

การจัดสรุปผลการพัฒนางาน /แนวปฏิบัติที่ดี  
ชื่อผลงาน ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์  
(Centralized Network Monitoring System)

ประเภทผลงาน

- สายวิชาการ  
 สายสนับสนุน โปรตระบุ  
 การพัฒนาระบบเทคโนโลยีสารสนเทศ  
 การพัฒนางาน/กระบวนการ/R2R  
 การพัฒนางานห้องปฏิบัติการ

ประเภทการนำไปใช้ประโยชน์

- นวัตกรรม  R2R  การพัฒนางาน/การลดขั้นตอน

ชื่อเจ้าของผลงาน นายสุรศักดิ์ ศรีวิเศษ ตำแหน่ง นักวิชาการคอมพิวเตอร์ หน่วยงานสำนักคอมพิวเตอร์และเครือข่าย

1.บทคัดย่อ

การพัฒนาเทคโนโลยีสารสนเทศและระบบเครือข่ายในปัจจุบันมีการเจริญเติบโตอย่างรวดเร็วและซับซ้อนมากขึ้น ส่งผลให้องค์กรต่างๆ ต้องพึ่งพาระบบเครือข่ายและอุปกรณ์ไอทีในการดำเนินธุรกิจมากยิ่งขึ้น การหยุดชะงักของระบบแม้เพียงช่วงเวลาสั้นๆ อาจส่งผลกระทบต่ออย่างมีนัยสำคัญต่อการดำเนินงานและความน่าเชื่อถือขององค์กร ดังนั้น การมีระบบตรวจสอบและเฝ้าระวังที่มีประสิทธิภาพจึงกลายเป็นความจำเป็นที่หลีกเลี่ยงไม่ได้

วัตถุประสงค์ของการพัฒนาระบบนี้ คือการศึกษาและพัฒนาระบบที่สามารถเฝ้าติดตามพารามิเตอร์สำคัญของระบบ ได้แก่ การรับส่งข้อมูลผ่านเครือข่าย (Network Traffic) การใช้งานซีพียู (CPU Utilization) การใช้งานหน่วยความจำ (Memory Usage) และการใช้งานพื้นที่จัดเก็บข้อมูล (Disk Usage) รวมถึงการตรวจสอบความพร้อมใช้งานของบริการต่างๆ เช่น HTTP DNS ICMP และฐานข้อมูล ระบบยังมีความสามารถในการกำหนดเกณฑ์การแจ้งเตือนที่ปรับแต่งได้ตามความต้องการและมีกลไกการส่งต่อข้อมูลไปยังผู้รับผิดชอบที่กำหนดไว้

ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์ (Centralized Network Monitoring System) เป็นระบบ Monitoring & Alerting ที่ออกแบบมาเพื่อติดตามสถานะของระบบเทคโนโลยีสารสนเทศ เครือข่าย แอปพลิเคชัน อุปกรณ์เครือข่าย และบริการต่างๆ โดยมีความสามารถในการส่งการแจ้งเตือนแบบทันทีเมื่อตรวจพบความผิดปกติ เพื่อให้ผู้ดูแลระบบสามารถดำเนินการแก้ไขได้อย่างรวดเร็ว

ระบบที่พัฒนาขึ้นมีจุดเด่นในการประมวลผลข้อมูลแบบเรียลไทม์ (Real-time Processing) และการจัดเก็บข้อมูล ประสิทธิภาพการทำงานในฐานข้อมูลเพื่อการวิเคราะห์แนวโน้มและการวางแผนในระยะยาว ระบบนี้มีส่วนติดต่อผู้ใช้แบบเว็บที่ใช้ งานง่ายและสามารถแสดงผลข้อมูลในรูปแบบกราฟิกที่เข้าใจง่าย พร้อมทั้งรองรับการเข้าถึงจากอุปกรณ์หลากหลายประเภท

ระบบที่พัฒนานี้แสดงให้เห็นว่าระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์สามารถลดเวลาในการ ตรวจสอบปัญหาได้อย่างมีนัยสำคัญ เพิ่มความเสถียรของระบบโดยรวม และช่วยให้ผู้ดูแลระบบสามารถตัดสินใจแก้ไขปัญหาได้ อย่างรวดเร็วและถูกต้อง การมีระบบเฝ้าระวังแบบรวมศูนย์นี้จึงเป็นเครื่องมือสำคัญที่ช่วยเสริมสร้างความมั่นคงและ ประสิทธิภาพในการดำเนินงานของระบบเทคโนโลยีสารสนเทศขององค์กรในยุคดิจิทัล

## 2. บทนำ

ความก้าวหน้าของเทคโนโลยีสารสนเทศในปัจจุบันส่งผลกระทบต่อระบบการดำเนินงานขององค์กร ต่างๆ ในยุคที่เครือข่ายอินเทอร์เน็ตมีการแพร่หลายและครอบคลุมอย่างกว้างขวาง การเข้าถึงข้อมูลและบริการต้องมีความ สะดวกรวดเร็วและสามารถตอบสนองได้แบบเรียลไทม์ ปัจจัยสำคัญที่นำไปสู่ความสำเร็จขององค์กรในปัจจุบันจึงหลีกเลี่ยงไม่ได้ จากการมีโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศที่แข็งแกร่ง การเชื่อมต่อเครือข่ายที่มีความเสถียร และอุปกรณ์เครือข่ายที่มี ประสิทธิภาพสูงเพื่อรองรับผู้ใช้งานจำนวนมาก

อย่างไรก็ตาม เมื่อพิจารณาถึงสถานการณ์ที่อุปกรณ์เครือข่าย หรือแอปพลิเคชันใดแอปพลิเคชันหนึ่งเกิดการหยุด ทำงานกะทันหันเนื่องจากภาระงานที่เกินขีดจำกัด (Overload) หรือเหตุการณ์ขัดข้องอื่นๆ เหตุการณ์ดังกล่าวจะส่งผลกระทบต่อ การดำเนินงานและการให้บริการอื่นๆ ในลักษณะห่วงโซ่ อันจะนำไปสู่การสูญเสียทางธุรกิจและความเสียหายของชื่อเสียง องค์กร

ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์จะทำการรวบรวมข้อมูลต่างๆ จากอุปกรณ์ที่ต้องการ ตรวจสอบ เช่น การใช้งานหน่วยประมวลผลกลาง (CPU Utilization) การใช้งานหน่วยความจำ (Memory Usage) ปริมาณ การใช้แบนด์วิดท์ (Bandwidth Utilization) และสถานะของบริการต่างๆ จากนั้นจะนำข้อมูลที่รวบรวมได้มาทำการวิเคราะห์ และแสดงผลผ่านทางกราฟและตาราง ทำให้ผู้ดูแลระบบสามารถเห็นภาพรวมของระบบได้อย่างชัดเจนและครอบคลุม ระบบนี้จะทำการเฝ้าติดตามระบบอย่างต่อเนื่องตลอดเวลา เมื่อเกิดปัญหา เช่น อุปกรณ์เครือข่ายหยุดทำงาน เครือข่ายขัดข้อง ระบบจะทำการแจ้งเตือนไปยังผู้รับผิดชอบทันที ทำให้สามารถดำเนินการแก้ไขปัญหาได้อย่างรวดเร็วก่อนที่จะส่งผลกระทบต่อ การดำเนินงานขององค์กร ข้อมูลที่ได้จากการตรวจสอบจะช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์ประสิทธิภาพของระบบได้อย่าง ละเอียดและวางแผนปรับปรุงระบบให้มีประสิทธิภาพที่ดีขึ้น รวมถึงการตรวจสอบปัญหาและแก้ไขได้อย่างรวดเร็ว

ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์ (Centralized Network Monitoring System) เป็น ระบบตรวจสอบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศแบบโอเพนซอร์ส (Open Source IT Infrastructure Monitoring) ที่พัฒนาขึ้นเพื่อใช้สำหรับตรวจสอบและติดตามการทำงานของอุปกรณ์เครือข่ายภายในองค์กร ระบบนี้ช่วยให้ ผู้ดูแลระบบสามารถตรวจจับปัญหาที่เกิดขึ้นในระบบได้อย่างรวดเร็วและดำเนินการแก้ไขได้อย่างทันท่วงที เพื่อให้ระบบ สามารถดำเนินงานได้อย่างมีประสิทธิภาพและเสถียร

โดยสรุป ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์เป็นเครื่องมือที่มีประสิทธิภาพสูงและมีความยืดหยุ่นสำหรับการตรวจสอบระบบเทคโนโลยีสารสนเทศ ซึ่งช่วยให้ผู้ดูแลระบบสามารถติดตามและจัดการระบบได้อย่างมีประสิทธิภาพ ส่งผลให้ระบบเทคโนโลยีสารสนเทศขององค์กรสามารถดำเนินงานได้อย่างราบรื่นและมีความเสถียรสูง

### 3. วัตถุประสงค์

- 3.1 เพื่อพัฒนาระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์ ที่สามารถติดตามสถานะและประสิทธิภาพการทำงานของอุปกรณ์เครือข่ายทั้งหมดในองค์กรจากจุดเดียว
- 3.2 เพื่อเพิ่มประสิทธิภาพในการตรวจจับและแจ้งเตือนปัญหา ของอุปกรณ์เครือข่ายแบบเรียลไทม์ เพื่อลดเวลาในการแก้ไขปัญหาและป้องกันการหยุดชะงักของระบบ
- 3.3 เพื่อจัดเก็บและวิเคราะห์ข้อมูลประวัติการทำงาน ของอุปกรณ์เครือข่ายเพื่อใช้ในการวางแผนการบำรุงรักษาเชิงป้องกันและการปรับปรุงประสิทธิภาพระบบ
- 3.4 เพื่อสร้างแดชบอร์ดและรายงานที่ครอบคลุม สำหรับการติดตามและประเมินสถานะเครือข่ายโดยรวม เพื่อสนับสนุนการตัดสินใจของผู้บริหาร

### 4. วิธีการ/เครื่องมือ

วิธีการและเครื่องมือ ที่ใช้ในการพัฒนาระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์มีประสิทธิภาพสูง มีความยืดหยุ่น สามารถแบ่งเป็น 2 ส่วน ดังนี้

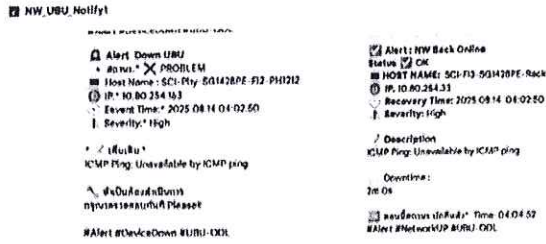
#### 4.1 เครื่องมือที่ใช้ในการพัฒนา

- 4.1.1 เครื่องคอมพิวเตอร์แม่ข่าย
- 4.1.2 OpenSource Zabbix
- 4.1.3 Ubuntu

#### 4.2 โปรแกรม และ Service ที่จำเป็นต่อการติดตั้ง

- 4.2.1 Zabbix Server สำหรับเป็นศูนย์กลางในการเก็บและประมวลผลข้อมูล
- 4.2.2 PostgreSQL สำหรับจัดเก็บข้อมูลการกำหนดค่าและข้อมูลประสิทธิภาพ
- 4.2.3 Web Frontend สำหรับส่วนติดต่อผู้ใช้งานผ่านเว็บเบราว์เซอร์
- 4.2.4 Agent สำหรับติดตั้งบนอุปกรณ์ที่ต้องการเฝ้าระวังแบบรายละเอียด
- 4.2.5 SNMP Monitoring สำหรับตรวจสอบอุปกรณ์เครือข่ายที่รองรับ SNMP Protocol
- 4.2.6 ICMP Ping Monitoring สำหรับตรวจสอบสถานะการเชื่อมต่อพื้นฐาน
- 4.2.7 แจ้งเตือนผ่าน Google Chat





รูปที่ 4 แสดงการแจ้งเตือนเมื่อระบบเครือข่ายมีปัญหา

การพัฒนาระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์ได้ดำเนินการ โดยมีการติดตั้งและกำหนดค่าระบบหลักเสร็จสมบูรณ์ รวมทั้งการเชื่อมต่อและตรวจสอบอุปกรณ์เครือข่ายต่าง ๆ ในองค์กร ระบบสามารถทำงานได้อย่างมีประสิทธิภาพและให้ข้อมูลที่แม่นยำสำหรับการติดตามสถานะเครือข่ายแบบเรียลไทม์

## 6.สรุป

ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์ด้วย Zabbix ได้รับการพัฒนาเสร็จสมบูรณ์และสามารถทำงานได้อย่างมีประสิทธิภาพ โดยสามารถเชื่อมต่อและตรวจสอบอุปกรณ์เครือข่ายทั้งหมด 207 เครื่องในองค์กร ประกอบด้วย Switch, Server พร้อมระบบแจ้งเตือนแบบเรียลไทม์และการตอบสนองเหตุการณ์

ผลการดำเนินงานแสดงให้เห็นว่าระบบสามารถลดเวลาในการแก้ไขปัญหาเครือข่ายลงอย่างมีนัยสำคัญ ระบบยังมีฟีเจอร์ครบครันตั้งแต่ Dashboard แบบ Real-time, การสร้างรายงานอัตโนมัติ, Network Mapping และการแจ้งเตือนทันที ทำให้การบริหารจัดการเครือข่ายมีประสิทธิภาพและเสถียรภาพสูงขึ้นอย่างเห็นได้ชัด

## 7. ความสามารถในการนำผลงานไปใช้ประโยชน์หรือต่อยอดเพื่อให้บุคคลหรือหน่วยงานอื่นไปใช้ประโยชน์ได้ในวงกว้าง (impact )

ระบบตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายแบบรวมศูนย์ด้วยนี้ สามารถนำไปขยายผลและประยุกต์ใช้ในหน่วยงานต่าง ๆ ได้อย่างกว้างขวาง เนื่องจากเป็นโซลูชันแบบ Open Source ที่มีความยืดหยุ่นสูงและสามารถปรับขนาดได้ตามความต้องการของแต่ละองค์กร Template และ Configuration ที่พัฒนาขึ้นสามารถนำไปใช้เป็นมาตรฐานสำหรับหน่วยงานราชการ สถาบันการศึกษา และองค์กรเอกชนที่มีความต้องการในการตรวจสอบเครือข่าย

นอกจากนี้ยังสามารถต่อยอดเป็นศูนย์กลางการตรวจสอบเครือข่ายในระดับจังหวัดหรือภูมิภาค รวมทั้งพัฒนาเป็นระบบ NOC (Network Operations Center) แบบรวมศูนย์ที่ให้บริการแก่หลายหน่วยงานพร้อมกัน ความรู้และประสบการณ์ที่ได้จากโครงการนี้ยังสามารถถ่ายทอดผ่านการฝึกอบรมและสร้างบุคลากรด้าน Network Monitoring ให้แก่หน่วยงานอื่น ๆ ได้อีกด้วย

ความเห็นจากหน่วยงาน

เห็นชอบให้ส่งผลงานเข้าร่วมโครงการ

ไม่เห็นชอบ

ลงนาม .....



(ผู้ช่วยศาสตราจารย์อติพงษ์ สุริยา)

ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย

15 ก.ย. 68