



เอกสารประกอบการรับการประเมิน
เพื่อดำรงตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
ตำแหน่งเลขที่ 4428

เรื่อง

การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและ
อุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี

Development of Host Computer and Network Device Monitoring
System for ODPC 8 Udon Thani

จัดทำโดย

นายกันตวุธ กันยานุช

กลุ่มพัฒนานวัตกรรม และวิจัย

สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี

กรมควบคุมโรค

บทคัดย่อ

การพัฒนากระบวนการตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย มีวัตถุประสงค์ในการพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย เพื่อตรวจสอบและแก้ไข การทำงานผิดปกติของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี

การศึกษากำหนดพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย เช่น การตรวจสอบสถานะของคอมพิวเตอร์แม่ข่าย เชื่อมต่อและประสิทธิภาพของเครือข่าย ระบบตรวจสอบควรสามารถระบุปัญหาหรือข้อผิดพลาดที่เกิดขึ้นได้ เพื่อให้ผู้ดูแลระบบสามารถรับรู้และแก้ไขปัญหาได้ทันเวลาที่ ระบบยังสามารถบันทึกข้อมูลเกี่ยวกับการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายเพื่อให้มีประสิทธิภาพในการวิเคราะห์และวางแผนการปรับปรุงระบบในอนาคต

ผลการศึกษาพบว่าระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย มีประโยชน์ในการบริหารจัดการระบบเครือข่ายอย่างมีประสิทธิภาพ ผู้ดูแลระบบสามารถตรวจสอบและวิเคราะห์ข้อมูลเพื่อปรับปรุงและเพิ่มประสิทธิภาพของระบบเครือข่าย นอกจากนี้ยังช่วยให้มีการดูแลระบบอย่างต่อเนื่องและป้องกันปัญหาที่อาจเกิดขึ้นก่อนที่จะส่งผลกระทบต่อผู้ใช้งาน ในหน่วยงาน โดยระบบนี้สามารถตรวจสอบและตรวจจับปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว และเป็นสิ่งสำคัญที่ช่วยให้ผู้ดูแลระบบสามารถรับทราบสถานะการทำงานของคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายได้อย่างสะดวกและรวดเร็ว ซึ่งเป็นการสนับสนุนในการดูแลรักษาความเสถียรภาพของระบบเครือข่ายอย่างมีประสิทธิภาพ

ข้อเสนอแนะการพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายควรให้ความสำคัญกับความต้องการและความเหมาะสมของระบบ การเก็บรวบรวมข้อมูลที่สมบูรณ์และแม่นยำ การแจ้งเตือนและการแก้ไขปัญหาอัตโนมัติ การวางแผนและการบำรุงรักษา ระบบ และกระบวนการทดสอบและประเมินผลเพื่อปรับปรุงระบบตรวจสอบให้มีประสิทธิภาพสูงสุด ในการดูแลและปรับปรุงระบบเครือข่ายในหน่วยงานที่สามารถพิจารณาได้ดังนี้

1. การเลือกใช้เครื่องมือและเทคโนโลยีที่เหมาะสม ควรเลือกใช้เครื่องมือและเทคโนโลยีที่มีความเหมาะสมกับความต้องการของระบบตรวจสอบ เช่น การใช้โปรแกรมตรวจสอบระบบที่มีฟีเจอร์ที่ตรวจจับปัญหาได้ครอบคลุมและมีการแจ้งเตือนที่ชัดเจน
2. ระบบตรวจสอบควรสามารถเก็บรวบรวมข้อมูลที่สมบูรณ์และครอบคลุมเกี่ยวกับการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ซึ่งอาจรวมถึงข้อมูลเชิงลึกเกี่ยวกับประสิทธิภาพการใช้งานทรัพยากร และปัญหาที่เกิดขึ้น

3. ระบบตรวจสอบควรมีความสามารถในการแจ้งเตือนผู้ดูแลระบบเมื่อเกิดปัญหาหรือข้อผิดพลาด เช่น การส่งอีเมลหรือข้อความแจ้งเตือน และสามารถดำเนินการแก้ไขปัญหาอัตโนมัติหรือนำเสนอวิธีการแก้ไข
4. ควรกำหนดตารางการตรวจสอบและบำรุงรักษาระบบเครือข่ายเพื่อให้มั่นใจได้ว่าระบบจะทำงานอย่างเสถียรและประสิทธิภาพ ซึ่งการตรวจสอบและอัปเดตซอฟต์แวร์ การตรวจสอบฮาร์ดแวร์ และการดำเนินการป้องกันการโจมตี
5. ควรมีกระบวนการทดสอบและประเมินผลเพื่อตรวจสอบประสิทธิภาพของระบบตรวจสอบ นอกจากนี้ยังควรรับข้อเสนอแนะจากผู้ใช้งาน และผู้ดูแลระบบเพื่อปรับปรุงระบบตรวจสอบให้มีประสิทธิภาพและครอบคลุมขึ้น

คำสำคัญ : ระบบตรวจสอบเครือข่าย, ระบบเครือข่าย, คอมพิวเตอร์แม่ข่าย, อุปกรณ์เครือข่าย, การบริหารจัดการเครือข่าย

กิตติกรรมประกาศ

รายงานการศึกษาการพัฒนากระบวนการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ซึ่งมีวัตถุประสงค์ เพื่อหน่วยงานมีระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย โดยมุ่งหวัง เพื่อสร้างเครื่องมือช่วยเหลือและอำนวยความสะดวกให้แก่ผู้ดูแลระบบสารสนเทศของหน่วยงานทราบ อย่างทันเวลา เมื่อมีความผิดปกติที่เกิดขึ้นกับอุปกรณ์ ในระบบเครือข่าย และสามารถบริหารจัดการ ระบบเครือข่ายด้วยความชำนาญมาก นอกจากนี้การตรวจสอบคอมพิวเตอร์แม่ข่าย และอุปกรณ์ เครือข่าย ยังช่วยเพิ่มความปลอดภัยให้กับระบบเครือข่าย และเพิ่มประสิทธิภาพในการทำงาน ของระบบเครือข่ายด้วย

การดำเนินงานครั้งนี้สำเร็จลุล่วงด้วยดีด้วยความร่วมมือจาก ผู้เชี่ยวชาญ ผู้ที่เกี่ยวข้องทุกท่าน ที่คอยให้การสนับสนุนการดำเนินการ ให้การสนับสนุนการศึกษาค้นคว้า ชี้แนะแนวทาง ให้ความรู้ ให้คำปรึกษา และข้อเสนอแนะต่าง ๆ ที่เป็นประโยชน์แก่ผู้ศึกษาจนสามารถนำมาพัฒนาระบบ ให้บรรลุตามวัตถุประสงค์สำเร็จลุล่วงไปได้ด้วยดี

นายกันตวุธ กัญยานุช

สารบัญ

	หน้า
บทคัดย่อ	ก
กิตติกรรมประกาศ	ค
สารบัญ	ง
สารบัญภาพ	ฉ
บทที่ 1 บทนำ	
ความเป็นมาและความสำคัญของปัญหา	1
คำถามวิจัย	2
วัตถุประสงค์การวิจัย	3
ขอบเขตการวิจัย	3
ประโยชน์ที่คาดว่าจะได้รับ	3
นิยามศัพท์เฉพาะ	3
บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง	
แนวคิดและทฤษฎีที่เกี่ยวข้องกับการพัฒนาระบบ	5
เครื่องมือที่ใช้ในการพัฒนาระบบ	13
งานวิจัยที่เกี่ยวข้อง	19
กรอบแนวคิด	25
บทที่ 3 วิธีการดำเนินการวิจัย	
รูปแบบการศึกษา	26
เครื่องมือที่ใช้ในการดำเนินการ	26
เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล	27
วิธีการสร้างเครื่องมือการวิจัย	27
ขั้นตอนการวิจัย	27
รายละเอียดการดำเนินงาน	31
บทที่ 4 ผลการศึกษา	
การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย	
และอุปกรณ์เครือข่าย ฯ	52
ผลจากการใช้งานระบบระบบพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์	56

บทที่ 5 สรุปผลการศึกษา อภิปรายผลและข้อเสนอแนะ	
สรุปผลการดำเนินการ	57
อภิปรายผลการศึกษา	58
ข้อเสนอแนะ	59
บรรณานุกรม	60
ภาคผนวก	62

สารบัญภาพ

	หน้า
ภาพที่ 1 การทำงานของโพรโทคอลเอสเอ็นเอ็มพี SNMP	8
ภาพที่ 2 การทำงานรับส่งข้อมูลของโพรโทคอล SNMP	9
ภาพที่ 3 ภาพแสดงองค์ประกอบของ Packet ภายใน PDU	10
ภาพที่ 4 แสดงรูปแบบของ Protocol UDP Connection	12
ภาพที่ 5 ภาพแสดงการเปรียบเทียบการพัฒนาเวอร์ชัน CentOS	14
ภาพที่ 6 ภาพแสดงเวอร์ชัน ของระบบปฏิบัติการ CentOS	14
ภาพที่ 7 ภาพแสดงโลโก้ของอะปาเช่เว็บเซิร์ฟเวอร์ (Apache Web Server)	15
ภาพที่ 8 ภาพแสดงโลโก้ของฐานข้อมูลมาเรียดีบี (MariaDB)	16
ภาพที่ 9 ภาพแสดง Login โปรแกรม Zabbix Monitoring System	17
ภาพที่ 10 ภาพรวมของโปรแกรม Zabbix Monitoring System	17
ภาพที่ 11 ภาพแสดงโลโก้ของ LINE Application	18
ภาพที่ 12 ภาพบริการรับการแจ้งเตือนจากเว็บเซอร์วิสทาง LINE Application	18
ภาพที่ 13 ภาพรวมการตรวจสอบการทำงานของระบบเดิม	30
ภาพที่ 14 ภาพรวมการทำงานของระบบ Zabbix Network Monitor	30
ภาพที่ 15 แสดงหน้าภาพรวมของระบบ Zabbix Network Monitoring	31
ภาพที่ 16 การติดตั้ง Zabbix Agent สำหรับคอมพิวเตอร์แม่ข่ายระบบปฏิบัติการ Windows	33
ภาพที่ 17 แสดงสถานะการทำงานของ Zabbix Agent	33
ภาพที่ 18 การกำหนดค่า Windows Firewall ในเครื่องคอมพิวเตอร์แม่ข่าย	34
ภาพที่ 19 การอนุญาต Zabbix Agent เชื่อมต่อกับ Zabbix Server	34
ภาพที่ 20 การทดสอบการเชื่อมต่อระหว่าง Zabbix Sever กับ Zabbix Agent	35
ภาพที่ 21 การทดสอบการเชื่อมต่อระหว่าง Zabbix Sever กับ Zabbix Agent	35
ภาพที่ 22 การตั้งค่าติดตั้ง Zabbix Agent สำหรับคอมพิวเตอร์แม่ข่ายที่ใช้ ระบบปฏิบัติการ Linux	36
ภาพที่ 23 การกำหนดค่า Windows Firewall อนุญาตให้ Zabbix Agent	36
ภาพที่ 24 การตั้งค่าไฟล์ zabbix_agentd.conf เพื่อเชื่อมต่อ Zabbix Server	36
ภาพที่ 25 การทดสอบการเชื่อมต่อระหว่าง Zabbix Sever กับ Zabbix Agent	37

ภาพที่ 26 การตั้งค่าโปรโตคอล SNMP สำหรับอุปกรณ์เครือข่าย	37
ภาพที่ 27 การทดสอบการเชื่อมต่อโปรโตคอล SNMP	37
ภาพที่ 28 หน้าล็อกอินเข้าโปรแกรม Zabbix Network Monitoring	38
ภาพที่ 29 แสดงกลุ่มโฮสทั้งหมด	38
ภาพที่ 30 การเพิ่มกลุ่มโฮสสำหรับการมอนิเตอร์	39
ภาพที่ 31 การเพิ่มโฮสสำหรับการมอนิเตอร์ในระบบ Zabbix Network Monitoring	39
ภาพที่ 32 การเพิ่มค่า SNMP Community สำหรับการตรวจสอบผ่านโปรโตคอล SNMP	40
ภาพที่ 33 แสดงโฮสที่เพิ่มเข้าในระบบ Zabbix Network Monitoring ทั้งหมด	40
ภาพที่ 34 การแจ้งเตือนความผิดปกติผ่านหน้า Dashboard Zabbix Network Monitoring	41
ภาพที่ 35 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Problems ในโปรแกรม Zabbix Network Monitoring	41
ภาพที่ 36 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Host ในโปรแกรม Zabbix Network Monitoring	42
ภาพที่ 37 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Map ในโปรแกรม Zabbix Network Monitoring	42
ภาพที่ 38 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Latest data เพื่อดูข้อมูลล่าสุด ในโปรแกรม Zabbix Network Monitoring	43
ภาพที่ 39 เข้าล็อกอินเข้าเว็บไซต์ LINE Application	43
ภาพที่ 40 เข้าหน้าเว็บสำหรับการออก LINE Token	44
ภาพที่ 41 ทำการ Generate access token	44
ภาพที่ 42 ตั้งชื่อสำหรับการแจ้งเตือน และเลือกกลุ่มหรือบุคคลที่ต้องการแจ้งเตือน	44
ภาพที่ 43 ภาพแสดง Token key สำหรับการแจ้งเตือน	45
ภาพที่ 44 ภาพแสดงการเชื่อมต่อการให้บริการ LINE Notify	45
ภาพที่ 45 หน้าแสดง Media types ทั้งหมดในระบบ	46
ภาพที่ 46 การสร้างไฟล์ LINE Notify สำหรับการเขียนคำสั่งในการแจ้งเตือน เขียนคำสั่งในไฟล์ LINE Notify	46
ภาพที่ 47 คำสั่งในการแจ้งเตือนไฟล์ LINE Notify	46
ภาพที่ 48 การทดสอบการแจ้งเตือนโดยการส่งข้อความที่กำหนดไปยัง LINE Notify	47
ภาพที่ 49 ข้อความที่ทดสอบแสดงการแจ้งเตือน LINE Notify	47

ภาพที่ 50 ข้อความที่ทดสอบแสดงการแจ้งเตือน LINE Notify	48
ภาพที่ 51 แสดง Media types การแจ้งเตือนที่ทำการเพิ่มเข้าในระบบ	48
ภาพที่ 52 ทดสอบการแจ้งเตือนของ Media types	48
ภาพที่ 53 การเพิ่ม Users สำหรับการแจ้งเตือน	49
ภาพที่ 54 การเพิ่ม Media สำหรับการแจ้งเตือน Users	49
ภาพที่ 55 การเพิ่ม Media กำหนดเวลา และเงื่อนไขการส่งข้อความแจ้งเตือนไปยัง Users	50
ภาพที่ 56 เป็นการแสดงรายละเอียดในการตั้งค่า Action ในหัวข้อ Action Users	50
ภาพที่ 57 เป็นการแสดงรายละเอียดในการตั้งค่า Action	51
ภาพที่ 58 เป็นการแสดง Trigger Action ที่สร้างขึ้น	51
ภาพที่ 59 หน้าแสดงหน้ารวมของระบบ Zabbix Network Monitoring	53
ภาพที่ 60 กราฟแสดงข้อมูล Traffic การใช้อินเทอร์เน็ตของหน่วยงาน	53
ภาพที่ 61 การตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย	54
ภาพที่ 62 แสดงการแจ้งเตือนของ Trigger เมื่อเกิดปัญหา	54
ภาพที่ 63 แสดงการแจ้งเตือนผ่าน LINE เมื่อเกิดปัญหา	55

บทที่ 1

บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี เป็นหน่วยงานที่ดำเนินงานด้านการป้องกันควบคุมโรคและภัยสุขภาพ ในพื้นที่เขตสุขภาพที่ 8 จำเป็นต้องมีระบบเทคโนโลยีสารสนเทศที่ทันสมัยเพื่อช่วยในการดำเนินงานเฝ้าระวังป้องกันควบคุมโรคและภัยสุขภาพให้รวดเร็ว และทันต่อสถานการณ์ ที่เปลี่ยนแปลงอย่างรวดเร็ว ทำให้มีปริมาณข้อมูลที่ต้องมีการจัดเก็บ และประมวลผลเพิ่มมากขึ้น ได้แก่ ฐานข้อมูลเว็บไซต์ สคร.8 อุดรธานี, ฐานข้อมูลระบบควบคุมติดตามงบประมาณ, ฐานข้อมูลระบบฐานข้อมูลโควิด - 19 สคร.8, ฐานข้อมูลระบบเงินเดือนพนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างโครงการ, ฐานข้อมูลระบบเงินเดือนข้าราชการ ลูกจ้างประจำ, ฐานข้อมูลระบบบริหารงานบุคคล (งานการเจ้าหน้าที่), ฐานข้อมูลระบบจองรถราชการออนไลน์, ระบบจองห้องประชุมการออนไลน์, ฐานข้อมูลระบบอนุมัติไปราชการออนไลน์, ฐานข้อมูลระบบจัดการไฟล์เอกสารการจัดประชุมออนไลน์, ฐานข้อมูลระบบรายงานการประชุมอบรมออนไลน์, ฐานข้อมูลระบบควบคุมโรคพยาธิใบไม้ตับด้วยระบบ GIS, ฐานข้อมูลระบบคัดกรองโควิด - 19 ด้านควบคุมโรค, ฐานข้อมูลระบบบริหารงานบุคคล (พัฒนาองค์กร), ฐานข้อมูลระบบการขอเบิก/ขอคืนพัสดุการลงสอบสวนโรคฯ, ฐานข้อมูลระบบการขอเอกสารรับรอง Vaccine Passport จึงมีการนำเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย (Network System) เข้ามาช่วยในการรองรับข้อมูลที่เกิดขึ้น ซึ่งฐานข้อมูลของสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ที่มีการดำเนินงานบนคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย (Network Devices)

ระบบเครือข่าย (Network System) คือ การเชื่อมต่อระบบคอมพิวเตอร์หลาย ๆ เครื่องเข้าด้วยกันโดยใช้สื่อสารทางเครือข่าย เช่น สาย LAN, สายแสดงผล, และเครือข่ายไร้สาย (Wireless Network) เพื่อให้สามารถแลกเปลี่ยนข้อมูล แชนร์ทรัพยากร และใช้งานโปรแกรม และแอปพลิเคชันต่าง ๆ ร่วมกันได้ ซึ่งระบบเครือข่ายสามารถแบ่งออกเป็นหลายชนิด เช่น Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN) ฯลฯ ส่วนคอมพิวเตอร์แม่ข่าย (Network Computer) คือ คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายและได้รับบริการจากคอมพิวเตอร์แม่ข่าย เพื่อใช้งานและเข้าถึงทรัพยากรในเครือข่ายต่าง ๆ

เช่น สามารถเข้าถึงเครื่องพิมพ์ร่วมกัน แชนร์ไฟล์ และโปรแกรมต่างๆ ซึ่งคอมพิวเตอร์แม่ข่ายทำหน้าที่เป็นตัวกลางในการจัดการ และควบคุมการเชื่อมต่อเครือข่ายให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ

จากดำเนินงานและเก็บรวบรวมข้อมูลในบทบาทนักวิชาการคอมพิวเตอร์ของหน่วยงานพบว่าในช่วงที่ผ่านมาเมื่อเกิดเหตุการณ์ความผิดปกติของระบบการทำงานด้านคอมพิวเตอร์และสารสนเทศไม่สามารถรับทราบปัญหาได้ทันที ต้องรอให้บุคลากรของหน่วยงานแจ้งการพบปัญหา ซึ่งการเกิดปัญหาดังกล่าวเกิดจากการที่หน่วยงานไม่มีเครื่องมือ ระบบ หรือซอฟต์แวร์ที่คอยตรวจสอบสภาพการทำงานของอุปกรณ์เครือข่าย ให้มีความเสถียร ปลอดภัย ก็จะไม่สามารถทราบถึงปัญหา และจุดที่ทำให้เกิดปัญหา ทำให้ไม่สามารถแก้ไขปัญหาดังกล่าวได้อย่างรวดเร็ว ทำให้เมื่อเกิดปัญหา ข้อผิดพลาด หรืออุปกรณ์ทำงานผิดปกติ ผู้ดูแลระบบ จะไม่สามารถทราบถึงปัญหาที่เกิดขึ้นจนกว่าระบบ และอุปกรณ์ใช้งานไม่ได้ หรือผู้ใช้งานแจ้งมาที่ผู้ดูแลระบบ จึงจะทราบถึงปัญหาที่เกิดขึ้นทำให้การทำงานในหน่วยงานเกิดการชะงัก ฉะนั้นการดำเนินการตรวจสอบสถานการณ์ทำงานต่าง ๆ ของคอมพิวเตอร์แม่ข่าย และอุปกรณ์ข่าย เป็นเครื่องมือที่สำคัญสำหรับติดตามและเฝ้าระวังระบบเครือข่าย ไม่ใช่เพียงแค่เอา Log มาจัดเก็บบันทึกและแสดงผลข้อมูลให้ผู้ดูแลระบบ แต่ยังสามารถช่วยวิเคราะห์ข้อมูลเหล่านั้นให้ผู้ดูแลระบบสามารถเข้าใจได้ง่ายขึ้น รวมไปถึงแจ้งเตือนพฤติกรรมการใช้งานที่ผิดปกติที่อาจส่งผลกระทบต่อการทำงานของบริการของหน่วยงาน

ดังนั้น เพื่อเป็นการเพิ่มประสิทธิภาพให้กับผู้ดูแลระบบของสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ในการตรวจสอบอุปกรณ์เครือข่ายและคอมพิวเตอร์แม่ข่าย เพื่อตรวจสอบและวิเคราะห์ระบบเครือข่ายและคอมพิวเตอร์แม่ข่าย ตรวจสอบปัญหาและความผิดปกติที่อาจเกิดขึ้น และหาวิธีแก้ไขปัญหานั้น การตรวจสอบระบบเครือข่ายและคอมพิวเตอร์แม่ข่ายช่วยให้ผู้ดูแลระบบสามารถตรวจสอบสถานะของระบบได้ เช่น สถานะของระบบเครือข่าย ประสิทธิภาพการทำงาน ประเภทของข้อผิดพลาด เป็นต้น นอกจากนี้การตรวจสอบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายยังช่วยเพิ่มความปลอดภัย และเพิ่มประสิทธิภาพในการทำงานของระบบเครือข่ายด้วย

2. คำถามวิจัย

ระบบการตรวจสอบอุปกรณ์เครือข่ายและคอมพิวเตอร์แม่ข่าย ในกรณีที่เกิดความผิดปกติที่เหมาะสมเป็นอย่างไร

3. วัตถุประสงค์การวิจัย

1. เพื่อพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี
2. เพื่อให้ผู้ดูแลระบบทราบอย่างทันเวลา เมื่อมีการทำงานผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี

4. ขอบเขตการวิจัย

4.1 ขอบเขตด้านเนื้อหา

1. คอมพิวเตอร์แม่ข่าย (Computer Server) ภายในสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี
2. ระบบเครือข่ายคอมพิวเตอร์ (Network System) ภายในสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี
3. ระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ผ่านโปรแกรม Network Monitoring System

4.2 ขอบเขตด้านเวลา

ในการศึกษาครั้งนี้ผู้ศึกษา วางแผนการดำเนินงานระยะเวลา 1 ปี ระหว่างวันที่ 1 ตุลาคม 2564 - 30 กันยายน 2565

5. ประโยชน์ที่คาดว่าจะได้รับ

1. หน่วยงานมีระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ที่มีประสิทธิภาพ
2. ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบและแก้ไขปัญหาที่เกิดขึ้นในเครือข่ายได้ทันที
3. ช่วยให้คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ทำงานได้อย่างมีประสิทธิภาพ

6. นิยามศัพท์เฉพาะ

1. ระบบเครือข่าย หมายถึง อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อถึงกันซึ่งสามารถแลกเปลี่ยนข้อมูลและแบ่งปันทรัพยากรระหว่างกันได้

2. คอมพิวเตอร์แม่ข่าย หมายถึง คอมพิวเตอร์เซิร์ฟเวอร์ (Computer Server) หรือเครื่องบริการ คือ เครื่องหรือโปรแกรมคอมพิวเตอร์ ซึ่งทำงานให้บริการ ในระบบเครือข่ายแก่ลูกข่าย

3. อุปกรณ์เครือข่าย หมายถึง อุปกรณ์ที่นำมาใช้ในเครือข่ายทำหน้าที่จัดการเกี่ยวกับการรับ การส่งข้อมูลในเครือข่าย หรือใช้สำหรับทวนสัญญาณเพื่อให้การรับ-ส่งข้อมูลได้ดี และส่งในระยะ ที่ไกลมากขึ้น หรือใช้สำหรับขยายเครือข่ายให้มีขนาดใหญ่ขึ้น อุปกรณ์เครือข่ายที่พบเห็นโดยทั่วไป เช่น ฮับ สวิตช์ เราท์เตอร์

4. โพรโทคอล หมายถึง ข้อกำหนดหรือข้อตกลงในการสื่อสารระหว่างคอมพิวเตอร์ หรือ ภาษาสื่อสารที่ใช้เป็นภาษา กลางในการสื่อสารระหว่างคอมพิวเตอร์ด้วยกัน การที่เครื่องคอมพิวเตอร์ ที่ถูกเชื่อมโยงกันไว้ในระบบจะสามารถติดต่อสื่อสารกันได้นั้น จำเป็นจะต้องมีการสื่อสารที่เรียกว่า โพรโทคอล (Protocol) เช่นเดียวกับคนเราที่ต้องมีภาษาพูดเพื่อให้สื่อสารเข้าใจกันได้ โพรโทคอลช่วยให้ระบบคอมพิวเตอร์สองระบบ ที่แตกต่างกันสามารถสื่อสารกันอย่างเข้าใจได้

5. มอนิเตอร์ หมายถึง การเก็บรวบรวมข้อมูลที่แสดงให้เห็นว่า ได้มีการดำเนินการใน ขั้นตอนต่างๆ ของโครงการที่กำหนดได้อย่างไร ข้อมูลที่ได้จะนำมาประกอบเป็นเครื่องมือ ควบคุม กำกับ การดำเนินงานในขณะที่ปฏิบัติโครงการโดยตรง ทั้งในด้านปัจจัย (Input) ด้านกระบวนการดำเนินงาน (Process) และ ด้านผลผลิต (Output)

6. ระบบปฏิบัติการ หมายถึง เป็นระบบซอฟต์แวร์ที่ทำหน้าที่จัดการอุปกรณ์คอมพิวเตอร์ และแหล่งซอฟต์แวร์และบริการโปรแกรมคอมพิวเตอร์

7. ผู้ดูแลระบบ หมายถึง บุคคลที่สามารถทำการเปลี่ยนแปลงบนคอมพิวเตอร์ที่จะส่งผลกระทบต่อผู้ใช้คอมพิวเตอร์อื่น ๆ ผู้ดูแลระบบสามารถเปลี่ยนการตั้งค่าความปลอดภัย ติดตั้งซอฟต์แวร์และฮาร์ดแวร์ เข้าถึงไฟล์ทั้งหมดบนคอมพิวเตอร์ และเปลี่ยนแปลงบัญชีผู้ใช้อื่น ๆ

8. เว็บเบราว์เซอร์ (Web browser) หมายถึง โปรแกรมคอมพิวเตอร์ที่ใช้ในการท่องเว็บ และมีการจัดเก็บข้อมูลสารสนเทศต่างๆ ด้วยภาษาเฉพาะ เช่น ภาษา HTML ซึ่งก็เปรียบเสมือนกับเป็นเครื่องมือที่ใช้ในการติดต่อกับเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่ เรียกว่า เวิลด์ ไวด์ เว็บ

9. ODPC8 หมายถึง สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี (The Office of Disease Prevention and Control 8 Udon Thani)

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการพัฒนาระบบระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ผู้พัฒนาได้ศึกษาแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องเพื่อเป็นแนวทางในการพัฒนาระบบ โดยมีสาระสำคัญในหัวข้อ ดังต่อไปนี้

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับการพัฒนาระบบ
2. เครื่องมือที่ใช้ในการพัฒนาระบบ
3. งานวิจัยที่เกี่ยวข้อง
4. กรอบแนวคิด

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับการพัฒนาระบบ

1.1 การบริหารจัดการระบบเครือข่าย (Network Management System : NMS)

การบริหารจัดการระบบเครือข่าย (Network Management System) เป็นกระบวนการหรือระบบที่ใช้ในการควบคุมและดูแลระบบเครือข่ายคอมพิวเตอร์ มีหน้าที่ในการจัดการ และควบคุมระบบเครือข่ายให้ทำงานอย่างมีประสิทธิภาพ รวดเร็ว และปลอดภัย โดยรวมไปถึงการดูแลและวิเคราะห์ปัญหาที่อาจเกิดขึ้นในระบบเครือข่ายนั้นด้วย เพื่อให้ระบบเครือข่ายสามารถทำงานได้ตลอดเวลา และให้บริการได้อย่างต่อเนื่อง

ระบบ Network Management System ทำหน้าที่เฝ้าระวังควบคุมระบบเครือข่ายภายในหน่วยงาน หากมีส่วนหนึ่งส่วนใดของระบบเครือข่ายทำงานผิดพลาด หรือเกิดข้อขัดข้อง ระบบจะมีการแจ้งเตือนทำให้ผู้ดูแลระบบทราบได้ทันที และเข้าไปทำการแก้ไขได้รวดเร็ว หน้าที่หลักของระบบคือการตรวจสอบเครือข่ายตลอดเวลา ทำรายงานสถิติการใช้เครือข่าย เช่น สถิติของปริมาณข้อมูลปริมาณ ผู้ใช้ สามารถเขียนเป็นกราฟ เพื่อให้ผู้ดูแลระบบนำไปวิเคราะห์ และวางแผนขยายเครือข่าย ผู้ดูแลระบบยังสามารถตรวจสอบระบบจากซอฟต์แวร์ได้ ปัจจุบันระบบเครือข่ายที่มีอยู่มีความซับซ้อนมากขึ้น ระบบ Network Management System จึงมีส่วนสำคัญในการบริหารและจัดการอย่างมาก

1.2 ระบบบริหารจัดการระบบเครือข่าย (Network Management System)

ประกอบด้วยส่วนสำคัญต่อไปนี้

1. การตรวจสอบ (Monitoring) ระบบเครือข่ายเพื่อรับข้อมูลเกี่ยวกับสถานะและประสิทธิภาพของอุปกรณ์และการสื่อสารในเครือข่าย เช่น ความเร็วของการส่งข้อมูล (Bandwidth) การใช้งานทรัพยากรเครือข่าย และข้อมูลเกี่ยวกับการเชื่อมต่อ (Connectivity) โดยทั่วไปใช้โปรแกรมตรวจสอบ (Monitoring tools) หรือตรวจสอบระบบ (Monitoring agents) เพื่อเก็บข้อมูลนี้ และแสดงผลในรูปแบบกราฟหรือรายงาน
2. การวิเคราะห์ (Analysis) ข้อมูลที่ระบบตรวจสอบได้เพื่อตรวจสอบปัญหาและแยกแยะข้อมูลเพื่อทำให้เกิดความเข้าใจในสถานะและประสิทธิภาพของระบบเครือข่ายมากขึ้น การวิเคราะห์นี้ช่วยในการตรวจสอบข้อกำหนดและคุณภาพของบริการ (Quality of Service, QoS) และการระบุปัญหาที่อาจเกิดขึ้น
3. การจัดการ (Management) เป็นการบริหารจัดการระบบเครือข่ายรวมถึงการควบคุมและแก้ไขปัญหาที่พบเจอ การจัดการรวมถึงการปรับปรุง และปรับแต่งการใช้งานทรัพยากรเครือข่าย เช่น การกำหนดความเร็วแบนด์วิดท์ หรือการจัดกลุ่มการเชื่อมต่อที่สำคัญ
4. การตรวจสอบความปลอดภัย (Security Monitoring) ของระบบเครือข่าย เพื่อตรวจสอบและป้องกันการแฮ็กหรือการเข้าถึงที่ไม่ถูกต้องในระบบเครือข่าย
5. การบันทึกเหตุการณ์ (Logging) ที่เกิดขึ้นในระบบเครือข่ายเพื่อให้ข้อมูลเพิ่มเติมในการวิเคราะห์และการสืบค้นปัญหาในระบบ
6. การจัดการการเปลี่ยนแปลง (Change Management) เป็นการจัดการการเปลี่ยนแปลงในระบบเครือข่าย เช่น การปรับปรุงเวอร์ชันของซอฟต์แวร์, การเพิ่มเครื่องแม่ข่ายใหม่, หรือการเปลี่ยนแปลงการกำหนดค่าการใช้งานทรัพยากรเครือข่าย

การบริหารจัดการระบบเครือข่าย (Network Management System) ช่วยให้หน่วยงานสามารถดูแล และควบคุมระบบเครือข่ายอย่างมีประสิทธิภาพและปลอดภัย และช่วยในการรักษาการทำงานของระบบเครือข่ายในระยะยาวๆ เพื่อให้สามารถให้บริการที่มีประสิทธิภาพได้ตลอดเวลา

1.3 ระบบเครือข่ายคอมพิวเตอร์ (Network System)

ระบบเครือข่ายคอมพิวเตอร์ (Computer Network System) คือระบบเครือข่ายที่มีการเชื่อมต่อระหว่างอุปกรณ์สื่อสารต่างๆ หรือคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป ซึ่งการเชื่อมต่อทั้งอุปกรณ์สื่อสารทั้งหมดและทำให้คอมพิวเตอร์ และอุปกรณ์เหล่านั้นสามารถสื่อสารและรับ-ส่งข้อมูลกันได้ โดยข้อมูลต่าง ๆ เหล่านั้นเป็นได้ทั้งข้อความ เสียง รูปภาพ ซึ่งรูปแบบการเชื่อมต่อของเน็ตเวิร์ก (Network) สามารถแบ่งออกหลักๆ ได้ดังนี้

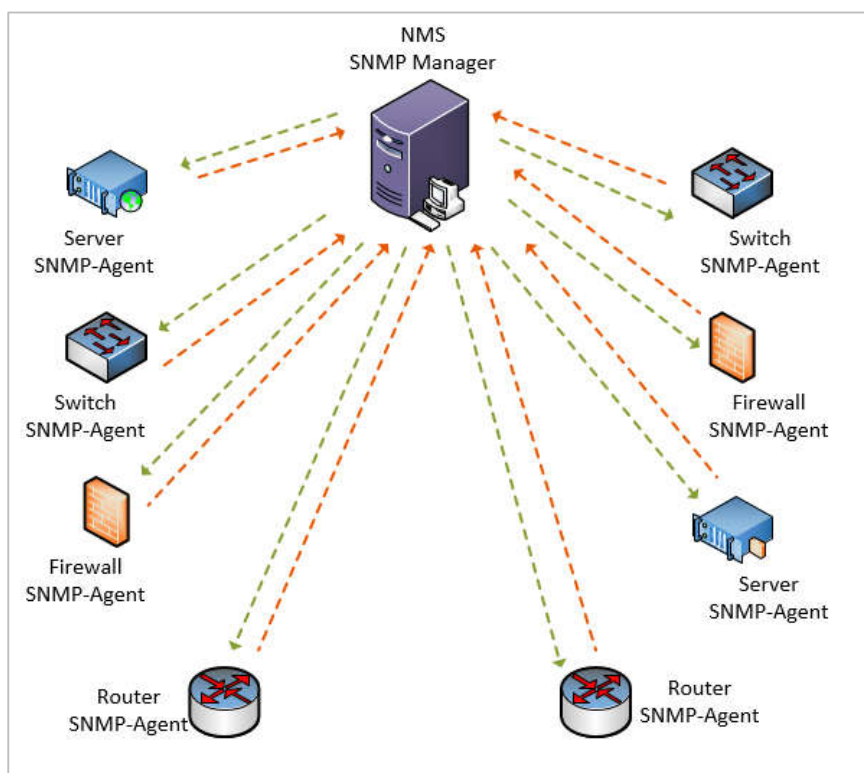
- PAN (Personal Area Network) เป็นระบบเครือข่ายส่วนบุคคลที่ใช้ในระยะใกล้ เช่น การเชื่อมต่ออุปกรณ์มือถือหรือบลูทูธ (Bluetooth)
- LAN (Local Area Network) เป็นระบบเครือข่ายที่ใช้ในพื้นที่จำกัด เช่น ในออฟฟิศ หรือบ้าน ที่คอมพิวเตอร์และอุปกรณ์เชื่อมต่อกันในพื้นที่เล็ก ๆ ด้วยสาย LAN
- WAN (Wide Area Network) เป็นระบบเครือข่ายที่ขยายพื้นที่การเชื่อมต่อไปยังพื้นที่กว้างมาก เช่น การเชื่อมต่อระหว่างเมือง
- WLAN (Wireless Local Area Network) ระบบเครือข่ายไร้สายที่ใช้เทคโนโลยีการสื่อสารไร้สาย เช่น Wi-Fi
- MAN (Metropolitan Area Network) เป็นระบบเครือข่ายที่ขยายเขตพื้นที่ระหว่าง LAN และ WAN ใช้ในเมือง หรือพื้นที่ใหญ่

ระบบเครือข่ายคอมพิวเตอร์มีหลายส่วนประกอบ เช่น อุปกรณ์เครือข่าย (Network Devices) เช่น เราเตอร์ (Router), สวิตช์ (Switch), ฮับ (Hub), และแอคเซสพอยต์ (Access Point) รวมถึงโพรโทคอลและมาตรฐานที่ใช้ในการสื่อสารระหว่างอุปกรณ์ เช่น TCP/IP (Transmission Control Protocol/Internet Protocol) และการจัดการเครือข่าย (Network Management) เพื่อควบคุมและดูแลระบบเครือข่ายให้ทำงานอย่างมีประสิทธิภาพ

1.4 โพรโทคอลเอสเอ็นเอ็มพี (Simple Network Management Protocol : SNMP)

ระบบบริหารจัดการเครือข่ายเป็นซอฟต์แวร์ที่ทำหน้าที่คอยตรวจสอบระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายเช่น Switch, Router หรืออุปกรณ์อื่นๆ ในเครือข่ายที่ระบบ Network Management System สามารถติดต่อสื่อสารได้ ด้วยโพรโทคอล SNMP (Simple Network Management Protocol) ซึ่งโพรโทคอล SNMP จะมีติดตั้งอยู่บนระบบคอมพิวเตอร์ และอุปกรณ์เครือข่าย เป็นโพรโทคอลที่อยู่ระดับบนในชั้นการประยุกต์และเป็นส่วนหนึ่งของชุดโพรโทคอล

TCP/IP ในการบริการและจัดการเครือข่ายต้องใช้อุปกรณ์ต่าง ๆ มีส่วนของการทำงานร่วมกับระบบจัดการเครือข่าย ซึ่งเราเรียกว่า เอเจนต์ (Agent) เอเจนต์เป็นส่วนของซอฟต์แวร์ที่อยู่ในอุปกรณ์ ที่เชื่อมอยู่ในเครือข่ายโดยมีคอมพิวเตอร์หลักในระบบหนึ่งเครื่องเป็นตัวจัดการและบริหารเครือข่าย หรือเรียกว่า Network Management System : NMS



ภาพที่ 1 การทำงานของโพรโทคอลเอสเอ็นเอ็มพี SNMP

SNMP เป็นคำย่อมาจาก Simple Network Management Protocol เป็นโพรโทคอลมาตรฐานที่ใช้รวบรวมจัดเรียงข้อมูลเกี่ยวกับอุปกรณ์เครือข่าย เมื่อมีการเปลี่ยนแปลงข้อมูลไปจากเดิมโดยผ่าน IP Address ของอุปกรณ์ เช่น Router, Modem, Switch, Server, Workstations, Printer เป็นต้น SNMP มีการใช้งานกันอย่างแพร่หลายสำหรับทำ Network Management หรือระบบการ Monitoring โดยโพรโทคอล SNMP จะเก็บข้อมูลในรูปแบบตัวแปร และจัดการด้วย Management Information Base (MIB) ซึ่งเป็นที่เก็บข้อมูลหรือ Database สำหรับการจัดการหรือเปลี่ยนแปลงค่าต่างๆบนอุปกรณ์ใน Network ปัจจุบัน SNMP ได้มีการพัฒนาเพื่อเพิ่ม

ขีดความสามารถ และความยืดหยุ่นในการใช้งานรวมถึงระบบ security แบ่งออกได้เป็น 3 เวอร์ชัน คือ SNMPv1, SNMPv2, SNMPv3

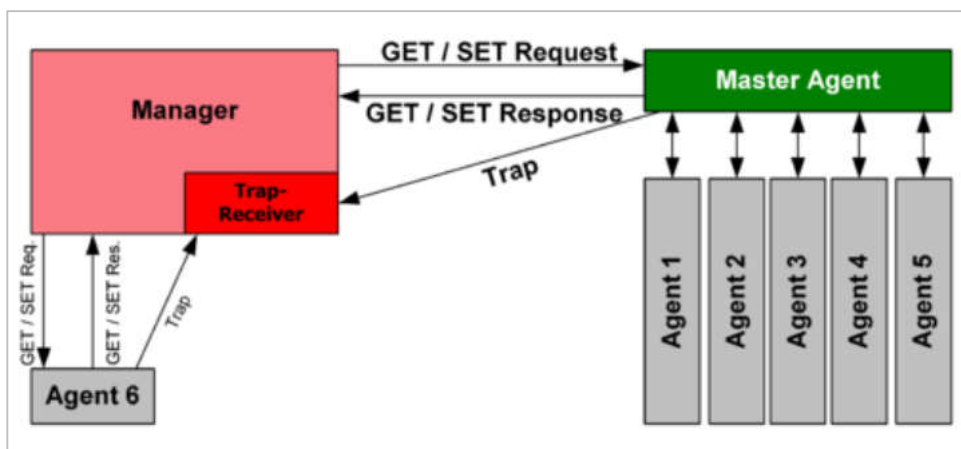
1.4.1 หลักการทำงานของ SNMP

การทำงานของโปรโตคอล SNMP ใช้สำหรับการบริหารจัดการระบบ Computer จำนวนมาก ซึ่งมีความสามารถในการ Monitor หรือจัดการกลุ่ม Host หรือ อุปกรณ์ ใน Network โดยอุปกรณ์ในระบบจะมี Agent ที่คอยทำงานเพื่อตรวจสอบสถานะอุปกรณ์ ตลอดเวลาและก็จะส่ง Report กลับไปหาตัว Manager ที่เป็นฝั่ง Server

SNMP โดยมีส่วนประกอบด้วยกัน 3 ตัว หลักคือ

- ตัวอุปกรณ์ที่อยู่ใน Network
- ตัว Agent เป็น Software ที่ต้องติดตั้งอยู่บนอุปกรณ์เพื่อทำการตรวจสอบและ Report สิ่งผิดปกติ

- Network Management Station (NMS) เป็น Software ของฝั่ง SNMP Server หรือที่เรียกว่า Manager คอยรับ และเก็บรวบรวมข้อมูลจาก agent



ภาพที่ 2 การทำงานรับส่งข้อมูลของโปรโตคอล SNMP

1.4.2 โครงสร้างของ Protocol SNMP

โพรโทคอล SNMP ทำงานในระดับ Application Layer ในรูปแบบ Internet Protocol Suit ซึ่ง SNMP Agent จะรับคำสั่งผ่านทาง UDP Port 161 โดยตัว Manager จะส่งคำสั่งไปยัง Port 161 บนอุปกรณ์ฝั่ง Agent จากนั้น Agent จะส่งข้อมูลกลับไปยัง Manager ตามที่ร้องขอมา ส่วนฝั่ง Manager จะมีการรับ Notification หรือที่เรียกกันว่า Traps (SNMP Traps) ที่ Port 162 โดยฝั่ง Agent จะเป็นคนส่ง Notification เมื่อพบสิ่งผิดปกติตามที่ตั้ง Rule เอาไว้ เพื่อส่งข้อมูลดังกล่าวไปยัง Manager port 162 แต่ถ้าใช้เป็น Secure Port หรือ Transport Layer Security (TLS) สำหรับ Agent จะเป็น port 10161 และ ฝั่ง Manager Trap จะเป็น port 10162

SNMPv1 ประกอบด้วย 5 Protocol Data Units (PDU) ส่วนอีก 2 PDUs คือ GetBulkRequest และ InformRequest ถูกเพิ่มเข้ามาใน SNMPv2 ส่วน Report PDU เพิ่มเข้ามาใน SNMPv3



ภาพที่ 3 ภาพแสดงองค์ประกอบของ Packet ภายใน PDU

1.4.3 Protocol Data Units (PDU) 8 ชนิด ดังนี้

1. GetRequest (Manager to Agent) เป็นการที่ฝั่ง Manger ส่งคำขอข้อมูลไปยัง Agent โดยจะกำหนดข้อมูลที่ต้องการไปใน Object ภายใน Message หรือที่เรียกว่า Object Identifier เช่น 1.3.6.1.2.1.1.1.0 หมายถึงต้องการทราบข้อมูล sysDescr หรือข้อมูลรายละเอียดของอุปกรณ์ที่ Agent ติดตั้งอยู่ ซึ่งทาง Agent เองก็จะตอบข้อมูลรายละเอียดดังกล่าวกลับไป

2. GetNextRequest (Manager to Agent) เป็น PDU ที่ทาง Manager ส่งไปหา Agent เพื่อเอาข้อมูลตัวแปร โดยค่าของ Object จาก Object ID ที่กำหนดใน MIB จะใช้ในการเอาค่าเข้าสู่ตาราง เพราะถ้า Manager ไม่ทราบ Index ที่จะดึง ก็จะไม่สามารถดึงค่าออกมาได้ แต่สำหรับ GetNextRequest จะกำหนด Object ID ในตารางของตัวถัดไปเรื่อยๆ

3. SetRequest (Manager to Agent) เป็นฝั่ง Manager ส่งคำสั่งไปยัง Agent เพื่อกำหนดค่าของตัวแปร หรือเปลี่ยนแปลงค่าที่ Configure ไว้ใน MIB ของอุปกรณ์นั้น ๆ

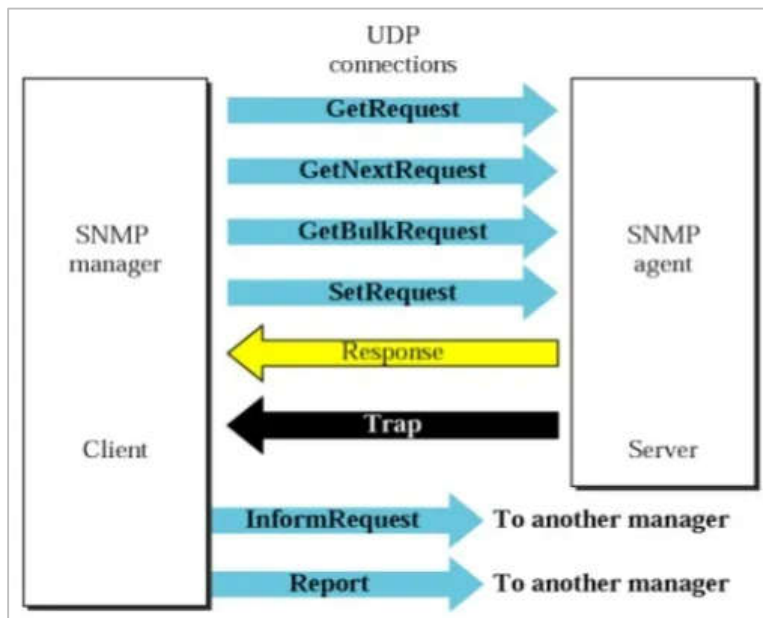
4. Response (Agent to Manager) เป็นฝั่ง Agent ส่งหา Manager เพื่อตอบกลับ ข้อมูลจากคำสั่ง Protocol Data Units (PDU) GetRequest หรือ GetNextRequest โดยจะส่งข้อมูลของตัวแปรที่ร้องขอกลับไปหา Manager

5. Trap (Agent to Manager) เป็นฝั่ง Agent ส่งหา Manager เพื่อแจ้งหรือ Notify เหตุการณ์ที่เกิดขึ้นบนฝั่ง Agent เอง เช่น เกิดการ Reboot Server หรือมีค่าบางอย่างที่สูงถึงค่า Trigger ที่กำหนดไว้

6. GetbulkRequest (Manager to Agent) ถูกเพิ่มเข้ามาหลังจากการพัฒนาเป็น Version 2 เป็นการที่ Manager ส่งคำสั่งไปหา Agent เพื่อเอาชุดข้อมูลขนาดใหญ่ แทนการ GetRequest หรือ GetNextRequest หลาย ๆ ครั้ง

7. InformRequest (Manager to Manager) ถูกเพิ่มเข้ามาหลังจากพัฒนา Version 2 เช่นเดียวกันเป็นฝั่ง manager ส่งหา manager กันเอง เพื่อรับค่าตัวแปร บางอย่างจาก Agent ที่อยู่ภายใต้การควบคุมของ Manager อีกตัวซึ่งจะต้องตอบกลับด้วย Response PDU เช่นกัน

8. Report (Manager to Manager) เป็นการส่งรายงานข้อผิดพลาดในระบบ ระหว่าง Manager ด้วยกันเอง เป็นส่วนที่เพิ่มขึ้นมาเมื่อพัฒนาเป็น Version 3



ภาพที่ 4 แสดงรูปแบบของ Protocol UDP Connection

1.5 โพรโทคอลไอซีเอ็มพี (Internet Control Message Protocol : ICMP)

Internet Control Message Protocol (ICMP) เป็นชุดของกฎการสื่อสารที่อุปกรณ์ใช้ในการสื่อสารข้อผิดพลาดในการรับส่งข้อมูลในเครือข่าย ในการแลกเปลี่ยนข้อความระหว่างผู้ส่งและผู้รับ ข้อผิดพลาดที่ไม่คาดคิดบางอย่างสามารถเกิดขึ้นได้ ตัวอย่างเช่นข้อความอาจยาวเกินไป หรือแพ็กเก็ตข้อมูลมาถึงไม่เรียงลำดับกันทำให้ผู้รับไม่สามารถประกอบข้อมูลเข้าด้วยกันได้ ในกรณีดังกล่าว ผู้รับจะใช้ ICMP เพื่อส่งข้อความแสดงข้อผิดพลาดแจ้งไปยังผู้ส่ง และขอส่งข้อความใหม่อีกครั้ง

การใช้งาน ICMP Internet Control Message Protocol (ICMP) เป็นเครือข่ายโพรโทคอลที่สำคัญในระบบเครือข่ายคอมพิวเตอร์ เป็นตัวกำหนดกลไกมาตรฐานสำหรับอุปกรณ์เครือข่ายในการสื่อสารข้อมูลที่สำคัญ เช่น การเชื่อมต่อ และสถานะเครือข่าย อุปกรณ์ทั้งหมดที่เชื่อมต่อกับเครือข่าย รวมถึงเราเตอร์ และอุปกรณ์ตำแหน่งข้อมูลสามารถประมวลผลข้อความ ICMP ได้ ICMP ได้ถูกดัดแปลงให้สามารถทำงานทั้งแบบ IPv4 และ IPv6 ได้

ICMP ทำงานอย่างไร Internet Control Message Protocol (ICMP) มักจะทำงานควบคู่ไปกับเครือข่ายโพรโทคอลอื่น ๆ เช่น TCP/IP หรือ User Datagram Protocol (UDP) โยสและเราเตอร์แลกเปลี่ยนข้อความ ICMP หรือแพ็กเก็ต ICMP เมื่อมีเหตุการณ์ในเครือข่ายบางอย่างเกิดขึ้น

2. เครื่องมือที่ใช้ในการพัฒนาระบบ

2.1 ระบบปฏิบัติการ Linux CentOS

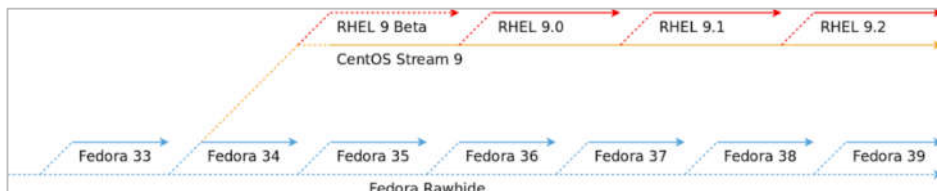
CentOS คือ ระบบปฏิบัติการ Community Enterprise Operating System หรือระบบปฏิบัติการ Linux เน้นเรื่องความเสถียรและมีการอัปเดตความปลอดภัยระดับสูง โดย CentOS มีเวอร์ชันใหม่ประมาณทุก 2 ปี โดยแต่ละเวอร์ชันมีอายุการใช้งานสูงสุด 10 ปี หรือตามข้อกำหนดระยะเวลาการสนับสนุนของ Red Hat Enterprise Linux (RHEL) และในแต่ละเวอร์ชันได้รับการอัปเดตประมาณทุก 6 เดือน ทำให้ระบบ Linux มีความปลอดภัย และมีความน่าเชื่อถือ

CentOS เปิดตัวอย่างเป็นทางการครั้งแรกในปี ค.ศ. 2004 โดย Gregory Kurtze เป็นผู้ก่อตั้ง ซึ่ง CentOS เป็น Open Source ที่พัฒนามาจากโค้ดต้นฉบับ (Source Code) ของ Red Hat Enterprise Linux (RHEL) ระบบปฏิบัติการที่มีความเสถียรรองรับ Workload ที่หลากหลายสามารถนำไปพัฒนาซอฟต์แวร์ Open Source อื่น ๆ ได้ ซึ่งเป็นลิขสิทธิ์แบบ GNU General Public License (GNU-GPL) หมายถึง สัญญาอนุญาตให้นักพัฒนาสามารถใช้ซอฟต์แวร์ หรือ License รวมถึงสามารถทำซ้ำ เผยแพร่ และดัดแปลงซอฟต์แวร์นั้นได้ เพื่อให้ให้นักพัฒนาทุกคนสามารถใช้งานซอฟต์แวร์ดังกล่าวได้อย่างอิสระเสรีและถูกต้องตามกฎหมาย

ในปัจจุบัน CentOS นิยมนำมาใช้ในการทำ Web Hosting เป็นพื้นที่รับฝากเว็บไซต์ เพื่อใช้ออนไลน์บนอินเทอร์เน็ต รวมถึงการทำ Server สำหรับการวางระบบในองค์กร ที่ได้รับความนิยมเป็นอย่างมาก เนื่องจากเป็นระบบปฏิบัติการที่ใช้ต้นแบบจาก Red Hat สามารถทำการติดตั้งแพ็คเกจย่อยภายในได้ ทั้ง RPM (RPM Package Manager), TAR (Tape Archive), APT (Advanced Packaging Tool) หรือใช้คำสั่ง YUM (Yellow Dog Updater Modified) ในการอัปเดตซอฟต์แวร์ได้แบบอัตโนมัติ

CentOS Stream เป็นการนำโค้ดต้นฉบับ (Source Code) ของ Red Hat Enterprise Linux (RHEL) มาเผยแพร่ให้ใช้ฟรี โดยไม่ต้องซื้อ Subscription โดยเวอร์ชันของ CentOS เท่ากับ RHEL หรือล่าช้ากว่า RHEL เพียงเล็กน้อย แต่ CentOS Stream คือ Upstream ของ RHEL โดยอยู่ตรงกลางระหว่าง Fedora ที่เป็น Linux Distribution จาก Red Hat Enterprise Linux สำหรับเชิงธุรกิจที่ออกเวอร์ชันใหม่ในทุก 6 เดือน

กับ RHEL ที่ออกเวอร์ชันล่าช้ากว่า โดยทีมพัฒนาของ Red Hat นำ CentOS Stream 9 ไปพัฒนาเป็น RHEL 9.x ซึ่งในปัจจุบันสถานะคือ RHEL 9.0 Beta โดย CentOS Stream 9 มีอายุการอัปเดตและการบำรุงรักษาไปจนถึงประมาณปี ค.ศ. 2027 หรือเทียบเท่ากับ ระยะการดูแลรักษาของ RHEL 9



ภาพที่ 5 ภาพแสดงการเปรียบเทียบการพัฒนาเวอร์ชัน CentOS

ปัจจุบัน CentOS มีระบบปฏิบัติการทั้งหมด 4 เวอร์ชัน ทั้ง CentOS เวอร์ชันเดิม และ CentOS Stream เวอร์ชันใหม่ โดยคุณยังสามารถเลือกใช้งาน CentOS เวอร์ชันเก่าได้ แต่อาจมีข้อจำกัดบางอย่างเมื่อเทียบกับ CentOS เวอร์ชันรุ่นที่ใหม่กว่า เนื่องจากมีการปรับปรุงข้อบกพร่องที่พบในเวอร์ชันเก่าให้ดีขึ้น อีกทั้งยังมีการอัปเดตและการบำรุงรักษาให้ทันสมัยอยู่เสมอ โดยแต่ละเวอร์ชันมีระยะ End of Life ดังนี้

รุ่น	วันที่เปิดให้ใช้งาน	อัปเดตเต็มรูปแบบ	อัปเดตและการบำรุงรักษา
3	ค.ศ. 2004 - 03 - 19	ค.ศ. 2006 - 07 - 20	ค.ศ. 2010 - 10 - 31
4	ค.ศ. 2005 - 03 - 09	ค.ศ. 2009 - 03 - 31	ค.ศ. 2012 - 02 - 29
5	ค.ศ. 2007 - 04 - 12	ค.ศ. 2014 - 01 - 31	ค.ศ. 2017 - 03 - 31
6	ค.ศ. 2011 - 07 - 10	ค.ศ. 2017 - 05 - 10	ค.ศ. 2020 - 11 - 30
7	ค.ศ. 2014 - 07 - 07	ค.ศ. 2020 - 08 - 06	ค.ศ. 2024 - 06 - 30
8	ค.ศ. 2019 - 09 - 24	ค.ศ. 2021 - 12 - 31	-
9	ค.ศ. 2021 - 04 - 26	ค.ศ. 2027	-

● CentOS เวอร์ชันเก่า ● CentOS เวอร์ชันเต็มล่าสุด
● CentOS เวอร์ชันเต็มที่ยังได้รับการอัปเดต ● CentOS Stream เวอร์ชันใหม่

ภาพที่ 6 ภาพแสดงเวอร์ชัน ของระบบปฏิบัติการ CentOS

2.2 เว็บเซิร์ฟเวอร์ (Web Server) และการทำงานของเว็บเซิร์ฟเวอร์อะปาเช่ (Apache)

เว็บเซิร์ฟเวอร์ (Web Server) เป็นเครื่องคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการข้อมูล แก่เครื่องคอมพิวเตอร์ไคลเอนต์ (Client) หรือเครื่องคอมพิวเตอร์ที่ขอรับบริการผ่าน

ระบบเครือข่าย โดยสามารถแสดงผลผ่านเว็บเบราว์เซอร์ หรืออาจเรียกได้ว่า เว็บเซิร์ฟเวอร์ (Web Server) คือ โปรแกรมที่คอยให้บริการแก่ ไคลเอนต์ (Client) ที่ร้องขอข้อมูลเข้ามา โดยผ่าน เว็บเบราว์เซอร์โปรแกรมที่นิยมนำไปใช้เป็นเครื่องบริการเว็บ ได้แก่ อะปาเช่ (Apache Web Server) และไมโครซอฟท์ไอไอเอส (Microsoft IIS = Internet Information Server)

Apache คือ เว็บเซิร์ฟเวอร์ (Web Server) ที่พัฒนามาจาก HTTPD Web Server โดยจะทำหน้าที่ในการจัดเก็บ Homepage และส่ง Homepage ไปยัง Browser ที่มีการเรียกใช้งานมายัง เว็บเซิร์ฟเวอร์ (Web Server) ที่ทำการเก็บ Homepages นั้น



ภาพที่ 7 ภาพแสดงโลโก้ของอะปาเช่เว็บเซิร์ฟเวอร์ (Apache Web Server)

2.3 ระบบฐานข้อมูล MariaDB

มาเรียดีบี (MariaDB) คือ ฟรีซอฟต์แวร์แบบโอเพนซอร์สสำหรับจัดการกับฐานข้อมูล มาเรียดีบี (MariaDB) เป็นหนึ่งในฐานข้อมูลที่ได้รับความนิยมมากที่สุดในโลกมาเรียดีบี (MariaDB) ถูกพัฒนาขึ้นโดยนักพัฒนาเดิมของมายเอชคิวแอล (MySQL) และรับประกันได้เลยว่ามาเรียดีบี (MariaDB) จะเป็นฟรีโอเพนซอร์ส ผู้ใช้ที่โดดเด่น ได้แก่ วิกิพีเดีย, WordPress.com และ Google มาเรียดีบี (MariaDB) เปลี่ยนข้อมูลเป็นฐานข้อมูลที่มีโครงสร้างในหลากหลายแอปพลิเคชัน ตั้งแต่ธนาคารไปจนถึงเว็บไซต์ต่าง ๆ เป็นการปรับปรุงและแทนที่ด้วยการแทนที่ของ มายเอชคิวแอล (MySQL) มาเธอร์ดีบีใช้เนื่องจากมีความรวดเร็วและสามารถปรับขนาดได้และมีปลั๊กอินและเครื่องมือ อื่น ๆ ทำให้สามารถใช้งานได้หลากหลาย มาเรียดีบี (MariaDB) ได้รับการพัฒนาเป็นซอฟต์แวร์โอเพนซอร์ส และเป็นฐานข้อมูลเชิงสัมพันธ์ซึ่งมีอินเทอร์เฟซเอสคิวแอล (SQL) สำหรับการเข้าถึงข้อมูล



ภาพที่ 8 ภาพแสดงโลโก้ของฐานข้อมูลมาเรียดีบี (MariaDB)

2.4 โปรแกรม Zabbix Network Monitoring

Zabbix คือ Monitoring Tool เป็นเป็นเครื่องมือที่นำมาใช้ในการจัดการและตรวจสอบระบบเครือข่ายและคอมพิวเตอร์ในองค์กร มีความยืดหยุ่น และความสามารถที่สูงสามารถการปรับแต่งตามความต้องการของแต่ละองค์กร ซึ่งเป็น Open Source ที่นิยมเนื่องจากมี Web GUI ที่สามารถดูข้อมูล ใช้งานง่าย และสามารถตั้งค่าการใช้งานได้อย่างครบครัน โดยมีฟังก์ชันที่มุ่งเน้นด้าน Monitoring และ Trending เป็นเครื่องมือที่ใช้ในการตรวจสอบ Server และ Hardware ของระบบเครือข่าย Network สามารถตรวจสอบ Networks, Servers, Cloud platforms และ Applications มีฟีเจอร์การสแกนค้นหาบนระบบ Network, Topology mapping, Bandwidth analysis และ Device status monitoring พร้อมกับระบบการแจ้งเตือนเมื่อเกิดปัญหาขึ้น Zabbix มีจุดเด่น คือ สามารถคาดการณ์พฤติกรรมในอนาคตจากประวัติการใช้งาน และคาดการณ์แนวโน้มของ Traffic ที่ผ่านมา ทำให้ผู้ดูแลระบบสามารถทราบถึงปัญหาได้

ZABBIX

Username

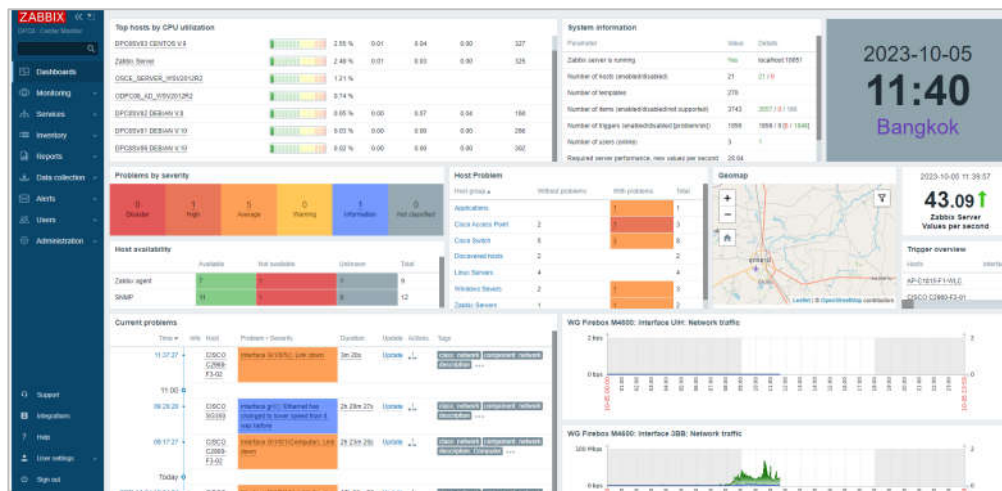
Password

Remember me for 30 days

Sign in

or sign in as guest

ภาพที่ 9 ภาพแสดง Login โปรแกรม Zabbix Monitoring System



ภาพที่ 10 ภาพรวมของโปรแกรม Zabbix Monitoring System

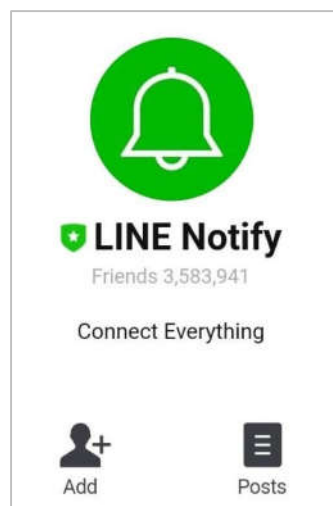
2.5 LINE Application

ไลน์ (LINE) เป็นแอปพลิเคชัน ที่ใช้ในการติดต่อพูดคุยสื่อสาร ซึ่งใช้อินเทอร์เน็ตในการพูดคุยติดต่อสื่อสาร ซึ่งติดต่อสื่อสารด้วยการโทรพูดคุยในรูปแบบเสียง วิดีโอคอล และสามารถส่งข้อความต่าง ๆ เช่น ส่งข้อความ แชร์ไฟล์รูปภาพ แชร์ไฟล์วิดีโอ รวมทั้งสามารถสร้างกลุ่มเพื่อพูดคุยหลายคนพร้อมกันได้



ภาพที่ 11 ภาพแสดงโลโก้ของ LINE Application

LINE Notify คือ บริการรับข้อความแจ้งเตือนจากเว็บเซอร์วิสต่างๆ โดยการออก Token Key มาเชื่อมต่อกับทางเว็บเซอร์วิสที่ต้องการรับจากแจ้งเตือน สามารถรับการแจ้งเตือนจากบัญชีทางการของ “LINE Notify” ซึ่งให้บริการโดย LINE สามารถเชื่อมต่อกับบริการที่หลากหลาย และยังสามารถรับการแจ้งเตือนทางกลุ่มได้



ภาพที่ 12 ภาพบริการรับการแจ้งเตือนจากเว็บเซอร์วิสทาง LINE Application

2.6 Shell Script (Bash command)

Shell Script (Bash command) คือ เป็นคำสั่งของโปรแกรม (Unix shell) ที่ใช้สั่งการคอมพิวเตอร์ให้ทำงานผ่าน Commands โดยการรวมเอาคำสั่ง เงื่อนไขต่าง ๆ ที่ผู้ใช้งานต้องการใส่ลงใน File และทำการ Execute File นั้น แล้วรอผลลัพธ์ที่ได้ในรูปแบบ Text โดยส่วนมากใช้งาน เพื่อให้ทำงานบนระบบอัตโนมัติตามเวลาที่เรต้องการ สำหรับบน Window หรือ DOS จะเรียกสิ่งนี้ว่า batch file ซึ่งก็คือการเอาชุดคำสั่งมาทำเป็น file เช่นเดียวกับ shell script และรันผ่าน cmd.exe

3. งานวิจัยที่เกี่ยวข้อง

เชษฐ ศรีแย้ม (2557) ได้ทำการศึกษาเรื่อง “การพัฒนาระบบติดตามสถานะเครือข่ายคอมพิวเตอร์ : กรณีศึกษามหาวิทยาลัยราชภัฏเพชรบุรี” การศึกษาค้นคว้าเพื่อพัฒนาระบบติดตามสถานะเครือข่ายคอมพิวเตอร์ และการประเมินผลของระบบติดตามสถานะเครือข่ายคอมพิวเตอร์ ของมหาวิทยาลัยราชภัฏเพชรบุรี กลุ่มตัวอย่างในการศึกษาวิจัยเป็นอุปกรณ์เครือข่ายคอมพิวเตอร์ที่ใช้ในมหาวิทยาลัยจำนวน 40 อุปกรณ์ และมีอุปกรณ์เครือข่ายที่มีความแตกต่างกัน 4 ชนิดเป็นกรณีศึกษา เครื่องมือที่ใช้ในการวิจัยประกอบด้วย 1) โปรแกรมติดตามสถานะเครือข่ายคอมพิวเตอร์ ที่พัฒนาขึ้นด้วยโปรแกรมภาษา PHP ทำการอ่านค่าความเปลี่ยนแปลงแบบเรียลไทม์ผ่าน SNMP โพรโทคอล 2) การประเมินจากผู้เชี่ยวชาญระบบเครือข่ายคอมพิวเตอร์จำนวน 3 ท่าน ผลการศึกษาพบว่า ระบบการทำงานของระบบมี 4 ระบบย่อย 1) ระบบติดตามสถานะอุปกรณ์เครือข่าย 2) ระบบติดตามสถานะเครื่องแม่ข่าย 3) ระบบติดตามการให้บริการเครื่องแม่ข่าย 4) ระบบจัดการข้อมูลผู้ใช้และอุปกรณ์ และการประเมินผล ผลการทดลองใช้งานระบบ พบว่าการประเมินคุณภาพโดยรวมอยู่ในระดับดี และความพึงพอใจของกลุ่มเป้าหมายที่มีต่อประสิทธิภาพระบบโดยรวมอยู่ในระดับดี

สันทัต มาทน (2557) ได้ทำการศึกษาเรื่อง “ระบบตรวจสอบการทำงานของเครื่องแม่ข่าย” การศึกษาค้นคว้าเพื่อสร้างเครื่องมือช่วยเหลือและอำนวยความสะดวกในการทำงานของเจ้าหน้าที่ที่ดูแลระบบให้เป็นไปอย่างมีประสิทธิภาพมากขึ้นและสอดคล้องกับความรู้ที่ได้ทำการศึกษาและค้นคว้าจากมหาวิทยาลัยเทคโนโลยีมหานคร แสดงให้เห็นว่าสามารถนำมาใช้ได้จริงในการทำงาน ผลการศึกษาพบว่า ตัวโปรแกรมจะทำงานจากการตั้งค่าคอนแทป (Crontab) จากนั้นโปรแกรมจะทำการเช็คสถานะและเก็บค่าซีพียู เมมโมรี่ ฮาร์ดดิส ลงในฐานข้อมูลและถ้ามีข้อมูลที่เกินค่าการเฝ้าระวังที่ตั้ง

ไว้ก็จะทำการแจ้งเตือนผู้ดูแลระบบผ่านอีเมล และเอสเอ็มเอส และสามารถนำข้อมูลที่ได้มาเป็นข้อมูลเพื่อไปใช้ในการวางแผนการพัฒนาและเป็นหลักฐานในการนำเสนอการปรับปรุงระบบภายในองค์กร ให้สอดคล้องกับการใช้งานต่างๆขององค์กร เช่น การเฝ้าดูเครือข่ายได้ตลอดเวลา และสามารถเก็บข้อมูลต่างๆ โดยการใช้ประโยชน์จากโพรโทคอลเอสเอ็นเอ็มพี เพื่อนำมาตรวจสอบและประยุกต์ใช้ในการทำงาน ทำให้ทางผู้ดูแลระบบทำงานได้อย่างสะดวกรวดเร็วและถูกต้องซึ่งทำให้ลดปัญหาเรื่องเวลาการทำงานและแก้ไขข้อบกพร่องของเครือข่ายได้ทันท่วงที

อติชาติ พชรภัก (2559) ได้ทำการศึกษารื่อง “ระบบการแจ้งเตือนและตอบโต้ของ ZABBIX ด้วยแอปพลิเคชัน LINE” การศึกษาค้นคว้าครั้งนี้เพื่อเป็นเครื่องมือที่จะช่วยแจ้งเตือนการใช้งานทรัพยากรของเซิร์ฟเวอร์ (Server) และแอปพลิเคชัน (Application) ซึ่งทำหน้าที่ในการส่งข้อมูลไปยังเจ้าหน้าที่ที่รับผิดชอบเมื่อเกิดความผิดปกติ เช่น แอปพลิเคชันมีการใช้งานทรัพยากรของเซิร์ฟเวอร์ผิดปกติ ดังนั้นแอปพลิเคชัน LINE สามารถช่วยแก้ปัญหาดังกล่าวได้ หากพบว่าเซิร์ฟเวอร์หรือแอปพลิเคชันมีการทำงานที่ผิดปกติ แอปพลิเคชัน LINE จะแสดงผลของสถานะที่กำลังเกิดขึ้นเพื่อให้ทราบถึงปัญหาที่เกิดขึ้นได้รวดเร็ว ผลการศึกษาค้นคว้า พบว่า ระบบการแจ้งเตือนและตอบโต้ของ ZABBIX ด้วยแอปพลิเคชัน LINE สามารถตรวจสอบการทำงานของระบบได้โดย วิธีการทดสอบการทำให้ CPU, Memory ถูกใช้งานไปเกินกว่า 80 % และหยุดการทำงานของ Zabbix agent ของเครื่องเซิร์ฟเวอร์ที่มี Zabbix agent ทำงานอยู่ พบว่า Zabbix Server มีการแสดงผล ไม่สามารถ Monitor อุปกรณ์ได้ที่หน้า Dashboard ของ Zabbix และสามารถส่งข้อความ ร้องขอการทำงานจากแอปพลิเคชัน LINE ตามที่ขอไปและได้ผลรับตอบกลับมา เป็นข้อความหรือรูปภาพที่ตรงกับความต้องการเมื่อไปเช็คกับเครื่องปลายทาง หรือ Zabbix ก็มีค่าที่ตรงกันถูกต้อง

ดิเรก พลูมาศ (2560) ได้ทำการศึกษารื่อง “ระบบมอนิเตอร์การทำงานของเครือข่าย กรณีศึกษา บริษัท พร้อม เทคโนโลยีคอล เซอร์วิส เซส จำกัด ” การศึกษาค้นคว้าครั้งนี้เพื่อใช้ในการตรวจสอบการทำงานของเครือข่ายของบริษัท โดยจะเป็นการตรวจสอบการทำงานและดูประสิทธิภาพของเครือข่ายบนตัวอุปกรณ์ต่าง ๆ แสดงข้อมูลที่จำเป็นของอุปกรณ์ต่าง ๆ เพื่อใช้ในการเฝ้าระวังและใช้ในการวิเคราะห์ป้องกันกับสิ่งที่จะเกิดขึ้นในระบบเครือข่ายของบริษัท รายละเอียดข้อมูลที่จะแสดงจะมีการทำงานของซีพียู ,Memory ,พัดลม , ทราฟฟิกขาเข้าและออกของอินเทอร์เฟซ , สถานะของฟิสิคัล , สถานะวีพีเอ็น และจะนำข้อมูลเหล่านี้ไปประเมินว่าเกินกว่าค่าของ Threshold ที่ตั้งไว้หรือไม่ถ้าเกินระบบก็จะทำการแจ้งเตือน ผลการศึกษาค้นคว้า ระบบมอนิเตอร์การทำงานของเครือข่ายสามารถตรวจสอบ

สถานะการทำงานของอุปกรณ์ (Agent) ว่ามีสถานะ ออนไลน์ / ออฟไลน์ ในระบบเครือข่ายโดยใช้ โพรโทคอลเอสเอ็นเอ็มพี (Protocol SNMP) และค่าของโอไอดีในการถามและตอบกลับจากอุปกรณ์ Agent ระบบสามารถแจ้งเตือนผู้ดูแลได้เมื่อเกิดข้อมูลเกินค่า Threshold หรืออินเทอร์เฟซ มีการดาวน์โหลดผ่านทางไลน์และอีเมลได้ และเว็บแอปพลิเคชัน สามารถดึงข้อมูลจากฐานข้อมูล แล้วนำมาแสดงที่หน้า Web ได้ ซึ่งสามารถแสดงข้อมูลในรูปแบบของข้อความ,ตัวเลขและกราฟของซีพียู, Memory และอินเทอร์เฟซได้

ถนนม กองใจ (2560) ได้ทำการศึกษารื่อง “การพัฒนา ระบบตรวจสอบสถานะการทำงานของระบบเครือข่ายและอุณหภูมิห้องแม่ข่าย” การศึกษาค้นคว้าเพื่อพัฒนาระบบตรวจสอบสถานะการทำงานของระบบเครือข่ายและอุณหภูมิภายในห้องแม่ข่ายที่สามารถเฝ้าติดตามและตรวจสอบความผิดปกติของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย โดยการประยุกต์ใช้งานซอฟต์แวร์ตรวจสอบสถานะการทำงาน ที่ได้รับการพัฒนาด้วยภาษา PHP และระบบวัดอุณหภูมิด้วยเซนเซอร์ DS18B20 ที่สามารถส่งผ่านข้อมูลด้วยโพรโทคอล SNMP การทดสอบใช้งานกับระบบเครือข่ายของภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ ซึ่งประกอบด้วย เครื่องคอมพิวเตอร์แม่ข่าย 12 เครื่อง อุปกรณ์เครือข่าย 6 เครื่องและอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย 8 เครื่อง ผลการศึกษาพบว่า ระบบสามารถตรวจสอบและแสดงผลสถานะการทำงานของอุปกรณ์เครือข่ายทั้งหมดและอุณหภูมิภายในห้องแม่ข่ายผ่านโปรแกรมอินเทอร์เน็ตเบราว์เซอร์ได้ อีกทั้งหากอุณหภูมิภายในห้องแม่ข่ายสูงเกินจุดวิกฤตที่กำหนดไว้ในโปรแกรม หรืออุปกรณ์เครือข่ายเกิดการขัดข้อง ระบบจะทำการแจ้งเตือนอัตโนมัติไปยังผู้ดูแลระบบเครือข่ายผ่านทางอีเมลเพื่อเข้าไปทำการแก้ไขให้ทันท่วงที ช่วยลดงบประมาณของหน่วยงานสำหรับจัดซื้อโปรแกรมตรวจสอบระบบเครือข่ายเข้ามาใช้งาน อีกทั้งข้อมูลที่บันทึกยังสามารถนำไปวิเคราะห์เพื่อวางแผนแก้ไขปัญหาก็ได้ หรือนำข้อมูลไปประกอบการศึกษา เช่น พฤติกรรมการใช้งานระบบเครือข่าย จากผลการทดลองหน้าจอดีแสดงผล

- 1) พบว่าโปรแกรมสามารถแสดงข้อมูลสถานะการทำงานของอุปกรณ์เครือข่ายปริมาณการใช้งานระบบเครือข่าย และอุณหภูมิภายในห้องแม่ข่าย โดยแสดงผลข้อมูลทั้งหมดไว้ในหน้าจอเดียวช่วยให้สะดวกต่อการตรวจสอบ
- 2) โปรแกรมตรวจสอบสถานะ การทำงานของอุปกรณ์เครือข่ายและเครื่องแม่ข่ายที่สร้างด้วยภาษา PHP ทำงานร่วมกับโปรแกรม Cacti พบว่าโปรแกรมช่วยสนับสนุนการทำงานของผู้ดูแลระบบด้วยการลดขั้นตอนและระยะเวลาที่ใช้ในการตรวจสอบการทำงานของ

ระบบเครือข่าย 3) โปรแกรมตรวจสอบอุณหภูมิภายใน ห้องแม่ข่าย โดยใช้หัววัดแบบ DS1820 ส่งผ่านข้อมูลด้วยโพรโทคอล SNMP และแสดงผลในรูปแบบเว็บเพจ

ธีรัช อารีราษฎร์ และวราภา อารีราษฎร์ (2560) ได้ทำการศึกษารายชื่อเรื่อง “การพัฒนาและจัดการระบบตรวจสอบและจัดการเครือข่าย มหาวิทยาลัยราชภัฏมหาสารคาม” การศึกษานี้เพื่อศึกษาสภาพของการตรวจสอบระบบเครือข่าย และพัฒนาระบบตรวจสอบและจัดการเครือข่าย ศึกษาการยอมรับระบบตรวจสอบและจัดการเครือข่ายมหาวิทยาลัยราชภัฏมหาสารคาม กลุ่มเป้าหมาย ได้แก่ อาจารย์และเจ้าหน้าที่ของมหาวิทยาลัยราชภัฏมหาสารคาม จำนวน 25 คน โดยใช้เครื่องมือในการวิจัย ได้แก่

- 1) แบบสอบถามสภาพของการตรวจสอบระบบเครือข่าย
- 2) ระบบตรวจสอบและจัดการเครือข่าย
- 3) แบบสอบถามต่อความเหมาะสมขององค์ประกอบระบบ และระบบตรวจสอบและจัดการเครือข่าย
- 4) แบบสอบถามความพึงพอใจที่มีต่อระบบตรวจสอบและจัดการเครือข่าย
- 5) แบบสอบถามการยอมรับระบบตรวจสอบและจัดการเครือข่าย

ผลการศึกษาพบว่า สถาปัตยกรรมของระบบจะมีโครงสร้างโดยข้อมูลของอุปกรณ์ WIFI ที่ติดตั้งตามจุดต่าง ๆ ที่มหาวิทยาลัยจะจัดเก็บที่ฐานข้อมูลของระบบ CACTI ผ่านระบบโพรโทคอล SNMP และ องค์ประกอบของ แอปพลิเคชันประกอบไปด้วย 6 ฟังก์ชัน ได้แก่ การแจ้งซ่อม WIFI การรายงานการใช้หน่วยความจำการรายงานข้อมูลรูปแบบกราฟ การรายงานอัตราการรับส่งข้อมูล และการรายงานข้อมูลผู้ใช้งานที่เชื่อมต่อสถาปัตยกรรมและองค์ประกอบของแอปพลิเคชันมีความเหมาะสมโดยรวมอยู่ในระดับมากที่สุด แอปพลิเคชันที่พัฒนาสามารถโหลดได้จาก Play Store และจาก APP Store ภายใต้ชื่อว่า RUnetmonitor ผลการทดลองใช้แอปพลิเคชัน พบว่า คุณภาพของแอปพลิเคชัน โดยรวมอยู่ในระดับมากที่สุด และความพึงพอใจของกลุ่มเป้าหมายที่มีต่อแอปพลิเคชันโดยรวมอยู่ในระดับมากที่สุดและความคิดเห็นในการยอมรับที่มีต่อแอปพลิเคชัน โดยรวมอยู่ในระดับมาก

ประพันธ์ ไชยชนะ (2561) ได้ทำการศึกษารายชื่อเรื่อง “ระบบตรวจสอบการทำงานของระบบเครือข่ายและแจ้งเตือนผ่านแอปพลิเคชัน LINE” การศึกษานี้เพื่อศึกษาระบบตรวจสอบการทำงานของระบบเครือข่ายให้มีการส่งข้อความแจ้งเตือนผ่านแอปพลิเคชัน LINE และผลการศึกษานำไปพัฒนาเป็นเครื่องมือสำหรับผู้ดูแลระบบเครือข่ายในการบริหารจัดการระบบ ช่วยในการแจ้งเตือนสถานะของอุปกรณ์ Switch และปริมาณ Traffic ของระบบเครือข่าย ด้วยการส่งข้อความแจ้งเตือนผ่านแอปพลิเคชัน LINE ให้ทราบถึงปัญหาที่เกิดขึ้นและสามารถแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็วเพื่อให้ระบบเครือข่ายใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ ผลการศึกษาพบว่า การดำเนินการ

ทดสอบโดยการทำให้อุปกรณ์เครือข่าย Down/Up ทำให้ Zabbix Network Monitoring สามารถทำการส่งข้อความแจ้งเตือนไปยังแอปพลิเคชัน LINE ได้ และโดยการทำให้ Traffic ที่วิ่งเข้าหา Port ของอุปกรณ์เครือข่าย สามารถรับข้อความแจ้งเตือนปัญหาอุปกรณ์ผ่านแอปพลิเคชัน LINE

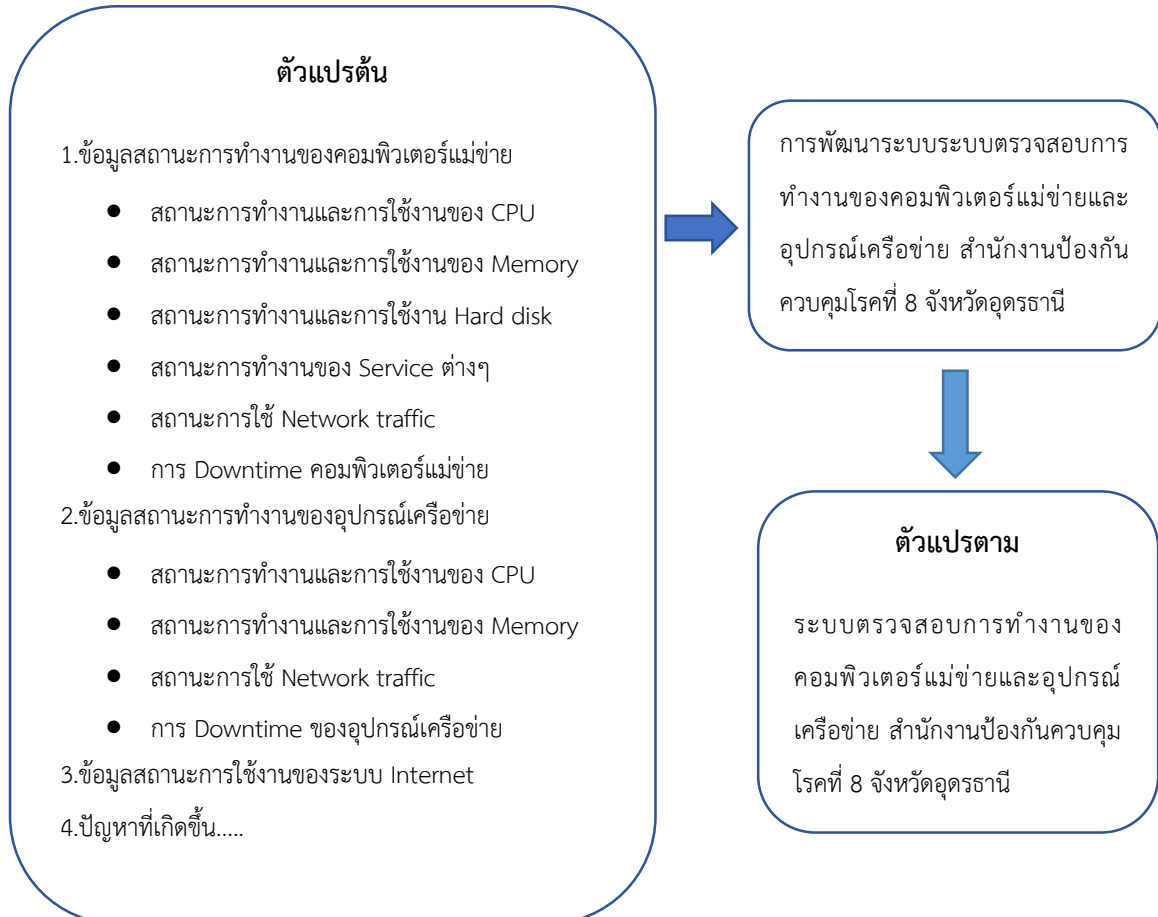
สิริวิชญ์ ธนาวิชญ์ (2561) ได้ทำการศึกษารื่อง “การตรวจสอบสถานะเครือข่ายด้วยแอปพลิเคชันไลน์” การศึกษาครั้งนี้เพื่อจัดการทำระบบมอนิเตอร์บนคอมพิวเตอร์ภายในเครือข่ายเพื่อจัดการควบคุมการทำงานของระบบต่าง ๆ ผ่านแอปพลิเคชัน โดยที่โปรแกรมจะสามารถจัดการผ่านทางแอปพลิเคชันไลน์ ทั้งบนมือถือ และเว็บไซต์ โปรแกรมดังกล่าวจะช่วยบริหารจัดการระบบเครือข่ายให้มีประสิทธิภาพ โดยตัวโปรแกรมจะทำงานผ่านระบบบอท ของแอปพลิเคชันไลน์ ผลการศึกษาพบว่า ระบบตรวจสอบสถานะเครือข่ายผ่านแอปพลิเคชันไลน์ สามารถตรวจสอบสถานะของเครื่องภายในเครือข่ายได้ สามารถสั่ง หยุด ทำงาน หรือรีสตาร์ทของระบบได้ สามารถแจ้งเตือนไปยังผู้ดูแล กรณีมีการเข้าใช้งานได้ และสามารถเรียก Animation ตรวจสอบสถานะของเครือข่ายได้

อนุพงษ์ โพธิ (2561) ได้ทำการศึกษารื่อง “การพัฒนา ระบบตรวจสอบการทำงานของระบบคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัยราชภัฏนครราชสีมา ผ่านเว็บเบราว์เซอร์” การศึกษาครั้งนี้เพื่อพัฒนาระบบตรวจสอบการทำงานของระบบคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัยราชภัฏนครราชสีมา ผ่านเว็บเบราว์เซอร์ที่มีการให้บริการระบบเครือข่ายเพื่อสนับสนุนการเรียน และการสอนรวมถึงงานบริการอื่น ๆ เช่นคอยเฝ้าระวังการใช้งานระบบเครือข่าย บริหารจัดการระบบเครือข่ายมหาวิทยาลัย เชื่อมระบบเครือข่ายอินเทอร์เน็ตและให้คำปรึกษาและแก้ไขปัญหาเกี่ยวกับงานระบบเครือข่ายคอมพิวเตอร์ให้แก่บุคลากรของมหาวิทยาลัยผลการศึกษาพบว่า ระบบตรวจสอบการทำงานของระบบคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัยราชภัฏนครราชสีมา ผ่านเว็บเบราว์เซอร์ โดยใช้ซอฟต์แวร์ประยุกต์ Cacti ติดต่อกับเครื่องคอมพิวเตอร์แม่ข่ายผ่านโพรโทคอล SNMP มาแสดงผลในระบบผ่านเว็บเบราว์เซอร์ เพื่อให้ผู้ดูแลระบบสามารถเข้าใจภาพรวมและตรวจสอบสถานะการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย โดยมีกลุ่มเป้าหมายคือ นักวิชาการคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏนครราชสีมาจำนวน 32 ท่าน ผลการทดลองใช้งานระบบและประเมินความพึงพอใจของกลุ่มเป้าหมายที่มีต่อประสิทธิภาพระบบโดยรวมอยู่ในระดับดีมาก

ณัฐพล ศิริรอดบาง (2563) ได้ทำการศึกษารื่อง “การออกแบบระบบติดตามสถานภาพเครื่องแม่ข่ายเสมือน และกู้คืนเว็บแอปพลิเคชัน ภายในระบบการประมวลผลแบบกลุ่มเมฆ ด้วยซอฟต์แวร์โอเพนซอร์ซ” การศึกษาครั้งนี้เพื่อ การออกแบบระบบติดตามสถานภาพเครื่องแม่ข่ายเสมือน

จากการศึกษา ได้แก่ 1) ออกแบบระบบติดตามสถานภาพเครื่องแม่ข่ายเสมือน 2) เพื่อให้มีระบบแจ้งเตือนผู้เกี่ยวข้องให้ทราบเมื่อเครื่องแม่ข่ายเสมือนทำงานผิดปกติ 3) เพื่อให้มีระบบตรวจสอบและการกู้คืนระบบเว็บแอปพลิเคชันภายในเครื่องแม่ข่ายเสมือน โดยระบบที่ออกแบบประกอบด้วย 4 ส่วนคือ 1) ส่วนฐานข้อมูลอนุกรมเวลาโดยใช้ซอฟต์แวร์ Prometheus 2) ส่วนชุดคำสั่งตรวจสอบสถานภาพเครื่องแม่ข่าย และเว็บแอปพลิเคชันโดยใช้โพรโทคอล SNMP, ICPM, TCP และ HTTP ร่วมกับชุดคำสั่งที่พัฒนาด้วยภาษาไพทอน 3) ส่วนแสดงผล และตรวจสอบสถานภาพโดยใช้ซอฟต์แวร์ Grafana 4) ส่วนชุดคำสั่งตรวจสอบ และกู้คืนระบบเว็บแอปพลิเคชัน ที่พัฒนาด้วยภาษาไพทอน ผลการศึกษาพบว่า จากการทดสอบส่วนติดตามสถานภาพ โดยการจำลองสถานการณ์ที่เครื่องแม่ข่ายเสมือนและเว็บแอปพลิเคชันมีสถานภาพผิดปกติ ระบบสามารถตรวจสอบพบความผิดปกติแล้วแจ้งเตือนไปยังผู้ดูแลระบบผ่านแอปพลิเคชัน LINE ได้ทุกครั้งที่ทดสอบ ในการทดสอบส่วนตรวจสอบ และกู้คืนเว็บแอปพลิเคชัน จากการจำลองสถานการณ์ความผิดปกติ พบว่าสามารถตรวจสอบปัญหา แล้วกู้คืนส่วนประกอบของเว็บแอปพลิเคชันให้กลับมาทำงานได้ปกติ และมีการแจ้งเตือนไปยังผู้ดูแลระบบผ่านแอปพลิเคชัน LINE

4. กรอบแนวคิดการพัฒนา



บทที่ 3

วิธีการดำเนินการ

การพัฒนากระบวนการตรวจสอบสถานการณ์ทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ผู้พัฒนาได้ดำเนินการขั้นตอน ดังต่อไปนี้

1. รูปแบบการศึกษา
2. เครื่องมือที่ใช้ในการดำเนินการ
3. เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล
4. วิธีการสร้างเครื่องมือการวิจัย
5. ขั้นตอนการวิจัย
6. รายละเอียดการดำเนินงาน

1. รูปแบบการศึกษา

การศึกษาครั้งนี้ผู้ศึกษาวางแผนการศึกษาในรูปแบบการวิจัยและพัฒนา (Research & Development)

2. เครื่องมือที่ใช้ในการดำเนินการ

เครื่องมือที่ใช้ในการศึกษา ออกแบบ และพัฒนา ระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ประกอบไปด้วย

2.1. อุปกรณ์คอมพิวเตอร์ (Hardware)

- เครื่องคอมพิวเตอร์แม่ข่าย HP ProLiant DL 360 Gen9 Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
- เครื่องคอมพิวเตอร์ Intel(R) Core (TM) i5 ขึ้นไป
- อุปกรณ์เครือข่ายคอมพิวเตอร์
- อุปกรณ์เครือข่ายคอมพิวเตอร์ไร้สาย

2.2. โปรแกรมคอมพิวเตอร์ (Software)

- ระบบปฏิบัติการ Linux CentOS (Version 9)
- ซอฟต์แวร์ Open Source Zabbix Version 6.4

- แอปพลิเคชันเซิร์ฟเวอร์ Apache (Version ไม่ต่ำกว่า 2.4)
- ระบบฐานข้อมูล MariaDB (Version ไม่ต่ำกว่า 10)

2.3. ภาษาคอมพิวเตอร์ (Computer Language)

- พีเอชพี (PHP Language)
- มายเอสคิวแอล (MySQL)

3. เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลในการศึกษาครั้งนี้ คือ ระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายผ่านโปรแกรม Zabbix Network Monitor (Open Source)

4. วิธีการสร้างเครื่องมือการวิจัย

วิธีการสร้างเครื่องมือที่ใช้ในการศึกษาครั้งนี้ ผู้ศึกษาได้ดำเนินการดังนี้ ดังต่อไปนี้

- 4.1 ศึกษาแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง เกี่ยวกับการตรวจสอบติดตามสถานะบนเครือข่าย เพื่อเป็นแนวทางในการพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
- 4.2 ศึกษาสำรวจ เปรียบเทียบ และการเลือกใช้งาน Network Monitoring Tools
- 4.3 ศึกษาการทำงานของ Zabbix Network Monitoring และ Zabbix Agent
- 4.4 ศึกษาการทำงานโพรโทคอลเอสเอ็นเอ็มพี (Protocol SNMP, ICMP)
- 4.5 ศึกษาการแจ้งเตือนผ่านแอปพลิเคชันไลน์ (LINE Notify, LINE TOKEN)
- 4.6 ศึกษาการใช้ Shell Script

5. ขั้นตอนการวิจัย

การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี จากการสำรวจ และเลือกใช้เครื่องมือการตรวจสอบเฝ้าระวังเครือข่าย (Network monitoring tools) ผู้ศึกษาได้ทำการเลือกใช้งาน Zabbix Network Monitoring ซึ่งมีเครื่องมือที่ใช้มีอินเตอร์ Web Application ,Hypervisor ,VM เหมาะสมกับการตรวจสอบคอมพิวเตอร์แม่ข่าย ซึ่งส่วนใหญ่จะเป็นรูปแบบ Virtual Machine นอกจากนี้ Zabbix

ยังสามารถติดตามการใช้งานผ่าน Zabbix Agent ทั้งยังรองรับการทำงานบนระบบปฏิบัติการที่หลากหลาย และอุปกรณ์เครือข่าย สามารถตรวจสอบได้โดยใช้โพรโตคอลเอสเอ็นเอ็มพี ซึ่งอุปกรณ์ที่ใช้งานส่วนใหญ่ ในปัจจุบันรองรับการทำงานบนโพรโตคอลเอสเอ็นเอ็มพี

5.1 การกำหนดปัญหา

5.1.1 ระบบการตรวจสอบสถานะทำงานแบบเดิม

จากการตรวจสอบสถานะทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายแบบเดิมพบว่าผู้ดูแลระบบจะต้องทำการตรวจสอบสถานะของอุปกรณ์ที่มีในหน่วยงานที่ละอุปกรณ์ ซึ่งในหน่วยงานมีจำนวนคอมพิวเตอร์แม่ข่ายทั้งหมด 5 เครื่อง และอุปกรณ์เครือข่าย Switch, Firewall, Access Point รวมทั้งหมด 18 เครื่อง ทำให้ต้องใช้เวลานานในการตรวจสอบสถานะ รวมถึงทำให้ไม่รู้ถึงปัญหาหรือความผิดปกติในระบบเครือข่ายจนกว่าปัญหาจะก่อให้เกิดผลกระทบต่อผู้ใช้งาน อาจทำให้การแก้ไขปัญหาใช้เวลาและทรัพยากรมากขึ้น

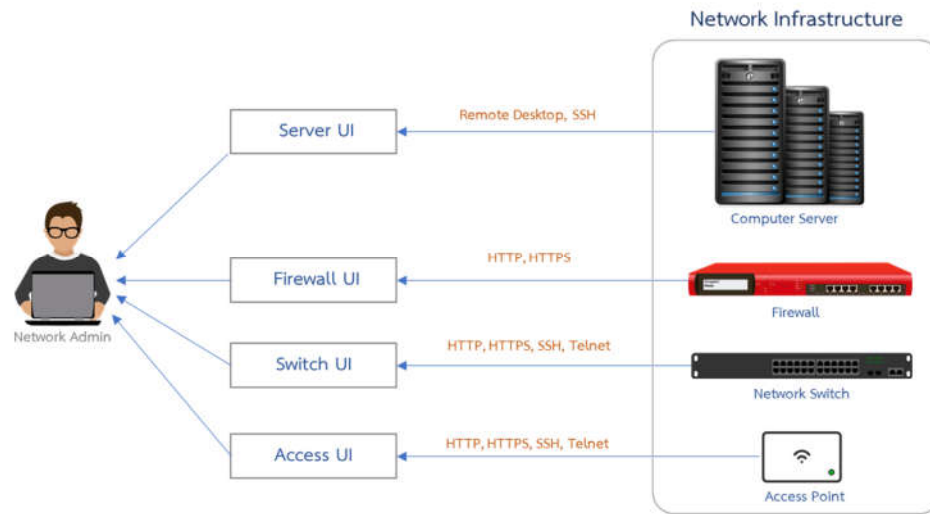
5.1.2 ระบบการตรวจสอบสถานะทำงานแบบใหม่

มีระบบตรวจสอบสถานะทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายที่สามารถตรวจสอบความผิดปกติได้ตลอดเวลา และสามารถแจ้งเตือนผู้ดูแลระบบหากมีความผิดปกติเกิดขึ้น

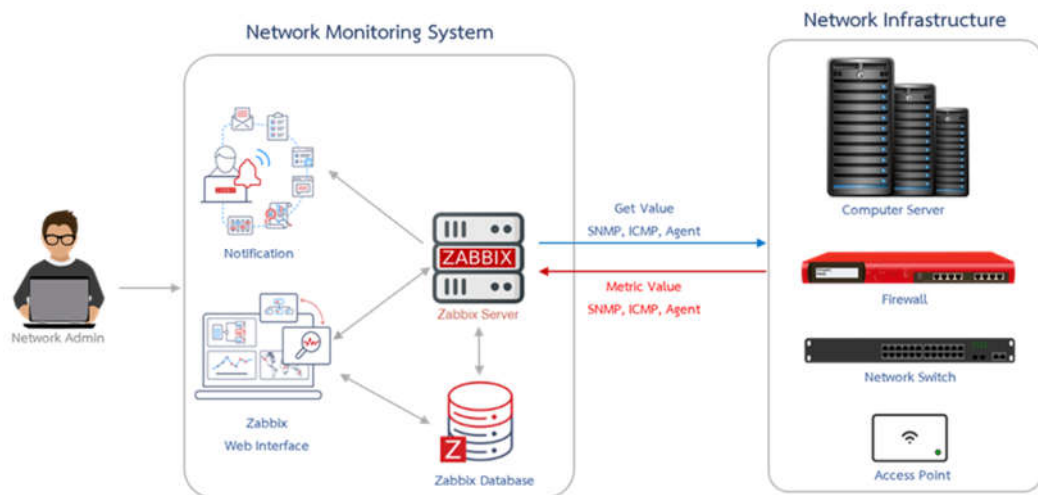
5.2 ศึกษาเอกสาร ผลงานวิชาการ ตำรา และงานวิจัยที่เกี่ยวข้อง

การวิเคราะห์ และออกแบบระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยการศึกษาการทำงานของระบบ Zabbix Network Monitoring เพื่อเก็บรายละเอียดสถานะการทำงานต่าง ๆ ของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ถ้ากรณีตัวอุปกรณ์มีปัญหาในการทำงานเกิดขึ้น เช่น เมื่อเกิดการ Up/Down ของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายตรงตามเงื่อนไขการติดตามสถานะที่ตั้งไว้ เมื่อตรงตามเงื่อนไขที่กำหนด ระบบก็จะทำการส่งแจ้งเตือนผ่านหน้า Dashboard Monitoring หรือแจ้งเตือนผ่านไลน์ให้ผู้ดูแลระบบทราบทันที การศึกษาระบบ Zabbix Network Monitoring จะอธิบายถึงการออกแบบและการพัฒนาโดยมีการเก็บข้อมูลดังต่อไปนี้

- 5.2.1 สถานะทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย รายละเอียดข้อมูลต่าง ๆ เช่น การใช้ซีพียู (CPU) ,หน่วยความจำ (Memory) ,การเชื่อมต่ออินเทอร์เน็ต (Interface) ,กราฟฟิกขาเข้า (traffic Sent) และขาออก (traffic received) เป็นต้น
- 5.2.2 การตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย ระบบจะทำการดึงข้อมูลจากตัว Agent โดยการติดตั้ง Zabbix Agent ที่เครื่องคอมพิวเตอร์แม่ข่าย สำหรับเก็บข้อมูลรายละเอียดสถานะการทำงานต่าง ๆ
- 5.2.3 การตรวจสอบการทำงานของอุปกรณ์เครือข่าย ระบบจะทำการดึงข้อมูลโดยผ่าน โพรโทคอลเอสเอ็นเอ็มพี (Protocol SNMP) ซึ่งเป็นการดึงค่าคอมมิวนิตีส์ตริงที่ได้ตั้งค่าไว้ในตัวอุปกรณ์เครือข่าย
- 5.2.4 ออกแบบระบบในส่วนของการแสดงผล ซึ่งจะทำการดึงข้อมูลมาจากฐานข้อมูล โดยในส่วนนี้จะมีการแสดงข้อมูลรายละเอียดต่าง ๆ สามารถทำการดึงข้อมูลออกมา แสดงให้อยู่ในรูปแบบของตัวเลข, ข้อความ และกราฟเพื่อให้ง่ายต่อการเข้าใจ ผ่านหน้า Dashboard
- 5.2.5 ออกแบบระบบในส่วนของการแจ้งเตือน และตรวจสอบโดยจะทำการตรวจสอบสถานะการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย สถานะออนไลน์ หรือออฟไลน์ รวมถึงการตรวจสอบกราฟฟิกขาเข้าและขาออกของแต่ละอินเทอร์เน็ตเฟซ กระทั่งตรวจสอบการทำงานของทรัพยากรที่อยู่บนคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ซึ่งการตรวจสอบจะตรวจสอบว่าหากเกินกว่าค่าที่กำหนดไว้หรือไม่ ถ้าเกินกว่าค่าที่กำหนดจะทำการแจ้งเตือนไปยังผู้ดูแลระบบ



ภาพที่ 13 ภาพรวมการตรวจสอบการทำงานของระบบเดิม



ภาพที่ 14 ภาพรวมการทำงานของระบบ Zabbix Network Monitor

6. รายละเอียดการดำเนินงาน

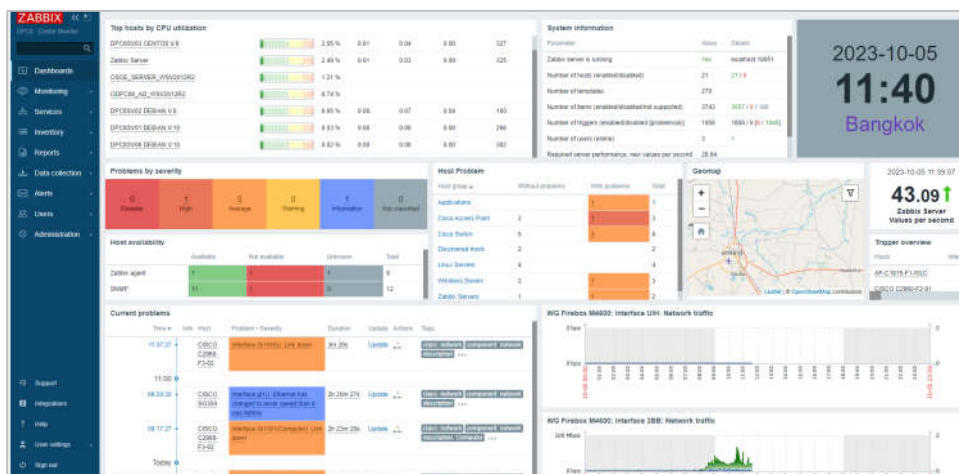
6.1. การจัดเตรียมเครื่องคอมพิวเตอร์แม่ข่าย

การเตรียมเครื่องคอมพิวเตอร์แม่ข่ายสำหรับการติดตั้ง Zabbix Server เพื่อระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ซึ่งโปรแกรม Zabbix Network Monitor เป็น Monitor Tools ที่ทำงานบนเว็บเซิร์ฟเวอร์ (Web Server) ดังนั้นจำเป็นต้องจัดเตรียมสภาพแวดล้อมให้พร้อมสำหรับการติดตั้ง Zabbix Network Monitor ดำเนินการดังนี้

- ติดตั้งและตั้งค่าระบบปฏิบัติการ Linux CentOS Version 9
- ติดตั้งแอปพลิเคชันเว็บเซิร์ฟเวอร์ Apache Version 2.4
- ติดตั้งและตั้งค่าฐานข้อมูล MariaDB Version 10
- ติดตั้งภาษาพีเอชพี PHP

6.2. การติดตั้ง Zabbix Server สำหรับโปรแกรม Zabbix Network Monitoring

การติดตั้งระบบตรวจสอบสถานะทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย หลังจากทำการจัดเตรียมสภาพแวดล้อมให้พร้อมสำหรับการติดตั้ง Zabbix Network Monitor ถัดไปจะเป็นการติดตั้ง Zabbix Server และทำการตั้งค่าการเชื่อมต่อฐานข้อมูล สำหรับเก็บข้อมูลการตรวจสอบสถานะการทำงานโดยมี Zabbix agent และโพรโทคอล SNMP คอยทำหน้าที่ส่งข้อมูลสถานะต่าง ๆ เข้ามาที่ Zabbix Server



ภาพที่ 15 แสดงหน้าภาพรวมของระบบ Zabbix Network Monitoring

6.3. การตั้งค่าคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

ก่อนที่จะทำการตั้งค่า Host เพื่อนำเข้ามาตรวจสอบสถานการณ์ทำงานในระบบ Zabbix Network Monitoring ให้ทำการติดตั้งและตั้งค่า Zabbix agent และโปรโตคอล SNMP ในเครื่องคอมพิวเตอร์แม่ข่ายและ อุปกรณ์เครือข่าย ที่จะนำข้อมูลเข้ามามอนิเตอร์ ดังต่อไปนี้

6.3.1 การติดตั้ง Zabbix Agent บนเครื่องคอมพิวเตอร์แม่ข่าย

- การติดตั้ง Zabbix Agent ระบบปฏิบัติการ Windows
- การติดตั้ง Zabbix Agent ระบบปฏิบัติการ Linux

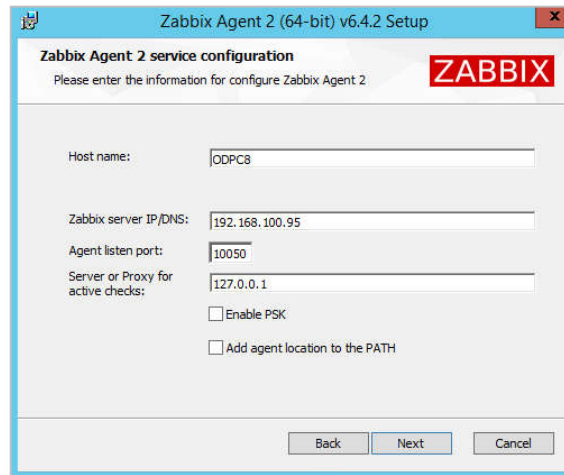
6.3.2 การตั้งค่าโปรโตคอล SNMP สำหรับมอนิเตอร์อุปกรณ์เครือข่าย

6.4. การติดตั้ง Zabbix Agent บนเครื่องคอมพิวเตอร์แม่ข่าย

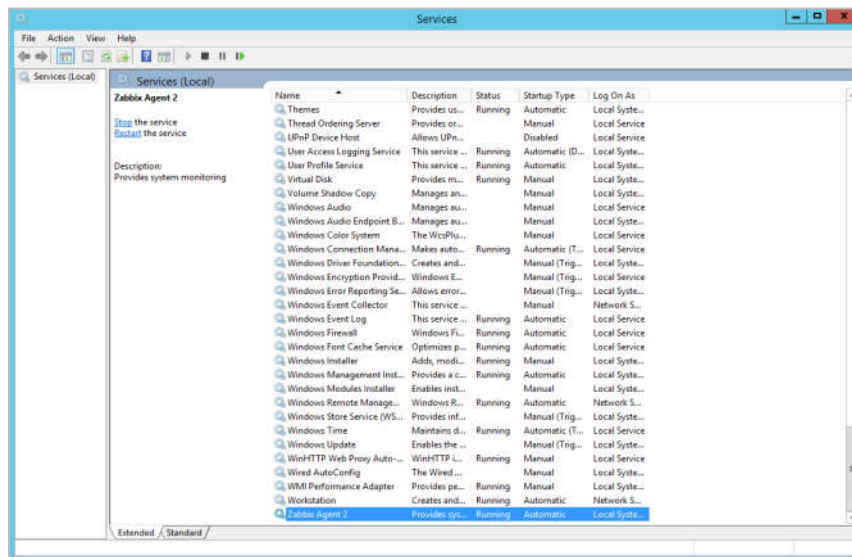
การตั้งค่าโปรโตคอล SNMP สำหรับมอนิเตอร์อุปกรณ์เครือข่าย การติดตั้ง Zabbix Agent บนเครื่องคอมพิวเตอร์แม่ข่าย เป็นการเชื่อมต่อระหว่าง Zabbix Server ให้สามารถรับข้อมูลค่าสถานะการทำงาน จากคอมพิวเตอร์แม่ข่าย เข้ามาจัดเก็บที่ฐานข้อมูลของระบบ Zabbix Network Monitoring และนำค่าที่ได้มาแสดงผลในรูปแบบต่าง ๆ เช่น ตัวเลข กราฟ เป็นต้น

6.4.1. การติดตั้ง Zabbix Agent ระบบปฏิบัติการ Windows

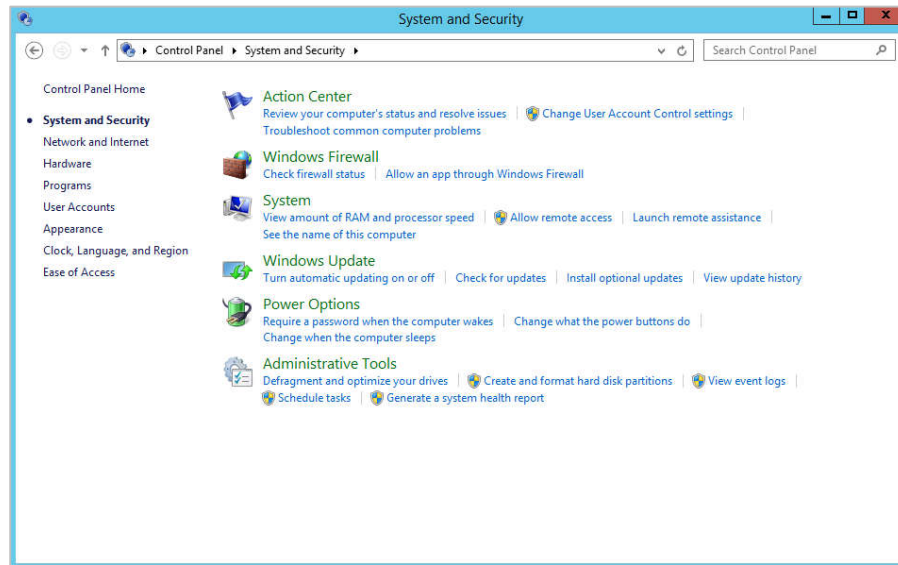
- ดาวน์โหลดและติดตั้ง Zabbix Agent สำหรับคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Windows
- กำหนดค่า Windows Firewall อนุญาตให้ Zabbix Agent สามารถสื่อสารกับ Zabbix Server
- ทำการทดสอบการทำงานของ Zabbix Agent บนคอมพิวเตอร์แม่ข่าย ให้สามารถเชื่อมต่อจาก Zabbix Server โดยใช้คำสั่ง telnet <Windows agent IP Address> 10050 หรือคำสั่ง ping <Windows agent IP Address>



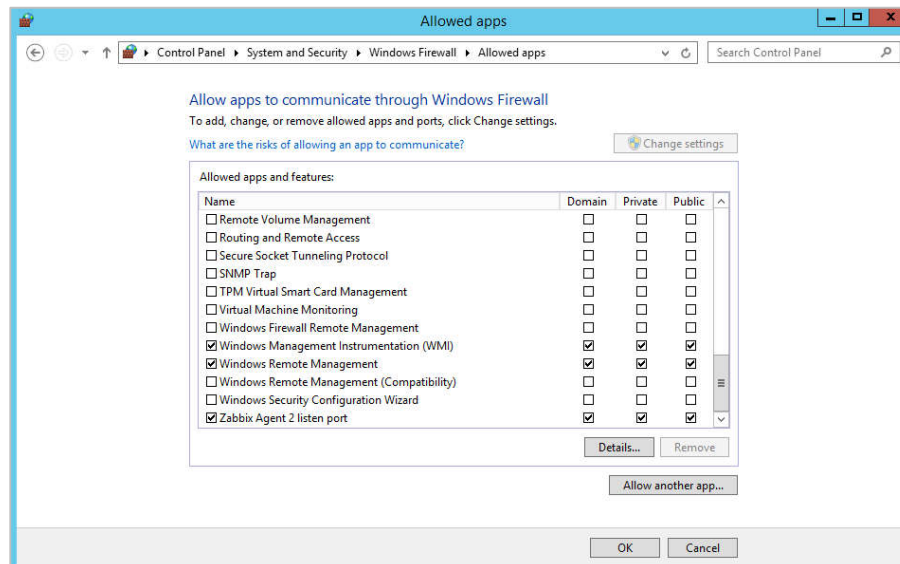
ภาพที่ 16 การติดตั้ง Zabbix Agent สำหรับคอมพิวเตอร์แม่ข่ายระบบปฏิบัติการ Windows



ภาพที่ 17 แสดงสถานะการทำงานของ Zabbix Agent



ภาพที่ 18 การกำหนดค่า Windows Firewall ในเครื่องคอมพิวเตอร์แม่ข่าย



ภาพที่ 19 การอนุญาต Zabbix Agent เชื่อมต่อกับ Zabbix Server

```
[root@localhost dpc8]# telnet 172.18.8.35 10050
Trying 172.18.8.35...
Connected to 172.18.8.35.
Escape character is '^'.
Connection closed by foreign host.
[root@localhost dpc8]#
```

ภาพที่ 20 การทดสอบการเชื่อมต่อระหว่าง Zabbix Sever กับ Zabbix Agent

```
[root@localhost dpc8]# ping 172.18.8.35
PING 172.18.8.35 (172.18.8.35) 56(84) bytes of data.
64 bytes from 172.18.8.35: icmp_seq=1 ttl=127 time=0.676 ms
64 bytes from 172.18.8.35: icmp_seq=2 ttl=127 time=0.651 ms
64 bytes from 172.18.8.35: icmp_seq=3 ttl=127 time=0.724 ms
64 bytes from 172.18.8.35: icmp_seq=4 ttl=127 time=0.676 ms
64 bytes from 172.18.8.35: icmp_seq=5 ttl=127 time=0.656 ms
64 bytes from 172.18.8.35: icmp_seq=6 ttl=127 time=0.674 ms
64 bytes from 172.18.8.35: icmp_seq=7 ttl=127 time=0.712 ms
64 bytes from 172.18.8.35: icmp_seq=8 ttl=127 time=0.702 ms
64 bytes from 172.18.8.35: icmp_seq=9 ttl=127 time=0.690 ms
```

ภาพที่ 21 การทดสอบการเชื่อมต่อระหว่าง Zabbix Sever กับ Zabbix Agent

6.4.2. การติดตั้ง Zabbix Agent ระบบปฏิบัติการ Linux

การติดตั้ง Zabbix Agent ระบบปฏิบัติการ Linux สามารถติดตั้งได้ทั้งแบบ Desktop หรือแบบ Command line ได้ ขึ้นอยู่กับเครื่องคอมพิวเตอร์แม่ข่าย ได้ลงระบบปฏิบัติการแบบใดไว้

- ดาวน์โหลดและติดตั้ง Zabbix Agent สำหรับคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Linux โดยใช้คำสั่ง `sudo apt-get install zabbix-agent -y`
- กำหนดค่าไฟร์วอลล์อนุญาตพอร์ต 10050, 10051 ให้ Zabbix Agent สามารถสื่อสารกับ Zabbix Server
- ตั้งค่าไฟล์ `zabbix_agentd.conf`
- โดยใช้คำสั่ง `nano /etc/zabbix/zabbix_agentd.conf` เปลี่ยน IP Address ให้เป็น IP Address ของเครื่องที่เป็น Zabbix Server แล้วทำการ Restart Zabbix agent service

- ทำการทดสอบการทำงานของ Zabbix Agent บนคอมพิวเตอร์แม่ข่าย ให้สามารถเชื่อมต่อจาก Zabbix Server โดยใช้คำสั่ง telnet <Windows agent IP Address> 10050 หรือคำสั่ง ping <Windows agent IP Address>

```
root@dpc8:/home/dpc8# sudo apt-get install zabbix-agent -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
zabbix-agent is already the newest version (1:4.0.4+dfsg-1+deb10u2).
The following package was automatically installed and is no longer required:
  linux-image-4.19.0-8-amd64
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 303 not upgraded.
root@dpc8:/home/dpc8#
```

ภาพที่ 22 การตั้งค่าติดตั้ง Zabbix Agent สำหรับคอมพิวเตอร์แม่ข่ายที่ใช้ ระบบปฏิบัติการ Linux

```
root@dpc8:/home/dpc8# sudo ufw allow 10050/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@dpc8:/home/dpc8# sudo ufw allow 10051/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@dpc8:/home/dpc8#
```

ภาพที่ 23 การกำหนดค่า Windows Firewall อนุญาตให้ Zabbix Agent

```
### Option: Server
# List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers and Zabbix proxies.
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', ':::127.0.0.1', '::ffff:127.0.0.1' are treated equally
# and ':::0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,:::1,2001:db8:::32,zabbix.example.com
#
Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=192.168.100.95

### Option: ListenPort
# Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
ListenPort=10050
```

ภาพที่ 24 การตั้งค่าไฟล์ zabbix_agentd.conf เพื่อเชื่อมต่อ Zabbix Server

```
[root@localhost dpc8]# telnet 192.168.100.92 10050
Trying 192.168.100.92...
Connected to 192.168.100.92.
Escape character is '^'.
Connection closed by foreign host.
[root@localhost dpc8]#
```

ภาพที่ 25 การทดสอบการเชื่อมต่อระหว่าง Zabbix Sever กับ Zabbix Agent

6.5. การตั้งค่าโปรโตคอล SNMP สำหรับอุปกรณ์เครือข่ายเพื่อตรวจสอบสถานะการทำงานผ่านโปรแกรม Zabbix Network Monitoring

```
Switch(config)#snmp-server community public ro
Switch(config)#snmp-server enable traps snmp
Switch(config)#snmp-server contact "NHA"
Switch(config)#snmp-server location "NHA"
Switch(config)#snmp-server host 172.16.4.180 version 2c public udp-port 162
Switch(config)#
```

ภาพที่ 26 การตั้งค่าโปรโตคอล SNMP สำหรับอุปกรณ์เครือข่าย

```
[root@zabbix-server-lab ~]# snmpwalk -v2c -c public 172.16.10.3
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software (C3750E-UNIVERSALK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 05-May-11 15:40 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.516
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (157929124) 18 days, 6:41:31.24
SNMPv2-MIB::sysContact.0 = STRING: "NHA"
SNMPv2-MIB::sysName.0 = STRING: Switch
SNMPv2-MIB::sysLocation.0 = STRING: "NHA"
SNMPv2-MIB::sysServices.0 = INTEGER: 6
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-SMI::enterprises.9.7.129
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-SMI::enterprises.9.7.115
SNMPv2-MIB::sysORID.3 = OID: SNMPv2-SMI::enterprises.9.7.205
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-SMI::enterprises.9.7.112
SNMPv2-MIB::sysORID.5 = OID: SNMPv2-SMI::enterprises.9.7.106
SNMPv2-MIB::sysORID.6 = OID: SNMPv2-SMI::enterprises.9.7.47
SNMPv2-MIB::sysORID.7 = OID: SNMPv2-SMI::enterprises.9.7.122
SNMPv2-MIB::sysORID.8 = OID: SNMPv2-SMI::enterprises.9.7.135
SNMPv2-MIB::sysORID.9 = OID: SNMPv2-SMI::enterprises.9.7.43
SNMPv2-MIB::sysORID.10 = OID: SNMPv2-SMI::enterprises.9.7.37
SNMPv2-MIB::sysORID.11 = OID: SNMPv2-SMI::enterprises.9.7.92
SNMPv2-MIB::sysORID.12 = OID: SNMPv2-SMI::enterprises.9.7.53
SNMPv2-MIB::sysORID.13 = OID: SNMPv2-SMI::enterprises.9.7.54
SNMPv2-MIB::sysORID.14 = OID: SNMPv2-SMI::enterprises.9.7.52
SNMPv2-MIB::sysORID.15 = OID: SNMPv2-SMI::enterprises.9.7.93
SNMPv2-MIB::sysORID.16 = OID: SNMPv2-SMI::enterprises.9.7.186
```

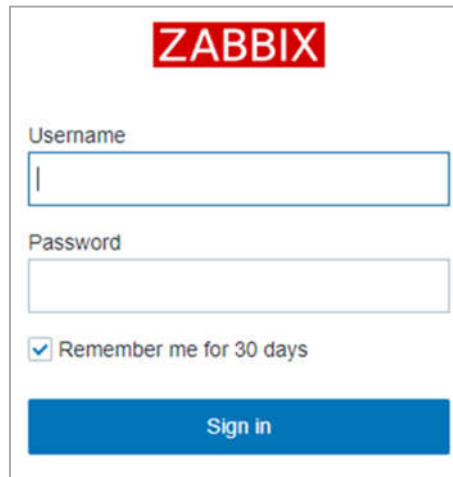
ภาพที่ 27 การทดสอบการเชื่อมต่อโปรโตคอล SNMP

6.6. การตั้งค่าโปรแกรม Zabbix Network Monitoring

เมื่อติดตั้ง Zabbix Server และทำการกำหนดค่าของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ให้สามารถส่งข้อมูลเพื่อสำหรับการมอนิเตอร์เสร็จแล้ว ขั้นตอนต่อไปคือการตั้งค่าระบบ Zabbix Network Monitoring ให้สามารถรับข้อมูลเพื่อตรวจสอบคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย และให้สามารถแจ้งเตือนไปยังผู้ดูแลระบบได้ ด้วยมีขั้นตอนดังต่อไปนี้

6.6.1 การเพิ่มกลุ่มโฮสสำหรับการมอนิเตอร์ (Create host group)

6.6.2 การเพิ่มโฮสสำหรับการมอนิเตอร์ (Create host)



ZABBIX

Username

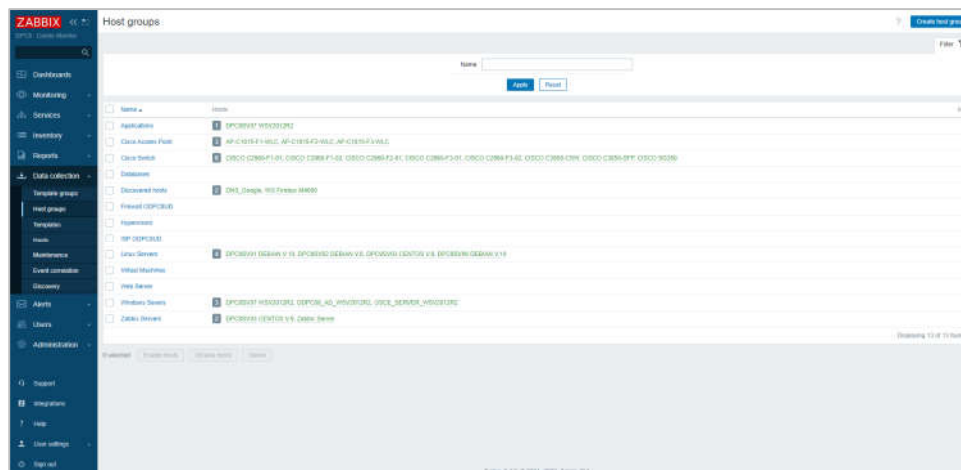
Password

Remember me for 30 days

Sign in

ภาพที่ 28 หน้าล็อกอินเข้าโปรแกรม Zabbix Network Monitoring

6.6.3 การเพิ่มกลุ่มโฮสสำหรับการมอนิเตอร์ (Create host group) เป็นการจัดกลุ่มของอุปกรณ์เครือข่ายภายในระบบ Zabbix Network Monitoring เพื่อให้ผู้ดูแลระบบสามารถจำแนกประเภทของอุปกรณ์เครือข่าย และง่ายต่อการบริหารจัดการอุปกรณ์ที่อยู่ในระบบ



ภาพที่ 29 แสดงกลุ่มโฮสทั้งหมด

ภาพที่ 30 การเพิ่มกลุ่มโฮสสำหรับการมอนิเตอร์

6.5.4 การเพิ่มโฮสสำหรับการมอนิเตอร์ เป็นการเพิ่มเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย เข้าระบบ Zabbix Network Monitoring โดยทำการ Create host ทำการตั้งค่า Host name, Templates, Host groups เลือก Interfaces เป็น Agent หรือ SNMP ในการส่งข้อมูลไปยัง Zabbix Server โดยเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ที่ทำการเพิ่มเข้าไปทั้งหมดจะแสดงในหน้า Host ในระบบ ในส่วนของ อุปกรณ์เครือข่ายตรงหัวข้อ Interfaces ให้เลือกเป็น SNMP และทำการใส่ค่า SNMP community ในหัวข้อ Macros

ภาพที่ 31 การเพิ่มโฮสสำหรับการมอนิเตอร์ในระบบ Zabbix Network Monitoring

The screenshot shows the 'New host' dialog box with the 'Macros' tab selected. There is a table for adding macros:

Macro	Value	Description
{SMACRO}	value	description

Buttons for 'Add' and 'Cancel' are visible at the bottom right.

ภาพที่ 32 การเพิ่มค่า SNMP Community สำหรับการตรวจสอบผ่านโปรโตคอล SNMP

Name	Hosts	Triggers	Graphs	Discovery	Web interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
AP-C1815-F1-W5.C	Items: 11	Triggers: 4	Graphs: 0	Discovery: 0	Web: 192.168.101.21:161		Giacca IOS by SNMP	Enabled	100%	None		
AP-C1815-F2-W5.C	Items: 11	Triggers: 4	Graphs: 0	Discovery: 0	Web: 192.168.102.21:161		Giacca IOS by SNMP	Enabled	100%	None		
AP-C1815-F3-W5.C	Items: 11	Triggers: 4	Graphs: 0	Discovery: 0	Web: 192.168.103.21:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C2386-F1-01	Items: 300	Triggers: 177	Graphs: 18	Discovery: 0	Web: 192.168.100.13:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C2386-F1-02	Items: 348	Triggers: 163	Graphs: 18	Discovery: 0	Web: 192.168.100.14:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C2386-F2-01	Items: 307	Triggers: 172	Graphs: 18	Discovery: 0	Web: 192.168.100.15:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C2386-F3-01	Items: 346	Triggers: 161	Graphs: 18	Discovery: 0	Web: 192.168.100.16:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C2386-F3-02	Items: 300	Triggers: 176	Graphs: 18	Discovery: 0	Web: 192.168.100.17:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C3850-C5W	Items: 105	Triggers: 104	Graphs: 10	Discovery: 0	Web: 192.168.100.10:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-C3850-SFP	Items: 302	Triggers: 151	Graphs: 12	Discovery: 0	Web: 192.168.100.11:161		Giacca IOS by SNMP	Enabled	100%	None		
CBSCO-SG350	Items: 381	Triggers: 175	Graphs: 12	Discovery: 0	Web: 192.168.100.18:161		Giacca IOS by SNMP	Enabled	100%	None		
ENS_Storage	Items: 3	Triggers: 2	Graphs: 0	Discovery: 0	Web: 8.8.8.8:10050		ICMP Ping	Enabled	100%	None		
EPIC85V01-DEWAN-V-10	Items: 11	Triggers: 23	Graphs: 10	Discovery: 0	Web: 192.168.100.100:10050		Linux by Zabbix agent	Enabled	100%	None		
EPIC85V02-DEWAN-V-8	Items: 11	Triggers: 23	Graphs: 10	Discovery: 0	Web: 192.168.100.90:10050		Linux by Zabbix agent	Enabled	100%	None		
EPIC85V03-CENTOS-V-9	Items: 79	Triggers: 35	Graphs: 15	Discovery: 0	Web: 192.168.100.85:10050		Linux by Zabbix agent	Enabled	100%	None		
EPIC85V06-DEWAN-V-10	Items: 11	Triggers: 23	Graphs: 10	Discovery: 0	Web: 192.168.100.62:10050		Linux by Zabbix agent	Enabled	100%	None		
EPIC85V07-WIN90012R2	Items: 127	Triggers: 62	Graphs: 14	Discovery: 0	Web: 192.168.100.8:10050		Windows by Zabbix agent	Enabled	100%	None		
OPPCBA_AD-WIN90012R2	Items: 108	Triggers: 45	Graphs: 11	Discovery: 0	Web: 172.16.8.35:10050		Windows by Zabbix agent	Enabled	100%	None		
OPPCBA_S6303R-WIN90012R2	Items: 108	Triggers: 23	Graphs: 11	Discovery: 0	Web: 172.16.8.201:10050		Windows by Zabbix agent	Enabled	100%	None		

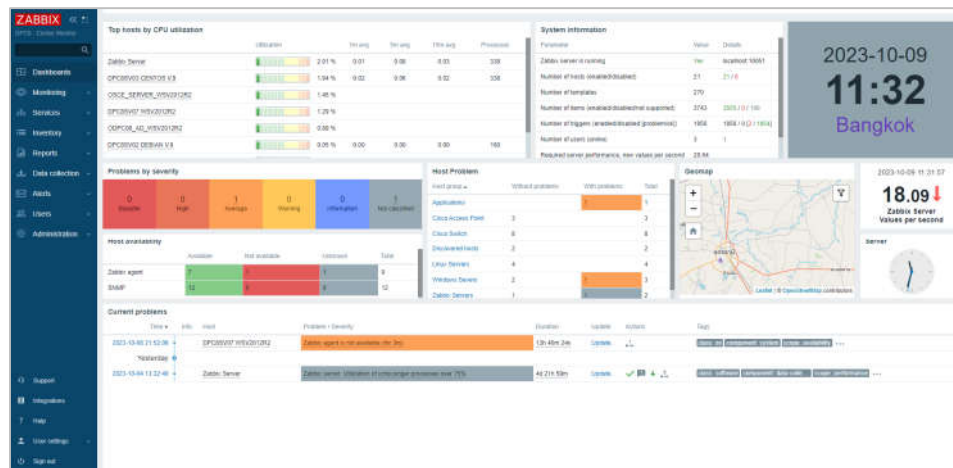
ภาพที่ 33 แสดงโฮสต์ที่เพิ่มเข้าในระบบ Zabbix Network Monitoring ทั้งหมด

6.7. การตั้งค่าการแจ้งเตือนไปยังผู้ดูแลระบบ

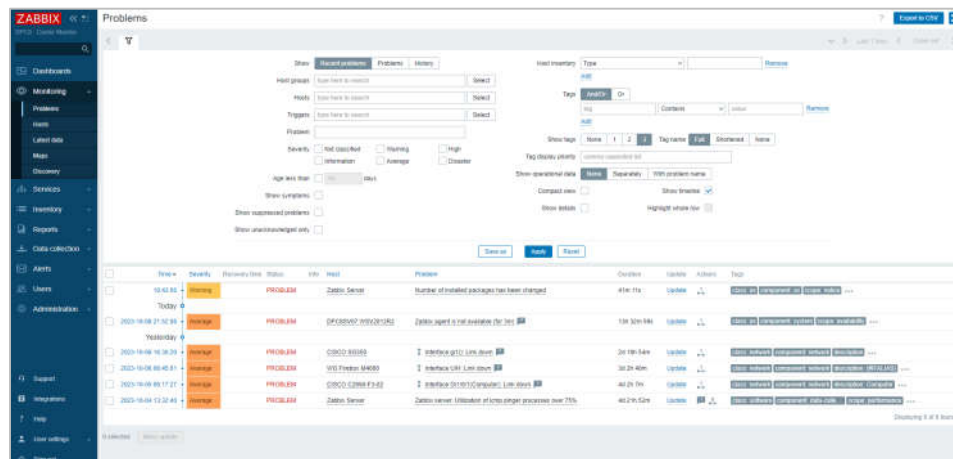
เมื่อทำการสร้าง Host groups และทำการเพิ่ม Host เสร็จเรียบร้อยแล้ว ขั้นตอนต่อไปจะเป็นการตั้งค่าการแจ้งเตือนให้ระบบ Zabbix Network Monitoring นั้น สามารถแจ้งเตือนการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ในช่องทางการแจ้งเตือนต่าง ๆ ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบประสิทธิภาพของระบบเครือข่าย และแก้ไขปัญหาที่เกิดขึ้นได้

การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี นั้น มีการแจ้งเตือนของระบบ Zabbix Network Monitoring หลัก ๆ อยู่ 2 ช่องทาง ดังนี้

6.7.1 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring และจะแสดงภาพรวมออกมาในหน้า Dashboard ของระบบ



ภาพที่ 34 การแจ้งเตือนความผิดปกติผ่านหน้า Dashboard Zabbix Network Monitoring

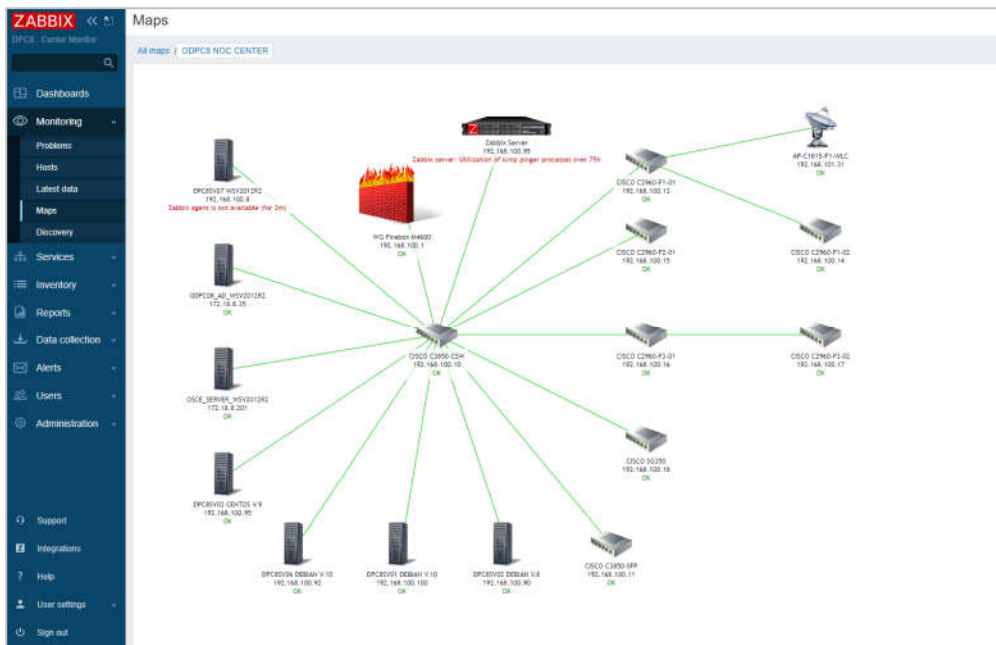


ภาพที่ 35 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Problems ในโปรแกรม Zabbix Network Monitoring

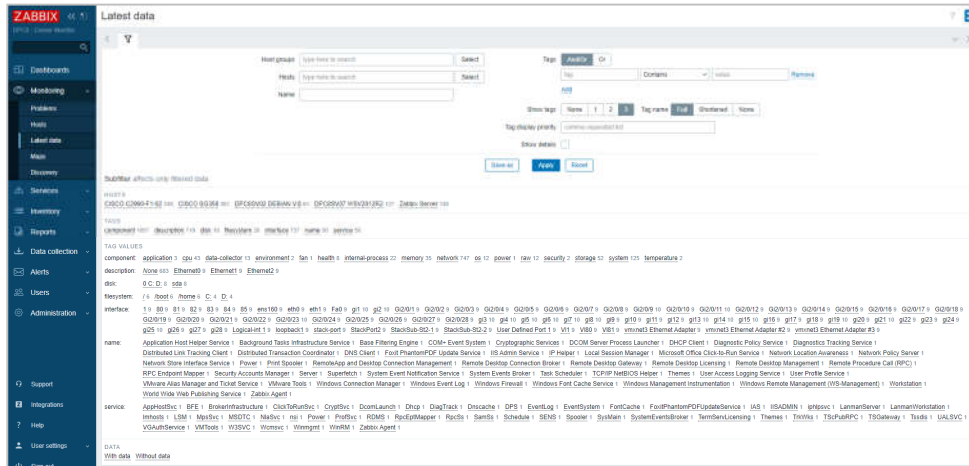
The screenshot shows the Zabbix web interface with the 'Monitoring' view selected. The main area displays a table of monitored hosts. Each row represents a host with various attributes. The 'Availability' column uses color-coded icons to indicate the health of the host. The 'Problems' column shows the number of active issues for each host. The 'Checks' column indicates the number of checks performed. The 'Dashboards' column lists the dashboards associated with each host. The 'Map' column shows the map associated with each host. The interface includes a sidebar with navigation options and a top navigation bar with filters and search options.

Name	Interface	Availability	Type	Status	Latest data	Problems	Checks	Dashboards	Map
AP-C1818F-P1-MLC	192.168.102.31-191	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
AP-C1818F-P2-MLC	192.168.102.31-191	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
AP-C1818F-P3-MLC	192.168.102.31-191	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.12-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-02	192.168.100.14-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.15-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.16-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.17-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.18-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.19-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.20-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.21-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.22-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.23-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.24-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.25-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.26-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.27-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.28-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.29-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.30-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.31-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.32-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.33-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.34-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.35-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.36-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.37-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.38-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.39-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.40-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.41-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.42-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.43-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.44-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.45-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.46-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.47-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.48-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.49-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map
OSCO-C2960-F2-01	192.168.100.50-181	OK	Cisco Catalyst	OK	Latest data: 15	Problems	Checks	Dashboards: 1	Map

ภาพที่ 36 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Host
 ในโปรแกรม Zabbix Network Monitoring



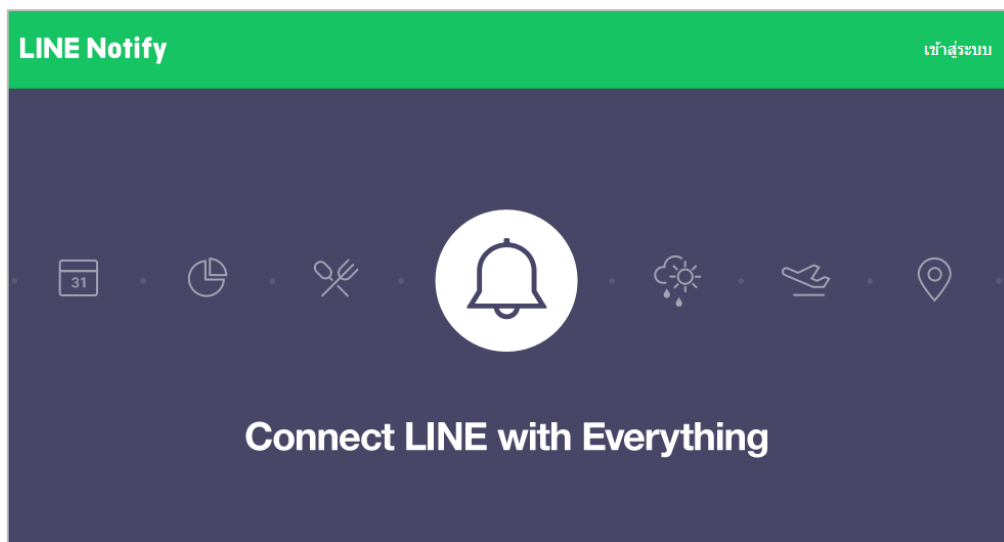
ภาพที่ 37 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Map
 ในโปรแกรม Zabbix Network Monitoring



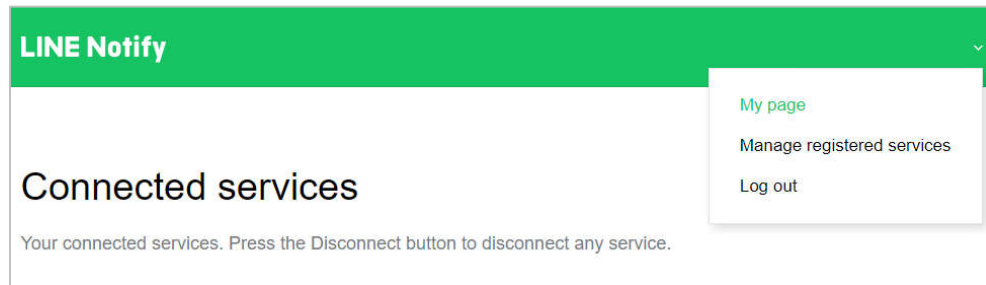
ภาพที่ 38 การแจ้งเตือนความผิดปกติผ่านหน้าเว็บเมนู Monitoring, Latest data เพื่อดูข้อมูลล่าสุด ในโปรแกรม Zabbix Network Monitoring

6.7.2 การแจ้งเตือนผ่าน LINE Application จะส่งข้อความแจ้งเตือนเมื่ออุปกรณ์ในระบบเครือข่ายทำงานผิดพลาด ตามที่ผู้ดูแลระบบได้กำหนดค่าไว้ โดยการตั้งค่าให้ระบบ Zabbix Network Monitoring ให้สามารถทำการแจ้งเตือนผ่าน LINE Application ได้มีขั้นตอนดังนี้

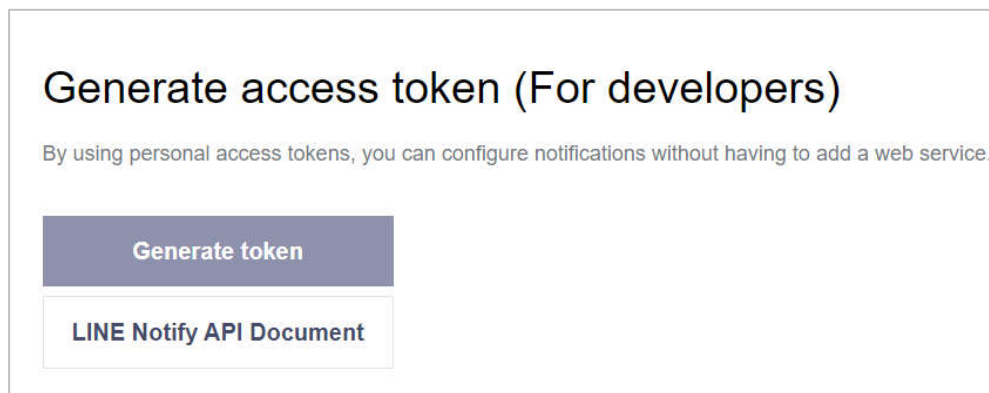
การส่งการแจ้งเตือนโปรแกรม Zabbix Network Monitoring จำเป็นต้องมี Token ของ LINE Notify เพื่อใช้เป็นช่องทางการเชื่อมต่อระหว่างตัวระบบกับ LINE Application โดยการออก Token ต้องล็อกอินเข้าเว็บไซต์ <https://notify-bot.line.me/th/>



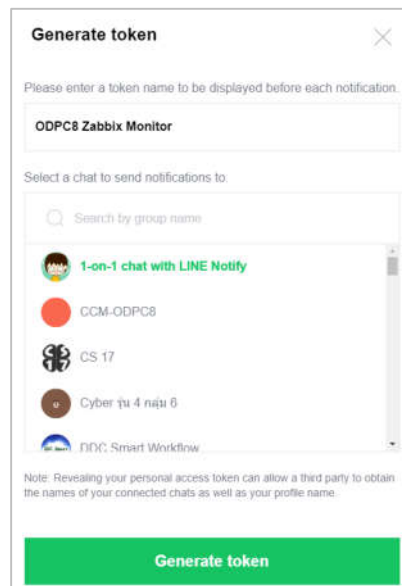
ภาพที่ 39 เข้าล็อกอินเข้าเว็บไซต์ LINE Application



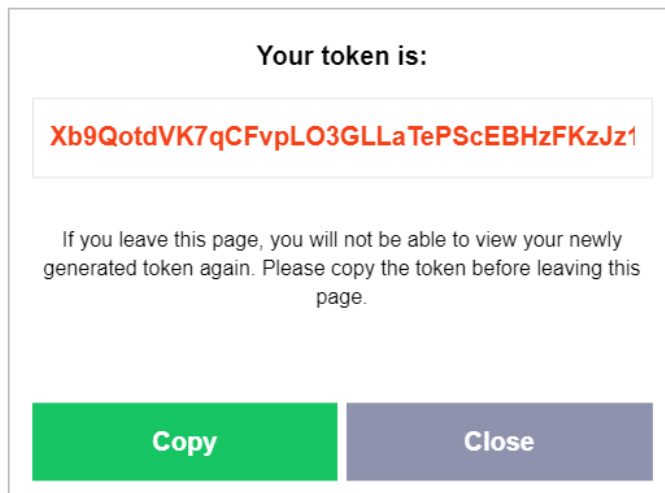
ภาพที่ 40 เข้าหน้าเว็บสำหรับการออก LINE Token



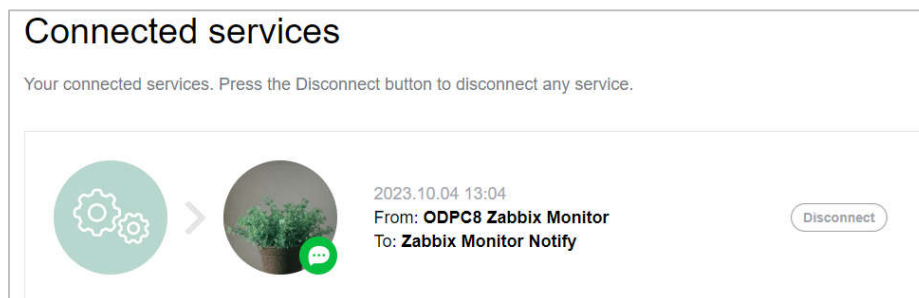
ภาพที่ 41 ทำการ Generate access token



ภาพที่ 42 ตั้งชื่อสำหรับการแจ้งเตือน และเลือกกลุ่มหรือบุคคลที่ต้องการแจ้งเตือน



ภาพที่ 43 ภาพแสดง Token key สำหรับการแจ้งเตือน



ภาพที่ 44 ภาพแสดงการเชื่อมต่อการให้บริการ LINE Notify

เมื่อทำการออก Token ทำการเชื่อมต่อระหว่างตัว LINE Application กับบริการ LINE Notify ขั้นตอนต่อไปทำการตั้งค่าแจ้งเตือนในโปรแกรม Zabbix Network Monitoring โดยการสร้าง Bash Script ให้ระบบ Zabbix Network Monitoring ซึ่งจะอยู่ใน Zabbix Sever ทำการเรียกใช้จาก Media types ซึ่งได้เขียนคำสั่งสำหรับการแจ้งเตือนเมื่ออุปกรณ์ทำงานผิดปกติ ประกอบไปด้วย ชื่อของ Media type รูปแบบการเรียกใช้งาน ชื่อของ Script พร้อมด้วย ตัวแปรที่จะถูกส่งต่อไปยัง LINE Notify

Name	Type	Status	Used in actions	Details	Action
Device one	Webhook	Disabled			Test
Device 2	Webhook	Disabled			Test
Email	Email	Disabled			Test
Email (HTML)	Email	Disabled			Test
Event Device/Device	Webhook	Disabled			Test
Equipment	Webhook	Disabled			Test
Canvas	Webhook	Disabled			Test
IPMI	Webhook	Disabled			Test
Console	Email	Disabled			Test
Console	Email	Disabled			Test
Cart	Webhook	Disabled			Test
File	Webhook	Disabled			Test
API	Webhook	Disabled			Test
Java RemoteControl	Webhook	Disabled			Test
API with CarbonFields	Webhook	Disabled			Test
Linux	Webhook	Disabled			Test
Line Notify	Script	Enabled	Line Notify Action	Script name: 'line-notify'	Test
Managed/Agent Service/Out	Webhook	Disabled			Test
Management	Webhook	Disabled			Test
MS Teams	Webhook	Disabled			Test
Outlook	Email	Disabled			Test
Outlook (new)	Email	Disabled			Test

ภาพที่ 45 หน้าแสดง Media types ทั้งหมดในระบบ

ทำการสร้างไฟล์ Bash Script ใน Directory Path : /usr/lib/zabbix/alertscripts/
สร้างไฟล์ line-notify

```
[root@localhost dpc8]# cd /usr/lib/zabbix/alertscripts/
[root@localhost alertscripts]# nano line-notify
[root@localhost alertscripts]#
```

ภาพที่ 46 การสร้างไฟล์ LINE Notify สำหรับการเขียนคำสั่งในการแจ้งเตือน
เขียนคำสั่งในไฟล์ LINE Notify

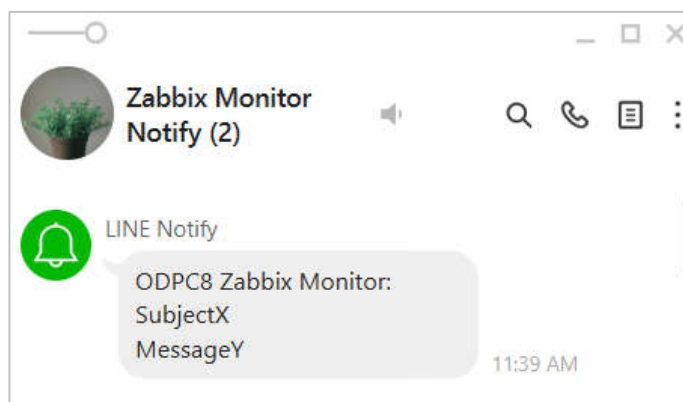
```
GNU nano 5.6.1 line-notify
#!/bin/bash
curl -X POST -H "Authorization: Bearer $1" -F "message=$2"
$3" https://notify-api.line.me/api/notify
```

ภาพที่ 47 คำสั่งในการแจ้งเตือนไฟล์ LINE Notify

ทดสอบการทำงานไฟล์ Script line-notify โดยใช้คำสั่ง #bash line-notify “ใส่ LINE TOKEN” SubjectX MessageY ระบบจะแจ้งเตือนตามข้อความที่ทำการทดสอบแสดงว่า LINE Notify สามารถทำการแจ้งเตือนได้

```
[root@localhost alertscripts]# bash line-notify mlx80NB4DwpDMPtVbxQ1D9NI3AlmHUAdAT35xB5R1vh SubjectX MessageY {"status":200,"message":"ok"}[root@localhost alertscripts]#
```

ภาพที่ 48 การทดสอบการแจ้งเตือนโดยการส่งข้อความที่กำหนดไปยัง LINE Notify



ภาพที่ 49 ข้อความที่ทดสอบแสดงการแจ้งเตือน LINE Notify

เมื่อทำการเพิ่ม Bash Script ลงใน Zabbix Server เรียบร้อยแล้ว ให้ทำการล็อกอินเข้าหน้าระบบ Zabbix Network Monitoring ผ่านหน้าเว็บ เพื่อทำการตั้งค่าการแจ้งเตือน

เมนู Media types ใส่รายละเอียดข้อมูล

- Name: Line-Notify (ชื่อ Media ที่ต้องการใส่)
- Type: Script (เลือก Type ให้ตรง)
- Script name: line-notify (ชื่อ Bash Script ที่เราสร้างและตั้งค่าใน Zabbix Server)
- Script parameters: เพิ่มเพื่อรับค่า Parameters ที่มาจาก Bash Script ต้องการแจ้งเตือน {ALERT.SENDTO}, {ALERT.SUBJECT}, {ALERT.MESSAGE}

Media types

Media type | Message templates | Options

* Name:

Type:

* Script name:

Script parameters ?

Value	Action
<input type="text" value="{ALERT.SENDTO}"/>	Remove
<input type="text" value="{ALERT.SUBJECT}"/>	Remove
<input type="text" value="{ALERT.MESSAGE}"/>	Remove
Add	

Description:

Enabled:

[Add](#) [Cancel](#)

ภาพที่ 50 ข้อความที่ทดสอบแสดงการแจ้งเตือน LINE Notify

Name	Type	Status	Script name
Line-Notify	Script	Enabled	line-notify
Line-Notify-Action	Line Notify Action	Enabled	Script name: "line-notify"

ภาพที่ 51 แสดง Media types การแจ้งเตือนที่ทำการเพิ่มเข้าในระบบ

Test media type "Line-Notify"

Media type test successful.

Script parameters ?

[Test](#) [Cancel](#)

ภาพที่ 52 ทดสอบการแจ้งเตือนของ Media types

6.8. การสร้าง Users เพื่อให้ระบบ Zabbix Network Monitoring แจ้งเตือน

เมื่อทำการสร้าง Media types เสร็จแล้ว ให้ทำการสร้าง Users เพื่อให้ระบบ Zabbix Network Monitoring แจ้งเตือนไป โดยการสร้าง Users ที่ต้องการ ในหัวข้อย่อย Users ใส่รายละเอียด Username, Groups, Time zone เป็นต้น ในหัวข้อย่อย Media เป็นการสร้าง Media โดยเลือกจาก Media types ใส่ LINE Token ตรงเมนู Send to แล้วกำหนดเวลาในการทำงาน เงื่อนไขที่จะทำการส่งข้อความแจ้งเตือน และทำการ Enabled Media เพื่อให้สามารถใช้งานได้

The screenshot shows the 'Users' configuration page in Zabbix. The 'User' tab is selected, and the following fields are visible:

- Username:** gantawut
- Name:** Gantawut
- Last name:** Ganyanuch
- Groups:** Internal, Zabbix administrators
- Password:** Change password
- Language:** English (en_US)
- Time zone:** System default: (UTC+07:00) Asia/Bangkok
- Theme:** Blue
- Auto-login:**
- Auto-logout:** 15m
- Refresh:** 30s
- Rows per page:** 50
- URL (after login):** (empty)

Buttons: Update, Delete, Cancel

ภาพที่ 53 การเพิ่ม Users สำหรับการแจ้งเตือน

The screenshot shows the 'Media' configuration page for the user 'gantawut'. The table below shows the media configuration:

Media	Type	Send to	When active	Use if severity	Status	Action
Line-Notify	m1xBONB4DwPpDMP1vbxQ1D9Ni3AlmHUAqAT35xB5R1vh	1-7,00:00-24:00	[N I W A H D]	Enabled	Edit	Remove

Buttons: Update, Delete, Cancel

ภาพที่ 54 การเพิ่ม Media สำหรับการแจ้งเตือน Users

ภาพที่ 55 การเพิ่ม Media กำหนดเวลา และเงื่อนไขสำหรับการส่งข้อความแจ้งเตือนไปยัง Users

6.9. การสร้าง Action เพื่อให้ระบบ Zabbix Network Monitoring แจ้งเตือน

เมื่อทำการสร้าง Users เสร็จแล้ว ให้ทำการสร้าง Action ขึ้นมาโดยเข้าไปที่เมนู Alerts -> Action -> Trigger action -> create action ทำการเพิ่มชื่อ Action และเพิ่มเงื่อนไขในการแจ้งเตือนตามค่าที่ได้กำหนดไว้

ภาพที่ 56 เป็นการแสดงรายละเอียดในการตั้งค่า Action ในหัวข้อ Action Users

เป็นการแสดงรายละเอียดในการตั้งค่า Action ในหัวข้อ Operation เพิ่มเข้าไปเป็นส่วนของการส่งข้อความแจ้งเตือน เมื่ออุปกรณ์เครือข่ายเกิดการทำงานผิดปกติ ระบบจะส่งข้อมูลแจ้งเตือน

ปัญหาที่เกิดขึ้น ตามที่ได้ตั้งค่าการแจ้งเตือนไว้ ทำการส่งเป็นข้อความไปยัง LINE Notify เพื่อส่งให้กลุ่มผู้ดูแลได้ทราบ และ ในหัวข้อ Recovery operations ระบบก็จะส่งข้อความแจ้งเตือนเมื่ออุปกรณ์เครือข่ายกลับมาทำงานได้อย่างเป็นปกติ

The screenshot shows the 'Action' configuration window. At the top, there's a 'Default operation step duration' set to '1h'. Below this, there are three sections: 'Operations', 'Recovery operations', and 'Update operations'. Each section has a table with columns for 'Steps', 'Details', 'Start in', 'Duration', and 'Action'. The 'Operations' section has one step: '1 Send message to users: gantawut (Gantawut Ganyanuch) via Line-Notify' with 'Immediately' start and 'Default' duration. The 'Recovery operations' and 'Update operations' sections are currently empty. There are 'Add' buttons for each section. Below these sections are three checkboxes: 'Pause operations for symptom problems', 'Pause operations for suppressed problems', and 'Notify about canceled escalations', all of which are checked. A note at the bottom says '* At least one operation must exist.' and there are buttons for 'Update', 'Clone', 'Delete', and 'Cancel'.

ภาพที่ 57 เป็นการแสดงรายละเอียดในการตั้งค่า Action

เป็นการแสดง Action ที่สร้างขึ้นมา เงื่อนไข การส่งข้อความไปยัง Users และสถานะการเปิดใช้งาน Action นั้นด้วย

The screenshot shows the 'Trigger actions' interface. It has a table with columns 'Name' and 'Conditions'. The first row is 'Line-Notify Action' with the condition 'Trigger severity is greater than or equals Not classified'. Below this, there's a table for 'Operations' with columns 'Operations' and 'Status'. The first row is 'Send message to users: gantawut (Gantawut Ganyanuch) via Line-Notify' with a status of 'Enabled'. At the bottom right, it says 'Displaying 1 of 1 found'.

ภาพที่ 58 เป็นการแสดง Trigger Action ที่สร้างขึ้น

บทที่ 4

ผลการดำเนินการ

การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี โดยใช้โปรแกรม Zabbix Network Monitoring เพื่อตรวจสอบสถานะการทำงาน และติดตามประสิทธิภาพ ความพร้อมใช้งานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายภายในหน่วยงาน ติดตามการทำงานของอุปกรณ์ดังกล่าวผ่านทาง Zabbix Agent ซึ่งรองรับการทำงานบนระบบปฏิบัติการที่หลากหลาย เช่น Windows, Linux เป็นต้น หรือในส่วนของอุปกรณ์เครือข่ายสามารถตรวจสอบผ่านโพรโทคอล SNMP โดยระบบ Zabbix Network Monitoring ยังมีการแจ้งเตือนเมื่อตรวจพบเหตุการณ์ที่ผิดปกติภายในระบบเครือข่าย สามารถคาดการณ์แนวโน้มของการใช้ traffic ทั้งยังสามารถคาดการณ์พฤติกรรมจากประวัติการใช้งาน รวมทั้งสามารถปรับแต่งตั้งค่า Web UI ได้ตามความต้องการ ทำให้ผู้ดูแลระบบสามารถตรวจสอบได้อย่างรวดเร็วและวิเคราะห์ข้อมูลเพื่อปรับปรุง เพิ่มประสิทธิภาพของระบบเครือข่าย นอกจากนี้ยังช่วยให้มีการดูแลระบบอย่างต่อเนื่องและป้องกันปัญหาที่อาจเกิดขึ้น และมีประสิทธิภาพมากขึ้น และมีผลการศึกษาเป็นไปตามวัตถุประสงค์ของการดำเนินงานในครั้งนี้ คือ

1. เพื่อพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี
2. เพื่อให้ผู้ดูแลระบบทราบอย่างทันเวลา เมื่อมีการทำงานผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี

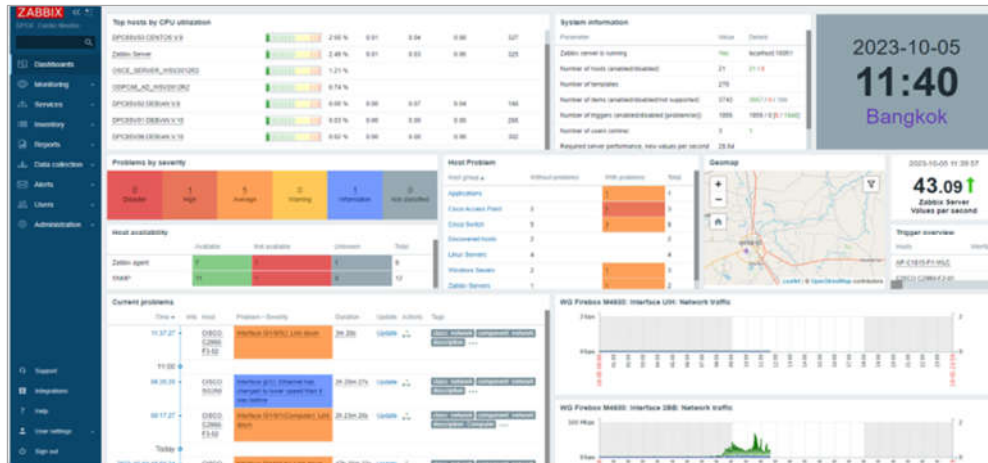
1. การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ฯ

ระบบ Zabbix Monitoring มีการทำงานในการตรวจสอบคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย จากค่าที่ได้ทำการตั้งค่าไว้ ซึ่งผู้ดูแลระบบสามารถเข้าใช้งานระบบผ่านทางเว็บเบราว์เซอร์ (Web Browser) ได้ ซึ่งการทำงานของระบบมีหลัก ๆ อยู่ 3 อย่าง ดังนี้

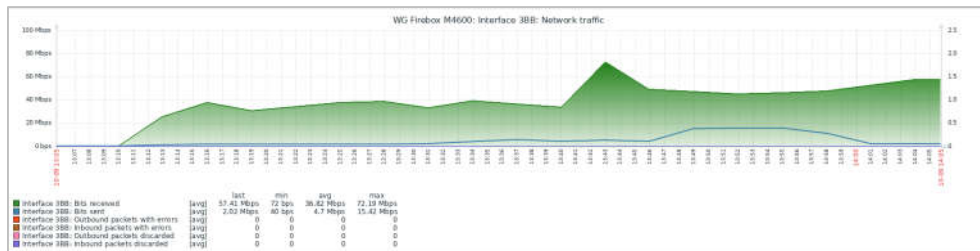
- 1.1 หน้าแสดงผลภาพรวมของระบบ Zabbix Network Monitoring
- 1.2 หน้าแสดงผลการตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย
- 1.3 การแจ้งเตือนข้อความไปยังผู้ดูแลระบบ

1.1 หน้าแสดงผลภาพรวมของระบบ Zabbix Network Monitoring

หน้าแสดงผลภาพรวมของระบบ Zabbix Network Monitoring เป็นการแสดงในรูปแบบของหน้าแดชบอร์ด (Dashboards) แสดงการแจ้งเตือนสถานะต่าง ๆ ของอุปกรณ์ภายในระบบเครือข่ายให้ผู้ดูแลระบบได้ทราบผ่านทางเว็บเบราว์เซอร์ (Web Browser)

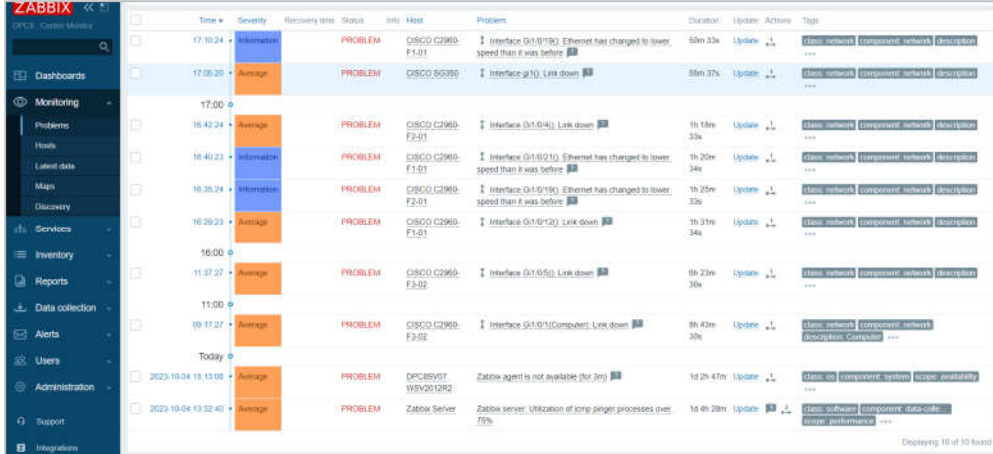


ภาพที่ 59 หน้าแสดงหน้ารวมของระบบ Zabbix Network Monitoring



ภาพที่ 60 กราฟแสดงข้อมูล Traffic การใช้อินเทอร์เน็ตของหน่วยงาน

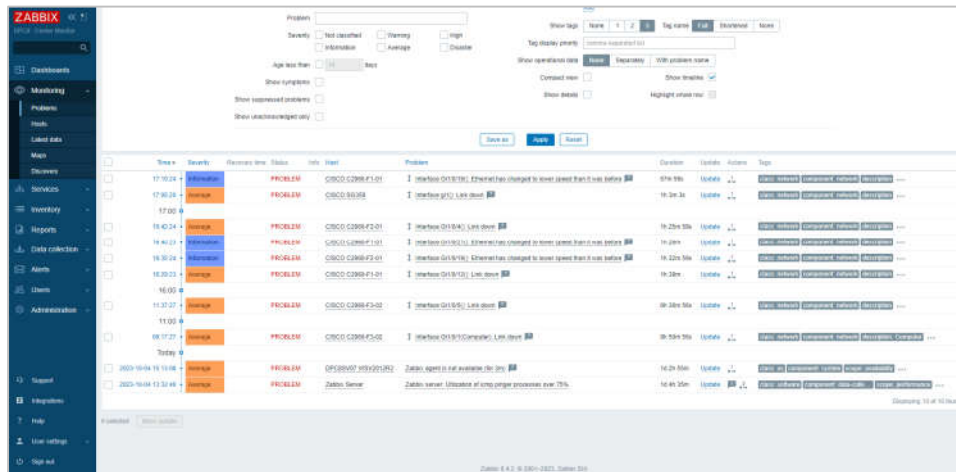
1.2 หน้าแสดงผลการตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย เมื่อมีการทำงานผิดปกติเกิดขึ้น



Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
17:10:24	Information		PROBLEM		CISCO-C2960-F1-01	Interface Gi1/0/120: Ethernet has changed to lower speed than it was before	50m 33s	Update	↓	class:network (component:network) (description:)
17:08:29	Average		PROBLEM		CISCO-S35380	Interface gi1/0: Link down	8m 37s	Update	↓	class:network (component:network) (description:)
17:00										
16:42:24	Average		PROBLEM		CISCO-C2960-F2-01	Interface Gi1/0/40: Link down	1h 18m 35s	Update	↓	class:network (component:network) (description:)
16:40:23	Information		PROBLEM		CISCO-C2960-F1-01	Interface Gi1/0/120: Ethernet has changed to lower speed than it was before	1h 20m 34s	Update	↓	class:network (component:network) (description:)
16:35:24	Information		PROBLEM		CISCO-C2960-F2-01	Interface Gi1/0/190: Ethernet has changed to lower speed than it was before	1h 25m 35s	Update	↓	class:network (component:network) (description:)
16:30:23	Average		PROBLEM		CISCO-C2960-F1-01	Interface Gi1/0/120: Link down	1h 31m 34s	Update	↓	class:network (component:network) (description:)
16:00										
11:37:27	Average		PROBLEM		CISCO-C2960-F3-02	Interface Gi1/0/50: Link down	6h 29m 30s	Update	↓	class:network (component:network) (description:)
09:17:27	Average		PROBLEM		CISCO-C2960-F3-02	Interface Gi1/0/1(Computer): Link down	8h 43m 30s	Update	↓	class:network (component:network) (description:Computer)
Today										
2023-10-04 15:13:03	Average		PROBLEM		DPCCBSVST-WBY2012R2	Zabbix agent is not available (for 3m)	1d 2h 47m	Update	↓	class:os (component:system) (scope:availability)
2023-10-04 13:32:40	Average		PROBLEM		Zabbix Server	Zabbix server: Utilization of icmp ping processes over 75%	1d 4h 28m	Update	↓	class:software (component:data:code) (scope:performance)

ภาพที่ 61 การตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

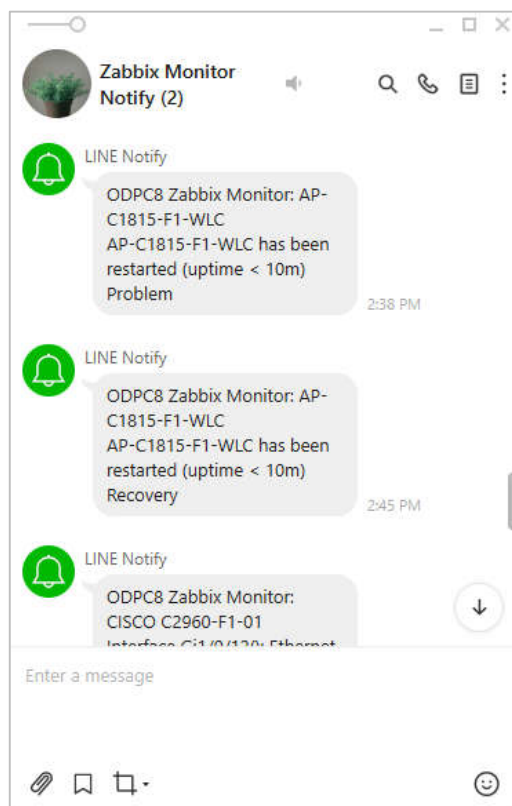
1.3 การแจ้งเตือนผู้ดูแลระบบ เมื่อการทำงานเกิดความผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ระบบ Zabbix Network Monitoring จะทำการแจ้งเตือนไปยัง ผู้ดูแลระบบ โดยแจ้งเตือนผ่านทางเว็บเบราว์เซอร์ (Web Browser) ของระบบและการแจ้ง เตือนผ่าน LINE Notify



Severity	Problem time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
Information	17:10:24	PROBLEM		CISCO-C2960-F1-01	Interface Gi1/0/120: Ethernet has changed to lower speed than it was before	50m 33s	Update	↓	class:network (component:network) (description:)
Average	17:08:29	PROBLEM		CISCO-S35380	Interface gi1/0: Link down	8m 37s	Update	↓	class:network (component:network) (description:)
	17:00								
Average	16:42:24	PROBLEM		CISCO-C2960-F2-01	Interface Gi1/0/40: Link down	1h 18m 35s	Update	↓	class:network (component:network) (description:)
Information	16:40:23	PROBLEM		CISCO-C2960-F1-01	Interface Gi1/0/120: Ethernet has changed to lower speed than it was before	1h 20m 34s	Update	↓	class:network (component:network) (description:)
Information	16:35:24	PROBLEM		CISCO-C2960-F2-01	Interface Gi1/0/190: Ethernet has changed to lower speed than it was before	1h 25m 35s	Update	↓	class:network (component:network) (description:)
Average	16:30:23	PROBLEM		CISCO-C2960-F1-01	Interface Gi1/0/120: Link down	1h 31m 34s	Update	↓	class:network (component:network) (description:)
	16:00								
Average	11:37:27	PROBLEM		CISCO-C2960-F3-02	Interface Gi1/0/50: Link down	6h 29m 30s	Update	↓	class:network (component:network) (description:)
Average	09:17:27	PROBLEM		CISCO-C2960-F3-02	Interface Gi1/0/1(Computer): Link down	8h 43m 30s	Update	↓	class:network (component:network) (description:Computer)
	Today								
Average	2023-10-04 15:13:03	PROBLEM		DPCCBSVST-WBY2012R2	Zabbix agent is not available (for 3m)	1d 2h 47m	Update	↓	class:os (component:system) (scope:availability)
Average	2023-10-04 13:32:40	PROBLEM		Zabbix Server	Zabbix server: Utilization of icmp ping processes over 75%	1d 4h 28m	Update	↓	class:software (component:data:code) (scope:performance)

ภาพที่ 62 แสดงการแจ้งเตือนของ Trigger เมื่อเกิดปัญหา

การแจ้งเตือนผ่านแจ้งเตือนผ่าน LINE Application เมื่อเกิดความผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายการทำงานผิดปกติ เช่น เกิดการ Down หรือ บริเวณที่มีอุปกรณ์เครือข่ายติดตั้งอยู่ เกิดไฟดับนานเกินที่เครื่องสำรองไฟจะทำงานได้ ระบบก็จะทำการแจ้งเตือนความผิดปกติที่เกิดขึ้น โดย Tigger จะทำการส่งให้ Action ทำงาน และเรียก Media ที่ตั้งค่าเรียกใช้ไฟล์ Alert Scripts บน Zabbix Server เพื่อทำการส่งข้อมูลไปยัง LINE Application ผ่านแจ้งเตือนผ่านบริการ LINE Notify และจะทำการแจ้งเตือนอีกครั้งหลังจากอุปกรณ์เครือข่าย หรือเหตุการณ์กลับมาเป็นปกติ



ภาพที่ 63 แสดงการแจ้งเตือนผ่าน LINE เมื่อเกิดปัญหา

สรุปผลการดำเนินการพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ทำผู้ดูแลระบบสามารถบริหารจัดการระบบเครือข่ายได้อย่างสะดวก รวดเร็ว สามารถตรวจสอบค่าข้อมูลสถานะต่าง ๆ

ในตัวของอุปกรณ์ ทำให้ระบบเครือข่ายทำงานอย่างมีประสิทธิภาพ ปลอดภัย นอกจากนี้ยังช่วยป้องกันปัญหาที่จะเกิดขึ้น ได้อย่างมีประสิทธิภาพ

2. ผลจากการใช้งานระบบระบบพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ฯ

จากการใช้งานระบบดังกล่าว ที่พัฒนาขึ้นมาพบว่ามีอาการแจ้งเตือนในกรณีที่เกิดความผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายของหน่วยงาน ซึ่งระบบมีการแจ้งเตือนผ่านหน้าเว็บเบราว์เซอร์ และผ่าน LINE Application ทันที เมื่ออุปกรณ์ในระบบเครือข่ายเกิดความผิดปกติ ทำให้ผู้รับผิดชอบสามารถรับทราบถึงปัญหา และดำเนินการแก้ไขได้อย่างทันเวลา โดยมีรายละเอียดดังต่อไปนี้

- จากการใช้งานระบบที่ผ่านมา มีการแจ้งเตือนความผิดปกติของคอมพิวเตอร์แม่ข่ายจำนวน 10 ครั้ง และการแจ้งเตือนความผิดปกติของอุปกรณ์เครือข่าย จำนวน 20 ครั้ง
- จากการแจ้งเตือนการทำงานที่ผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย คิดเป็นร้อยละ 90% ที่ผู้ดูแลระบบสามารถแก้ไขปัญหาได้ทันทีหลังจากเกิดการแจ้งเตือน นั้น ผลการใช้งานตรงตามวัตถุประสงค์ของผู้ศึกษา และประสิทธิภาพของระบบโดยรวมอยู่ในระดับดี

บทที่ 5

สรุปผลการศึกษา อภิปรายผลการศึกษา และข้อเสนอแนะ

การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี มีวัตถุประสงค์ 1) เพื่อพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี 2) เพื่อให้ผู้ดูแลระบบของหน่วยงานทราบอย่างทันเวลา เมื่อมีการทำงานผิดปกติของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายสำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี สรุปผลได้ดังนี้

1. สรุปผลการศึกษา

จากการศึกษาการพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ผู้ศึกษาได้บรรลุวัตถุประสงค์ การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ตามวัตถุประสงค์ที่ 1 ทำให้หน่วยงานมีระบบเพื่อช่วยในการตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายได้อย่างมีประสิทธิภาพและปลอดภัย เช่น การตรวจสอบฮาร์ดแวร์ การตรวจสอบการทำงานของเครือข่าย การบันทึกเหตุการณ์ และการดูแลรักษาอุปกรณ์ ทำให้ผู้ดูแลระบบของหน่วยงาน ได้ทราบถึงเหตุการณ์ที่เกิดขึ้นเพื่อตรวจสอบความผิดปกติ และปัญหาในระบบ ลดความเสี่ยงที่จะเกิด และดำเนินการแก้ไขได้อย่างเหมาะสม มีประสิทธิภาพ

การแจ้งเตือนการทำงานของระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย มีระบบแจ้งเตือนให้ผู้ดูแลระบบทราบ เมื่อมีเหตุการณ์ที่ผิดปกติที่เกิดขึ้นในเครือข่ายของหน่วยงาน ทำการแจ้งเตือนผ่านหน้าเว็บเบราว์เซอร์ (Web Browser) ของระบบ Zabbix Network Monitoring แสดงในรูปแบบของหน้า Dashboards และการแจ้งเตือนผ่าน LINE Application โดยการใช้บริการ LINE Notify ทำให้ผู้ดูแลระบบสามารถแก้ไขปัญหาได้ทันที สามารถช่วยลดเวลาตรวจสอบปัญหาที่เกิดขึ้นในระบบ และยังช่วยลดเวลาในการกู้คืนระบบได้

2. อภิปรายผลการศึกษา

จากผลการศึกษาเรื่อง การพัฒนาระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี ผู้ศึกษาสามารถอภิปรายผลได้ดังนี้

2.1 จากผลการพัฒนาระบบทำให้ สำนักงานป้องกันควบคุมโรคที่ 8 จังหวัดอุดรธานี มีระบบตรวจสอบการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายในหน่วยงาน ซึ่งการทำงานของระบบพบว่าโปรแกรมสามารถแสดงข้อมูลสถานะการทำงานของคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ปริมาณการใช้งานในระบบเครือข่าย โดยส่งข้อมูลผ่าน Zabbix Agent และโพรโทคอล SNMP สามารถแสดงผลข้อมูลผ่านหน้า Dashboard ของระบบ เป็นหน้าจอที่สรุปข้อมูลทุกอย่างให้อยู่ในหน้าจอเดียว เพื่อช่วยให้สะดวกต่อการตรวจสอบสถานะการทำงานของ และยังทำให้ผู้ดูแลระบบเครือข่ายเข้าใจได้ทันที เมื่อมีเหตุการณ์ที่ผิดปกติที่เกิดขึ้นในระบบเครือข่ายของหน่วยงานทำให้สามารถตรวจสอบ วิเคราะห์ ปัญหาที่เกิดขึ้นได้ ซึ่งสอดคล้องกับการศึกษาของ อติชาติ พัทธรักษ์ ที่ได้ทำการศึกษาเรื่อง “ระบบการแจ้งเตือนและตอบโต้ของ ZABBIX ด้วยแอปพลิเคชัน LINE (ZABBIX Monitoring Alert and Reply with LINE Application)” ประพันธ์ ไชยชนะ ได้ทำการศึกษาเรื่อง “ระบบตรวจสอบการทำงานของระบบเครือข่ายและแจ้งเตือนผ่านแอปพลิเคชัน LINE” และ ณัฐพล ศรีรอดบาง ได้ทำการศึกษาเรื่อง “การออกแบบระบบติดตามสถานะภาพเครื่องแม่ข่ายเสมือน และกู้คืนเว็บแอปพลิเคชัน ภายในระบบการประมวลผลแบบกลุ่มเมฆด้วยซอฟต์แวร์โอเพนซอร์ซ” โดยการศึกษาทำให้มีระบบที่สามารถตรวจสอบทำงานของอุปกรณ์ภายในระบบเครือข่าย เมื่ออุปกรณ์ในระบบเครือข่าย เช่น คอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายที่มีสถานะการทำงานผิดปกติ และสามารถกู้คืนระบบเว็บแอปพลิเคชันภายในเครื่องแม่ข่ายระบบก็จะแจ้งเตือนข้อผิดพลาดไปยังผู้รับผิดชอบ ทำให้ผู้รับผิดชอบบริหารจัดการระบบ และสามารถใช้ความผิดปกตินั้นได้ทันเวลา

2.2 จากผลการพัฒนาระบบทำให้ มีระบบแจ้งเตือนให้ผู้ดูแลระบบทราบ เมื่อมีเหตุการณ์ที่ผิดปกติที่เกิดขึ้นในระบบเครือข่ายของหน่วยงาน โดยทำการแจ้งเตือนผ่านหน้าเว็บเบราว์เซอร์ (Web Browser) ของระบบ Zabbix Network Monitoring แสดงในรูปแบบของหน้า Dashboards และการแจ้งเตือนผ่าน LINE Application ซึ่งสอดคล้องกับงานวิจัยของ อติชาติ พัทธรักษ์ ที่ได้ทำการศึกษาเรื่อง “ระบบการแจ้งเตือนและตอบโต้ของ ZABBIX ด้วยแอปพลิเคชัน LINE”

และ ประพันธ์ ไชยชนะ ได้ทำการศึกษาค้นคว้าเรื่อง “ระบบตรวจสอบการทำงานของระบบเครือข่ายและแจ้งเตือนผ่านแอปพลิเคชัน LINE” มีการแจ้งเตือนของระบบเมื่ออุปกรณ์ทำงานผิดปกติ จะทำการแจ้งเตือนผ่านหน้าเว็บเบราว์เซอร์ (Web Browser) และการแจ้งเตือนผ่าน LINE Application ได้

3. ข้อเสนอแนะ

3.1 จากผลการศึกษา Zabbix Network Monitoring สามารถนำไปพัฒนาประยุกต์ใช้ในการตรวจสอบสถานะการทำงานอย่างอื่นได้ นอกเหนือจากเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย เช่น เว็บไซต์ (Website), ฐานข้อมูล (Database) เป็นต้น

3.2 จากการแจ้งเตือนทั่วไปที่ระบบสามารถทำได้ การพัฒนาต่อไปจำเป็นต้องมีการแจ้งเตือนผ่านระบบให้รองรับการแจ้งเตือนในช่องทางอื่นนอกเหนือจาก LINE Application เพื่อให้มีความหลากหลายในการแจ้งเตือน

3.3 เนื่องจากระบบ Zabbix Network Monitoring เป็น Open source ทำให้ผู้ใช้งานสามารถตั้งค่าการใช้งาน และการแจ้งเตือนได้อย่างอิสระ ดังนั้นในการตั้งค่าการแจ้งเตือนผู้ใช้งานจำเป็นต้องศึกษาเรื่องของการเขียน Shell Script, Tagging, Macros เพื่อใช้ในการระบบแจ้งเตือนได้ตามความต้องการ

3.4 พัฒนาฐานข้อมูลเพื่อรองรับการเก็บข้อมูลค่าสถานะ นำมาบันทึกจัดเก็บ ประมวลผล แสดงผลข้อมูลให้ผู้ดูแลระบบ แต่ยังสามารถช่วยวิเคราะห์ข้อมูลเหล่านั้น และยังสามารถทำการออกรายงานได้

3.5 สามารถนำระบบ Zabbix Network Monitoring ไปพัฒนาร่วมกับ Opensource Dashboard tool เพื่อเน้นการนำเสนอ Metrics ที่เฉพาะเจาะจง แสดงผลออกมาเป็น กราฟข้อมูล Matrix ต่าง ๆ โดยดึงข้อมูลออกมาได้ในระดับ Realtime และสามารถดึงข้อมูลมาจาก Data Source หลายแหล่งมารวมกัน อีกทั้ง Dashboard ยังมีความสวยงาม เข้าใจได้ง่ายมากขึ้น

บรรณานุกรม

- อติชาติ พัทธภัก. ระบบการแจ้งเตือนและตอบโต้ของ ZABBIX ด้วยแอปพลิเคชัน LINE ZABBIX Monitoring Alert and Reply with LINE Application. สารนิพนธ์ มหาวิทยาลัยเทคโนโลยีมหานคร. 2559; 4-8.
- ประพันธ์ ไชยชนะ. ระบบตรวจสอบการทำงานของระบบเครือข่ายและแจ้งเตือนผ่านแอปพลิเคชัน LINE Network Traffic Monitoring and LINE Application Notification 2561 ; 5-9.
- สิริวิษณุ ธนาวิษณุ. การตรวจสอบสถานะเครือข่ายด้วยแอปพลิเคชันไลน์ 2561; 3-10.
- ณัฐพล ศรีรอดบาง. การออกแบบระบบติดตามสถานภาพเครื่องแม่ข่ายเสมือน และกู้คืนเว็บแอปพลิเคชัน ภายในระบบการประมวลผลแบบกลุ่มเมฆ ด้วยซอฟต์แวร์โอเพนซอร์ซ. สารนิพนธ์บัณฑิตวิทยาลัย สถาบันเทคโนโลยีไทย-ญี่ปุ่น. 2563; 6.
- ธรัช อารีราษฎร์ และ วรภา อารีราษฎร์. (2560). การพัฒนาระบบตรวจสอบและจัดการเครือข่าย มหาวิทยาลัยราชภัฏมหาสารคาม. เข้าถึงได้จาก <https://ph02.tcithaijo.org/index.php/itm-journal/article/view/115256>
- วรากร ศรีเขงทรัพย์. (2554). การอ้างอิงถึงเครื่องคอมพิวเตอร์ในระบบเครือข่ายอินเทอร์เน็ต สาขาวิชาวิศวกรรมคอมพิวเตอร์คณะวิศวกรรมศาสตร์สถาบันเทคโนโลยีไทย-ญี่ปุ่น. เข้าถึงได้จาก <https://ejournals.swu.ac.th/index.php/jindedu/article/view/1879/1922>
- Personet. ระบบเซิร์ฟเวอร์ คืออะไร ทำหน้าที่อะไร มีกี่ประเภท. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 15 ก.พ. 2565]. แหล่งข้อมูล: <https://personet.co.th/what-is-server/>
- Personet. Network หรือ ระบบเครือข่าย คืออะไร. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 1 ม.ค. 2565]. แหล่งข้อมูล: <https://personet.co.th/what-is-computer-network/>
- Konicaminolta. เลือกเซิร์ฟเวอร์ให้เหมาะกับองค์กร. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 5 ก.พ. 2565]. แหล่งข้อมูล: <https://onestopitservices.konicaminolta.co.th/th/physical-server-vs-cloud-server/>
- Openlandscape. CentOS ระบบปฏิบัติการ Linux สำหรับจัดทำ Server. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 12 มี.ค. 2565]. แหล่งข้อมูล: <https://blog.openlandscape.cloud/centos>
- Aws. ระบบเครือข่ายคอมพิวเตอร์. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 21 มี.ค. 2565]. แหล่งข้อมูล: <https://aws.amazon.com/th/what-is/computer-networking/>
- Aws. ICMP คืออะไร. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 5 เม.ย. 2565]. แหล่งข้อมูล: <https://aws.amazon.com/th/what-is/icmp/>

- Prospace. Network Protocol. [อินเทอร์เน็ต]. 2018. [สืบค้นเมื่อ 24 มี.ค. 2564].
แหล่งข้อมูล: <https://www.mediathailand.org/2012/04/web-technology.html>
- Zabbix . Zabbix Network Monitoring. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 12 ก.ค. 2565].
แหล่งข้อมูล: <https://www.zabbix.com/>
- pi-tech. SNMP - Simple Network Management Protocol. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 10 พ.ค. 2565]. แหล่งข้อมูล: <https://www.pi-tech.biz/17251146/snmp-simple-network-management-protocol>
- Saixiii. SNMP คืออะไร SNMP คือ โพรโทคอลสำหรับมอนิเตอร์อุปกรณ์ในระบบ. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 1 มิ.ย. 2565]. แหล่งข้อมูล: <https://saixiii.com/what-is-snmp/>
- Mindphp. Apache คืออะไร อาปาเช่ คือ เว็บเซิร์ฟเวอร์. [อินเทอร์เน็ต]. 2019 [สืบค้นเมื่อ 12 ก.ค. 2566]. แหล่งข้อมูล: <https://www.mindphp.com/คู่มือ/73-คืออะไร/2265-apache-คืออะไร.html>
- Linux-Console. MariaDB คืออะไร? MariaDB ทำงานอย่างไร. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 5 ก.ค. 2565]. แหล่งข้อมูล: <https://th.linux-console.net/?p=1854>
- Line. Line Notify รับการแจ้งเตือนจากเว็บเซอร์วิสทาง LINE. [อินเทอร์เน็ต]. 2022 [สืบค้นเมื่อ 12 ส.ค. 2565]. แหล่งข้อมูล: <https://notify-bot.line.me/th/>

ภาคผนวก

ภาคผนวก ก
การติดตั้งและตั้งค่าโปรแกรม ZABBIX

การติดตั้งและตั้งค่าโปรแกรม ZABBIX

สำหรับการ Monitor คอมพิวเตอร์เซิร์ฟเวอร์และอุปกรณ์เครือข่าย

1. การติดตั้งโปรแกรม ZABBIX

ขั้นตอนที่ 1: เลือกตัวติดตั้ง และดาวน์โหลดโปรแกรม Zabbix ตามที่เตรียม OS Linux

Server โดยเลือกผ่านหน้าเว็บ <https://www.zabbix.com/download>

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER
6.4	Alma Linux	9 Stream	Server, Frontend, Agent	MySQL	Apache
6.0 LTS	CentOS	8 Stream	Proxy	PostgreSQL	Nginx
5.0 LTS	Debian	7	Agent		
4.0 LTS	OpenSUSE Leap	6	Agent 2		
7.0 PRE-RELEASE	Oracle Linux		Java Gateway		
	Raspberry Pi OS		Web Service		
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				
	Ubuntu (arm64)				

- Install and configure Zabbix for your platform

```
# rpm -Uvh https://repo.zabbix.com/zabbix/6.4/rhel/9/x86\_64/zabbix-release-6.4-1.el9.noarch.rpm
```

```
# dnf clean all
```

- Install Zabbix server, frontend, agent

```
# dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent
```

- Create initial database

```
# mysql -uroot -p password
```

```
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

- On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p Zabbix
```

- Disable `log_bin_trust_function_creators` option after importing database schema.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

- Configure the database for Zabbix server

Edit file `/etc/zabbix/zabbix_server.conf`

```
DBPassword=password
```

- Start Zabbix server and agent processes

```
# systemctl restart zabbix-server zabbix-agent httpd php-fpm
```

```
# systemctl enable zabbix-server zabbix-agent httpd php-fpm
```

2. การตั้งค่าโปรแกรม ZABBIX

2.1 หลังจากติดตั้งโปรแกรม ZABBIX เรียบร้อยแล้ว

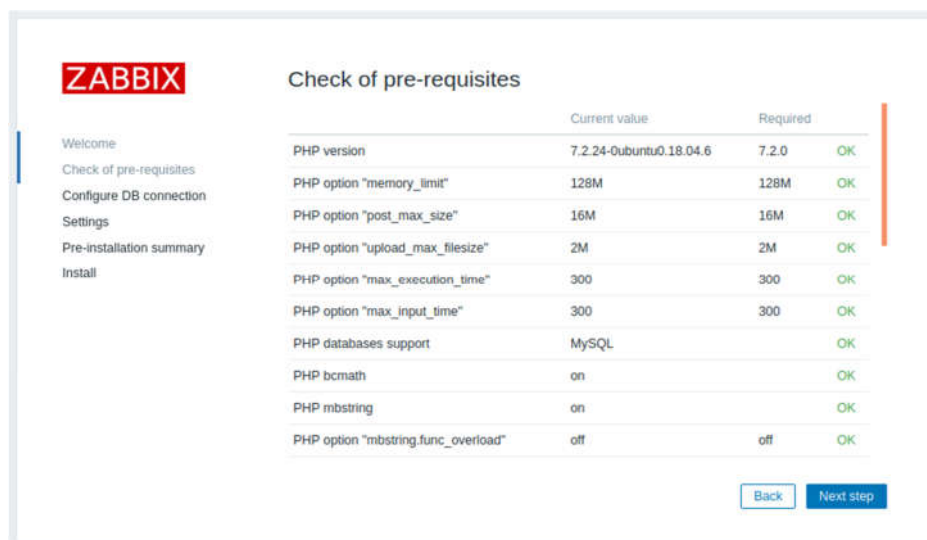
- ให้เข้าด้วย URL `http://server_ip_or_dns_name/zabbix` เพื่อเข้าไปตั้งค่า Web

Frontend


- เลือกภาษาที่ต้องการใช้งาน



2.2 ตรวจสอบการตั้งค่าต่าง ๆ ในระบบ



2.3 ตั้งค่า DB Connection



Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Database type

Database host

Database port 0 - use default port

Database name

Store credentials in Plain text HashiCorp Vault CyberArk Vault

User

Password

Database TLS encryption Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

Welcome

Check of pre-requisites


Configure DB connection

Settings

Pre-installation summary

Install

2.4 ตั้งค่า Zabbix server และ Time Zone



Settings

Zabbix server name

Default time zone

Default theme

Welcome

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

2.5 การตั้งค่าโดยรวมทั้งหมด

ZABBIX

- Welcome
- Check of pre-requisites
- Configure DB connection
- Settings
- Pre-installation summary
- Install**

Pre-installation summary

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type	MySQL
Database server	localhost
Database port	default
Database name	zabbix
Database user	zabbix
Database password	*****
TLS encryption	false
Zabbix server	localhost
Zabbix server port	10051
Zabbix server name	

Back
Next step

2.6 การตั้งค่าโดยรวมทั้งหมดเสร็จสิ้น

ZABBIX

- Welcome
- Check of pre-requisites
- Configure DB connection
- Settings
- Pre-installation summary
- Install**

Install

Congratulations! You have successfully installed Zabbix frontend.

Configuration file "/var/www/html/zabbix/conf/zabbix.conf.php" created.

Back
Finish

3. การติดตั้งและตั้งค่าโปรโตคอล SNMP ของอุปกรณ์เครือข่าย สำหรับมอนิเตอร์ในโปรแกรม ZABBIX

3.1 เมื่อทำการติดตั้งเซิร์ฟเวอร์ Zabbix Network Monitoring เสร็จแล้ว ก่อนที่ทำการเพิ่มอุปกรณ์เครือข่ายที่ต้องการ Monitor ให้ดำเนินการดังนี้

- ทำการติดตั้ง Zabbix Agents สำหรับ คอมพิวเตอร์แม่ข่ายตามเวอร์ชันของระบบปฏิบัติการและเวอร์ชัน Zabbix Server โดยสามารถดาวน์โหลด Zabbix Agents ได้ที่

https://www.zabbix.com/download_agents

Download pre-compiled Zabbix agent binaries

For Agent DEBs and RPMs please visit [Zabbix packages](#)

Show legacy downloads

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	6.4	OpenSSL	MSI
Linux		i386	6.2	No encryption	Archive
macOS			6.0 LTS		
AIX			5.4		
FreeBSD			5.2		
OpenBSD			5.0 LTS		
Solaris			4.4		

- ทำการตั้งค่า SNMP Community ให้กับอุปกรณ์เครือข่าย เช่น Switch, Router, Access Point, Firewall

3.2 ทำการทดสอบ ping และ snmpwalk จากเครื่องเซิร์ฟเวอร์ Zabbix Network Monitoring ไปยังอุปกรณ์เครือข่ายที่จะทำการ Monitor

```

[root@zabbix-server-lab ~]# snmpwalk -v2c -c public 172.16.10.3
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software (C3750E-UNIVERSALK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 05-May-11 15:40 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.516
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (157929124) 18 days, 6:41:31.24
SNMPv2-MIB::sysContact.0 = STRING: \NHA\
SNMPv2-MIB::sysName.0 = STRING: Switch
SNMPv2-MIB::sysLocation.0 = STRING: \NHA\
SNMPv2-MIB::sysServices.0 = INTEGER: 6
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-SMI::enterprises.9.7.129
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-SMI::enterprises.9.7.115
SNMPv2-MIB::sysORID.3 = OID: SNMPv2-SMI::enterprises.9.7.265
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-SMI::enterprises.9.7.112
SNMPv2-MIB::sysORID.5 = OID: SNMPv2-SMI::enterprises.9.7.106
SNMPv2-MIB::sysORID.6 = OID: SNMPv2-SMI::enterprises.9.7.47

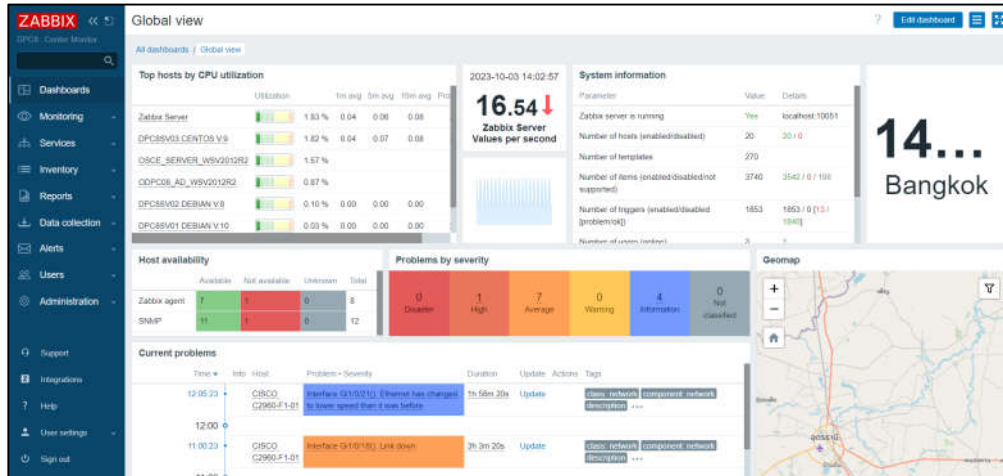
```

3.3 หลังจากทำการติดตั้งและตั้งค่า Zabbix Agent และ SNMP ให้กับคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายเสร็จแล้วให้เข้าไปตั้งค่าเพื่อที่จะนำอุปกรณ์ดังกล่าวเข้ามาทำการ Monitor

- เปิด Zabbix UI Web Server is <http://host/zabbix>
- Username: Admin
- Password: Zabbix

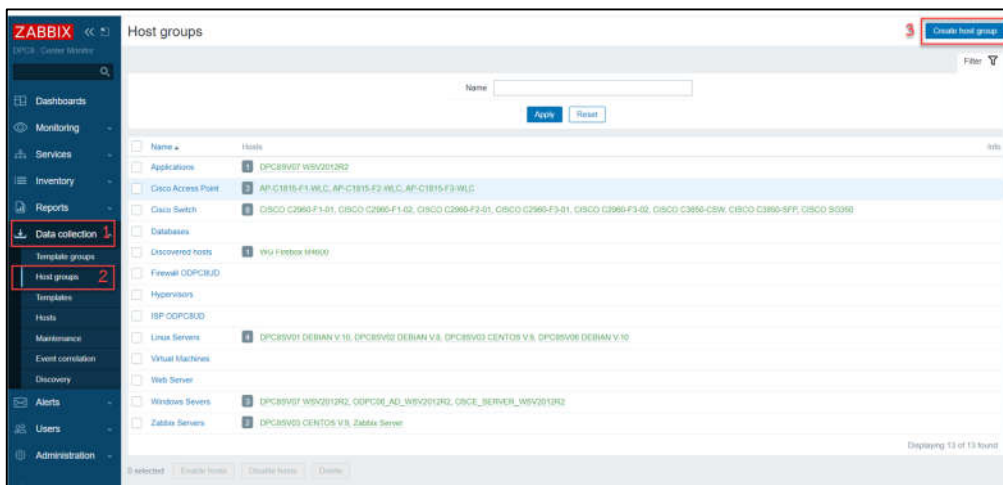
(Note: Username & Password Default of Zabbix Server)

2.4 เมื่อ Login เข้ามาจะเจอหน้า Dashboard ของระบบเอาไว้ดูสถานะโดยรวมของ Host ที่กำลังทำการ Monitor ภายในระบบเครือข่าย



2.5 การนำคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายมาทำการ Monitoring ในโปรแกรม Zabbix

- ทำการสร้าง Host Group เพื่อจัดกลุ่มให้กับอุปกรณ์ที่นำมา Monitor ไปที่ เมนู Data Collection --> Host Group --> Create Host Group



- ทำการสร้าง Group name ของอุปกรณ์ แล้วทำการกด Add

New host group ? ✕

* Group name

Add
Cancel

- การสร้าง Host เพื่อทำการ Monitor ไปที่ เมนู Data Collection --> Host --> Create

Host

Name	Items	Triggers	Graphs	Discovery	Web interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
APC1815-F1-WLC	Items 15	Triggers 0	Graphs 0	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
APC1815-F2-WLC	Items 15	Triggers 0	Graphs 0	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
APC1815-F3-WLC	Items 15	Triggers 0	Graphs 0	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C2960-F1-01	Items 162	Triggers 177	Graphs 39	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C2960-F1-02	Items 160	Triggers 163	Graphs 39	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C2960-F3-01	Items 167	Triggers 172	Graphs 39	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C2960-F3-01	Items 146	Triggers 161	Graphs 39	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C2960-F3-02	Items 166	Triggers 170	Graphs 40	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C3850-CSM	Items 175	Triggers 194	Graphs 39	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO C3850-SFP	Items 168	Triggers 191	Graphs 32	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
CISCO S0356	Items 181	Triggers 175	Graphs 39	Discovery 0	Web		Cisco IOS by SNMP	Enabled	OK	None		
DPC85V01 DEBIAN V 10	Items 61	Triggers 23	Graphs 10	Discovery 3	Web		Linux by Zabbix agent	Enabled	OK	None		
DPC85V02 DEBIAN V 8	Items 61	Triggers 23	Graphs 10	Discovery 3	Web		Linux by Zabbix agent	Enabled	OK	None		
DPC85V03 CENTOS V 8	Items 79	Triggers 30	Graphs 10	Discovery 3	Web		Linux by Zabbix agent	Enabled	OK	None		
DPC85V08 DEBIAN V 10	Items 61	Triggers 23	Graphs 10	Discovery 3	Web		Linux by Zabbix agent	Enabled	OK	None		
DPC85V07 WW2012R2	Items 127	Triggers 62	Graphs 14	Discovery 4	Web		Windows by Zabbix agent	Enabled	OK	None		
DDPC08_AD_WV2012R2	Items 16	Triggers 40	Graphs 11	Discovery 4	Web		Windows by Zabbix agent	Enabled	OK	None		
OSCE_SERVER_WV2012R2	Items 106	Triggers 73	Graphs 12	Discovery 4	Web		Windows by Zabbix agent	Enabled	OK	None		
WS2 Python M480	Items 116	Triggers 66	Graphs 15	Discovery 3	Web		Windows, Python (Linux by SNMP) (Discovered by SNMP)	Enabled	OK	None		

- แถบเมนู Host รายละเอียดของ Host

- Host Name: ชื่อ Host
- Visible name: ชื่อที่แสดง
- Templates: เลือกเทมเพลตที่ต้องการ
- Host groups: เลือก Host Group
- Interfaces: เลือกการเชื่อมต่อ
- Description: รายละเอียดที่ต้องการ

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name

Visible name

Templates

* Host groups

Interfaces No interfaces are defined.
[Add](#)

Description

Monitored by proxy (no proxy)

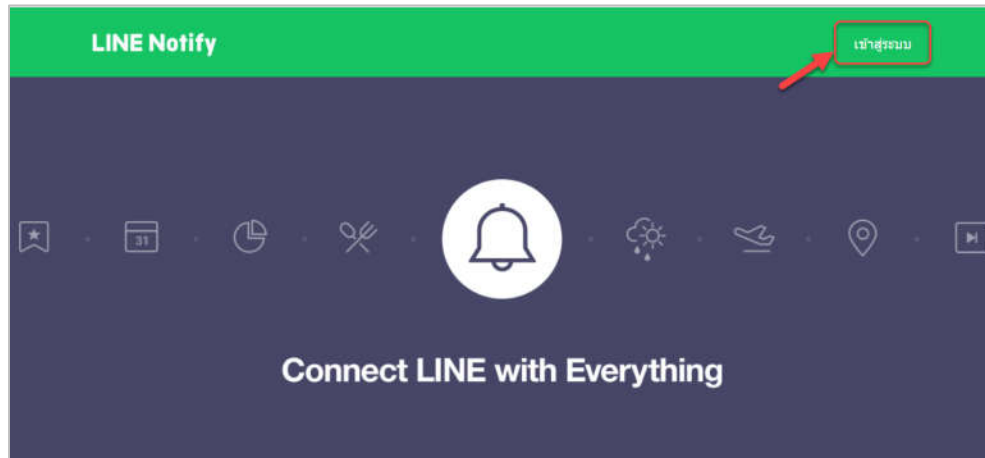
Enabled

ภาคผนวก ข

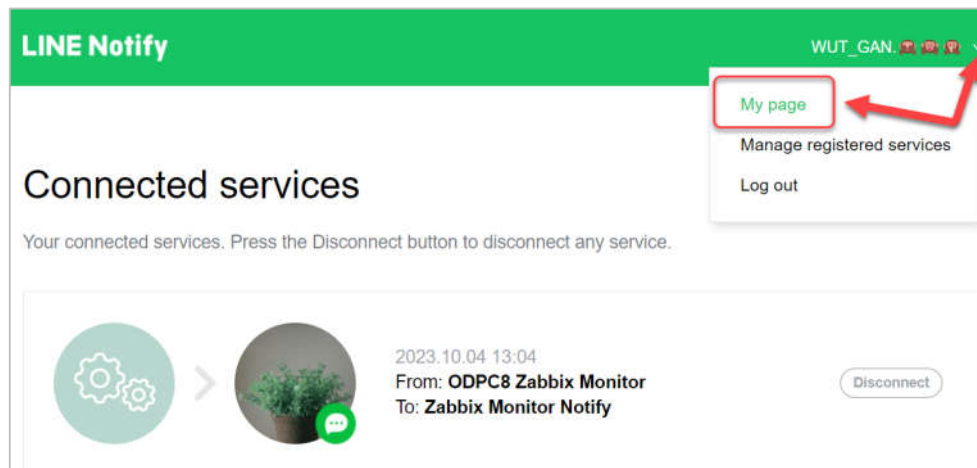
การส่งการแจ้งเตือนโปรแกรม Zabbix ผ่าน Line Notify

การส่งการแจ้งเตือนโปรแกรม Zabbix ผ่าน LINE Notify

- การส่งการแจ้งเตือนโปรแกรม Zabbix จำเป็นต้องมี Token ของ LINE Notify
การออก Token โดยล็อกอินเข้าเว็บไซต์ <https://notify-bot.line.me/th/>



- เมื่อล็อกอินเข้ามา กด Dropdown เลือก My Page เลื่อนลงมาด้านล่างสุดเพื่อออก Token



- กด Generate Token --> ใส่ชื่อ Token --> เลือกกลุ่มที่ต้องการแจ้งเตือน --> กด Generate Token

Generate access token (For developers)

By using personal access tokens, you can configure notifications without having to add a web service.

Generate token

→

LINE Notify API Document

Generate token ✕

Please enter a token name to be displayed before each notification.

Zabbix Monitor ใส่ชื่อ Line Token ที่ต้องการ

Select a chat to send notifications to.

ค้นหากลุ่มที่ต้องการแจ้งเตือน

Zabbix Monitor Notify เลือกกลุ่มที่ต้องการแจ้งเตือน

FINCA-Cyber 2023 รุ่น#4

VDOConDDC

กรม_DDC OpenData & PredictiveAnalytic

กรม_เครือข่าย IT DDC

Note: Revealing your personal access token can allow a third party to obtain the names of your connected chats as well as your profile name.

กด Generate Token

Generate token
→

- Copy Token เพื่อใช้แจ้งเตือนในโปรแกรม Zabbix

Your token is:

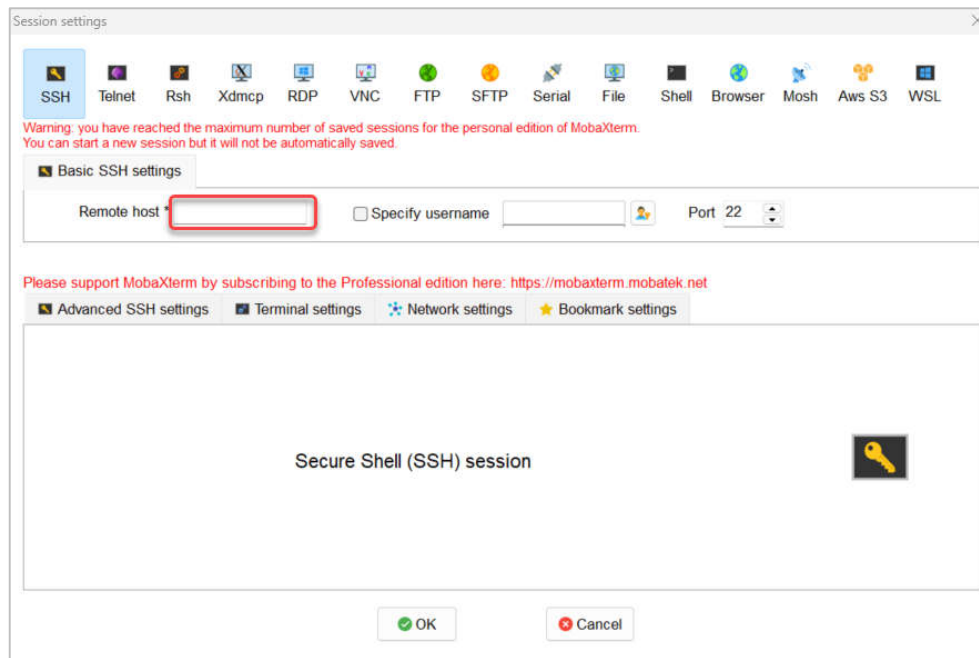
Sfh3gjYjK5kfabcgMnygBMgnRRDbI3g1V03rmD

If you leave this page, you will not be able to view your newly generated token again. Please copy the token before leaving this page.

Copy**Close**

การตั้งค่าการแจ้งเตือนโปรแกรม Zabbix Server

การตั้งค่าใน Zabbix Server โดยการ Remote Login เข้าสู่ IP Address คอมพิวเตอร์
แม่ข่ายที่ได้ทำการลง Zabbix Server



1. เข้าไป Config โดยผ่าน SSH ใส่ IP Address Host เข้าไปสร้าง Bash Script ใน Directory

Path : /usr/lib/zabbix/alertscripts/ โดยคำสั่ง

```
# cd /usr/lib/zabbix/alertscripts/
```

- สร้างไฟล์ line-notify โดยคำสั่ง

```
# nano line-notify
```

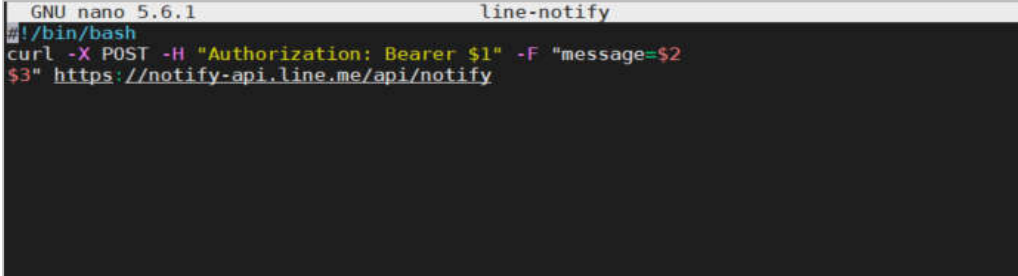
```
[root@localhost dpc8]# cd /lib/zabbix/alertscripts/
[root@localhost alertscripts]# nano line-notify
[root@localhost alertscripts]# █
```

- เพิ่ม Bash Script ในไฟล์ line-notify แล้ว Save file

```
#!/bin/bash
```

```
curl -X POST -H "Authorization: Bearer $1" -F "message=$2
```

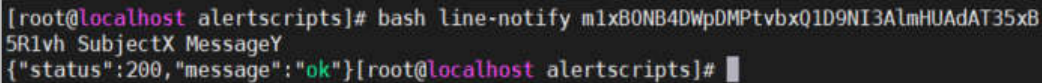
```
$3" https://notify-api.line.me/api/notify
```



```
GNU nano 5.6.1 line-notify
#!/bin/bash
curl -X POST -H "Authorization: Bearer $1" -F "message=$2
$3" https://notify-api.line.me/api/notify
```

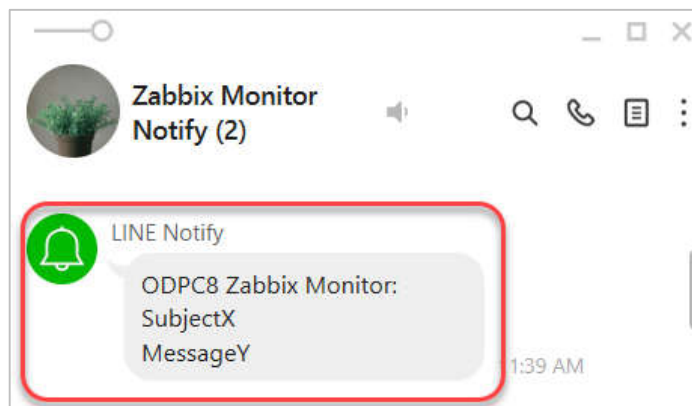
- ทดสอบการทำงาน line-notify โดยใช้คำสั่ง

```
# bash line-notify "ใส่ Line TOKEN" SubjectX MessageY
```



```
[root@localhost alertscripts]# bash line-notify m1xB0NB4DWpDMptvbxQ1D9NI3AImHUAAdAT35xB5R1vh SubjectX MessageY
{"status":200,"message":"ok"}[root@localhost alertscripts]#
```

- ระบบก็จะแจ้งเตือนตามข้อความที่เราทดสอบ แสดงว่า Line Notify สามารถแจ้งเตือนได้แล้ว



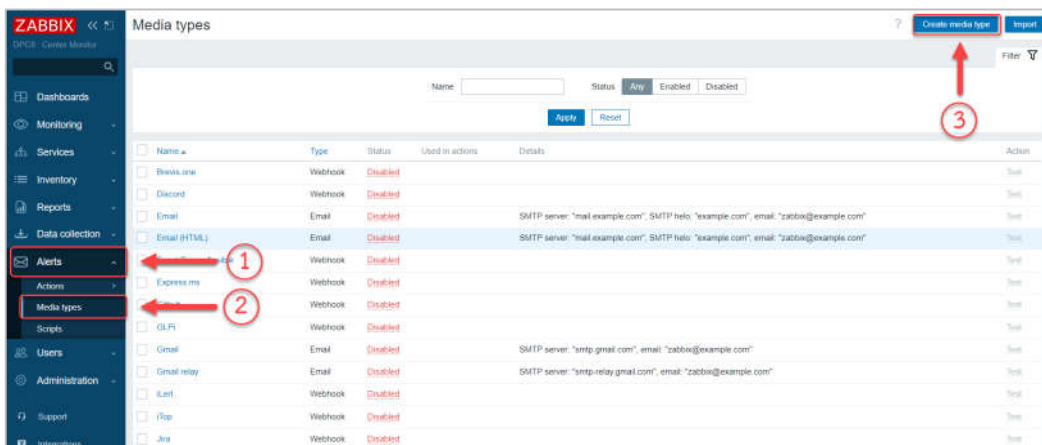
- กำหนดไฟล์ line-notify ให้สามารถ Execute ได้ โดยใช้คำสั่ง
chmod +x line-notify
- แสดงรายชื่อไฟล์ โดยใช้คำสั่ง
- # ls

```
[root@localhost alertscripts]# chmod +x line-notify
[root@localhost alertscripts]# ls
line-notify
[root@localhost alertscripts]#
```

Remark: การ Config line-notify ต้องเข้าไปทำใน Directory path:

/usr/lib/zabbix/alertscripts/

- หลังจากที่ทำการเพิ่ม Bash Script ใน Zabbix Server เรียบร้อยแล้ว ให้ทำการล็อกอินเข้าหน้าระบบ Zabbix Web UI เพื่อทำการตั้งค่าการแจ้งเตือน
 - ไปที่เมนู Alerts → Media types → Create media types



- เมนู Media types ใส่รายละเอียดข้อมูล แล้วทำการเพิ่ม (Add)
Name: Line-Notify (ชื่อ Media ที่ต้องการใส่)
Type: Script (เลือก Type ให้ตรง)
Script name: line-notify (ชื่อ Bash Script ที่เราสร้างและตั้งค่าใน Zabbix Server)
Script parameters: เพิ่มเพื่อรับค่า Parameters ที่มาจาก Bash Script ต้องการแจ้งเตือน {ALERT.SENDTO}, {ALERT.SUBJECT}, {ALERT.MESSAGE}

Media types

Media type | Message templates | Options

* Name:

Type:

* Script name:

Script parameters ?

Value	Action
<input type="text" value="{ALERT.SENDTO}"/>	Remove
<input type="text" value="{ALERT.SUBJECT}"/>	Remove
<input type="text" value="{ALERT.MESSAGE}"/>	Remove

[Add](#)

Description:

Enabled:

[Add](#) [Cancel](#)

- เมื่อทำการเพิ่มแล้ว Media ก็จะแสดงในหน้า Media types

Media type	Type	Status	Line-Notify Action	Script name	Test
Gmail relay	Email	Disabled	SMTP server: "smtp-relay.gmail.com", email: "zabbix@example.com"		Test
Mail	Webhook	Disabled			Test
IFTOP	Webhook	Disabled			Test
Jira	Webhook	Disabled			Test
Jira ServiceDesk	Webhook	Disabled			Test
Jira with CustomFields	Webhook	Disabled			Test
Line	Webhook	Disabled			Test
Line-Notify	Script	Enabled	Line-Notify Action	Script name: "line-notify"	Test
ManageEngine ServiceDesk	Webhook	Disabled			Test
Mattermost	Webhook	Disabled			Test
MS Teams	Webhook	Disabled			Test
Office365	Email	Disabled	SMTP server: "smtp.office365.com", email: "zabbix@example.com"		Test
Office365 relay	Email	Disabled	SMTP server: "smtp.office365.com", email: "zabbix@example.com"		Test
Openfire	Webhook	Disabled	SMTP server: "example.com.mail.protection.outlook.com", email: "zabbix@example.com"		Test
OTRS	Webhook	Disabled			Test

- ทำการทดสอบ Media โดยการกด Test จะขึ้นหน้าให้ Test parameters

Media type	Type	Status	Line-Notify Action	Script name	Test
Gmail relay	Email	Disabled	SMTP server: "smtp-relay.gmail.com", email: "zabbix@example.com"		Test
Mail	Webhook	Disabled			Test
IFTOP	Webhook	Disabled			Test
Jira	Webhook	Disabled			Test
Jira ServiceDesk	Webhook	Disabled			Test
Jira with CustomFields	Webhook	Disabled			Test
Line	Webhook	Disabled			Test
Line-Notify	Script	Enabled	Line-Notify Action	Script name: "line-notify"	Test
ManageEngine ServiceDesk	Webhook	Disabled			Test
Mattermost	Webhook	Disabled			Test
MS Teams	Webhook	Disabled			Test
Office365	Email	Disabled	SMTP server: "smtp.office365.com", email: "zabbix@example.com"		Test
Office365 relay	Email	Disabled	SMTP server: "smtp.office365.com", email: "zabbix@example.com"		Test
Openfire	Webhook	Disabled	SMTP server: "example.com.mail.protection.outlook.com", email: "zabbix@example.com"		Test
OTRS	Webhook	Disabled			Test

Test media type "Line-Notify"

Script parameters ? {ALERT.SENDTO}

{ALERT.SUBJECT}

{ALERT.MESSAGE}

Test **Cancel**

- เมื่อทำการกด Test ทดสอบระบบ Media จะแจ้งกลับมา Media type test successful แสดงว่า Media สามารถใช้งานได้

Test media type "Line-Notify"

Media type test successful.

Script parameters ? {ALERT.SENDTO}

{ALERT.SUBJECT}

{ALERT.MESSAGE}

Test **Cancel**

- หลังจากเพิ่ม Media Type แล้ว ให้ทำการเพิ่ม Action ของ Script
- ไปที่เมนู Action -> Trigger action -> create action

ZABBIX << >> Trigger actions

Name: Status: **Apply** Enabled Disabled

Apply **Reset**

Name	Conditions	Operations	Status
<input type="checkbox"/> Line-Notify Action	Trigger severity is greater than or equals Not classified	Send message to users: garfavut (Garfavut Ganyanuch) via Line-Notify	Enabled

0 selected **Refresh** **Change** **Delete** Displaying 1 of 1 found

- กด create action -> เมนู Action -> ใส่ชื่อ -> ใส่เงื่อนไข

New action

Action Operations

* Name | ชื่อ Action ที่ต้องการ เช่น Line-Notify Action

Conditions | Add | Name | Action

Enabled

* At least one operation must exist.

Add Cancel

- เลือกเงื่อนไขที่ต้องการ กด Add

New condition

Type | Trigger severity

Operator | equals | does not equal | is greater than or equals | is less than or equals

Severity | Not classified | Information | Warning | Average | High | Disaster

Add Cancel

- ไปที่เมนู Operations -> กด Add

New action

Action Operations

* Default operation step duration | 1h

Operations	Steps	Details	Start in	Duration	Action
	Add				

Recovery operations | Details | Add | Action

Update operations | Details | Add | Action

Pause operations for symptom problems

Pause operations for suppressed problems

Notify about canceled escalations

* At least one operation must exist.

Add Cancel

- ในส่วน Operation --> Operation details --> ใส่รายละเอียดตามรูป

Operation details ✕

Operation Send message

Steps - (0 - infinitely)

Step duration (0 - use action default)

* At least one user or user group must be selected.

Send to user groups Select ← ส่งเป็นกลุ่ม

Send to users Admin (Zabbix Administrator) ✕ Select ← ส่งเป็นบุคคล

Send only to ← เลือก Media Type ที่เราสร้างไว้

Custom message

Subject ใส่หัวข้อ หรือดึงจากค่าของ Zabbix

Message ใส่ Event ที่ต้องการส่ง พร้อมข้อความแจ้งเตือน

Conditions	Label	Name	Action
	Add		

Add
Cancel

- ในส่วน Recovery operations --> กด Add --> Operation details --> ใส่รายละเอียดตามรูป

Operation details ✕

Operation

* At least one user or user group must be selected.

Send to user groups

Send to users

Send only to

Custom message

Subject

Message

- เมื่อทำการ Add Action ทั้งเมนู Action และ Operations เสร็จแล้ว กด Add

New action

Action Operations 2

* Default operation step duration: 1h

Steps	Details	Start in	Duration	Action
1	Send message to users: Admin (Zabbix Administrator) via Line-Notify	Immediately	Default	Edit Remove

Add

Recovery operations

Details	Action
Send message to users: Admin (Zabbix Administrator) via Line-Notify	Edit Remove

Add

Update operations

Details	Action

Add

Pause operations for symptom problems:

Pause operations for suppressed problems:

Notify about canceled escalations:

* At least one operation must exist.

Add Cancel

- ตรวจสอบ Action ที่ทำการ Add ในหน้า Trigger Action

ZABBIX Trigger actions

Name: Status: Any Enabled Disabled Filter

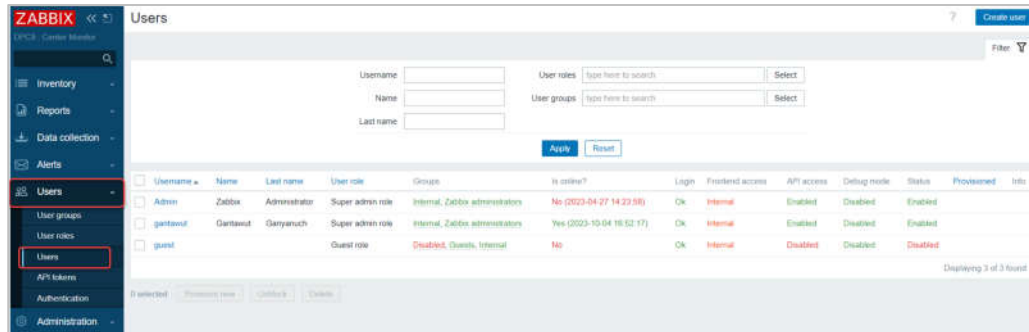
Apply Reset

Name	Conditions	Operations	Status
<input type="checkbox"/> Line-Notify Action	Trigger severity is greater than or equals fatal classified	Send message to users: gantawut (Gantawut Ganyanuch) via Line-Notify	Enabled

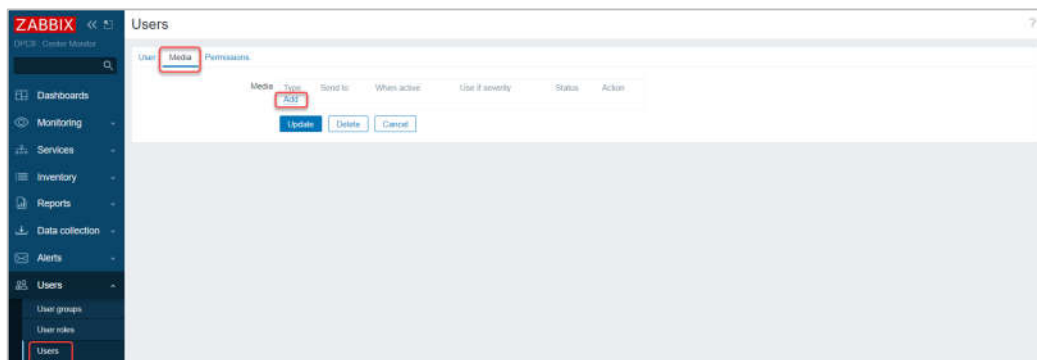
0 selected Enable Disable Delete

Displaying 1 of 1 found

- ขั้นตอนต่อไป ไปที่เมนู Users --> Users เพื่อทำการ Add Media ให้ User ในระบบ Zabbix ที่ต้องการทำการแจ้งเตือน จะเลือก User ที่มีอยู่หรือ Create Users ใหม่ก็ได้



- ไปที่ Users --> Media --> กด Add



- เลือก Type Media --> Send to: LINE TOKEN --> When active: วันและเวลาที่ต้องการ --> เลือก Use if severity ที่ต้องการส่งแจ้งเตือน --> ติ๊ก Enabled --> กด Add Media

Media ✕

Type

* Send to

* When active

Use if severity

Not classified

Information

Warning

Average

High

Disaster

Enabled

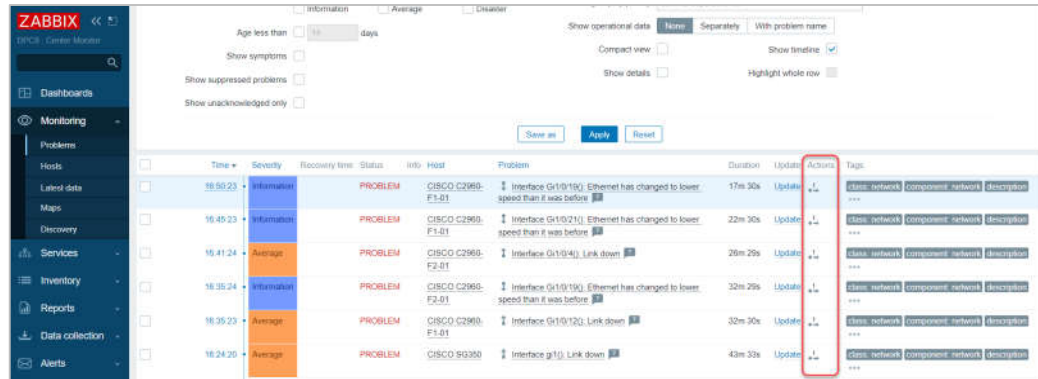
- จะได้ Users ตามรูป และ Status Enabled

ZABBIX << >>
Users Create user

<input type="checkbox"/>	Username	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
<input type="checkbox"/>	Admin	Zalbox	Administrator	Super admin role	Internal_Zabbix_administrators	No (2023-04-27 14:33:56)	OK	Internal	Enabled	Disabled	Enabled		
<input type="checkbox"/>	garlawut	Garlawut	Gaiyanuch	Super admin role	Internal_Zabbix_administrators	Yes (2023-10-04 17:54:04)	OK	Internal	Enabled	Disabled	Enabled		
<input type="checkbox"/>	guest			Guest role	Disabled, Guests, Internal	No	OK	Internal	Disabled	Disabled	Disabled		

Displaying 3 of 3 found

- เมื่ออุปกรณ์เครือข่ายมีปัญหาระบบก็จะแจ้งเตือนผ่าน TOKEN LINE Notify ที่เราได้เพิ่มไว้ ให้ทำการแจ้งเตือนตามกลุ่ม LINE นั้น ตามรูป



- เมื่อกดตรง Action ดูก็จะขึ้นสถานะการส่งแจ้งเตือนตามที่ได้กำหนดไว้



- ตัวอย่างการแจ้งเตือนตามที่ได้กำหนดไว้ สามารถปรับแต่งการแจ้งเตือนตามความต้องการของผู้ดูแลระบบได้เลย

