
7. ระบบการแก้ปัญหาระบบเบื้องต้น

โดยการพัฒนาระบบการทำงานผ่านทางหน้าเวบ ช่วยในการตรวจสอบระบบเครือข่ายสำหรับผู้ดูแลระบบ และสามารถจัดการสิทธิ์ในการเข้าถึงผ่านการจัดการ

5.2 อุปสรรคในการพัฒนาระบบ

ฟังก์ชันการทำงานของการตรวจสอบระบบแต่ละระบบที่ผู้ใช้ต้องการตรวจสอบ มีความซับซ้อน เมื่อต้องไปตรวจสอบลึกถึงการทำงานของแต่การจัดการ ซึ่งอาจจะยังไม่ครอบคลุมในการ

ตรวจสอบการทำงานของระบบทั้งหมด ต้องรู้เกี่ยวกับการทำงานระบบแต่ละส่วน นั้นเป็นอย่างดี ว่าต้องประกอบไปด้วยส่วนการทำงานของ Service อะไรบ้าง การเชื่อมต่อกับส่วนไหนบ้าง โปโตคอลที่สำคัญที่จะทำให้ทำงานได้ปกติ และสาเหตุอะไรบ้างที่ระบบจะหยุดการทำงานให้บริการลง

5.3 ข้อเสนอแนะเพิ่มเติม

5.3.1 นำไปพัฒนาต่อให้ระบบมีความยืดหยุ่นกับการตรวจสอบระบบที่ครอบคลุมการทำงานของหลายส่วนในองค์กร และเพิ่มแนวทางการแก้ไขปัญหาโดยอัตโนมัติ ให้ครอบคลุมในทุกปัญหาของระบบได้มากขึ้น เพิ่มการ Import และ Export ค่าที่ตั้งค่าระบบ เอาไว้เพื่อ Backup และ Restore ได้

5.3.2 เพิ่มการทำงานส่วนการ Remote Control เพื่อสามารถสั่งงานเครื่องคอมพิวเตอร์จากระยะไกลได้ โดยเข้าไปเลื่อนเม้าส์และกดปุ่มแป้นพิมพ์ ส่งคำสั่ง คลิกการทำงานได้ โดยการ Access เข้าไปในเครื่องที่ควบคุมอยู่ โดยผู้ดูแลระบบไม่ต้องเข้าถึงตัวเครื่องโดยตรง

5.3.3 สามารถตรวจสอบการทำงานระบบและเซอร์วิสต่าง ๆ ที่ทำงานบนระบบ Cloud ได้

บรรณานุกรม

พิศาล พิทยาธุรวิวัฒน์. 2551.**ติดตั้งระบบเครือข่ายคอมพิวเตอร์ Intranet/Internet**.กรุงเทพฯ: ซีเอ็ดยูเคชั่น.

พงศ์ธรณ์ กิตติศีรีชัยกุล และ ศิกวัส ชีชนะ. 2554. **ระบบบริหารจัดการเครือข่ายที่ใช้ง่ายและมีประสิทธิภาพ** .ปริญญานิพนธ์ หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

สุรชัย ชัยสิริเจริญกุล. 2553. **ระบบมอนิเตอร์และวางแผนสำหรับความสามารถของเครื่องเซิร์ฟเวอร์.** การศึกษาอิสระ หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกลาเจ้าคุณทหารลาดกระบัง.

สุดาพร ฮุยสูงเนิน. 2557. **ระบบการจัดการบัญชีผู้ใช้บนแอคทีฟไดเร็กทอรี่ผ่านเว็บ.** การศึกษาอิสระ หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกลาเจ้าคุณทหารลาดกระบัง.

ประวัติผู้เขียน

ชื่อผู้จัดทำโครงการ	นางสาวสุทธินีย์ เตชะปรัชญา
วันเดือนปีเกิด	08 เมษายน 2529
สถานที่เกิด	นครศรีธรรมราช
ประวัติการศึกษา	
มัธยมศึกษาตอนต้น	โรงเรียนท่าศาลาประสิทธิ์ศึกษา
มัธยมศึกษาตอนปลาย	โรงเรียนท่าศาลาประสิทธิ์ศึกษา
อุดมศึกษา (ปริญญาตรี)	วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยวลัยลักษณ์
ประสบการณ์การทำงาน	
พ.ศ.2556-ปัจจุบัน	บริษัทแบงคอคซิสเท็มแอนด์ซอฟแวร์จำกัด