



## รายงานสหกิจศึกษาฉบับสมบูรณ์

การติดตั้งระบบคลาวด์ส่วนตัวและการย้ายเซิร์ฟเวอร์

Private Cloud Setup & Server Migration

คุณสนันท์ นิธิพานิช

สาขาวิศวกรรมสารสนเทศ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2562

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อโครงการสหกิจศึกษา	การติดตั้งระบบคลาวด์ส่วนตัวและการย้ายเซิร์ฟเวอร์
ชื่อ-สกุล นักศึกษา	นายคณัสนันท์ นิธิพานิช
คณะ วิศวกรรมศาสตร์	ภาควิชา วิศวกรรมคอมพิวเตอร์ สาขาวิชา วิศวกรรมสารสนเทศ
ชื่อ-สกุล อาจารย์นิเทศน์	ผศ.มยุรี เลิศเวชกุล
ชื่อ-สกุล ผู้นิเทศน์งาน	นายบัญชา เต๋นประยูรวงศ์
ชื่อสถานประกอบการ	บริษัท ดีทีซี อินเทอร์เน็ตเวิร์คกิ้ง จำกัด

### บทคัดย่อ

บริษัท ดีทีซี อินเทอร์เน็ตเวิร์คกิ้ง จำกัด เป็นบริษัทที่ให้บริการด้านการวางระบบในเรื่องการสร้างและพัฒนาระบบเซิร์ฟเวอร์ และระบบเครือข่าย มีความต้องการที่จะจัดระเบียบเซิร์ฟเวอร์ภายในองค์กร โดยการย้ายเซิร์ฟเวอร์ขึ้นระบบคลาวด์ส่วนตัวเพื่อความสะดวกสบายต่อการจัดการและตรวจสอบเซิร์ฟเวอร์ภายในองค์กรและทำการสำรองข้อมูลเซิร์ฟเวอร์ที่อยู่บนคลาวด์ส่วนตัว เพื่อเพิ่มความปลอดภัยให้กับเซิร์ฟเวอร์ เมื่อเซิร์ฟเวอร์เกิดความเสียหาย ก็สามารถกู้คืนข้อมูลได้อย่างรวดเร็ว

**Co-operative Title:** Private Cloud Setup & Server Migration

**Student Intern Name:** Kanutsanun Nithipanich

**Faculty:** Engineering      **Department:** Computer Engineering

**Major:** Information Engineering

**Advisor Name:** Asst. Prof. Mayuree Lertwatechakul

**Mentor Name:** Mr. Bancha Denprawyoowong

**Company:** DTC Internetworking Co.,Ltd.

## ABSTRACT

DTC Internetworking Company Limited is a company that provides system solutions for customers such as servers and network. The company want to upgrade the existing servers to be more secure and more easily to manage. This could be done by employing cloud technology. This project was implemented by moving the servers to a private cloud. After server migration, it is more convenient to manage and monitor the servers. Besides, automatically backing up increases the server security and data recovery could be done quickly if any system crash happens.

## กิตติกรรมประกาศ

ข้าพเจ้าได้รับผิดชอบและปฏิบัติหน้าที่ในบริษัท ดีทีซี อินเทอร์เน็ตเวิร์คกิ้ง จำกัด ระหว่างวันที่ 5 สิงหาคม ถึงวันที่ 22 พฤศจิกายน พ.ศ.2562 ในโครงการวิชาสหกิจศึกษาที่ทางคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และบริษัทฯร่วมมือกันจัดตั้งขึ้นในหัวข้อโครงการ การติดตั้งระบบคลาวด์ส่วนตัวและการย้ายเซิร์ฟเวอร์ ซึ่งข้าพเจ้าได้รับความรู้ ความเข้าใจและประสบการณ์ในการทำงานที่เป็นประโยชน์อย่างมาก อีกทั้งการดูแลและการช่วยเหลือต่าง ๆ ตลอดระยะเวลาการทำงาน โดยการปฏิบัติงานสหกิจศึกษาในครั้งนี้สำเร็จลุล่วงได้ เพราะมีการชี้แนะและได้รับความร่วมมือจากบุคคลต่าง ๆ ดังต่อไปนี้

### พนักงานแผนก Services

- คุณบัญชา เต็นประยูรวงศ์
- คุณฐาธิกา ตั้งกัลยานนท์
- คุณพัชรภรณ์ อออุดมยุทธ
- คุณพัฒนรัตน์ เขียรเหรียญ
- คุณกฤษฎา กาญจะแสน

### พนักงานแผนกทรัพยากรบุคคล

- คุณศิริลักษณ์ หาญวิริยะพันธุ์

และข้าพเจ้าขอขอบคุณอาจารย์ที่ปรึกษา ผศ.มยุรี เลิศเวชกุล ที่คอยให้คำแนะนำ คำปรึกษาและคอยรับฟัง และช่วยเหลือปัญหาต่าง ๆ ในการทำโครงการครั้งนี้ และท้ายที่สุดข้าพเจ้าขอขอบคุณครอบครัวที่คอยให้กำลังใจที่ดีแก่ข้าพเจ้าเสมอมาทำให้ปริญญาบัตรฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

คนี่สนันท์ นิธิพานิช

# สารบัญ

	หน้า
บทคัดย่อ.....	II
ABSTRACT.....	III
กิตติกรรมประกาศ.....	IV
สารบัญ.....	V
สารบัญรูปภาพ.....	VIII
สารบัญตาราง.....	XIII
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญ.....	1
1.2 วัตถุประสงค์ของการปฏิบัติงาน.....	1
1.3 ขอบเขตของงาน.....	1
1.4 วิธีการดำเนินงาน.....	2
1.5 ประโยชน์ที่คาดว่าจะได้รับ.....	2
บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง.....	3
2.1 VMware.....	3
2.1.1 VMware vSphere.....	3
2.1.2 VMware infrastructure.....	4
2.1.3 Physical topology of VMware Infrastructure Data center.....	5
2.1.4 VMware vMotion.....	7
2.1.5 VMware DRS.....	7
2.2 Veeam Backup and Replication.....	8
2.3 Next-generation firewalls.....	10

## สารบัญ(ต่อ)

	หน้า
2.3.1 Port Forward.....	11
2.3.2 VPN (Virtual Private Network).....	12
บทที่ 3 ขั้นตอนการดำเนินงาน .....	14
3.1 จัดเตรียมเครื่องมือและอุปกรณ์ที่ใช้.....	14
3.1.2 เครื่องเซิร์ฟเวอร์ 1 เครื่องสำหรับติดตั้ง VMware ESXi version 6.5 .....	14
3.1.3 VMware vSphere Client version 5.5.....	15
3.1.4 Veeam Backup & Replication.....	15
3.1.5 Firewall ของ ZyXel (USG310) เป็น Next Generation Firewall.....	15
3.2 ศึกษาข้อมูลการใช้งานของอุปกรณ์และโปรแกรม .....	16
3.2.1 ศึกษาการใช้งานซอฟต์แวร์ VMware ESXi version 6.5.....	16
3.2.2 ศึกษาการใช้งานซอฟต์แวร์ VMware vSphere Client .....	16
3.2.3 ศึกษาการใช้งานซอฟต์แวร์ Veeam Backup & Replication.....	16
3.2.4 ศึกษาการใช้งาน Firewall ของ ZyXEL ( ZyWall USG310 ) .....	17
3.3 วิเคราะห์และออกแบบ .....	17
3.4 ติดตั้ง VMware ESXi version 6.5.....	18
3.5 ติดตั้งโปรแกรม VMware vSphere Client.....	23
3.6 ติดตั้งเซิร์ฟเวอร์ VtigerCRM Version 7.0.0.....	31
3.7 ติดตั้งโปรแกรม VMware vCenter Converter Standalone Client.....	39
3.8 ติดตั้ง Veeam Backup & Replication.....	48
3.9 Config Firewall รุ่น ZyXel USG310.....	55
บทที่ 4 ผลการทดลอง.....	63

## สารบัญ(ต่อ)

หน้า

4.1 การเข้าใช้งานระบบคลาวด์ส่วนตัวโดยการใช้งาน VPN แบบ Client to Site .....	63
4.2 ตรวจสอบเซิร์ฟเวอร์การทำงานเซิร์ฟเวอร์บนระบบคลาวด์ส่วนตัว .....	64
4.3 ตรวจสอบการทำงานของเซิร์ฟเวอร์สำรองข้อมูลของตัว Virtual Machine .....	65
4.4 ตรวจสอบการใช้งาน VPN.....	65
4.5 ตรวจสอบการเข้าใช้งานเซิร์ฟเวอร์ VtigerCRM ผ่านเครือข่ายภายนอกได้ .....	67
บทที่ 5 สรุปผลการวิจัย และข้อเสนอแนะ .....	68
5.1 สรุปผลการวิจัย .....	68
5.2 ปัญหา และอุปสรรคในการดำเนินงาน.....	68
5.3 ข้อเสนอแนะ .....	68
เอกสารอ้างอิง .....	69

## สารบัญรูปภาพ

	หน้า
รูปที่ 2.1 VMware vSphere .....	3
รูปที่ 2.2 VMware infrastructure .....	4
รูปที่ 2.3 VMware vCenter .....	5
รูปที่ 2.4 Virtual Data Center Architecture .....	6
รูปที่ 2.5 การจัดการหน่วยจัดเก็บในคอมพิวเตอร์เสมือน .....	6
รูปที่ 2.6 VMware vMotion .....	7
รูปที่ 2.7 VMware DRS .....	7
รูปที่ 2.8 Veeam Backup & Replication .....	8
รูปที่ 2.9 Virtual Infrastructure .....	9
รูปที่ 2.10 สัญลักษณ์ Firewall .....	10
รูปที่ 2.11 Port Forwarding .....	11
รูปที่ 2.12 Virtual Private Network .....	12
รูปที่ 3.1 VMware ESXi .....	14
รูปที่ 3.2 เครื่องเซิร์ฟเวอร์ .....	14
รูปที่ 3.3 VMware vSphere .....	15
รูปที่ 3.4 Veeam .....	15
รูปที่ 3.5 Firewall ZyXel (USG310) .....	15
รูปที่ 3.6 ไดอะแกรม .....	17
รูปที่ 3.7 หน้าเว็บเพจของ VMware สำหรับดาวน์โหลดไฟล์ .....	18
รูปที่ 3.8 โปรแกรม Rufus .....	18
รูปที่ 3.9 บุต VMware ESXi version 6.5 ผ่านแฟลชไดรฟ์ .....	19
รูปที่ 3.10 หน้าจอการติดตั้ง VMware ESXi .....	19
รูปที่ 3.11 หลังการติดตั้งเสร็จ .....	20
รูปที่ 3.12 ข้อตกลงการใช้งานของ VMware ESXi .....	20
รูปที่ 3.13 ทำการรีบูตเครื่องเซิร์ฟเวอร์ .....	21
รูปที่ 3.14 เข้าสู่หน้า Vmware ESXi .....	21

## สารบัญรูปภาพ(ต่อ)

	หน้า
รูปที่ 3.15 หน้าจอแสดงถึงการทำงานของ VMware ESXi .....	22
รูปที่ 3.16 หน้า Customization .....	22
รูปที่ 3.17 ไฟล์ตัวติดตั้ง VMware vSphere Client .....	23
รูปที่ 3.18 หน้า install VMware vSphere Client.....	23
รูปที่ 3.19 หน้าเข้าสู่ระบบ VMware vSphere Client.....	24
รูปที่ 3.20 หน้าแรกหลังจากเข้าสู่ระบบ.....	24
รูปที่ 3.21 สร้างคอมพิวเตอร์เสมือน .....	25
รูปที่ 3.22 Config คอมพิวเตอร์เสมือนเป็นชนิด Typical.....	25
รูปที่ 3.23 ตั้งชื่อให้คอมพิวเตอร์เสมือน .....	26
รูปที่ 3.24 เลือกพื้นที่จัดเก็บ.....	26
รูปที่ 3.25 เลือกระบบปฏิบัติการให้กับคอมพิวเตอร์เสมือน .....	27
รูปที่ 3.26 เพิ่ม NIC ( Network Interface Card ).....	27
รูปที่ 3.27 กำหนดค่าดิสก์ให้กับ GuestOS.....	28
รูปที่ 3.28 ตรวจสอบอีกครั้งก่อนยืนยันการสร้าง .....	29
รูปที่ 3.29 ทำการติดตั้งระบบปฏิบัติการ .....	29
รูปที่ 3.30 เพิ่มไฟล์ตัวติดตั้งเข้าไปในหน่วยเก็บของเครื่องเซิร์ฟเวอร์.....	30
รูปที่ 3.31 ค้นหาไฟล์ตัวที่จะติดตั้งลงบนคอมพิวเตอร์เสมือน .....	30
รูปที่ 3.32 เลือกไฟล์ตัวติดตั้งคอมพิวเตอร์เสมือนและทำการติดตั้ง.....	31
รูปที่ 3.33 หน้าเว็บเพจของ Xampp สำหรับดาวน์โหลดไฟล์ .....	31
รูปที่ 3.34 ติดตั้ง Xampp .....	32
รูปที่ 3.35 หน้าเว็บเพจของ VtigerCRM สำหรับดาวน์โหลดไฟล์ .....	32
รูปที่ 3.36 แยกไฟล์ Zip.....	33
รูปที่ 3.37 เข้าสู่หน้าติดตั้ง VtigerCRM.....	33
รูปที่ 3.38 ตั้งค่าระบบเซิร์ฟเวอร์ VtigerCRM.....	34
รูปที่ 3.39 เข้าสู่ระบบ MySQL.....	34
รูปที่ 3.40 หน้าแรกเมื่อเข้าสู่ระบบ .....	35

## สารบัญรูปภาพ(ต่อ)

	หน้า
รูปที่ 3.41 การส่งออกฐานข้อมูล .....	35
รูปที่ 3.42 ไฟล์ SQL ที่ได้จากการส่งออก .....	36
รูปที่ 3.43 เลือกฐานข้อมูลที่จะนำเข้า.....	36
รูปที่ 3.44 การนำเข้าฐานข้อมูล.....	37
รูปที่ 3.45 แก้ไขค่า Config .....	37
รูปที่ 3.46 หน้าเข้าสู่ระบบของ VitgerCRM.....	38
รูปที่ 3.47 หน้าเว็บเพจของ VMware สำหรับดาวน์โหลดไฟล์.....	39
รูปที่ 3.48 ตัวติดตั้ง VMware Converter .....	39
รูปที่ 3.49 หน้าติดตั้ง VMware vCenter Converter .....	40
รูปที่ 3.50 หน้าแรกของโปรแกรม VMware vCenter Converter .....	40
รูปที่ 3.51 migrate แบบ V2V ( Virtual to Virtual ) .....	41
รูปที่ 3.52 เลือกเซิร์ฟเวอร์ที่เป็นคอมพิวเตอร์เสมือนเพื่อทำการ migrate .....	41
รูปที่ 3.53 กรอกที่อยู่ของเซิร์ฟเวอร์ที่ติดตั้ง VMware ESXi version 6.5.....	42
รูปที่ 3.54 ตั้งชื่อให้กับคอมพิวเตอร์เสมือน .....	42
รูปที่ 3.55 เลือกหน่วยจัดเก็บข้อมูล.....	43
รูปที่ 3.56 ปรับค่าทรัพยากรตามความต้องการของเซิร์ฟเวอร์ .....	43
รูปที่ 3.57 ตรวจสอบการตั้งค่า .....	44
รูปที่ 3.58 การย้ายแบบ P2V ( Physical to Virtual ).....	44
รูปที่ 3.59 เข้าสู่ระบบเครื่องเซิร์ฟเวอร์ที่ติดตั้ง ESXi version 6.5.....	45
รูปที่ 3.60 ตั้งชื่อคอมพิวเตอร์เสมือน .....	45
รูปที่ 3.61 เลือกหน่วยเก็บข้อมูล.....	46
รูปที่ 3.62 ปรับค่าทรัพยากรตามความต้องการของเซิร์ฟเวอร์ .....	46
รูปที่ 3.63 ตรวจสอบการตั้งค่า.....	47
รูปที่ 3.64 หน้าเว็บเพจของ Veeam สำหรับดาวน์โหลดไฟล์.....	48
รูปที่ 3.65 ไฟล์ตัวติดตั้ง Veeam .....	48
รูปที่ 3.66 ตัวติดตั้ง Veeam.....	49

## สารบัญรูปภาพ(ต่อ)

	หน้า
รูปที่ 3.67 หน้าต่างติดตั้ง Veeam.....	49
รูปที่ 3.68 เพิ่มใบอนุญาตของ Veeam.....	50
รูปที่ 3.69 ทำการเข้าสู่ระบบ Veeam.....	50
รูปที่ 3.70 หน้าแรกเมื่อเข้าสู่ระบบสำเร็จ .....	51
รูปที่ 3.71 หน้าต่าง Backup Job .....	51
รูปที่ 3.72 เลือกเครื่องเซิร์ฟเวอร์เพื่อทำการสำรองข้อมูล .....	52
รูปที่ 3.73 เลือก Backup Repository.....	52
รูปที่ 3.74 หน้า Guest Processing.....	53
รูปที่ 3.75 กำหนดเวลาการสำรองข้อมูล.....	53
รูปที่ 3.76 หน้า summary.....	54
รูปที่ 3.77 แสดงสถานะการสำรองข้อมูล.....	54
รูปที่ 3.78 หน้า GUI (Graphical User Interface) ของ Firewall รุ่น ZyXel USG310 .....	55
รูปที่ 3.79 หน้าตั้งค่า interface ของ Firewall.....	55
รูปที่ 3.80 หน้าการตั้งค่าของแต่ละ Interface (1) .....	56
รูปที่ 3.81 หน้าการตั้งค่าของแต่ละ Interface (2) .....	57
รูปที่ 3.82 หน้าตั้งค่า NAT (Network Address Translation).....	57
รูปที่ 3.83 หน้าต่างการตั้งค่า NAT .....	58
รูปที่ 3.84 หน้าตั้งค่า Policy Control.....	59
รูปที่ 3.85 หน้าต่างการตั้งค่า Policy.....	60
รูปที่ 3.86 หน้าตั้งค่า SSL VPN.....	60
รูปที่ 3.87 หน้าต่างการตั้งค่า SSL VPN (1).....	61
รูปที่ 3.88 หน้าต่างการตั้งค่า SSL VPN (2).....	62
รูปที่ 4.1 หน้าเข้าสู่ระบบของ VMware ESXi version 6.5.....	63
รูปที่ 4.2 หน้าแรกหลังจากการเข้าสู่ระบบ .....	64
รูปที่ 4.3 สถานะของเซิร์ฟเวอร์ .....	64
รูปที่ 4.4 สถานการณ์ทำงานของเซิร์ฟเวอร์สำรองข้อมูล.....	65

## สารบัญรูปภาพ(ต่อ)

หน้า

รูปที่ 4.5	ไอคอนซอฟต์แวร์ที่ใช้ในการทำ VPN.....	65
รูปที่ 4.6	หน้าเข้าสู่ระบบ VPN แบบ Client to Site .....	65
รูปที่ 4.7	หน้ายืนยันการเข้าใช้งาน VPN.....	66
รูปที่ 4.8	สถานะของการทำ VPN แบบ Client to Site.....	66
รูปที่ 4.9	หน้าเข้าสู่ระบบ VtigerCRM ของบริษัท.....	67



## สารบัญตาราง

หน้า

ตาราง 3.1 แสดงชื่ออุปกรณ์และ IP Address ที่กำหนด..... 17



# บทที่ 1

## บทนำ

### 1.1 ความเป็นมาและความสำคัญ

เนื่องจาก บริษัท ดีทีซี อินเทอร์เน็ตเวิร์คกิ้ง จำกัด ได้จัดโครงการสหกิจศึกษาระหว่างบริษัท ดีทีซี อินเทอร์เน็ตเวิร์คกิ้ง จำกัด กับ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในส่วนงานของฝ่ายนั้น ได้มีการคิดที่จะเอาเซิร์ฟเวอร์ขึ้นเป็นระบบคลาวด์ส่วนตัวโดยใช้ภายในองค์กร จึงได้มีการมอบหมายงานให้นักศึกษาทำการศึกษา และหาความรู้เกี่ยวกับเทคโนโลยีการทำระบบคลาวด์ส่วนตัวที่ใช้ภายในองค์กร ซึ่งเป็นผลิตภัณฑ์ซอฟต์แวร์ชนิดหนึ่ง รวมถึงวิธีการติดตั้ง และการตั้งค่า เพื่อให้ นักศึกษามีความรู้ความสามารถทำการตั้งค่าและติดตั้งระบบได้

### 1.2 วัตถุประสงค์ของการปฏิบัติงาน

เนื่องจากบริษัท ดีทีซี อินเทอร์เน็ตเวิร์คกิ้ง จำกัด เป็นบริษัทที่ให้บริการโซลูชันทางด้านไอทีแก่ธุรกิจต่าง ๆ มีความต้องการที่จะจัดระเบียบเซิร์ฟเวอร์ภายในองค์กร โดยการสร้างระบบคลาวด์ส่วนตัวขึ้นมาแล้วทำการย้ายเซิร์ฟเวอร์ที่เป็นคอมพิวเตอร์เสมือนไปอยู่บนระบบคลาวด์ส่วนตัวและทำการสำรองข้อมูลโดยใช้ซอฟต์แวร์ที่ใช้สำรองข้อมูลเซิร์ฟเวอร์ที่เป็นคอมพิวเตอร์เสมือน เพื่อป้องกันความเสียหายของเซิร์ฟเวอร์ภายในองค์กร

### 1.3 ขอบเขตของงาน

- 1) เรียนรู้การทำงานและศึกษาโครงสร้างระบบของเซิร์ฟเวอร์ที่จะนำซอฟต์แวร์ไปติดตั้ง
- 2) กำหนดทรัพยากรที่ใช้ของเซิร์ฟเวอร์ที่จะนำขึ้นระบบคลาวด์ส่วนตัว
- 3) กำหนดสิทธิ์ของบุคลากรที่ทำหน้าที่เข้ามาดูแลระบบ
- 4) จัดการชุดคำสั่งในการตั้งค่าระบบ
- 5) เสนอแนะแนวทางการเพิ่มประสิทธิภาพให้กับระบบคลาวด์ส่วนตัว

#### 1.4 วิธีการดำเนินงาน

- 1) ศึกษาระบบ และเทคโนโลยีของซอฟต์แวร์รวมถึงคุณสมบัติการทำงานต่าง ๆ
- 2) วิเคราะห์อุปกรณ์ และซอฟต์แวร์ที่จำเป็นต้องใช้ในการดำเนินการโครงการ
- 3) ติดตั้งระบบ และตั้งค่าซอฟต์แวร์ให้ตรงตามความต้องการ
- 4) ทดสอบระบบ
- 5) วิเคราะห์ปัญหาที่เกิดขึ้น
- 6) เสนอแนะแนวทางการเพิ่มประสิทธิภาพ
- 7) สรุปผล

#### 1.5 ประโยชน์ที่คาดว่าจะได้รับ

- 1) ระบบเซิร์ฟเวอร์ของบริษัทฯที่ได้รับการติดตั้ง จะมีประสิทธิภาพในการทำงาน และการจัดการทรัพยากรมากยิ่งขึ้น
- 2) เซิร์ฟเวอร์ของบริษัทฯถูกจัดให้เป็นระเบียบมากขึ้น
- 3) บริษัทฯได้รับแนวทางในการติดตั้งระบบและการตั้งค่าการใช้งานตามการออกแบบและความต้องการ

## บทที่ 2

### เอกสารและงานวิจัยที่เกี่ยวข้อง

#### 2.1 VMware

##### 2.1.1 VMware vSphere

VMware เป็นโปรแกรมชนิดหนึ่งซึ่งทำหน้าที่ในการจำลองเป็นคอมพิวเตอร์เสมือน (Virtual Machine) หรือ Hypervisor ทำหน้าที่ในการจัดสรรทรัพยากรบนเครื่องคอมพิวเตอร์ปกติ (Physical Machine) ให้แก่เครื่องคอมพิวเตอร์เสมือนให้สามารถทำงานได้

ซึ่ง Hypervisor สามารถแยกออกได้เป็น 2 ชนิดคือ

- 1) Native หรือ bare metal
- 2) Hosted



รูปที่ 2.1 VMware vSphere

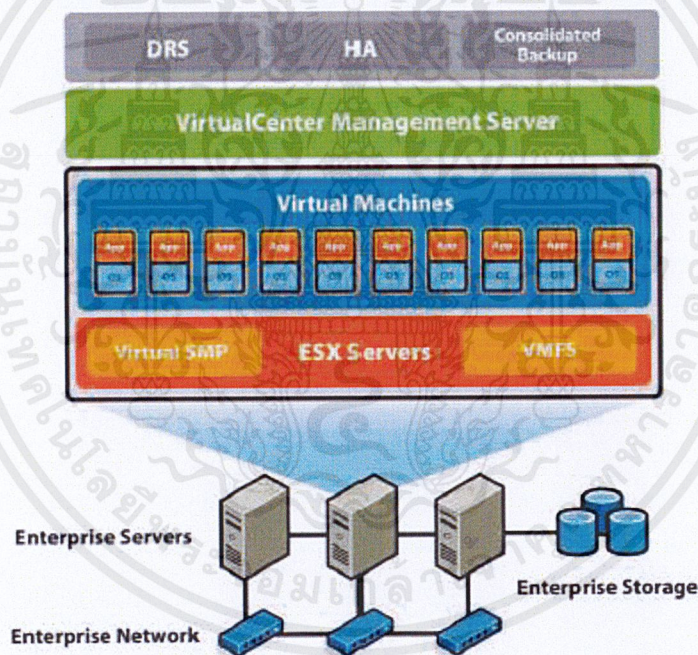
ข้อแตกต่างระหว่าง 2 สถาปัตยกรรมคือ hosted จะทำงานบนระบบปฏิบัติการ เช่น Windows ส่วนของ bare metal จะเชื่อมต่อกับ Physical Machine ได้โดยตรง โดยมีระบบปฏิบัติการเป็นของตัวเอง ทำให้เกิดความรวดเร็วในการทำงานจะแตกต่างกันเป็นอย่างมาก ตัวอย่างของ hosted เช่น VMware server, VMware player, VMware view, Virtualbox ( Oracle ) ส่วนสถาปัตยกรรมแบบ native หรือ bare metal เช่น ESX, ESXi, Hyper-V

ในส่วนนี้จะขอกล่าวถึงเฉพาะ VMware เท่านั้น ซึ่ง VMware สามารถแบ่งได้เป็น 3 กลุ่มตามการใช้งานได้ดังต่อไปนี้

- 1) กลุ่มที่ติดตั้งบนเครื่องคอมพิวเตอร์เดสก์ทอป เช่น VMware Workstation, VMware Fusion เป็นโปรแกรม Virtualization ที่ติดตั้งลงบนระบบปฏิบัติการ Windows
- 2) กลุ่มที่ติดตั้งบนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์มีชื่อว่า VMware vSphere ซึ่งใช้งานกันในระดับองค์กรเป็นการลงบนเครื่องเปล่า ( เครื่องเซิร์ฟเวอร์ ) เป็นการมองว่า VMware เป็นระบบปฏิบัติการของเครื่องเซิร์ฟเวอร์นั้น ๆ มี 2 ชื่อคือ ESX และ ESXi
- 3) กลุ่มที่มี vCenter เป็นตัวกลางคอยดูแลจัดการ VMware ESX, ESXi หลาย ๆ ตัว

### 2.1.2 VMware infrastructure

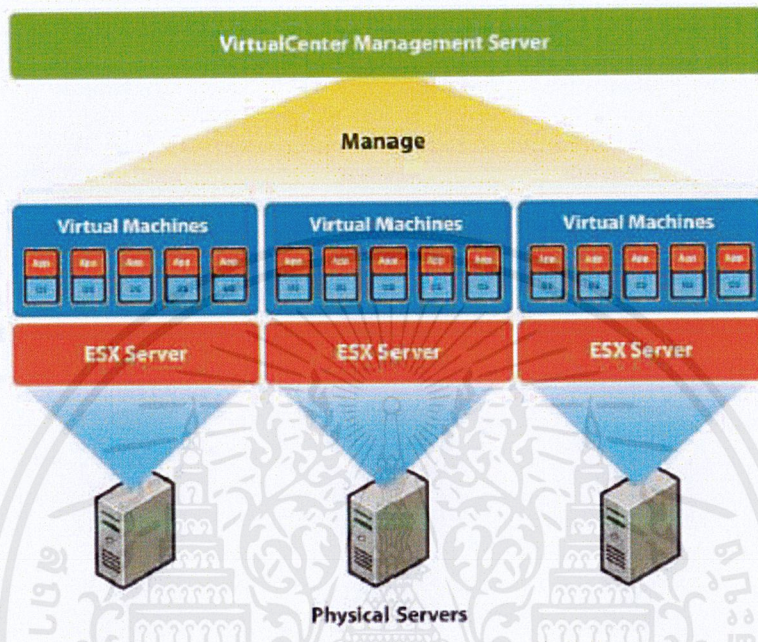
VMware สามารถจัดการทรัพยากรบนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ ซึ่งโครงสร้างของ VMware จะประกอบด้วยส่วนต่าง ๆ ดังต่อไปนี้



รูปที่ 2.2 VMware infrastructure

- 1) VMware ESXi Server ทำหน้าที่ในการบริหารจัดการทรัพยากรต่าง ๆ บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ให้กับเครื่องคอมพิวเตอร์เสมือนที่ทำงานอยู่ในเครื่องนั้น เช่น จัดการซีพียู, หน่วยความจำ, เครือข่าย รวมไปถึงเรื่องของหน่วยจัดเก็บที่อยู่บน Hypervisor
- 2) VMware vCenter คือ ตัวกลางที่ช่วยในการจัดการระบบของ VMware ESXi Server ทั้งหมดโดย vCenter Server สามารถเป็นได้ทั้งคอมพิวเตอร์ปกติหรือคอมพิวเตอร์เสมือนก็ได้

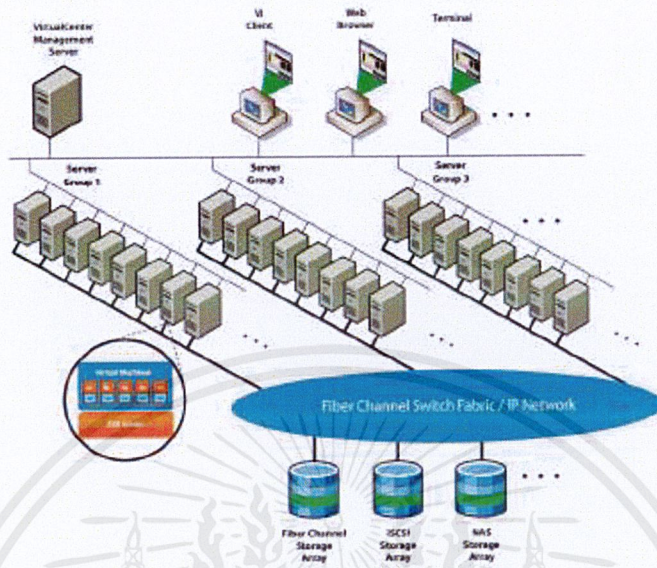
ได้ ซึ่ง vCenter ช่วยให้ผู้ดูแลระบบ (Administrator) สามารถที่จะเข้าถึง vSphere เพื่อใช้กำหนดค่า clusters, hosts, VMs, storage, guest OS และคุณสมบัติอื่น ๆ ของ virtual infrastructure ทั้งหมดจากที่เดียว



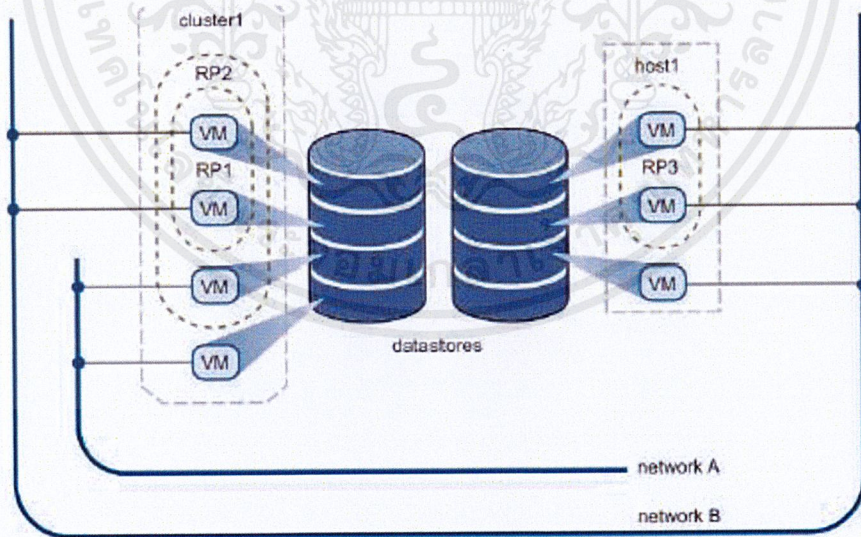
รูปที่ 2.3 VMware vCenter

### 2.1.3 Physical topology of VMware Infrastructure Data center

ในการใช้งานจริง ๆ นอกเหนือจากเครื่องคอมพิวเตอร์เซิร์ฟเวอร์แล้ว ยังมีอุปกรณ์อื่นเข้ามาเชื่อมต่อด้วย เช่น หน่วยจัดเก็บข้อมูล หรือระบบเครือข่าย ซึ่งการบริการจัดการถ้าเป็นแบบเดิมจะค่อนข้างยากเพราะจะต้องเข้าไปตรวจสอบที่เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ในแต่ละตัว แต่ถ้าเป็นโครงสร้างของ VMware จะสามารถจัดการจากส่วนกลางที่ VMware vCenter รวมไปถึงการจัดการเกี่ยวกับหน่วยจัดเก็บข้อมูลในแต่ละตัวว่าจะสามารถให้ Virtual Machine Guest ตัวไหนใช้งานที่หน่วยจัดเก็บแบบไหน ทำให้สามารถจัดการประสิทธิภาพของระบบได้อย่างเต็มที่

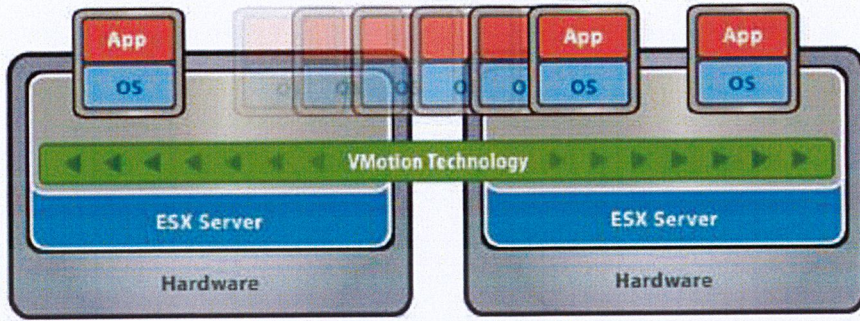


รูปที่ 2.4 Virtual Data Center Architecture



รูปที่ 2.5 การจัดการหน่วยจัดเก็บในคอมพิวเตอร์เสมือน

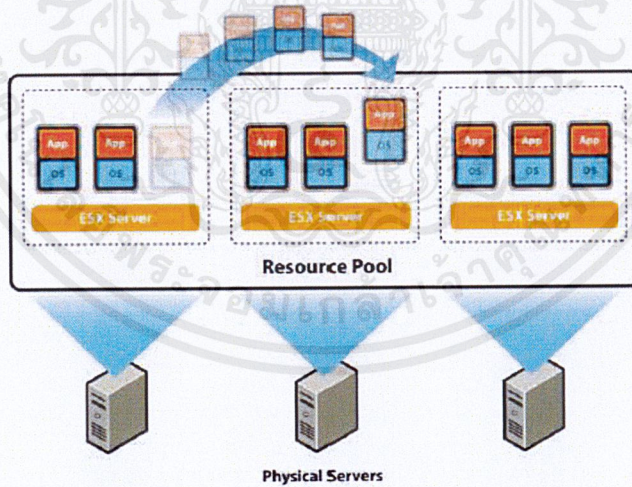
## 2.1.4 VMware vMotion



รูปที่ 2.6 VMware vMotion

อีกหนึ่งความสามารถของ VMware เมื่อนำมาต่อกับ vCenter เพื่อทำงานเป็น Cluster คือคุณสมบัติที่มีชื่อว่า vMotion เป็นความสามารถที่จะย้าย VMware Guest จาก host หนึ่งไปยังอีก host หนึ่งที่มีทรัพยากรเพียงพอ โดยระบบจะไม่ล่ม

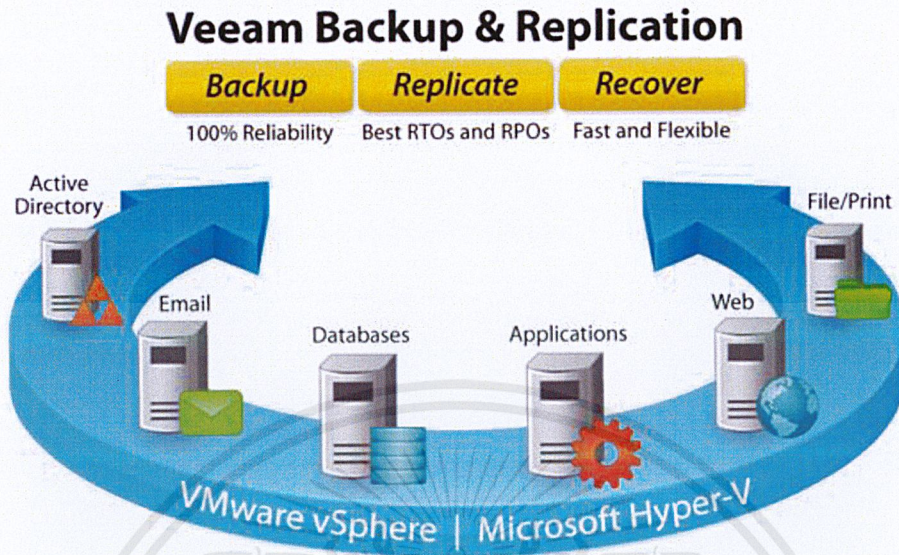
## 2.1.5 VMware DRS



รูปที่ 2.7 VMware DRS

VMware DRS เป็นความสามารถที่ใช้ในการค้นหาทรัพยากรที่ว่างในแต่ละ host ใน cluster แล้วทำการย้าย VMware guest ไปยัง host ที่เหมาะสมได้ โดยเราสามารถสร้างเป็นนโยบายในการย้ายได้

## 2.2 Veeam Backup and Replication



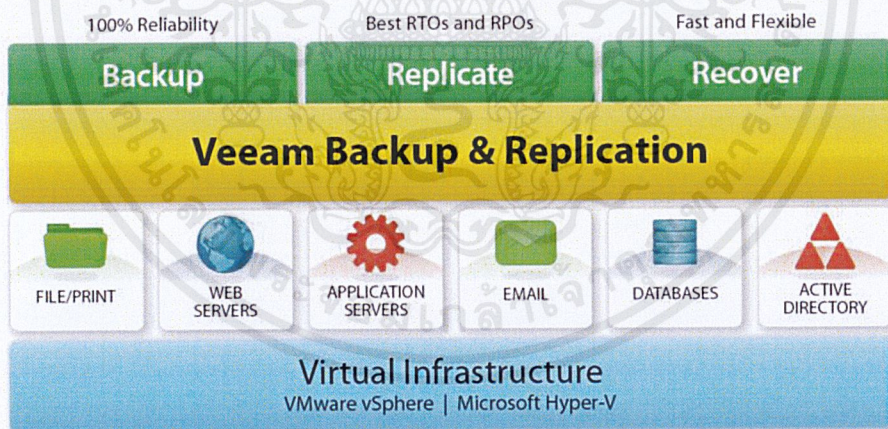
รูปที่ 2.8 Veeam Backup & Replication

(ที่มา: <http://www.mydaas.com.au/mydaas-backup-recovery.php>)

Veeam Backup and Replication เป็นซอฟต์แวร์ที่ใช้ในการสำรองข้อมูลและกู้คืนข้อมูลในระบบเสมือน (Virtualization) ได้อย่างรวดเร็วและง่ายดาย โดยรองรับระบบ Virtualization ชั้นนำ เช่น VMware หรือ Hyper-V ในแบบ Agent-less คือการที่ไม่ต้องติดตั้งซอฟต์แวร์ใด ๆ ลงใน VMguest นั้น ๆ เลย และสามารถทำการคัดลอกสำเนาไปยัง Site สำรองได้อย่างง่ายดาย โดยไม่ต้องซื้อเพิ่ม โดยการสำรอง VM-Guests ในลักษณะที่เรียกว่า Incremental Forever คือการสำรองข้อมูลเฉพาะบล็อกที่มีการเปลี่ยนแปลง และรองรับการทำ Deduplication ซึ่งเป็นการเก็บเฉพาะข้อมูลที่ซ้ำซ้อนลงดิสก์ ทำให้ประหยัดเวลา และเนื้อที่ในการจัดเก็บได้อย่างมีประสิทธิภาพมากขึ้น โดยที่การกู้คืน (Recover) ข้อมูลนั้นสามารถกู้คืนได้ ทั้งแบบ VM หรือบางส่วน ( Individual Object ) เช่น ไฟล์หรือ โพลเดอร์ ที่ต้องการ

ความสามารถหลักของ Veeam backup & Replication มี 5 ข้อ

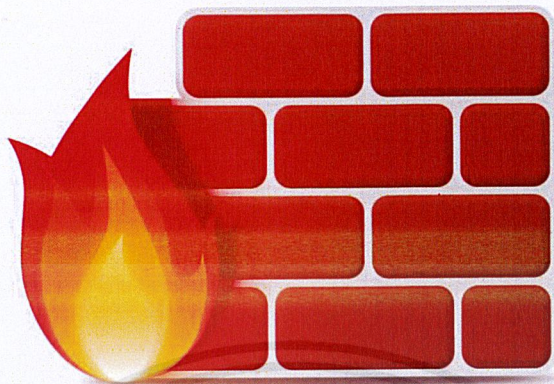
- 1) High-Speed Recovery เรื่องนี้ถือเป็นเรื่องที่เด่นสุดของ Veeam นั่นคือความสามารถในการกู้คืนข้อมูลได้อย่างรวดเร็ว โดยใช้เวลาน้อยกว่า 15 นาที
- 2) Data Loss Avoidance คือการคัดลอกสำเนาซ้ำของข้อมูลข้าม site หรือเรียกอีกอย่างว่า DR Site Solution
- 3) Verified Protection Veeam มีคุณสมบัติที่เรียกว่า SureBackup® และ SureReplica ซึ่งทั้ง 2 ตัวนี้เป็นการทดสอบว่า ข้อมูลที่ได้ทำการสำรองหรือการทำซ้ำไปนั้น สามารถกู้คืนได้จริงหรือไม่
- 4) Leveraged Data เป็นความสามารถที่ใช้ประโยชน์จากไฟล์ที่ทำการสำรอง โดยการทำเป็นแลปจำลองเพื่อทดสอบก่อนที่จะเอาแอปพลิเคชันไปใช้งานจริง และไม่ต้องกังวลว่าจะเกิดความเสียหายกับไฟล์ที่ทำการสำรองเพราะเมื่อทดสอบเสร็จแล้วข้อมูลจะกลับไปเป็นเวอร์ชันต้นฉบับอีกครั้ง
- 5) Complete Visibility เป็นเครื่องมือสำหรับผู้ดูแลระบบไอทีที่ใช้ในการทำเรื่องของ Real Time Monitoring



รูปที่ 2.9 Virtual Infrastructure

(ที่มา: <https://www.microsystems.co.th/news/มาทำความรู้จักกับ-veeam-backup-replication/>)

## 2.3 Next-generation firewalls

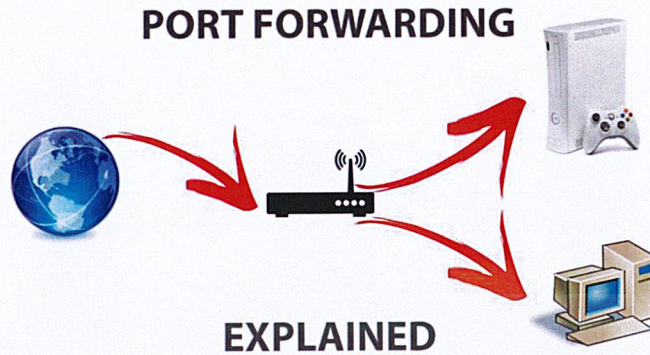


รูปที่ 2.10 สัญลักษณ์ Firewall

(ที่มา: <https://www.anteracorp.com/blog/index.php/component/content/article?id=27:firewall-utm>)

เป็นไฟร์วอลล์สถาปัตยกรรมใหม่ที่ถูกออกแบบมาให้สามารถคัดกรองทราฟฟิกและควบคุมการใช้งานในชั้นแอปพลิเคชัน ซึ่งถูกพัฒนาต่อยอดมาจากไฟร์วอลล์สมัยเก่าที่รับรู้ได้เพียงหมายเลข IP และหมายเลขพอร์ต การรู้จักและสามารถมองเห็นแอปพลิเคชันเป็นคุณสมบัติพื้นฐานของ NGFWs ในปัจจุบันมีแอปพลิเคชันให้เลือกใช้งานมากมาย แต่ละประเภทไม่ขึ้นกับหมายเลขพอร์ต หรืออาจใช้พอร์ตร่วมกับแอปพลิเคชันอื่น เช่น พอร์ต 80 HTTP ที่ยินยอมให้สามารถเข้าถึงเว็บไซต์ รับส่งอีเมล ดูวิดีโอ หรือคุยโทรศัพท์หากันได้ การปิดพอร์ต 80 หมายถึงการปิดบริการเหล่านั้นทั้งหมดโดยไม่สามารถใช้งานแอปพลิเคชันได้ NGFWs จึงเข้ามามีบทบาทให้การควบคุมแอปพลิเคชันโดยไม่จำกัดว่าแอปพลิเคชันเหล่านั้นทำงานอยู่บนพอร์ตใด

### 2.3.1 Port Forward



รูปที่ 2.11 Port Forwarding

(ที่มา: <http://ccnaeducation.com/port-forwarding/>)

Port forwarding หรือ Forward port คือ การที่ทำให้อุปกรณ์ในอินเทอร์เน็ตภายนอกสามารถเชื่อมต่อมาหาคอมพิวเตอร์ได้ นิยมใช้สำหรับการใช้งานด้านเกมส์ออนไลน์, กล้องวงจรปิด และ voice over ip (VoIP) รวมถึงดาวน์โหลดไฟล์จากคอมพิวเตอร์โดยปกติทาง ISP (Internet Service Provider) จะแจก 1 Public IP มาให้แต่ละวงเครือข่ายที่ใช้บริการ

หลักการของ Port forwarding

วิธีการที่อุปกรณ์ภายนอกต้องการติดต่อมายัง อุปกรณ์ภายใน จำเป็นต้องมีข้อมูล IP และพอร์ตที่ต้องการเชื่อมต่อ ซึ่งสำหรับ IP ต้องเป็น static IP และมี 1 IP ต่อ 1 วงเครือข่าย แต่สำหรับ Port มีตั้งแต่ 0 – 65535 ด้วยหลักการ forward port สามารถตั้งให้เราเตอร์ทำการจอร์นพอร์ตไว้ให้กับ NAT IP ภายในวงเครือข่ายได้

## 2.3.2 VPN (Virtual Private Network)



รูปที่ 2.12 Virtual Private Network

(ที่มา: <https://pixabay.com/th/illustrations/vpn-ข้อมูลส่วนตัว-สตรีมมิ่ง-ปลดล็อค-4341596/>)

VPN คือเครือข่ายเสมือนส่วนตัวที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะหรืออาจจะวิ่งบนเครือข่ายโอเพ่นก็ได้แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสแพ็กเก็ตก่อนส่ง เพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น อย่างไรก็ตาม VPN จะครอบคลุมทั้งอุปกรณ์ฮาร์ดแวร์ (เช่น Gateway และ Router), ซอฟต์แวร์ และส่วนที่เป็นไฟร์วอลล์ การเข้ารหัสแพ็กเก็ตเพื่อทำให้ข้อมูลมีความปลอดภัย มีอยู่หลายกลไกด้วยกัน ซึ่งวิธีเข้ารหัสข้อมูล (encryption) จะทำอยู่บนเลเยอร์ 2 คือ Data Link Layer แต่ปัจจุบันมีการเข้ารหัสใน IP Layer โดยมักใช้เทคโนโลยี IPSec (IP Security)

VPN ถูกนำมาใช้กับองค์กรขนาดใหญ่ ที่มีสาขาอยู่ตามที่แตกต่างกัน และต้องการ ต่อเชื่อมเข้าหากัน โดยยังคงสามารถรักษาเครือข่ายให้ใช้ได้เฉพาะคนภายในองค์กรหรือคนที่เกี่ยวข้อง เช่น ลูกค้า, ผู้จัดการขนส่งสินค้า เป็นต้น

กลไกในการสร้างโครงข่าย VPN อีกประเภทหนึ่ง คือ MPLS (Multiprotocol Label Switch) เป็นวิธีการส่งแพ็กเก็ต โดยการใส่ label ที่ส่วนหัวของข้อความและเข้ารหัสข้อมูล จากนั้นจึงส่งไปยังจุดหมายปลายทาง เมื่อถึงปลายทางจะทำการถอดรหัสที่ส่วนหัวออก วิธีการนี้ช่วยให้ผู้วางระบบเครือข่ายสามารถแบ่ง Virtual LAN เป็นวงย่อยให้เป็นเครือข่ายเดียวกันได้

## รูปแบบบริการ VPN

บริการ VPN แบ่งออกเป็น 3 รูปแบบ

1.) Access VPN: เป็นรูปแบบในการเข้าถึงเครือข่าย VPN จากอุปกรณ์เคลื่อนที่ต่าง ๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ โดยลักษณะแรกเป็นการเข้าถึงจากผู้ใช้คนใดก็ได้ โดยอาศัย ผู้ให้บริการอินเทอร์เน็ตเป็นตัวกลางในการติดต่อ ซึ่งจะมีการเข้ารหัสในการส่งสัญญาณจากเครื่องผู้ใช้ไปยัง ไอเอสพี และลักษณะที่สอง เป็นการเข้าถึงจากเครื่องแอ็กเซสเซอร์ฟเวอร์ (Network Access Server-NAS) ทำงานโดยการผู้ใช้หมุนโมเด็มติดต่อมายังไอเอสพีและจากนั้นจะมีการเข้ารหัสข้อมูลและส่งต่อไปยังปลายทาง

2.) Intranet VPN: เป็นรูปแบบในการเข้าถึงเครือข่าย VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น การต่อเชื่อมเครือข่าย ระหว่างสำนักงานใหญ่ และสาขาย่อย โดยที่แต่ละสาขาสามารถต่อเชื่อมเข้ากับผู้ใช้บริการอินเทอร์เน็ตในท้องถิ่นของตนเพื่อเชื่อมต่อเข้าโครงข่าย VPN ขององค์กรอีกทีหนึ่ง

3.) Extranet VPN: เป็นรูปแบบในการเข้าถึงเครือข่ายที่คล้ายกับอินเทอร์เน็ต VPN โดยมีการขยายวงออกไปยังกลุ่มลูกค้าที่เป็นผู้จัดสรรสินค้า และพาร์ตเนอร์เพื่อให้ใช้เครือข่ายได้ สิ่งสำคัญอย่างหนึ่งในการเลือกติดตั้ง VPN คือการเลือกผู้ให้บริการอินเทอร์เน็ตที่วางระบบรักษาความปลอดภัยเป็นอย่างดี

## บทที่ 3

### ขั้นตอนการดำเนินงาน

#### 3.1 จัดเตรียมเครื่องมือและอุปกรณ์ที่ใช้

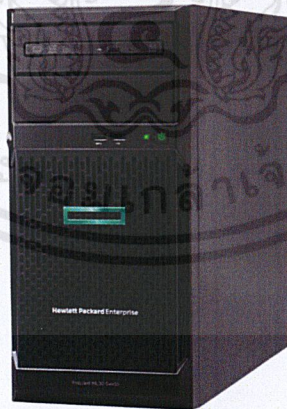
##### 3.1.1 VMware ESXi version 6.5



รูปที่ 3.1 VMware ESXi

(ที่มา: <https://www.codexploitcybersecurity.com/2017/02/data-center-virtualization-with-vmvisor.html>)

##### 3.1.2 เครื่องเซิร์ฟเวอร์ 1 เครื่องสำหรับติดตั้ง VMware ESXi version 6.5



รูปที่ 3.2 เครื่องเซิร์ฟเวอร์

(ที่มา: <https://asis.co.th/server/hp.php>)

### 3.1.3 VMware vSphere Client version 5.5



รูปที่ 3.3 VMware vSphere

(ที่มา: <https://logodix.com/vsphere>)

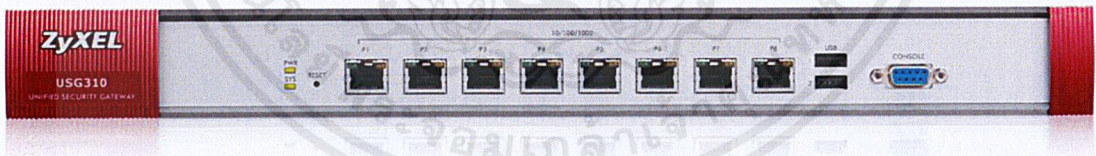
### 3.1.4 Veeam Backup & Replication



รูปที่ 3.4 Veeam

(ที่มา: <https://www.veeam.com/>)

### 3.1.5 Firewall ของ ZyXel (USG310) เป็น Next Generation Firewall



รูปที่ 3.5 Firewall ZyXel (USG310)

(ที่มา: <http://www.zyxelguard.com/USG310.asp>)

## 3.2 ศึกษาข้อมูลการใช้งานของอุปกรณ์และโปรแกรม

### 3.2.1 ศึกษาการใช้งานซอฟต์แวร์ VMware ESXi version 6.5

การใช้งานนั้นมีหลากหลายรูปแบบให้เลือกใช้ตามความเหมาะสมของเครือข่ายที่ต้องการที่จะจำลองขึ้นมา ซึ่งในโครงการนี้ได้สนใจเพียงบางส่วนนั้นคือ

- ศึกษาวิธีการติดตั้งโปรแกรม
- ศึกษาวิธีการตั้งค่าโปรแกรม
- ศึกษาวิธีการกำหนดค่า Virtual Machine
- ศึกษาวิธีการจัดการทรัพยากรของเซิร์ฟเวอร์
- ศึกษาวิธีการเชื่อมต่อระหว่างเน็ตเวิร์คอินเทอร์เน็ตเฟส
- ศึกษาวิธีการเชื่อมต่อ OS ที่จำลองไว้ไปยังซอฟต์แวร์ตัวอื่นๆ รวมถึงการตั้งค่าเน็ตเวิร์คอินเทอร์เน็ตเฟสของ OS นั้น
- ศึกษาการจำลอง OS ต่างๆ

### 3.2.2 ศึกษาการใช้งานซอฟต์แวร์ VMware vSphere Client

- ศึกษาการติดตั้งโปรแกรม
- ศึกษาการตั้งค่า Virtual Machine
- ศึกษาการตั้งค่าเน็ตเวิร์คอินเทอร์เน็ตเฟส
- ศึกษาการกำหนด Permission
- ศึกษาการติดตั้ง Plug-in ของแต่ละ OS
- ศึกษาวิธีการดู Performance
- ศึกษาวิธีการทำ Report
- ศึกษาวิธีการตั้งค่าเพื่อให้สามารถเชื่อมต่อระหว่าง VM และ PC ได้

### 3.2.3 ศึกษาการใช้งานซอฟต์แวร์ Veeam Backup & Replication

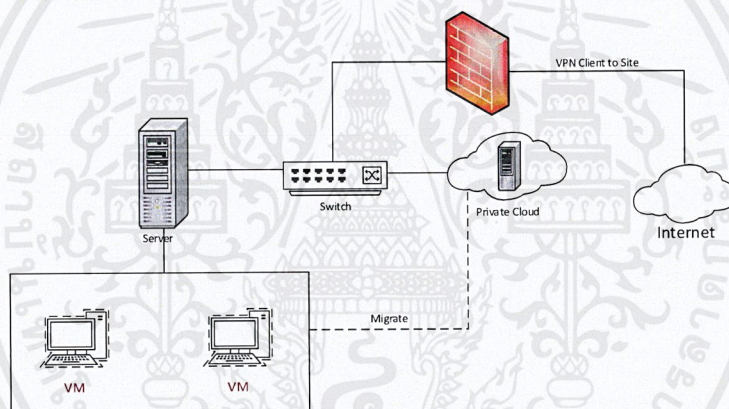
- ศึกษาวิธีการติดตั้งโปรแกรม
- ศึกษาวิธีการทำ Backup
- ศึกษาวิธีการทำ Replication
- ศึกษาวิธีการตั้งค่า Backup
- ศึกษาวิธีการตั้งค่า Replication

### 3.2.4 ศึกษาการใช้งาน Firewall ของ ZyXEL ( ZyWall USG310 )

- ศึกษาวิธีการตั้งค่า firewall
- ศึกษาวิธีการตั้งค่า VPN
- ศึกษาวิธีการตั้งค่า Port Forward

### 3.3 วิเคราะห์และออกแบบ

โครงการนี้ใช้ในการศึกษาวิธีการย้ายเซิร์ฟเวอร์จากเซิร์ฟเวอร์ปกติไปยังเซิร์ฟเวอร์ที่เป็นระบบคลาวด์ส่วนตัว (Private Cloud) โดยทำไปเพื่อให้สามารถจัดการโครงสร้างของเซิร์ฟเวอร์ของบริษัทผ่านอินเทอร์เน็ตได้และสามารถติดตามสถานะของเซิร์ฟเวอร์เพื่อความสะดวกและง่ายต่อการจัดการและทำการติดตั้งระบบสำรองข้อมูลอัตโนมัติเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับเซิร์ฟเวอร์ได้



รูปที่ 3.6 ไดอะแกรม

จากไดอะแกรมที่ได้ออกแบบไว้ข้างต้นได้มีการกำหนด IP Address และ Port ที่ใช้ในการทดลอง ตารางดังกล่าวต่อไปนี้

ตาราง 3.1 แสดงชื่ออุปกรณ์และ IP Address ที่กำหนด

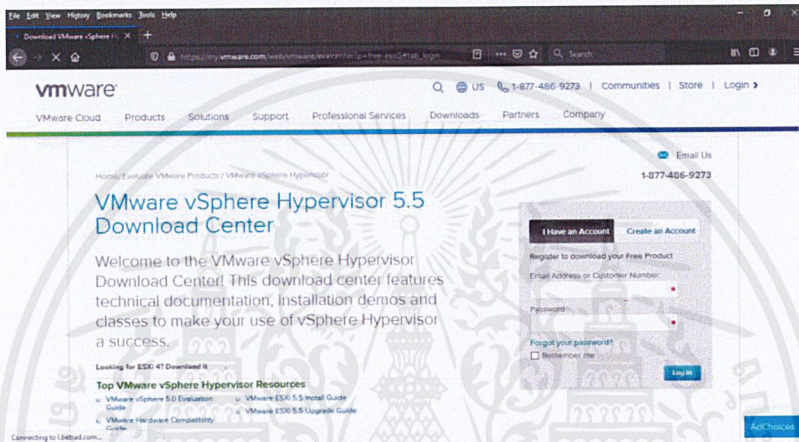
Devices	IP Address
Firewall	192.168.10.254
Server ESXi v.5.5	192.168.10.195
Server ESXi v.6.5	192.168.10.5
Server ( VM ) VtigerCRM	192.168.10.42
Veeam Backup & Replication ( VM )	192.168.10.16

### 3.4 ติดตั้ง VMware ESXi version 6.5

การทดลองนี้เป็นการทดลองเพื่อให้นักศึกษาได้มีความรู้และความเข้าใจในการย้ายเซิร์ฟเวอร์จากเซิร์ฟเวอร์ปกติไปยังเซิร์ฟเวอร์ที่เป็นคลาวด์ส่วนตัวเพื่อให้นักศึกษาเข้าใจกระบวนการทั้งหมดและสามารถนำไปใช้ในการติดตั้งเซิร์ฟเวอร์

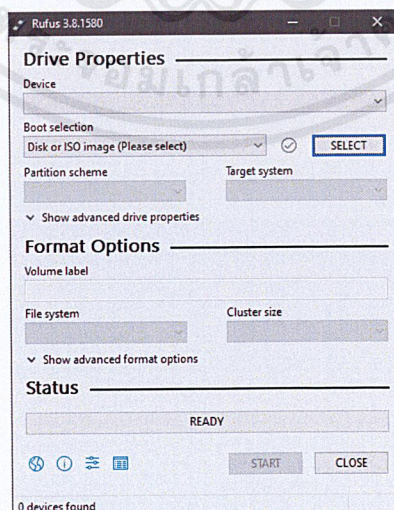
- 1) ทำการดาวน์โหลดซอฟต์แวร์ VMware ESXi version 6.5 ได้จาก

<https://my.vmware.com/group/vmware/> แต่ต้องทำการสมัครสมาชิกแล้วเข้าสู่ระบบก่อนถึงจะสามารถดาวน์โหลดซอฟต์แวร์ได้



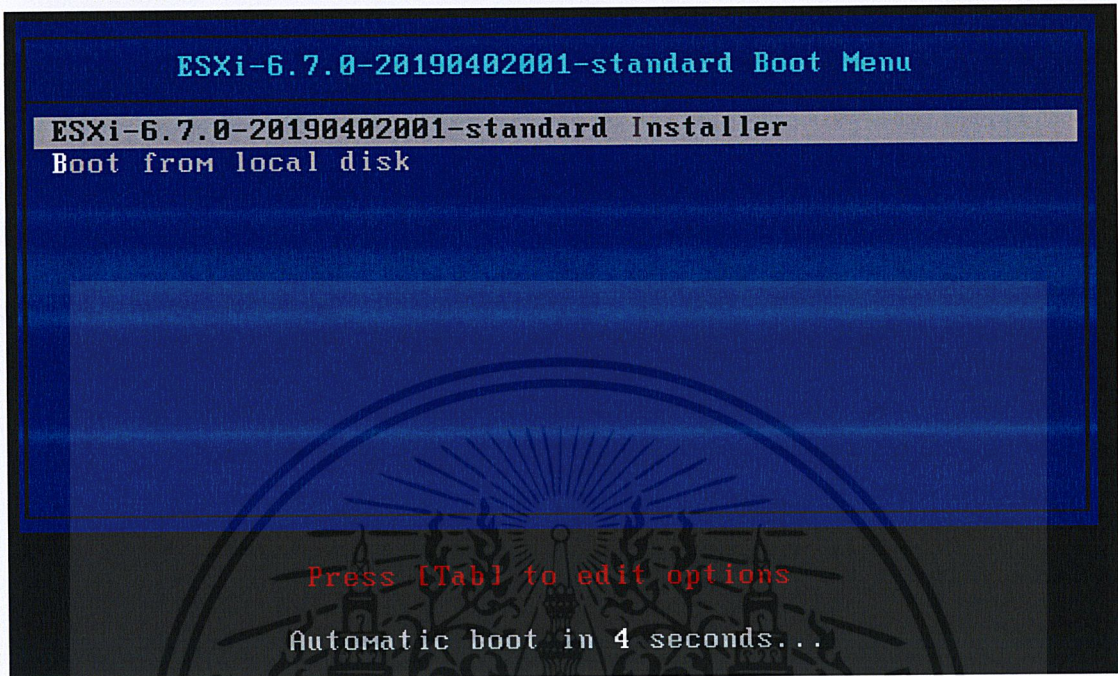
รูปที่ 3.7 หน้าเว็บเพจของ VMware สำหรับดาวน์โหลดไฟล์

- 2) สร้างตัวไดรฟ์บูตยูเอสบีเพื่อติดตั้งไฟล์อิมเมจของ VMware ESXi version 6.5 ลงบนเครื่องเซิร์ฟเวอร์โดยใช้โปรแกรม Rufus ในการบูตไฟล์อิมเมจลงแฟลชไดรฟ์โดยดาวน์โหลดตัวติดตั้ง Rufus ได้จาก <https://rufus.ie/>



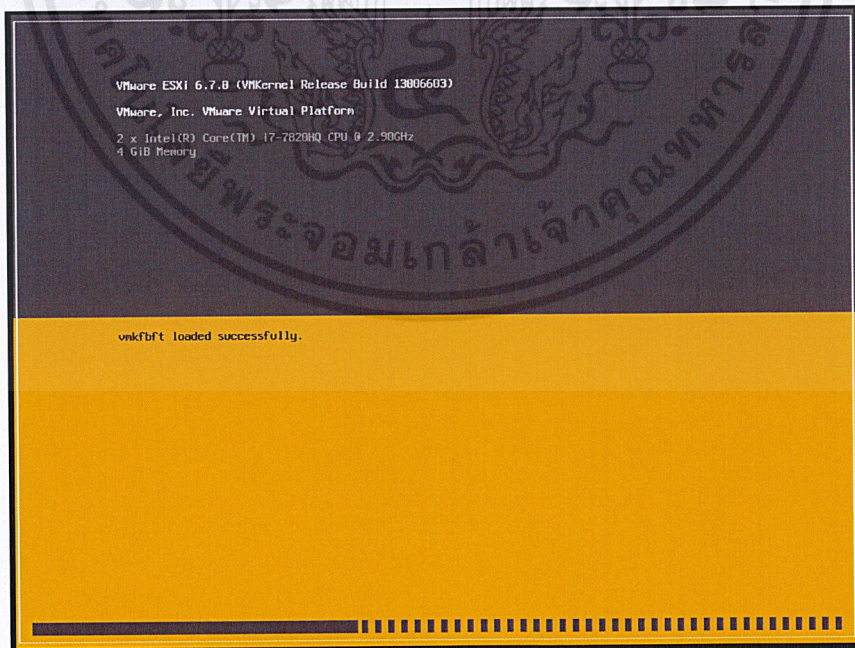
รูปที่ 3.8 โปรแกรม Rufus

3) นำไปติดตั้งที่เครื่องเซิร์ฟเวอร์โดยการบูตผ่านแฟลชไดรฟ์



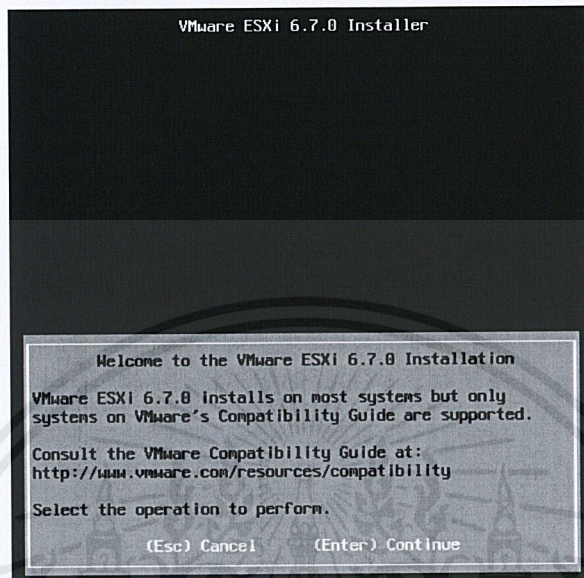
รูปที่ 3.9 บูต VMware ESXi version 6.5 ผ่านแฟลชไดรฟ์

4) ทำการเข้าสู่หน้าจอการติดตั้ง



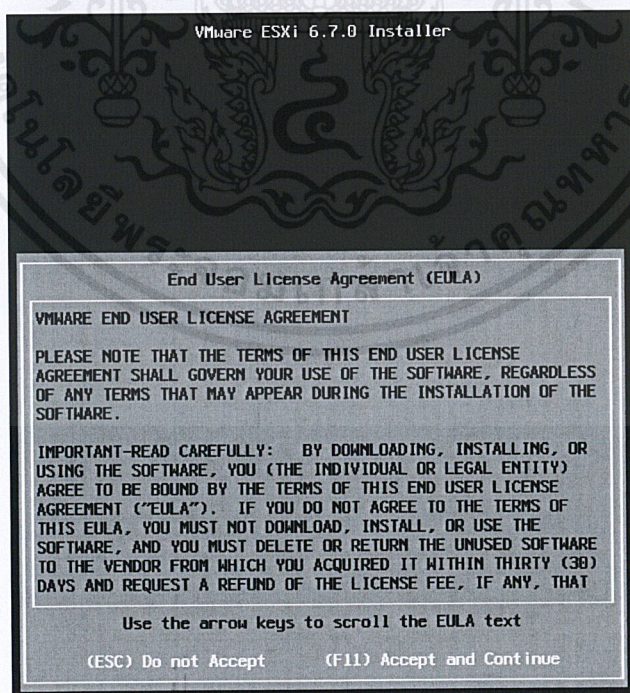
รูปที่ 3.10 หน้าจอการติดตั้ง VMware ESXi

5) เมื่อติดตั้งเสร็จจะแสดงหน้าต่างดังรูปด้านล่าง



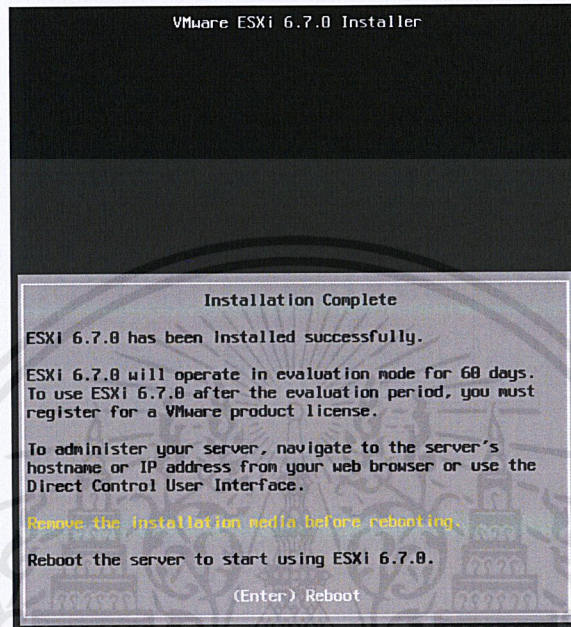
รูปที่ 3.11 หลังการติดตั้งเสร็จ

6) ยอมรับข้อตกลงของ VMware ESXi



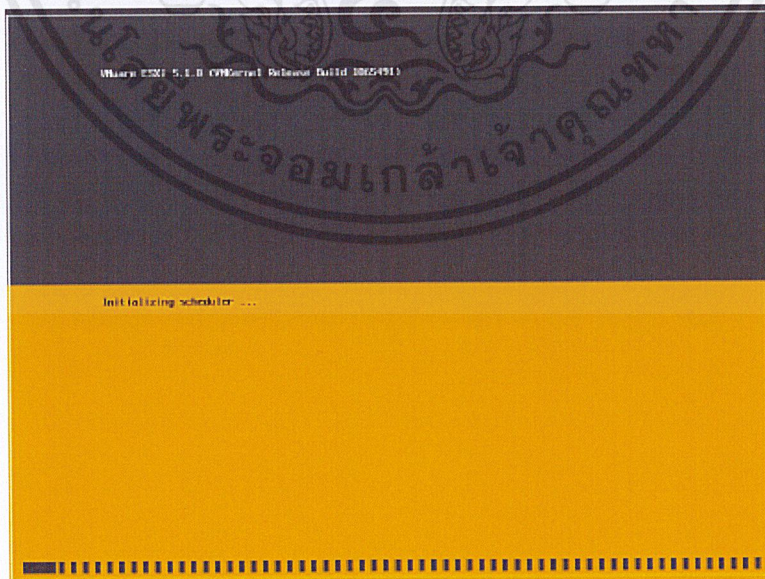
รูปที่ 3.12 ข้อตกลงการใช้งานของ VMware ESXi

7) เมื่อติดตั้งเสร็จจะทำการรีบูตเครื่องเซิร์ฟเวอร์



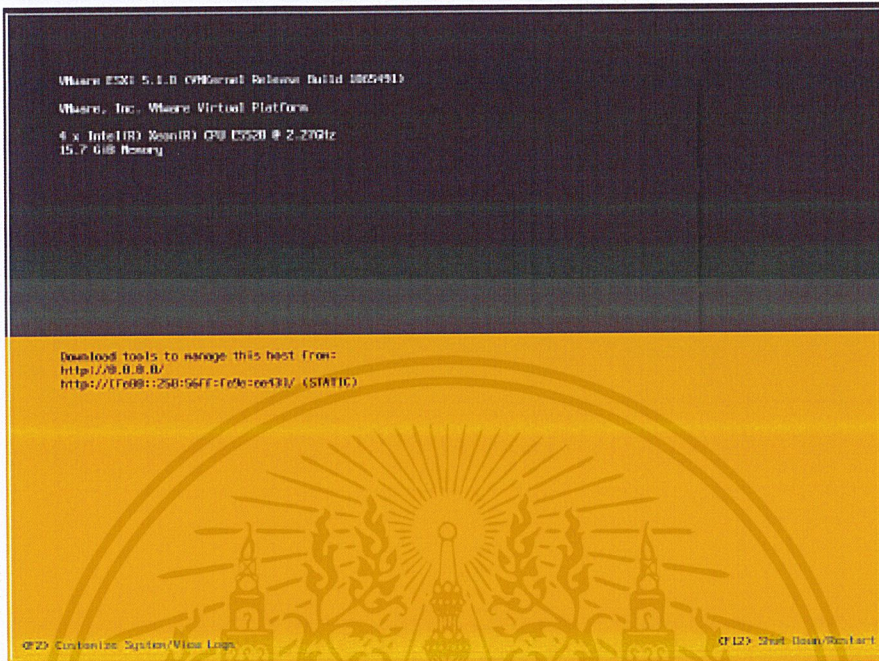
รูปที่ 3.13 ทำการรีบูตเครื่องเซิร์ฟเวอร์

8) เริ่มเข้าสู่หน้า VMware ESXi Version 6.5



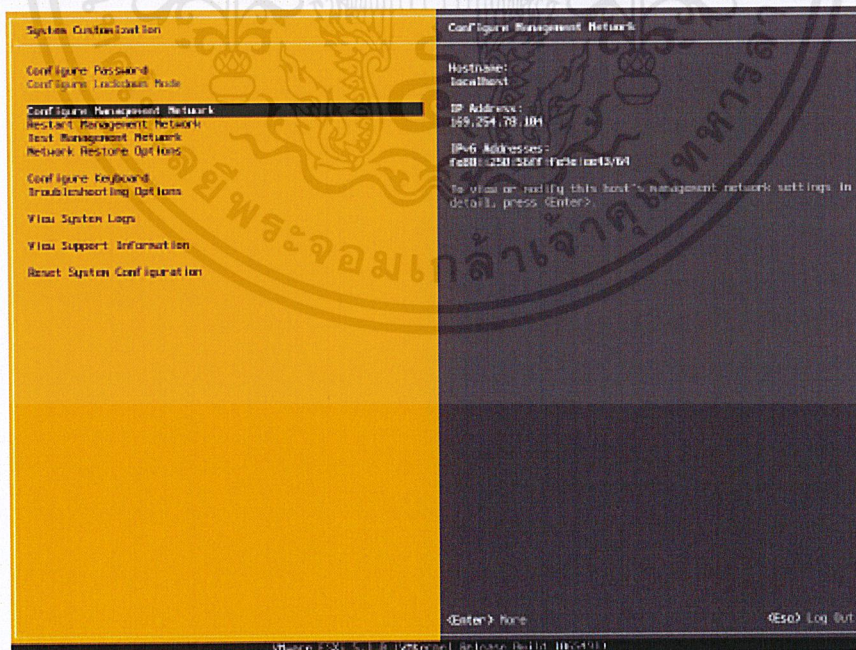
รูปที่ 3.14 เข้าสู่หน้า VMware ESXi

9) หน้าจอการทำงานของ VMware ESXi version 6.5 เข้าไปหน้า Customize โดยกดปุ่ม F12



รูปที่ 3.15 หน้าจอแสดงถึงการทำงานของ VMware ESXi

10) หน้า System Customization

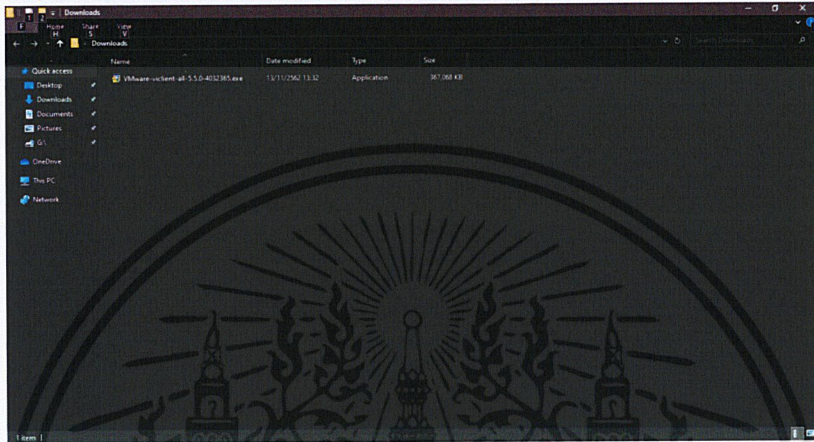


รูปที่ 3.16 หน้า Customization

### 3.5 ติดตั้งโปรแกรม VMware vSphere Client

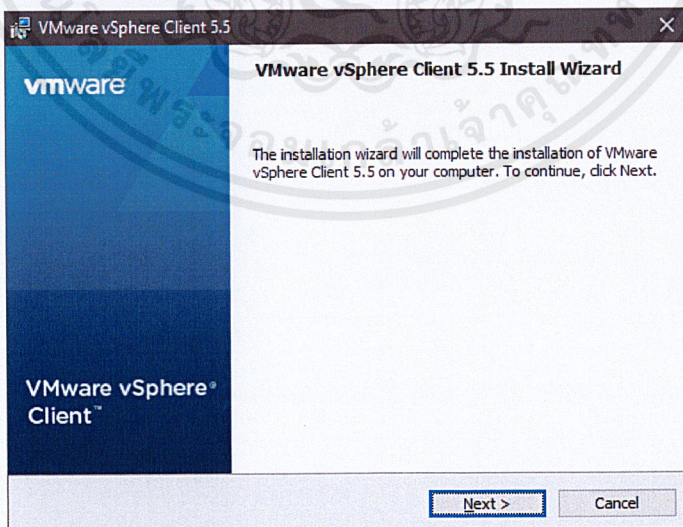
เป็นซอฟต์แวร์ที่ใช้งานการจัดการเซิร์ฟเวอร์ VMware ESXi version 5.5

- 1) ทำการดาวน์โหลดได้จาก <https://kb.vmware.com/s/article/2089791?/>
- 2) เมื่อดาวน์โหลดเรียบร้อยแล้ว จะได้ไฟล์ VMware-viclient-all-5.5.0-4032365.exe



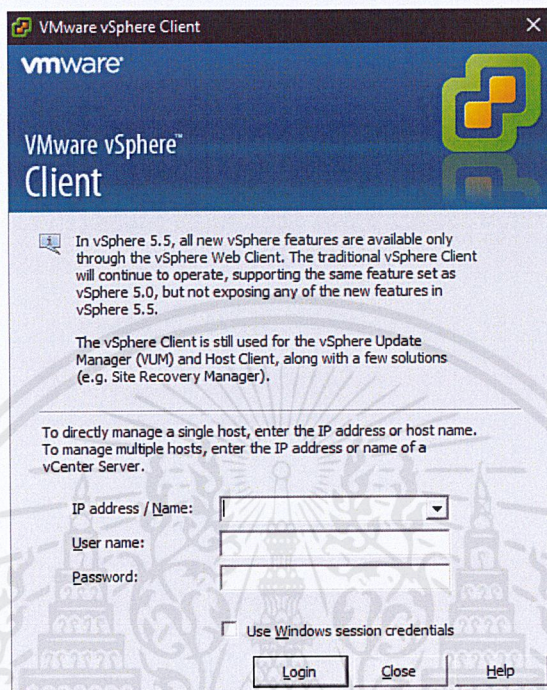
รูปที่ 3.17 ไฟล์ตัวติดตั้ง VMware vSphere Client

- 3) ทำการดับเบิลคลิก ที่ไฟล์เพื่อทำการติดตั้ง
- 4) จะปรากฏหน้าต่างสำหรับการติดตั้ง VMware vSphere



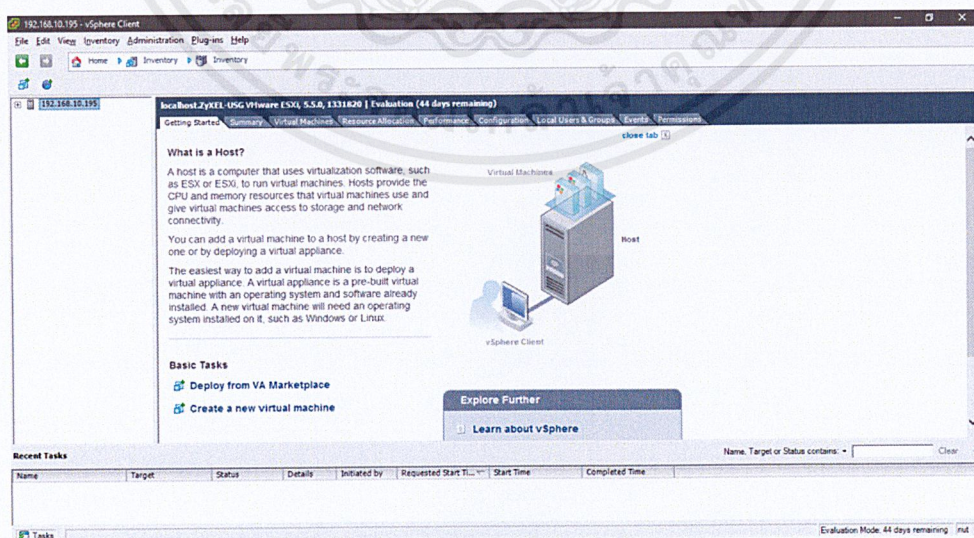
รูปที่ 3.18 หน้า install VMware vSphere Client

- 5) ทำการเข้าโปรแกรมและล็อกอินเข้าสู่ระบบ VMware ESXi version 5.5 โดยใช้ VMware vSphere Client



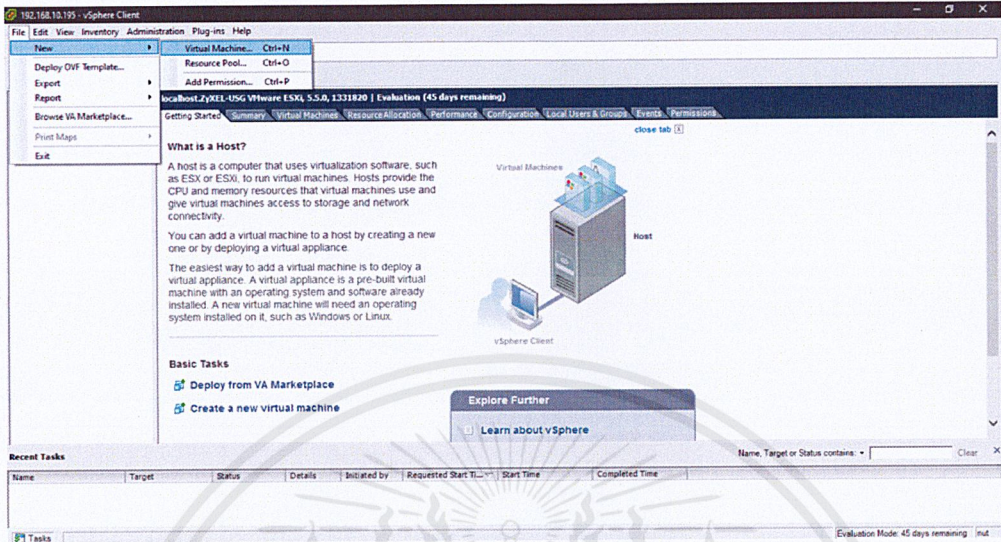
รูปที่ 3.19 หน้าเข้าสู่ระบบ VMware vSphere Client

- 6) หลังจากทำการเข้าสู่ระบบจะพบหน้าต่างดังรูป



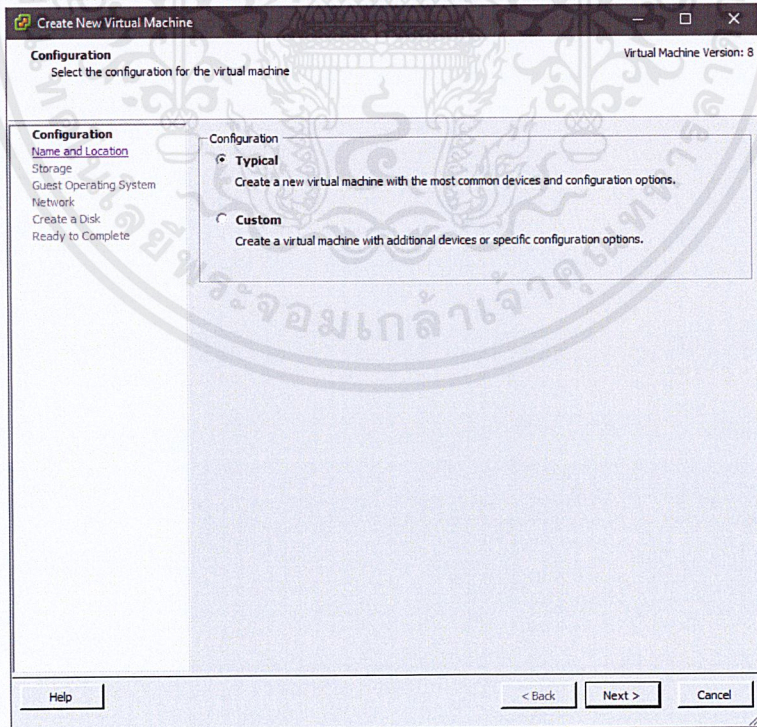
รูปที่ 3.20 หน้าแรกหลังจากเข้าสู่ระบบ

7) สร้างคอมพิวเตอร์เสมือน (Virtual Machine) ขึ้นมา 1 ตัว



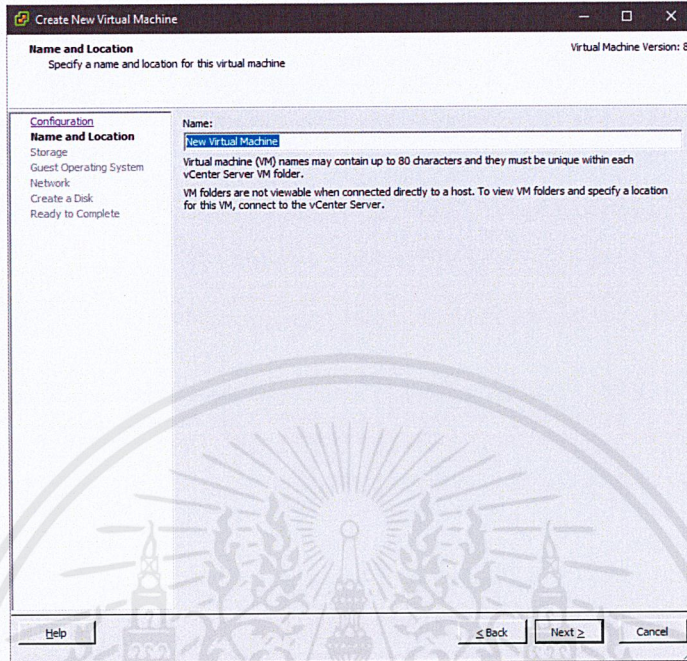
รูปที่ 3.21 สร้างคอมพิวเตอร์เสมือน

8) เลือกการกำหนดค่าแบบ Typical



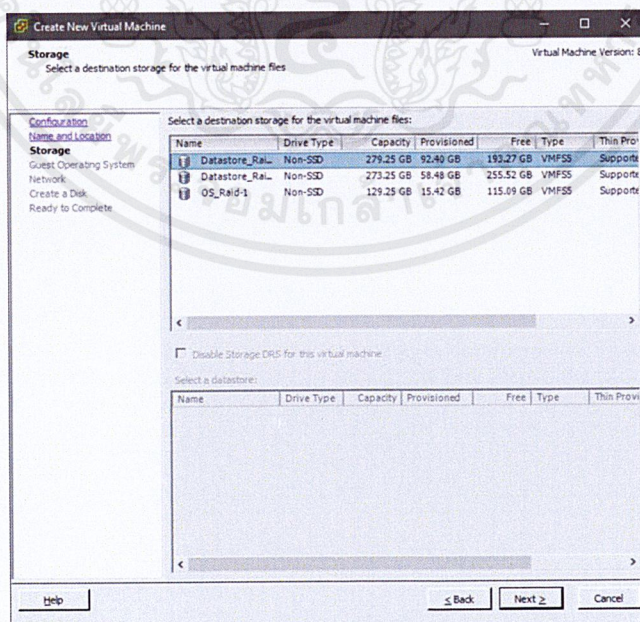
รูปที่ 3.22 Config คอมพิวเตอร์เสมือนเป็นชนิด Typical

9) ตั้งชื่อคอมพิวเตอร์เสมือน



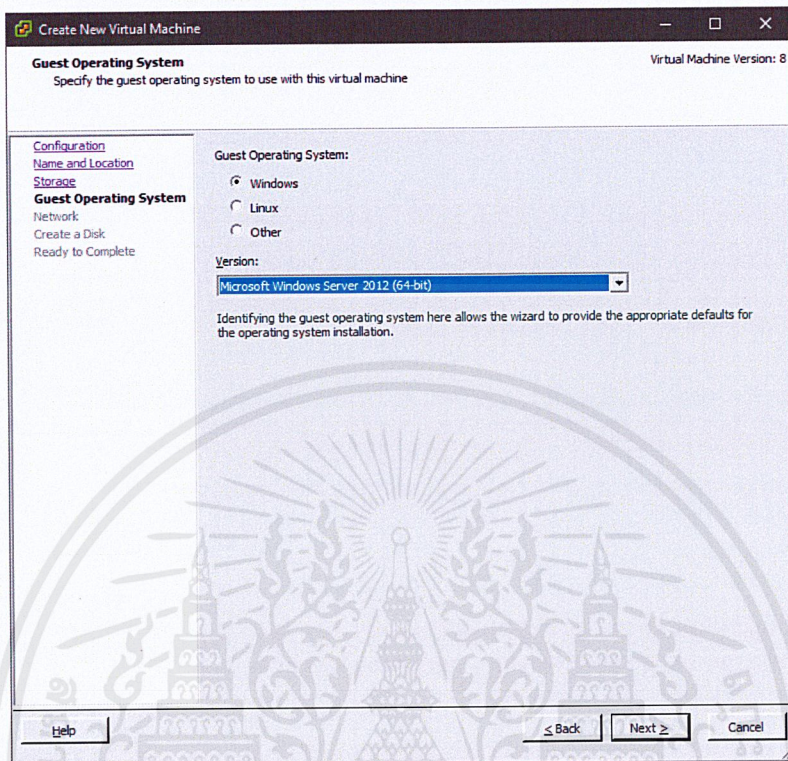
รูปที่ 3.23 ตั้งชื่อให้คอมพิวเตอร์เสมือน

10) เลือกพื้นที่จัดเก็บ (Storage) ที่จะทำการติดตั้ง



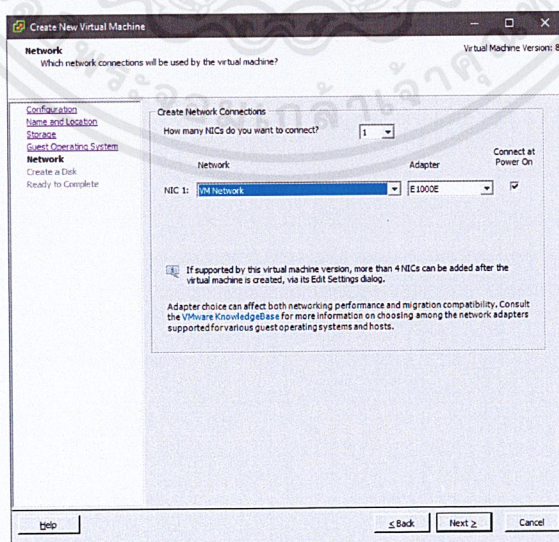
รูปที่ 3.24 เลือกพื้นที่จัดเก็บ

## 11) เลือกระบบปฏิบัติการให้กับคอมพิวเตอร์เสมือน (Virtual Machine)



รูปที่ 3.25 เลือกระบบปฏิบัติการให้กับคอมพิวเตอร์เสมือน

## 12) ทำการเพิ่ม NIC (Network Interface Card)



รูปที่ 3.26 เพิ่ม NIC ( Network Interface Card )

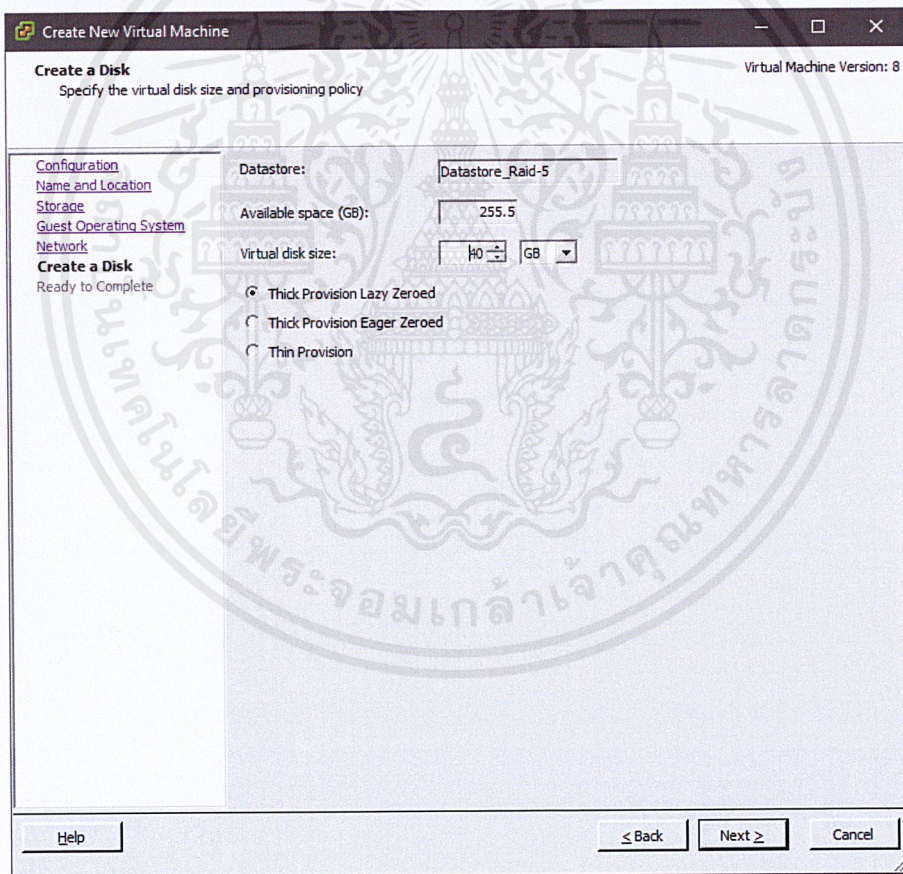
13) กำหนดค่าดิสก์ให้ GuestOS พร้อมกับเลือกชนิดของ Disk Provisioning เป็นแบบ Thick Provision Lazy Zeroed

บน VMware ESXi มีอยู่ด้วยกัน 3 รูปแบบ

1. Thick Provision Eager Zeroed เป็นการกันพื้นที่ให้เท่าที่เรากำหนดจริง และจะทำการ zero fill (การใส่ค่า 0 ลงไปทุก ๆ เซกเตอร์ เพื่อเป็นการเคลียร์ข้อมูลใหม่ทั้งหมด)

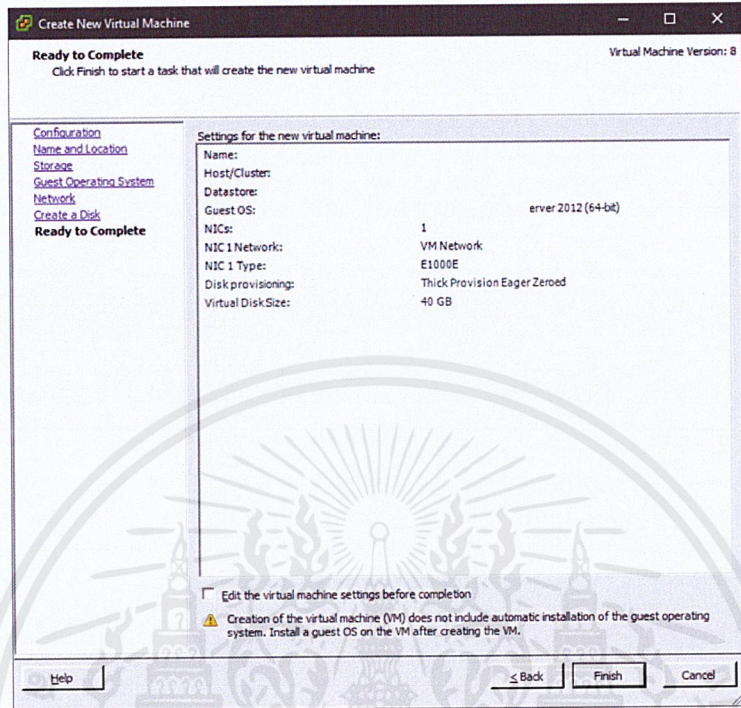
2. Thick Provision Lazy Zeroed คล้าย ๆ กับแบบแรก แต่ไม่ได้ทำ zero fill ให้แบบนี้จะมีประสิทธิภาพไม่ดีเท่าแบบแรก

3. Thin Provision จะช่วยในเรื่องประหยัดพื้นที่ดิสก์จริง ขนาดจะค่อย ๆ โตขึ้นเรื่อย ๆ ตามข้อมูลที่จัดเก็บจริง



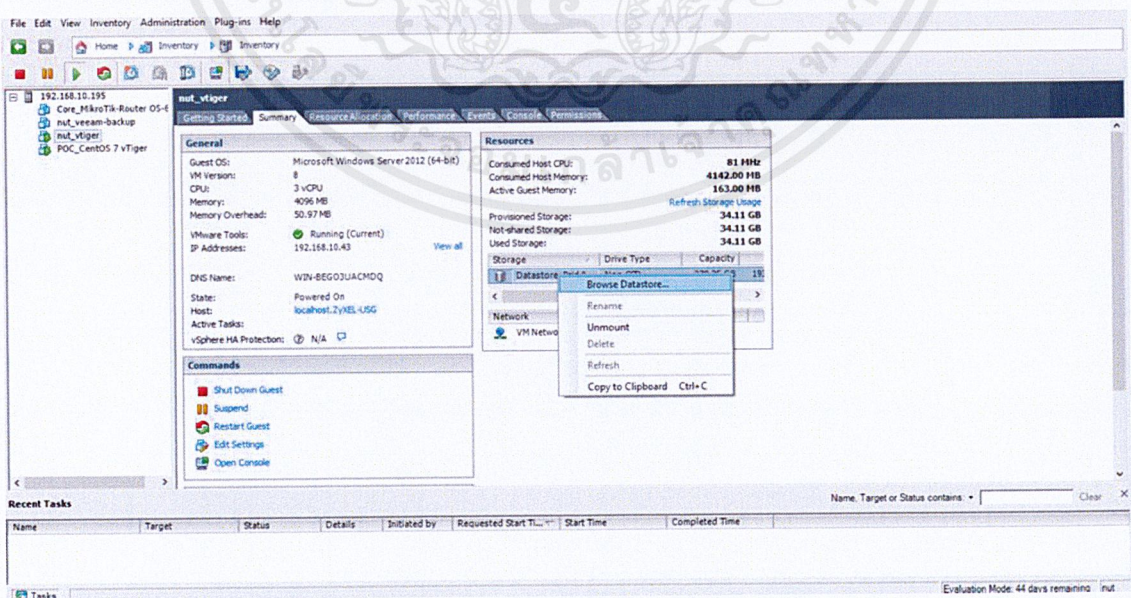
รูปที่ 3.27 กำหนดค่าดิสก์ให้กับ GuestOS

14) ตรวจสอบอีกครั้งก่อนยืนยันการสร้าง



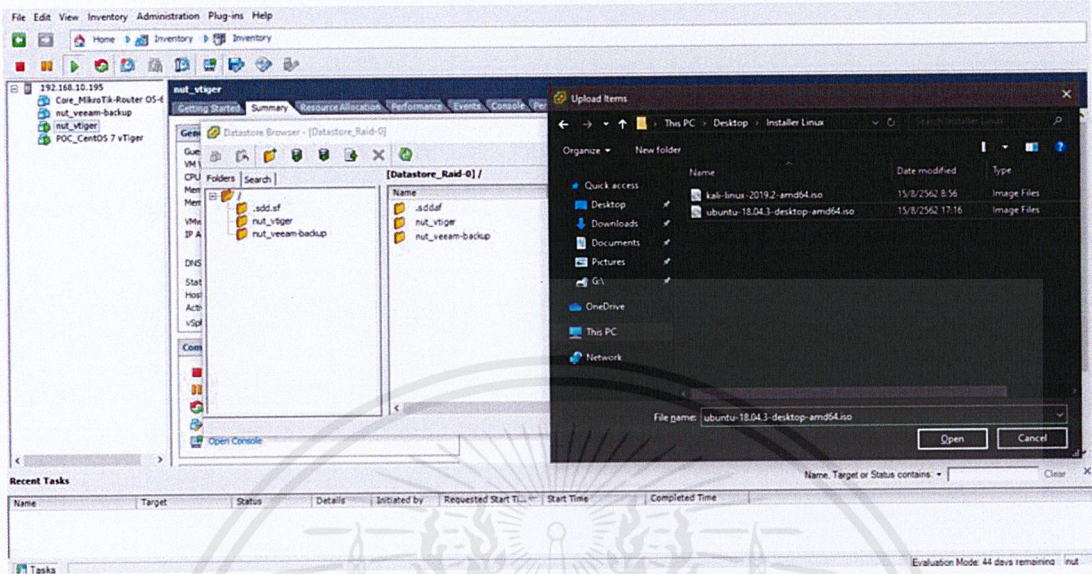
รูปที่ 3.28 ตรวจสอบอีกครั้งก่อนยืนยันการสร้าง

15) ทำการติดตั้งระบบปฏิบัติการที่ต้องการลงในคอมพิวเตอร์เสมือน (Virtual Machine)



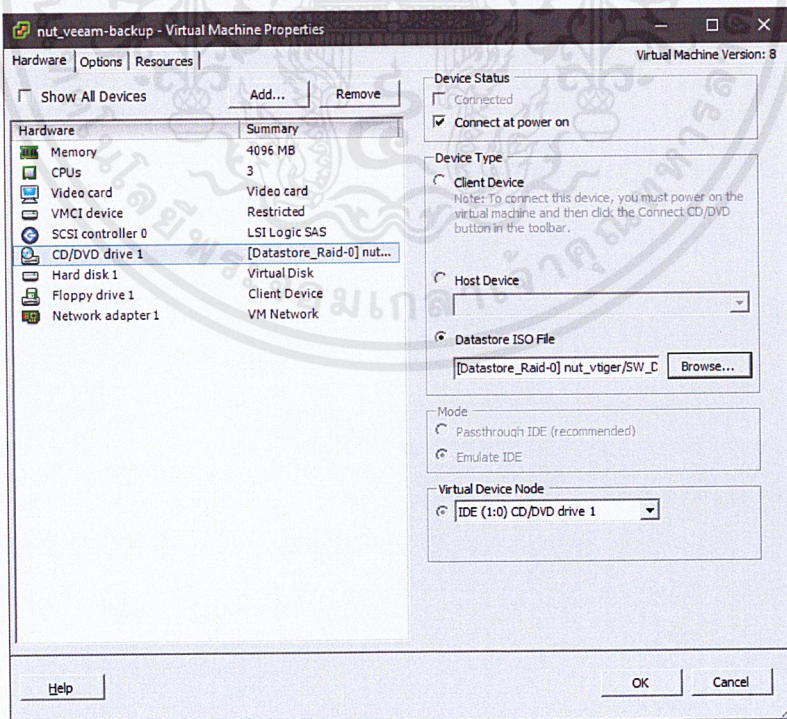
รูปที่ 3.29 ทำการติดตั้งระบบปฏิบัติการ

16) เพิ่มไฟล์ตัวติดตั้งระบบปฏิบัติการลงในหน่วยเก็บของตัวเครื่องเซิร์ฟเวอร์



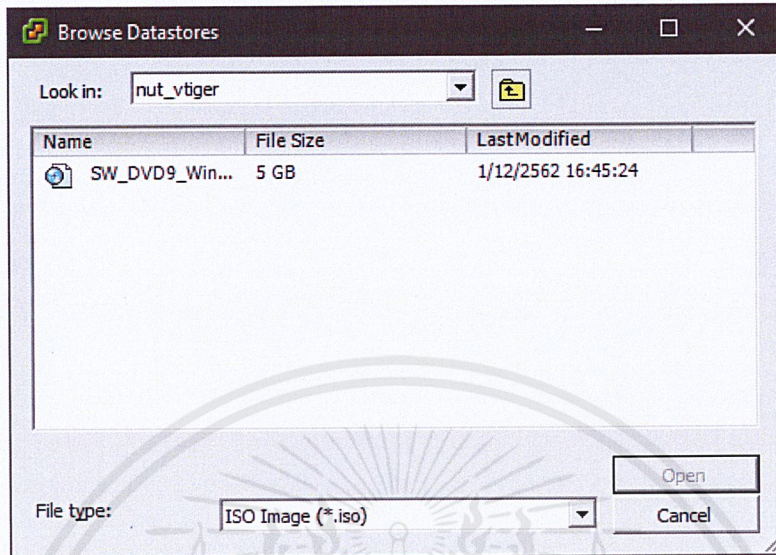
รูปที่ 3.30 เพิ่มไฟล์ตัวติดตั้งเข้าไปในหน่วยเก็บของเครื่องเซิร์ฟเวอร์

17) ทำการเพิ่มไฟล์ไปที่ CD/DVD เพื่อใช้ในการอ่านไฟล์ตัวติดตั้งระบบปฏิบัติการ



รูปที่ 3.31 ค้นหาไฟล์ที่จะติดตั้งลงบนคอมพิวเตอร์เสมือน

18) กด Browse เพื่อหาไฟล์ที่ต้องการติดตั้ง

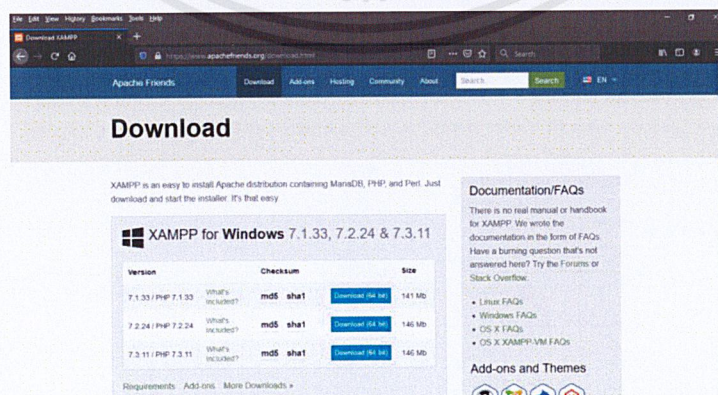


รูปที่ 3.32 เลือกไฟล์ตัวติดตั้งคอมพิวเตอร์เสมือนและทำการติดตั้ง

### 3.6 ติดตั้งเซิร์ฟเวอร์ VtigerCRM Version 7.0.0

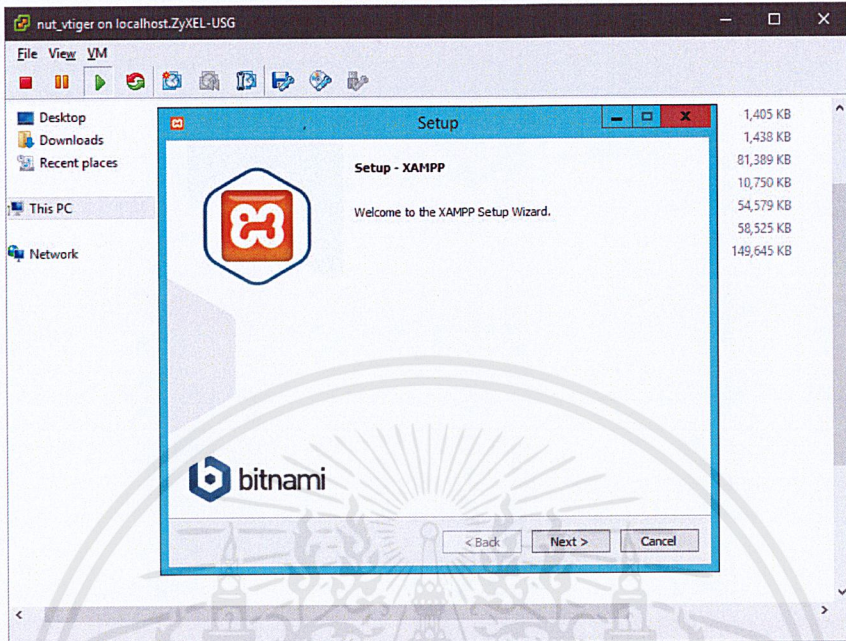
เป็นโปรแกรมโอเพนซอร์สซอฟต์แวร์ที่เปิดให้ใช้งานได้ฟรีเหมาะสำหรับธุรกิจขนาดกลางและขนาดย่อม VtigerCRM สามารถปรับแต่งตามความต้องการ และยังให้บริการปรับแต่งหรือเพิ่มเติมในส่วนขอความต้องการใหม่ ๆ

- 1) ทำการดาวน์โหลดตัว Apache เพื่อใช้งาน Web Server โดยตัวที่ใช้เป็น Xampp โดยสามารถโหลดได้จาก <https://www.apachefriends.org/download.html>



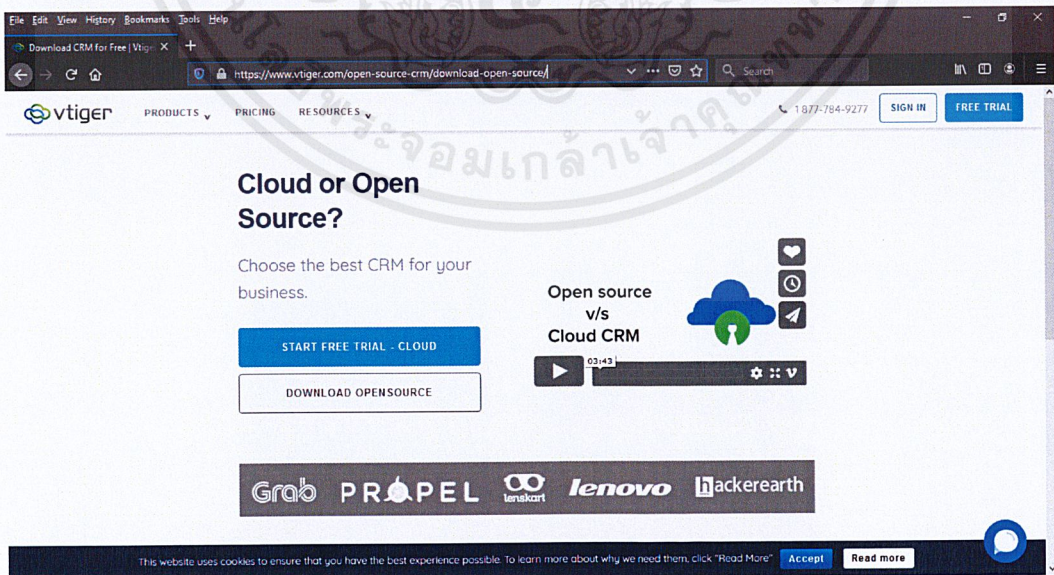
รูปที่ 3.33 หน้าเว็บเพจของ Xampp สำหรับดาวน์โหลดไฟล์

2) ทำการติดตั้ง Xampp ในตัวคอมพิวเตอร์เสมือน



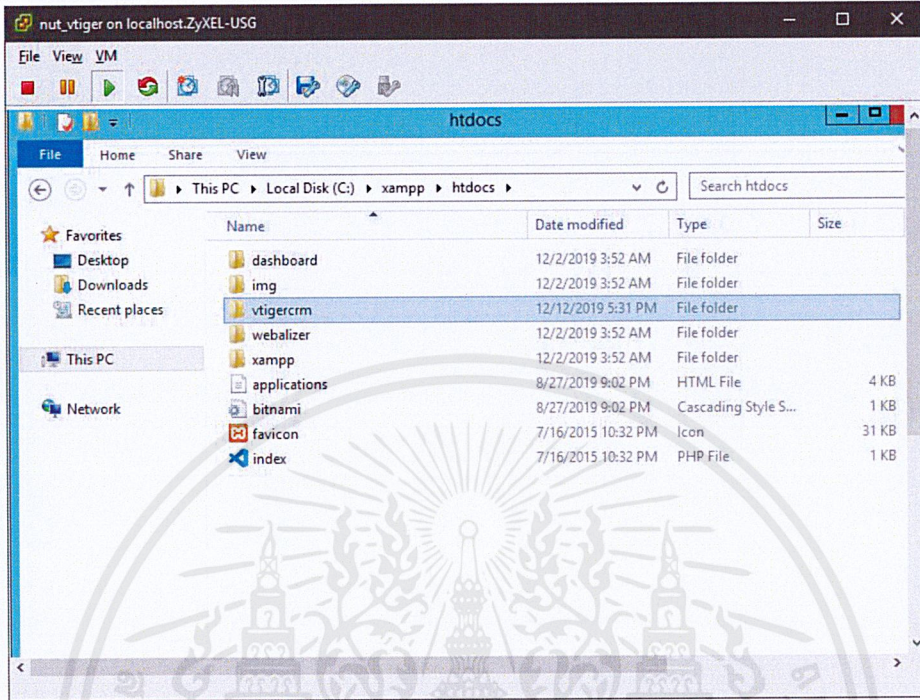
รูปที่ 3.34 ติดตั้ง Xampp

3) ทำการดาวน์โหลดตัวติดตั้ง VtigerCRM ได้จาก <https://www.vtiger.com/open-source-crm/download-open-source/>



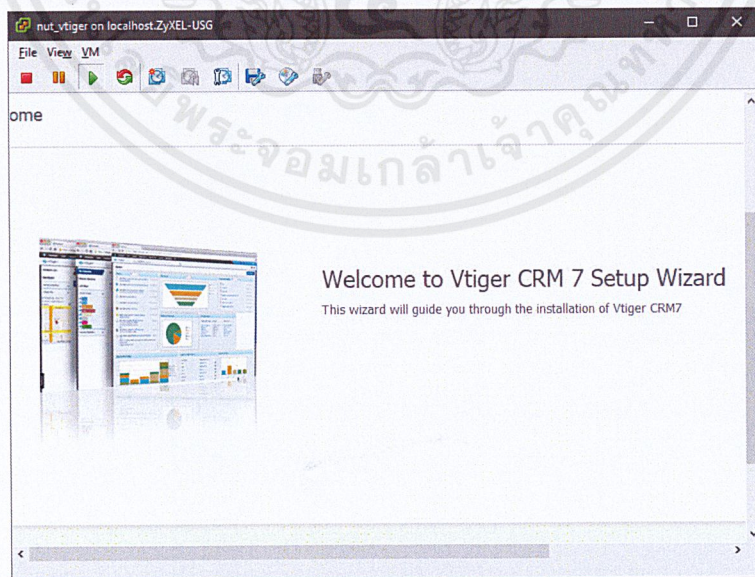
รูปที่ 3.35 หน้าเว็บเพจของ VtigerCRM สำหรับดาวน์โหลดไฟล์

4) ทำการแตกไฟล์ Zip แล้วนำไฟล์เตอร์ไปไว้ที่ htdocs ซึ่งอยู่ในโฟลเดอร์ที่ติดตั้งของ Xampp



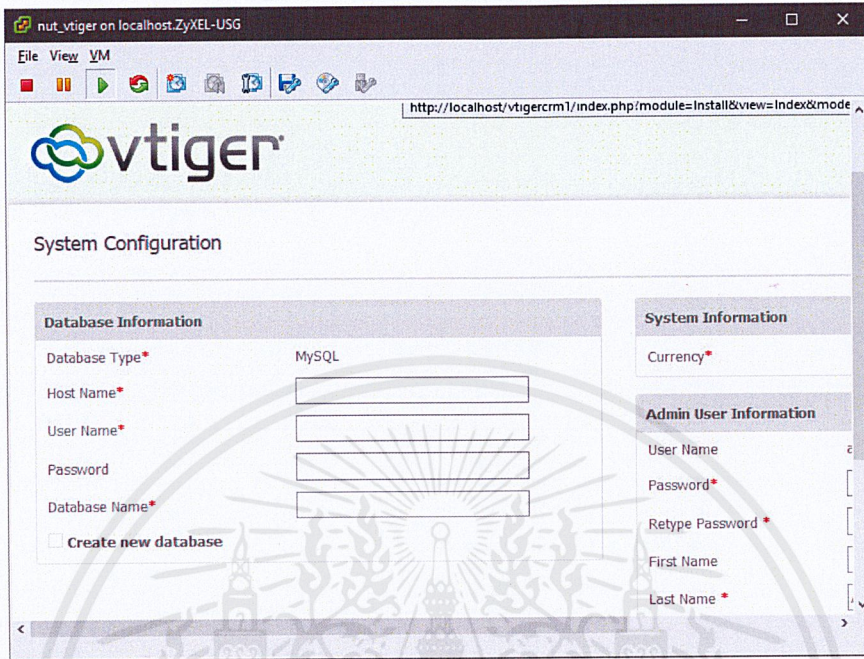
รูปที่ 3.36 แยกไฟล์ Zip

5) ทำการเข้าถึง <http://localhost/> (ตามด้วยชื่อโฟลเดอร์ของ VtigerCRM)



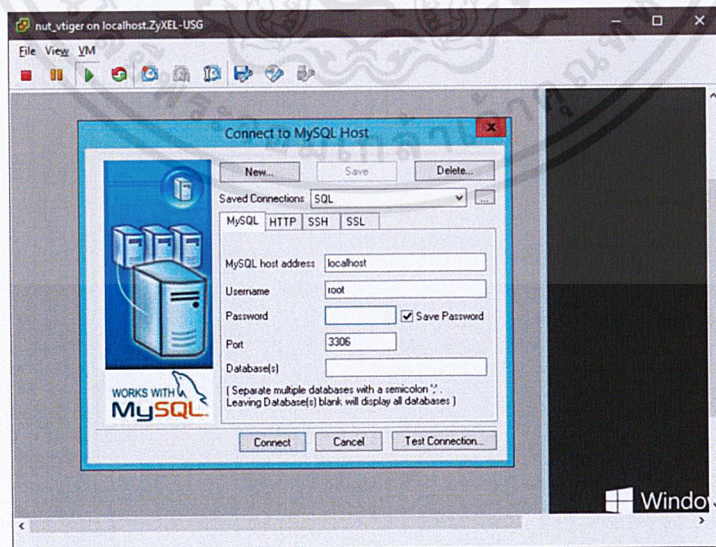
รูปที่ 3.37 เข้าสู่หน้าติดตั้ง VtigerCRM

6) ทำการตั้งค่าระบบของเซิร์ฟเวอร์ VtigerCRM



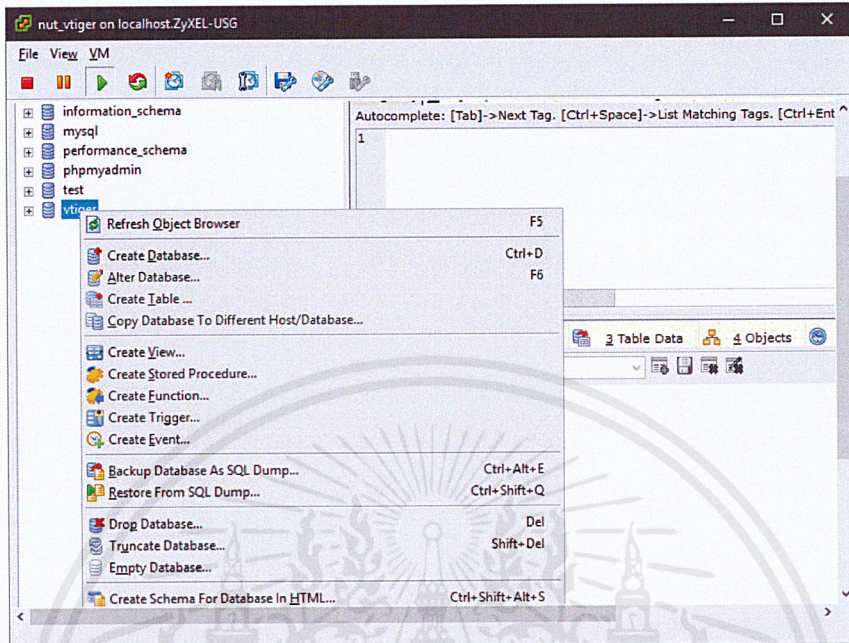
รูปที่ 3.38 ตั้งค่าระบบเซิร์ฟเวอร์ VtigerCRM

7) ทำการเข้าสู่ระบบ MySQL โดยใช้โปรแกรม SQLyog โดยสามารถดาวน์โหลดตัวติดตั้ง SQLyog ได้จาก <https://sqlyog.th.softonic.com/>



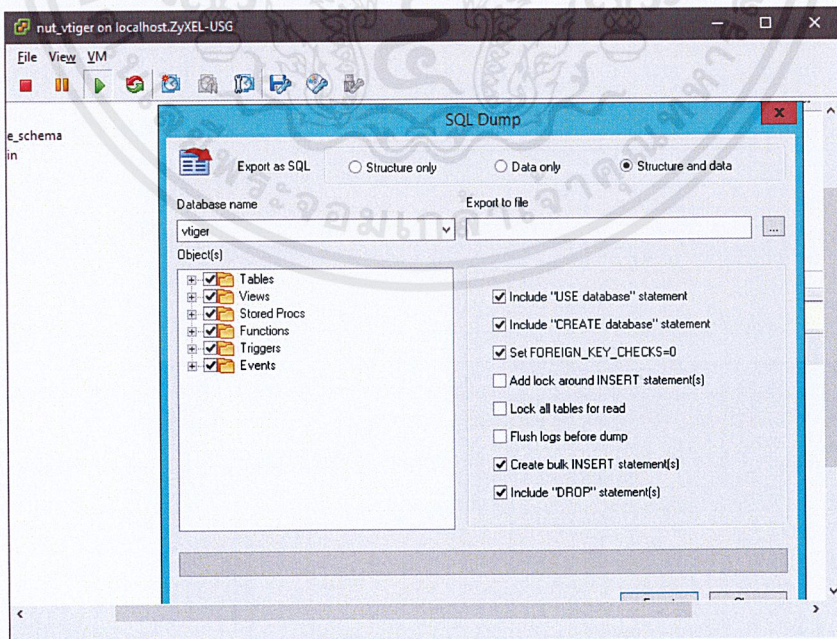
รูปที่ 3.39 เข้าสู่ระบบ MySQL

8) คลิกขวาที่ฐานข้อมูลของเซิร์ฟเวอร์ VtigerCRM



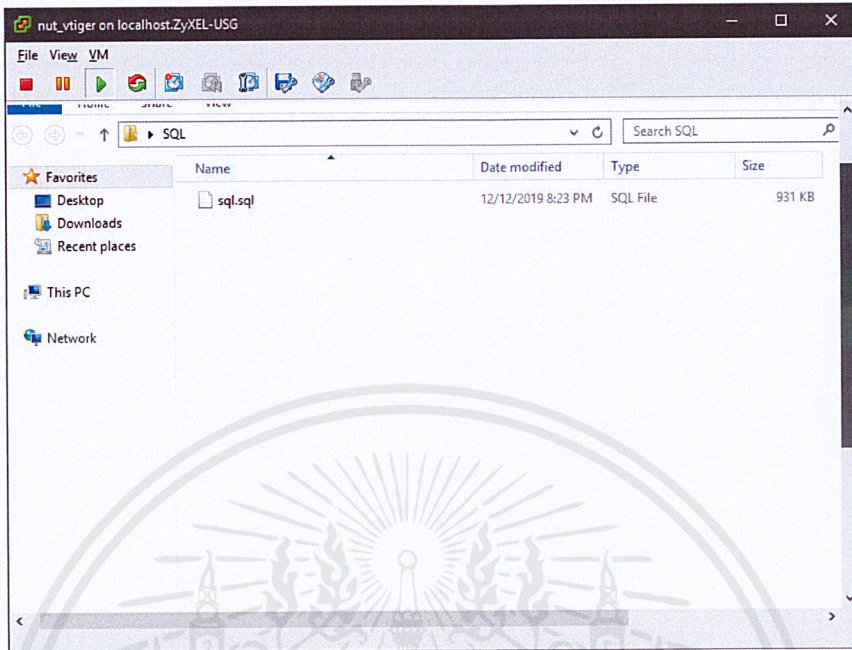
รูปที่ 3.40 หน้าแรกเมื่อเข้าสู่ระบบ

9) ทำการส่งออกฐานข้อมูลของตัว VtigerCRM ที่บริษัทใช้อยู่โดยใช้โปรแกรม SQLyog



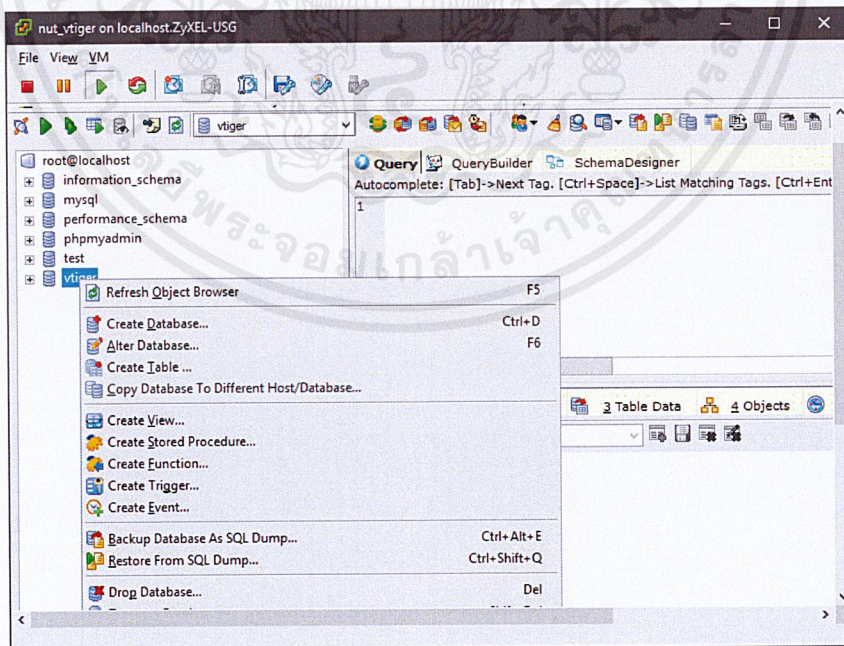
รูปที่ 3.41 การส่งออกฐานข้อมูล

10) จะได้ไฟล์ .SQL มาดังรูป



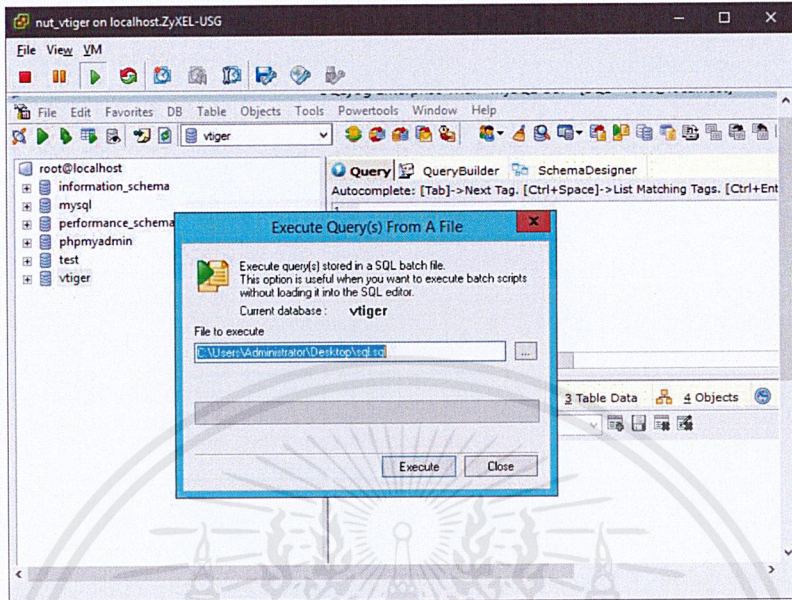
รูปที่ 3.42 ไฟล์ SQL ที่ได้จากการส่งออก

11) ทำการกู้คืนข้อมูลโดยคลิกขวาที่ฐานข้อมูลที่เราต้องการนำข้อมูลเข้าไปที่ตัวฐานข้อมูล



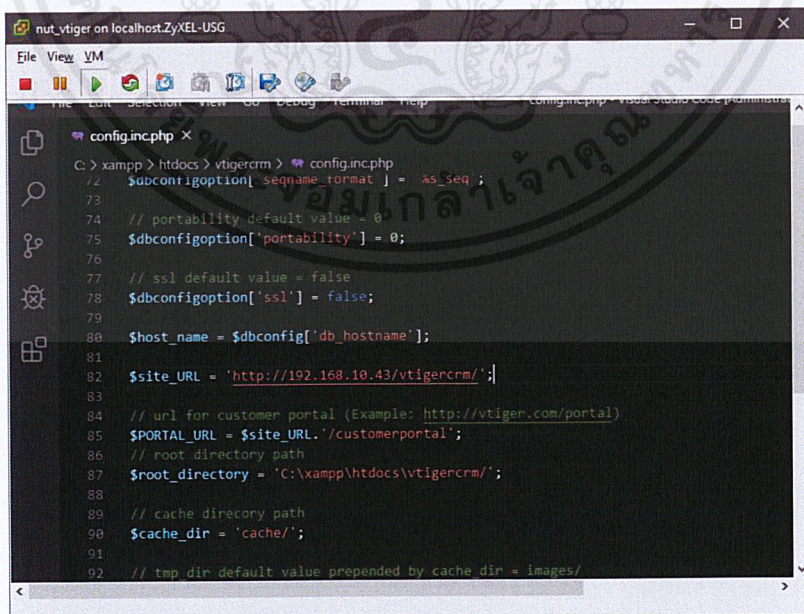
รูปที่ 3.43 เลือกฐานข้อมูลที่จะนำเข้า

12) ทำการเลือกที่มาของไฟล์ที่เราได้จัดเก็บไว้ก่อนหน้านี้แล้วกด Execute และรอจนเสร็จสิ้น



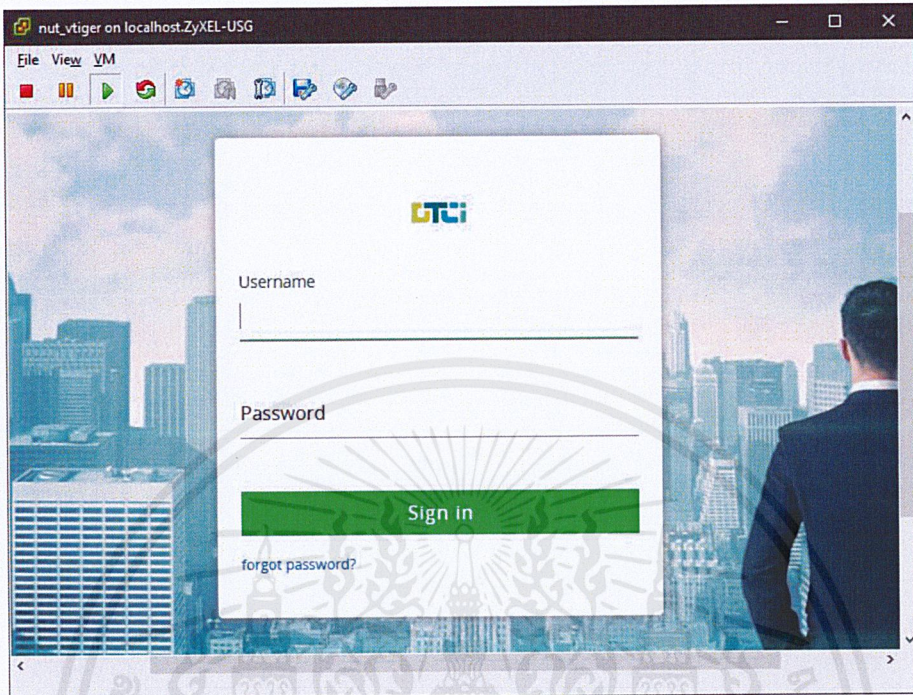
รูปที่ 3.44 การนำเข้าฐานข้อมูล

13) ทำการแก้ไขไฟล์ config โดยตั้ง Site URL ให้เป็น IP เครื่องของเซิร์ฟเวอร์ VtigerCRM เพื่อให้เครื่องที่อยู่ในวง LAN (Local Area Network) ของบริษัทสามารถเข้าใช้งาน VtigerCRM ได้



รูปที่ 3.45 แก้ไขค่า Config

14) ลองเข้าใช้ VtigerCRM โดยเข้าตาม URL ที่ได้ตั้งค่าไปก่อนหน้านี้



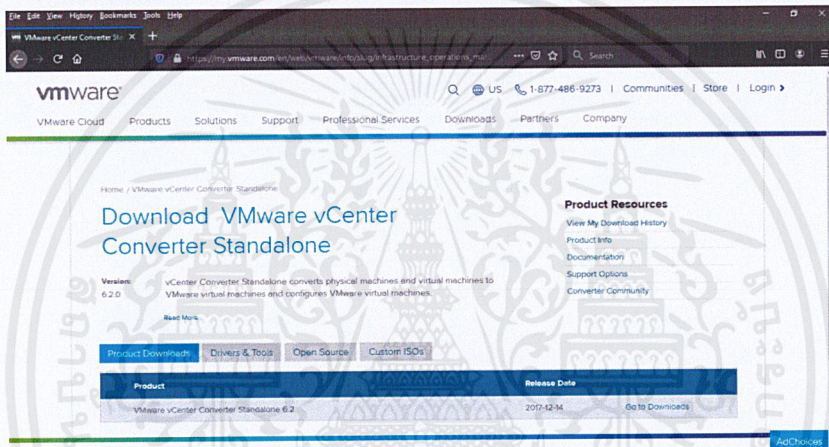
รูปที่ 3.46 หน้าเข้าสู่ระบบของ VtigerCRM

### 3.7 ติดตั้งโปรแกรม VMware vCenter Converter Standalone Client

โปรแกรมนี้เป็นโปรแกรมที่ใช้ในการย้ายเซิร์ฟเวอร์ที่เป็นคอมพิวเตอร์เสมือน (Virtual Machine) จากเซิร์ฟเวอร์อีกตัวไปยังเซิร์ฟเวอร์อีกตัว

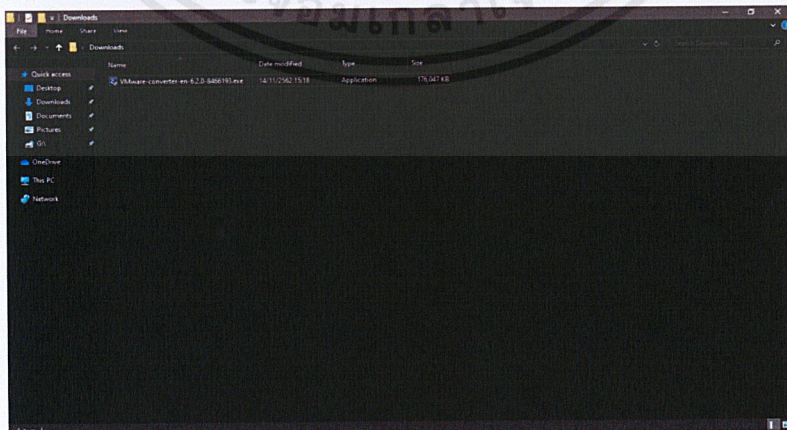
1) ทำการดาวน์โหลดได้จาก

[https://my.vmware.com/en/web/vmware/info/slug/infrastructure\\_operations\\_management/vmware\\_vcenter\\_converter\\_standalone/6\\_2\\_0](https://my.vmware.com/en/web/vmware/info/slug/infrastructure_operations_management/vmware_vcenter_converter_standalone/6_2_0) โดยต้องทำการลงทะเบียนและเข้าสู่ระบบก่อนถึงจะทำการดาวน์โหลดไฟล์ได้



รูปที่ 3.47 หน้าเว็บเพจของ VMware สำหรับดาวน์โหลดไฟล์

2) เมื่อดาวน์โหลดเสร็จเรียบร้อยจะได้ไฟล์ VMware-converter-en-6.2.0-8466193.exe



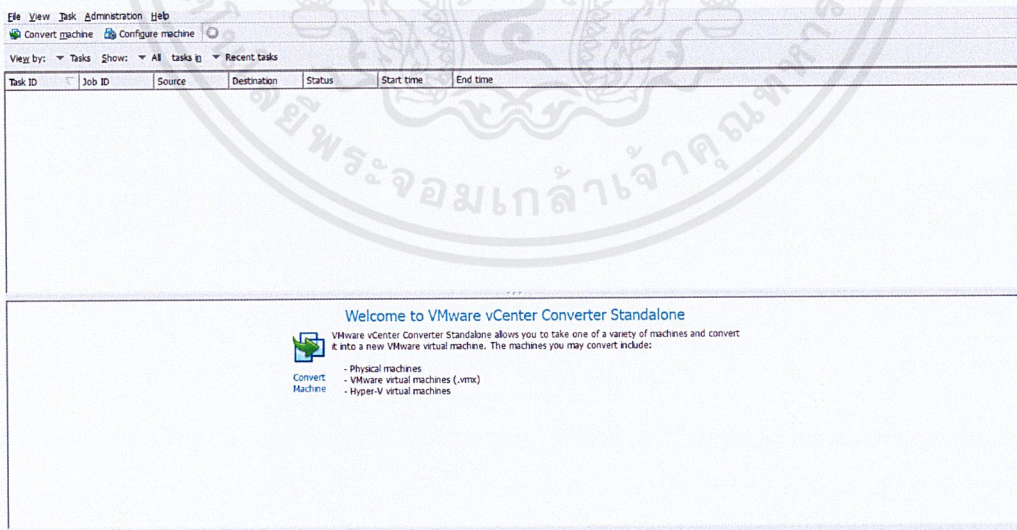
รูปที่ 3.48 ตัวติดตั้ง VMware Converter

3) ทำเปิดไฟล์เพื่อทำการติดตั้ง



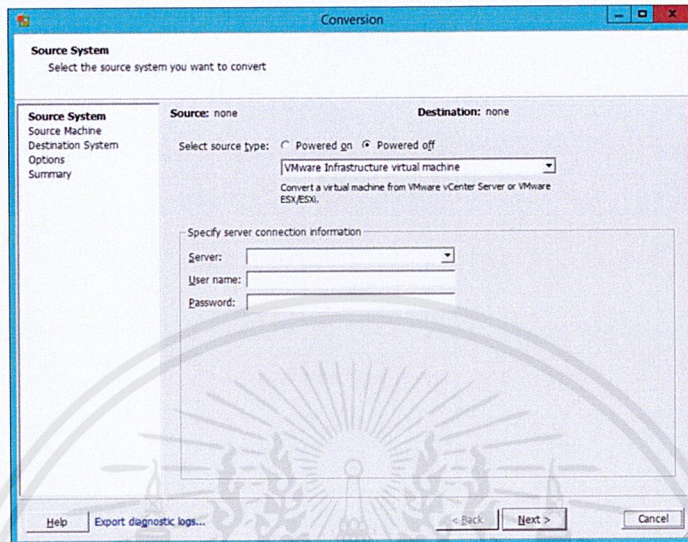
รูปที่ 3.49 หน้าติดตั้ง VMware vCenter Converter

4) เข้าโปรแกรม VMware vCenter Converter Standalone Client



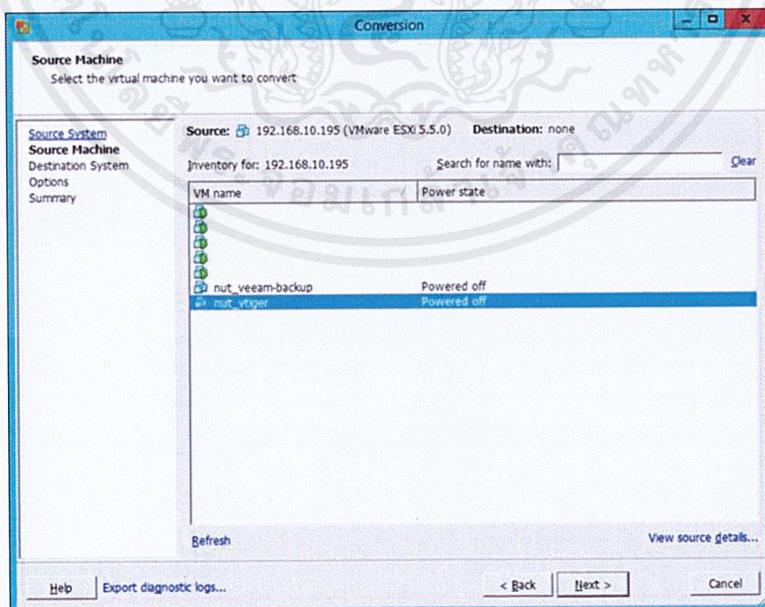
รูปที่ 3.50 หน้าแรกของโปรแกรม VMware vCenter Converter

- 5) กดไปที่คำว่า Convert Machine เพื่อทำการ Migrate แบบ V2V (Virtual to Virtual)แล้วจะตั้งหน้าต่างดังรูป



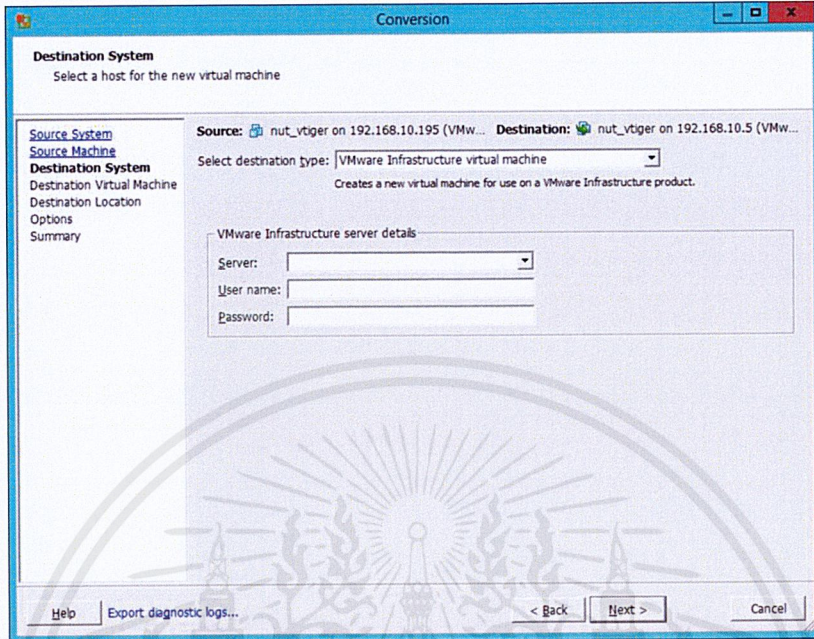
รูปที่ 3.51 migrate แบบ V2V ( Virtual to Virtual )

- 6) กรอกที่อยู่ของเซิร์ฟเวอร์ VMware ESXi version 5.5 ที่มีเซิร์ฟเวอร์ VtigerCRM (ก่อนจะทำการ migrate ต้องปิดการทำงานของเซิร์ฟเวอร์ที่จะทำการย้ายก่อน)



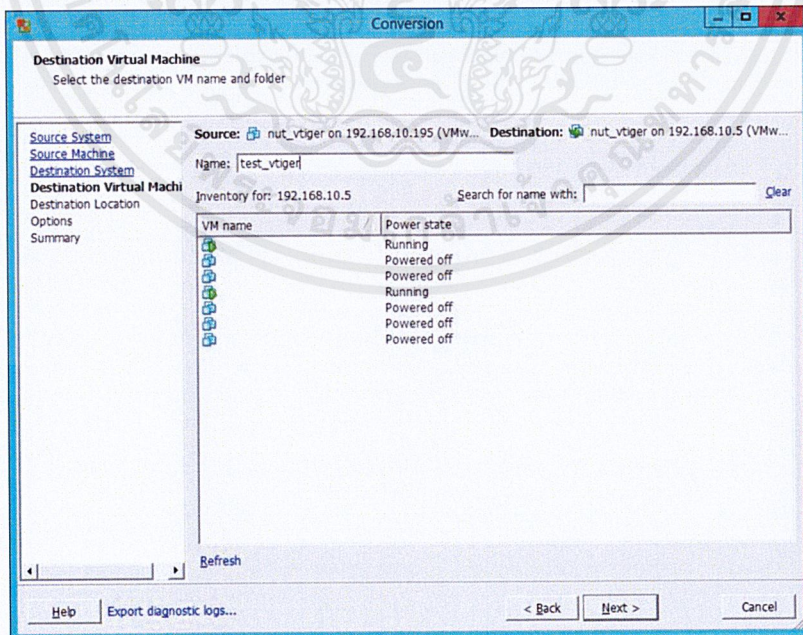
รูปที่ 3.52 เลือกเซิร์ฟเวอร์ที่เป็นคอมพิวเตอร์เสมือนเพื่อทำการ migrate

7) กรอกที่อยู่ของ VMware ESXi version 6.5 ที่จะทำเป็นระบบคลาวด์ส่วนตัว



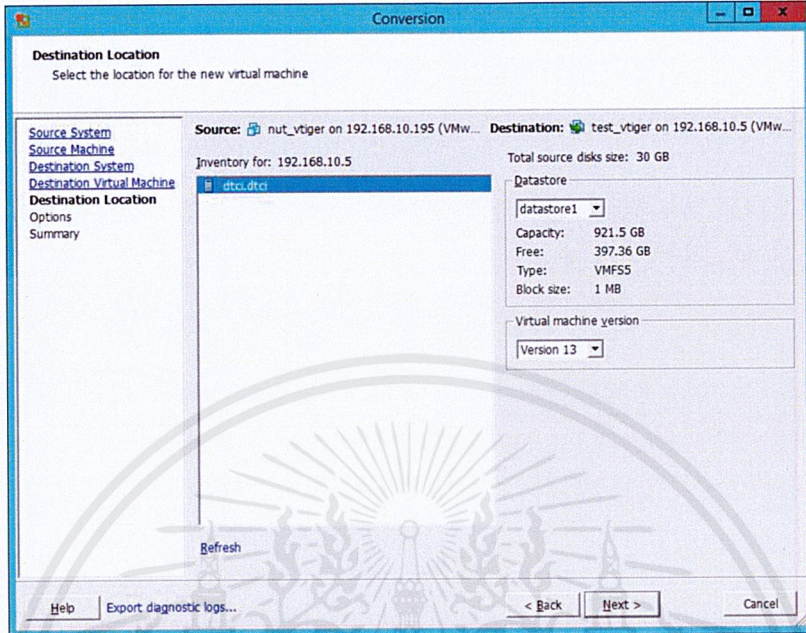
รูปที่ 3.53 กรอกที่อยู่ของเซิร์ฟเวอร์ที่ติดตั้ง VMware ESXi version 6.5

8) ตั้งชื่อคอมพิวเตอร์เสมือน (Virtual Machine)



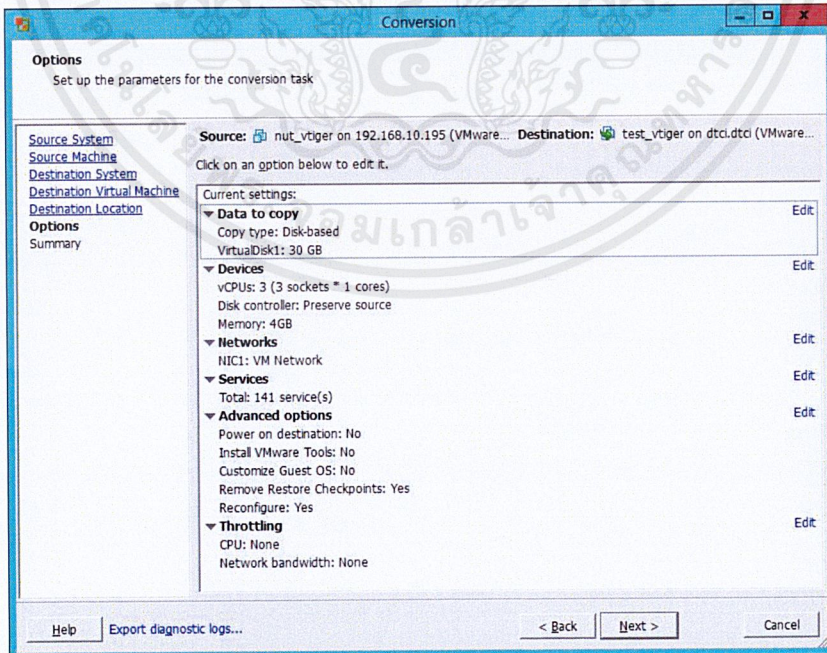
รูปที่ 3.54 ตั้งชื่อให้กับคอมพิวเตอร์เสมือน

9) เลือกหน่วยจัดเก็บข้อมูลที่จะทำการติดตั้ง



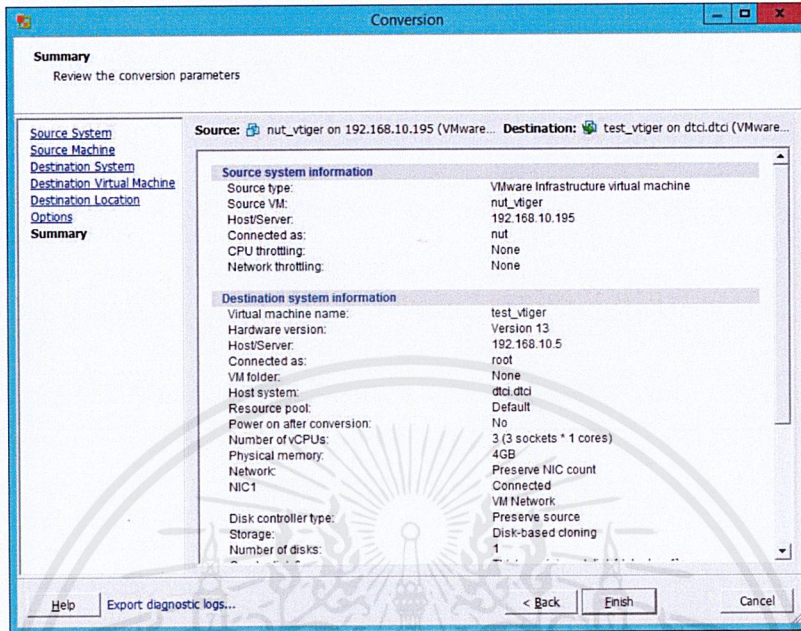
รูปที่ 3.55 เลือกหน่วยจัดเก็บข้อมูล

10) ปรับค่าทรัพยากรตามความต้องการของเซิร์ฟเวอร์



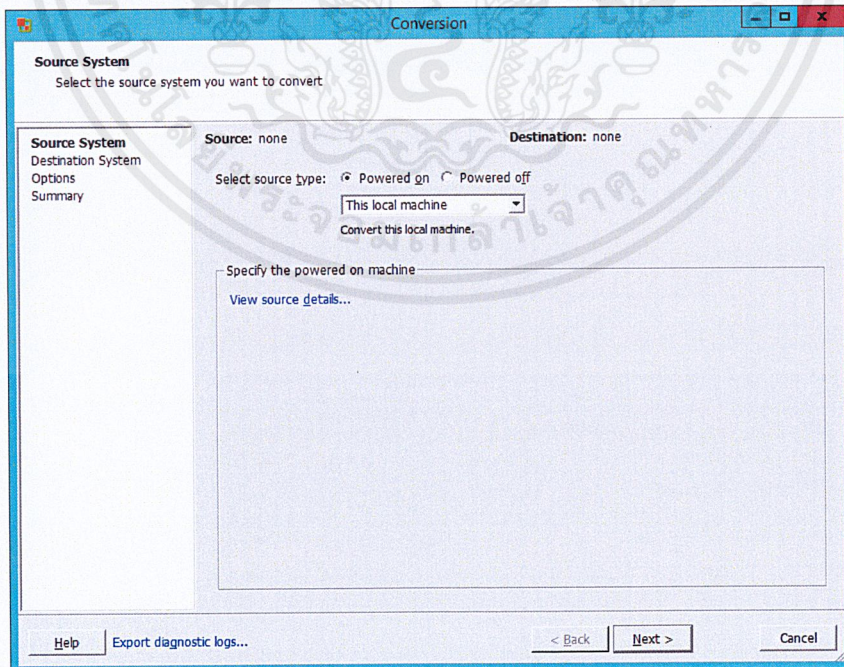
รูปที่ 3.56 ปรับค่าทรัพยากรตามความต้องการของเซิร์ฟเวอร์

11) ตรวจสอบการตั้งค่าอีกครั้ง แล้วกด Finish



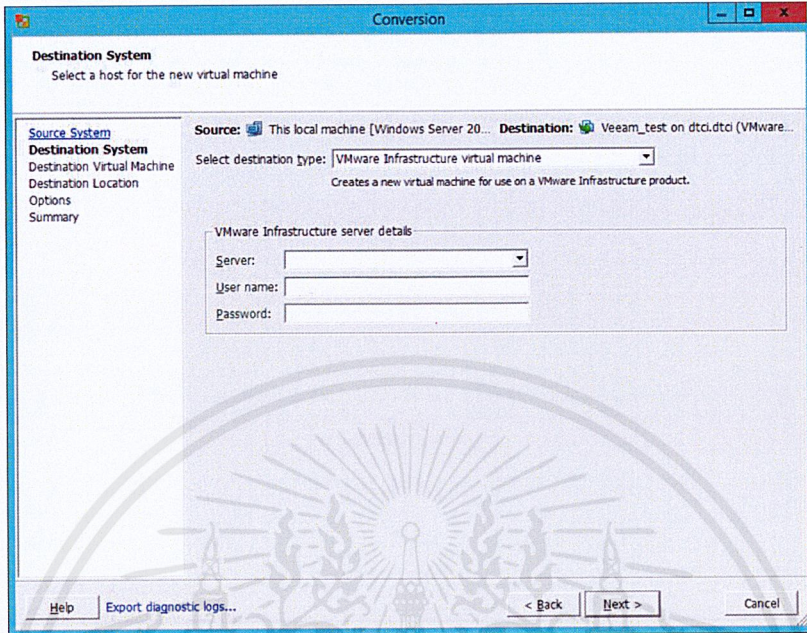
รูปที่ 3.57 ตรวจสอบการตั้งค่า

12) การ migrate แบบ P2V (Physical to Virtual)



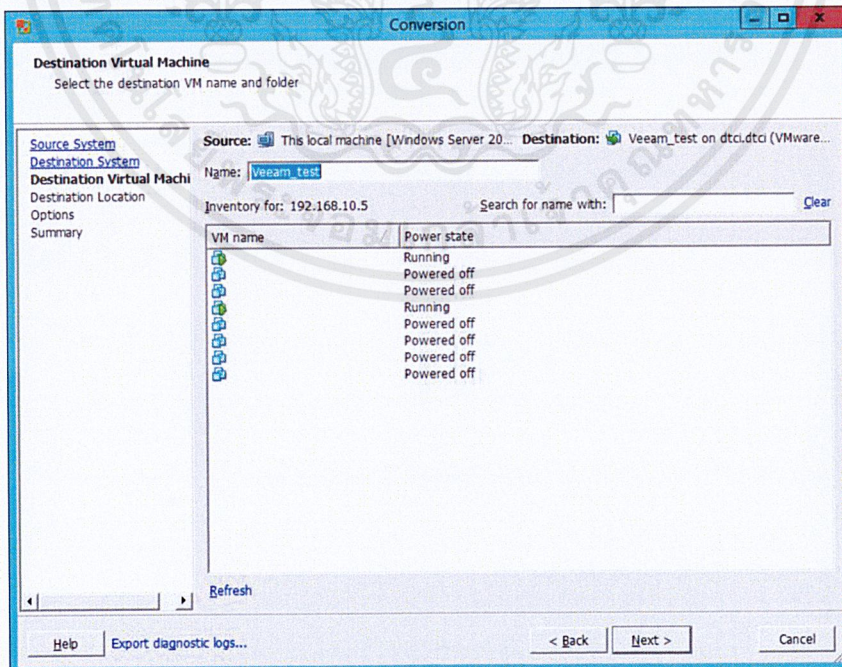
รูปที่ 3.58 การย้ายแบบ P2V ( Physical to Virtual )

13) ทำการเข้าสู่ระบบเซิร์ฟเวอร์ที่จะทำการ migrate เซิร์ฟเวอร์



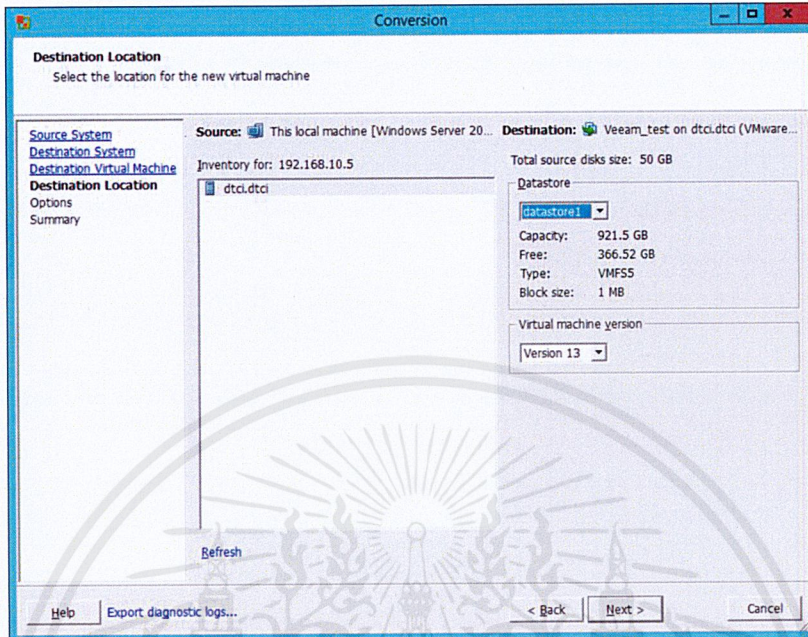
รูปที่ 3.59 เข้าสู่ระบบเครื่องเซิร์ฟเวอร์ที่ติดตั้ง ESXi version 6.5

14) ตั้งชื่อคอมพิวเตอร์เสมือน



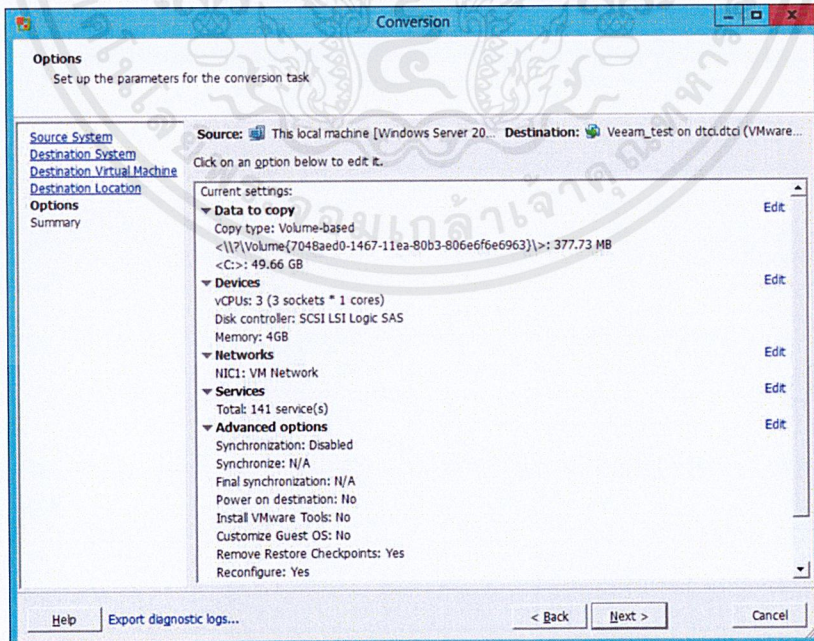
รูปที่ 3.60 ตั้งชื่อคอมพิวเตอร์เสมือน

15) เลือกหน่วยเก็บข้อมูลที่จะทำการติดตั้ง



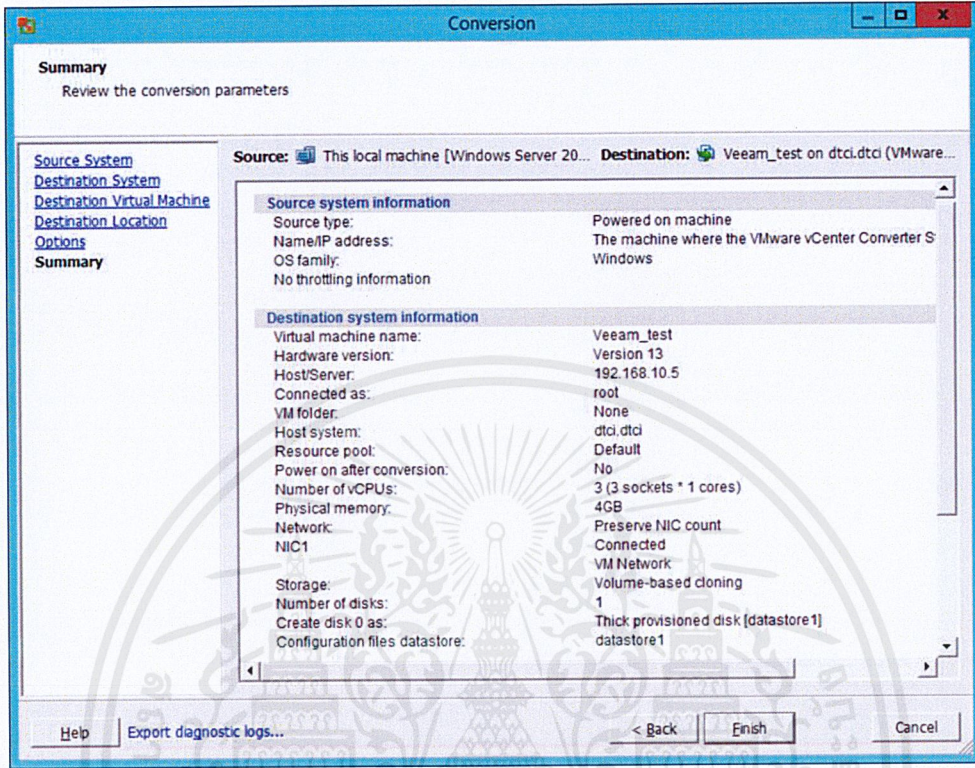
รูปที่ 3.61 เลือกหน่วยเก็บข้อมูล

16) ปรับค่าทรัพยากรตามความต้องการของเซิร์ฟเวอร์



รูปที่ 3.62 ปรับค่าทรัพยากรตามความต้องการของเซิร์ฟเวอร์

17) ตรวจสอบการตั้งค่าทั้งหมดแล้วกด Finish



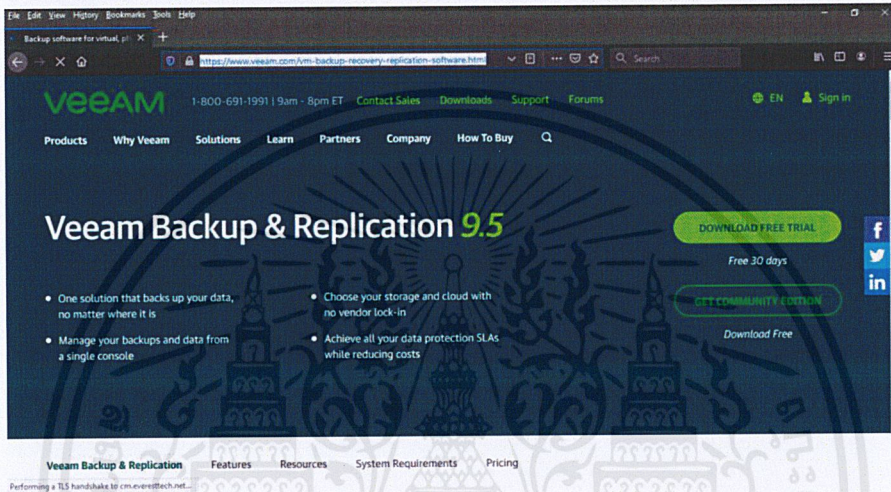
รูปที่ 3.63 ตรวจสอบการตั้งค่า

### 3.8 ติดตั้ง Veeam Backup & Replication

การทดลองนี้เป็นการทดลองเพื่อให้นักศึกษาได้มีความรู้และความเข้าใจระบบสำรองข้อมูลของคอมพิวเตอร์เสมือน (Virtual Machine)

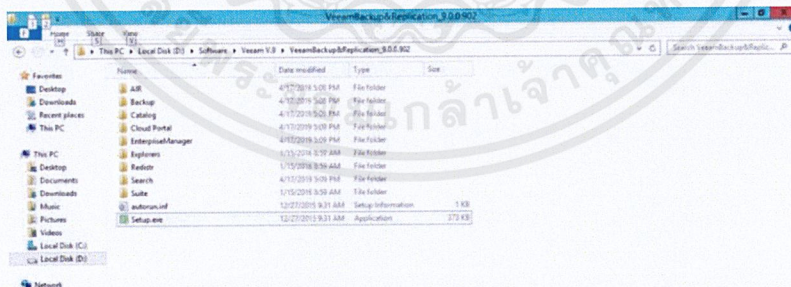
1) ทำการดาวน์โหลดโปรแกรม Veeam Backup & Replication ได้จาก

<https://www.veeam.com/vm-backup-recovery-replication-software.html>



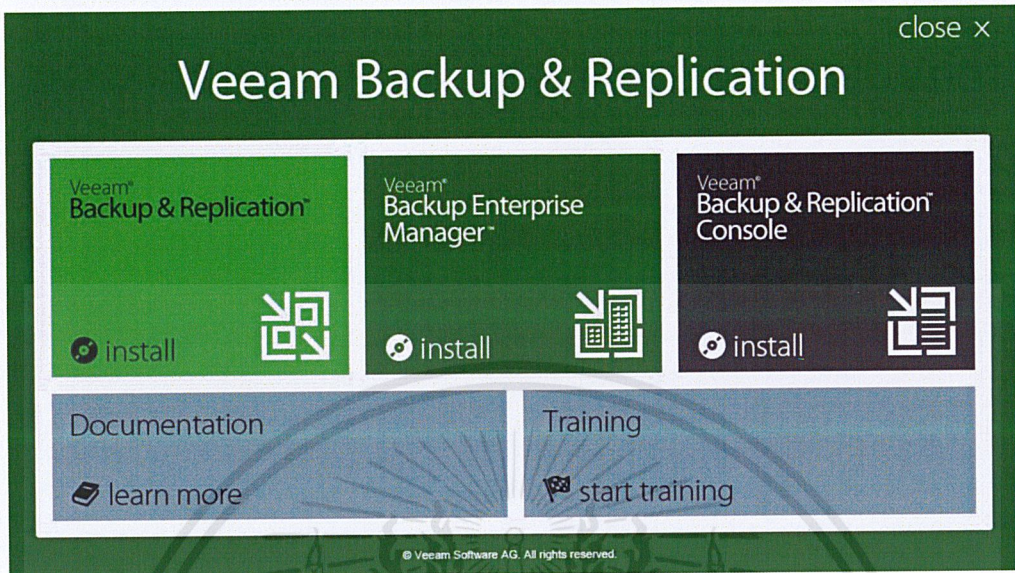
รูปที่ 3.64 หน้าเว็บเพจของ Veeam สำหรับดาวน์โหลดไฟล์

2) เมื่อดาวน์โหลดเสร็จแล้วจะได้ไฟล์ที่แสดงดังรูปด้านล่าง



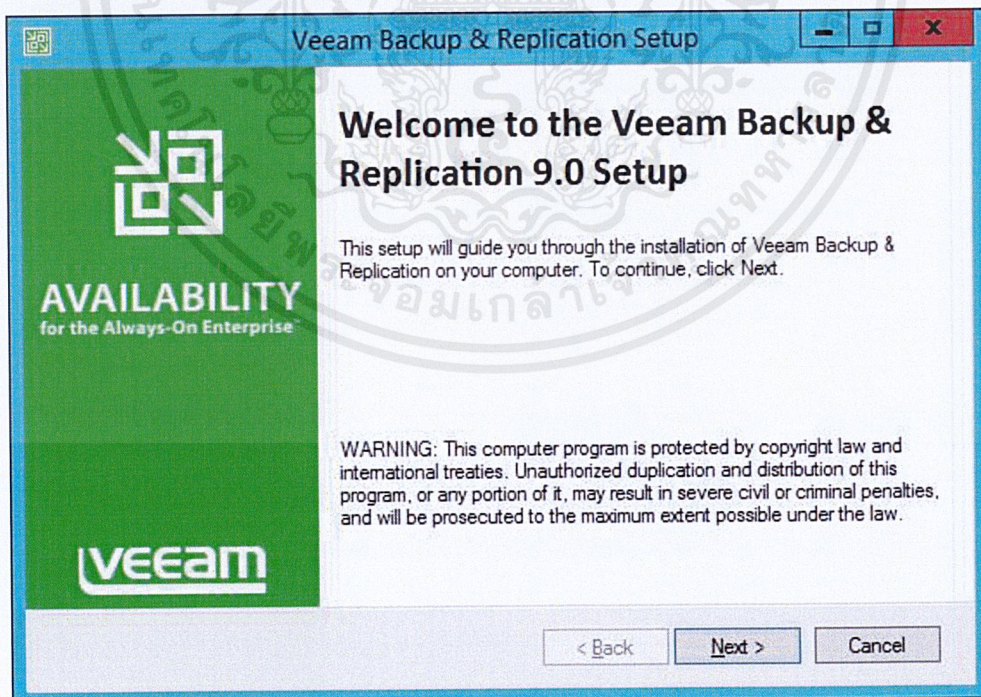
รูปที่ 3.65 ไฟล์ตัวติดตั้ง Veeam

3) ทำการคลิก 2 ครั้งไปที่ไฟล์ Setup.exe แล้วจะขึ้นหน้าต่างดังรูป



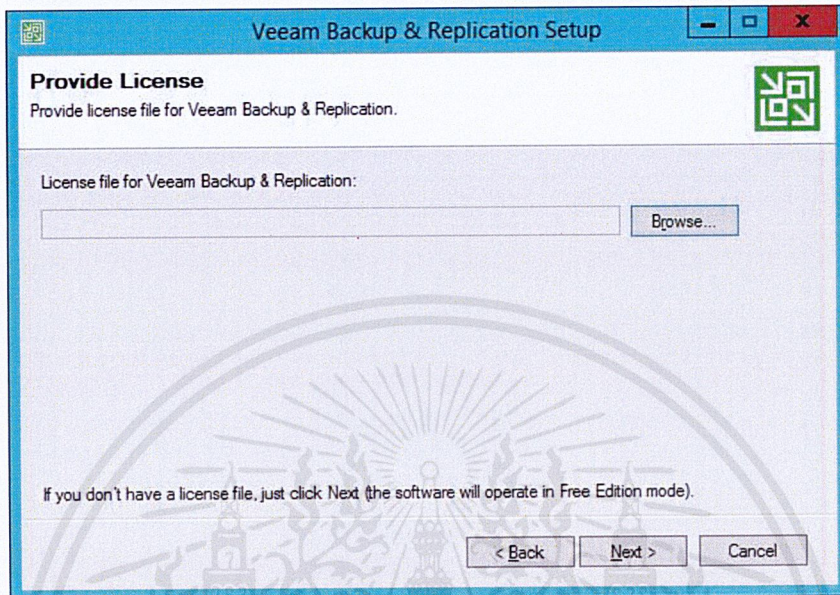
รูปที่ 3.66 ตัวติดตั้ง Veeam

4) ทำการกดไปที่ช่อง Install Backup & Replication



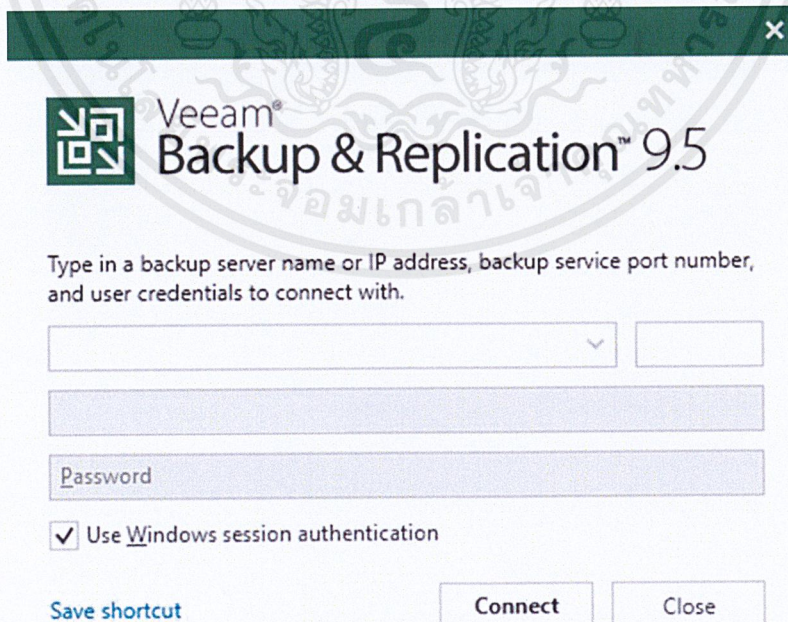
รูปที่ 3.67 หน้าต่างติดตั้ง Veeam

- 5) เพิ่มใบอนุญาตที่มาพร้อมกับตัวติดตั้ง โดยการลงทะเบียนครั้งแรกจะมีใบอนุญาตให้ทดลองใช้ฟรี 30 วัน



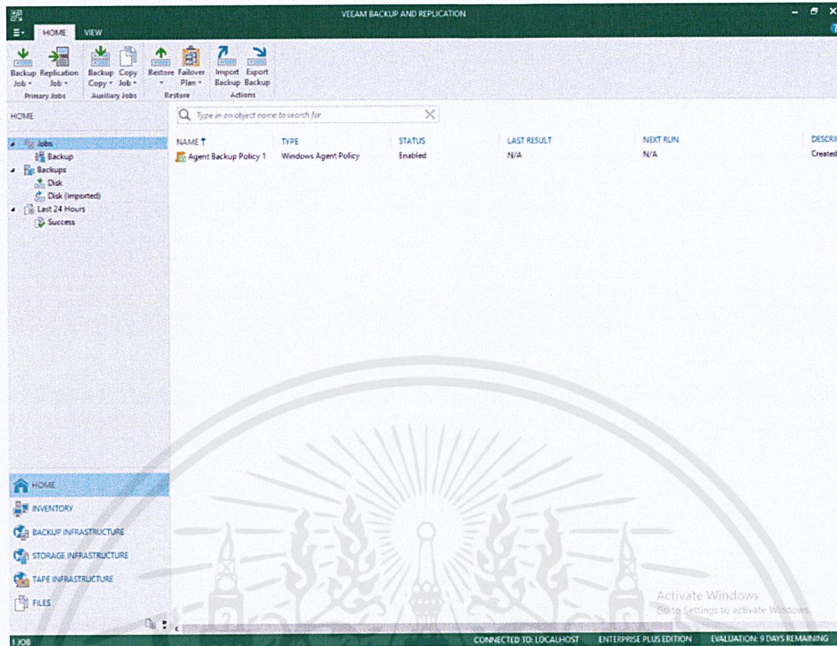
รูปที่ 3.68 เพิ่มใบอนุญาตของ Veeam

- 6) เปิดโปรแกรมแล้วทำการเข้าสู่ระบบตามรูปด้านล่าง



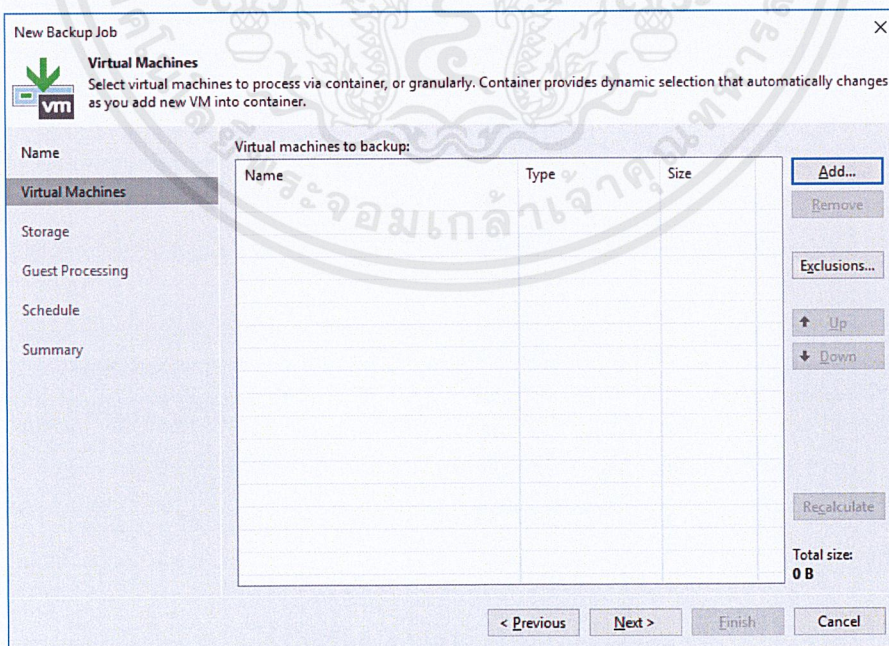
รูปที่ 3.69 ทำการเข้าสู่ระบบ Veeam

7) เชื่อมต่อเข้าสู่ระบบแล้วจะพบหน้าต่างดังรูป



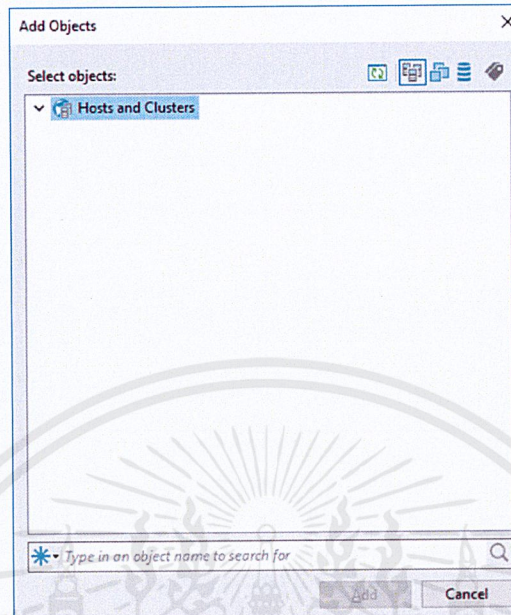
รูปที่ 3.70 หน้าแรกเมื่อเข้าสู่ระบบสำเร็จ

8) กดไปที่ Backup Job ที่อยู่แถบด้านบนแล้วจะปรากฏหน้าต่างดังรูป



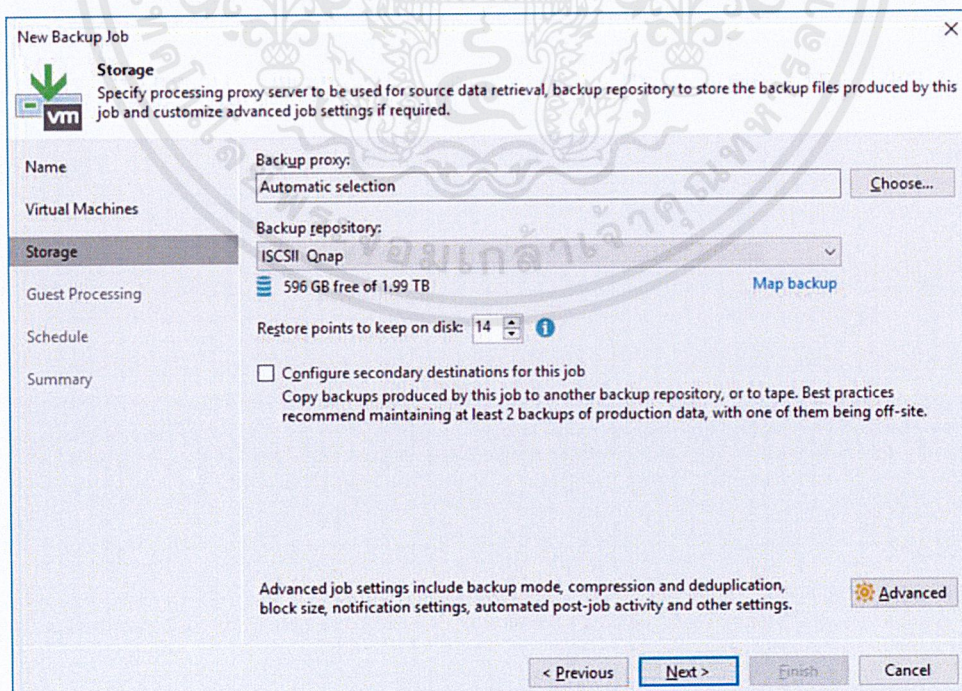
รูปที่ 3.71 หน้าต่าง Backup Job

9) เลือกเซิร์ฟเวอร์ที่เป็นคอมพิวเตอร์เสมือนที่จะทำการสำรองข้อมูล



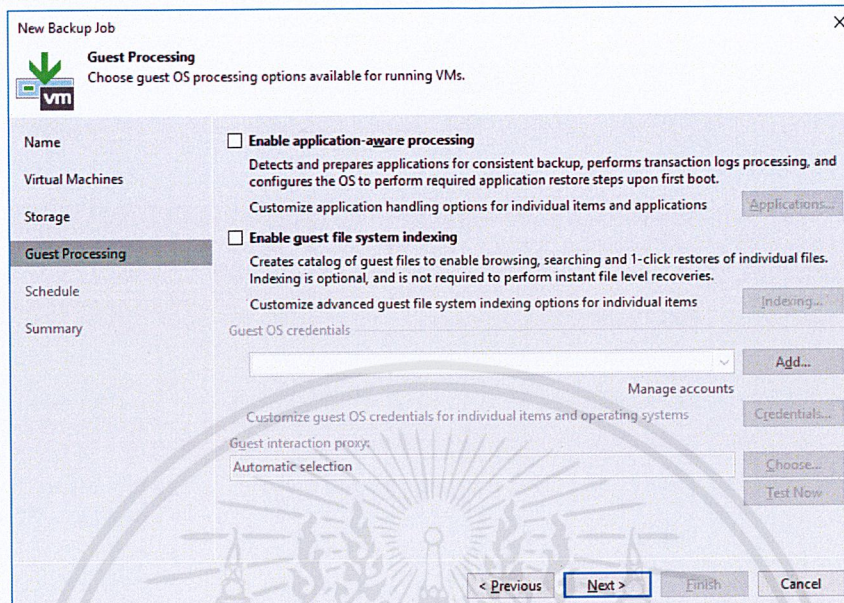
รูปที่ 3.72 เลือกเครื่องเซิร์ฟเวอร์เพื่อทำการสำรองข้อมูล

10) เลือกที่จัดเก็บไฟล์สำรองข้อมูล



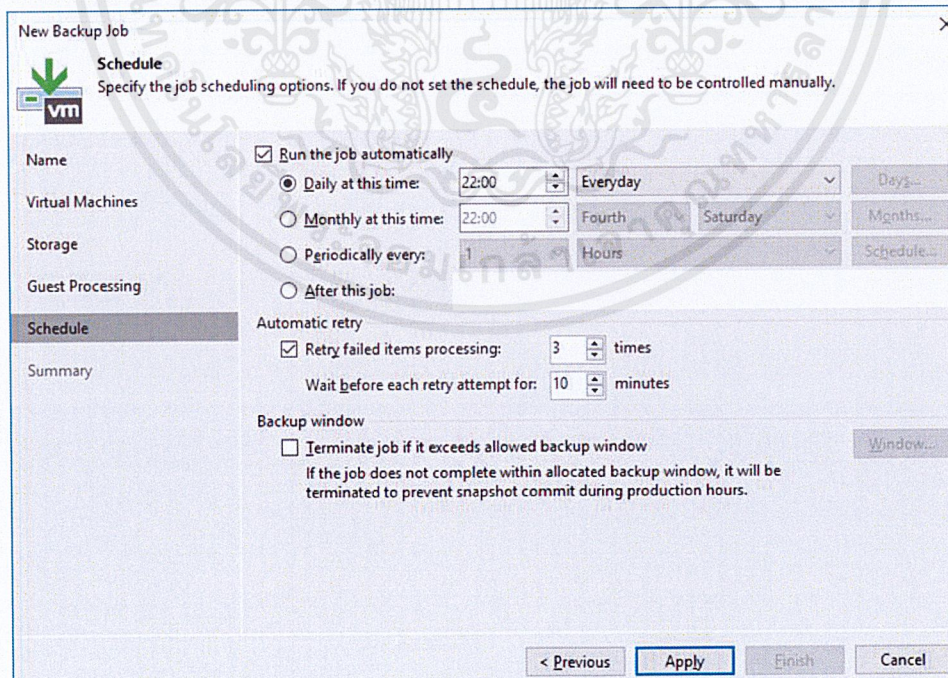
รูปที่ 3.73 เลือก Backup Repository

11) กด Next ข้ามไป



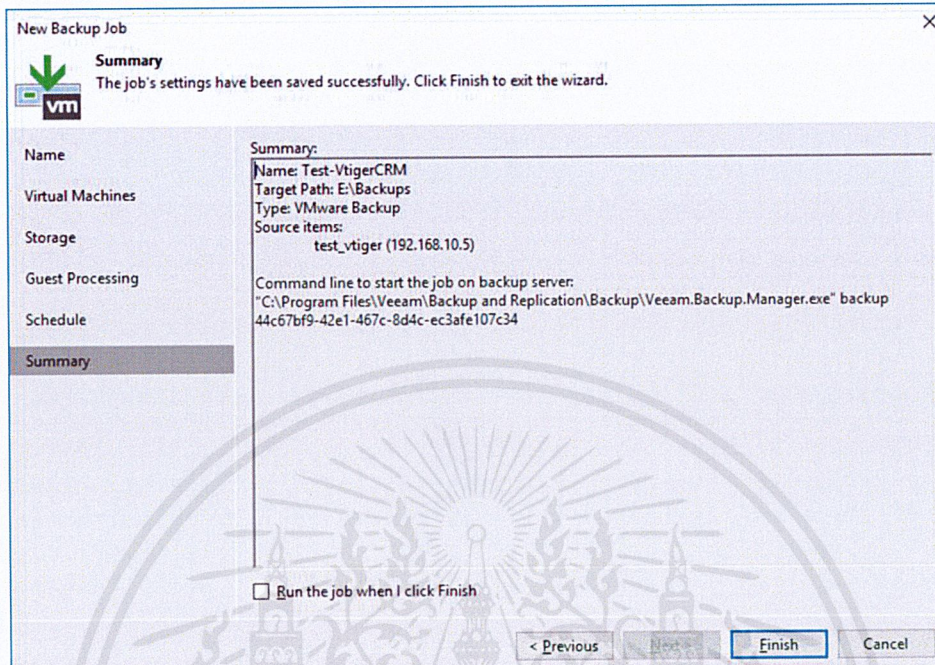
รูปที่ 3.74 หน้า Guest Processing

12) กำหนดเวลาที่จะให้ทำการสำรองข้อมูล



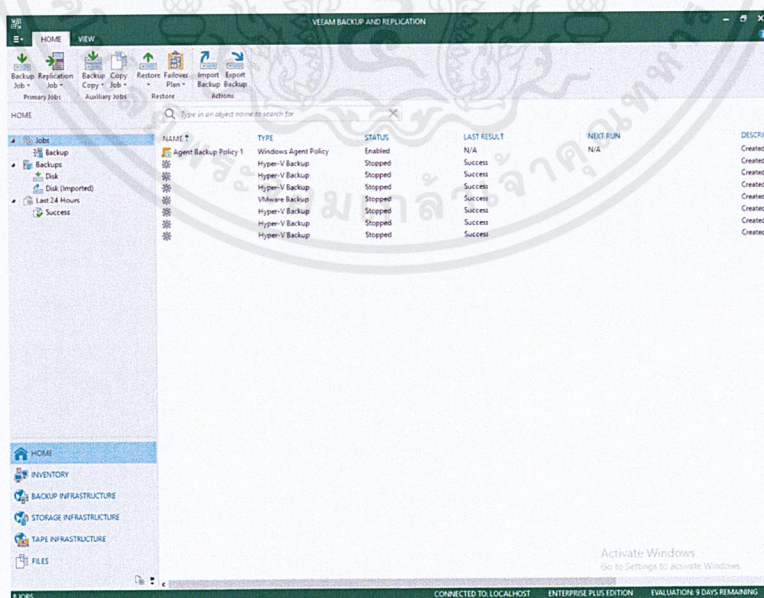
รูปที่ 3.75 กำหนดเวลาการสำรองข้อมูล

### 13) ตรวจสอบดูความเรียบร้อยก่อนกด Finish



รูปที่ 3.76 หน้า summary

### 14) เสร็จสิ้น

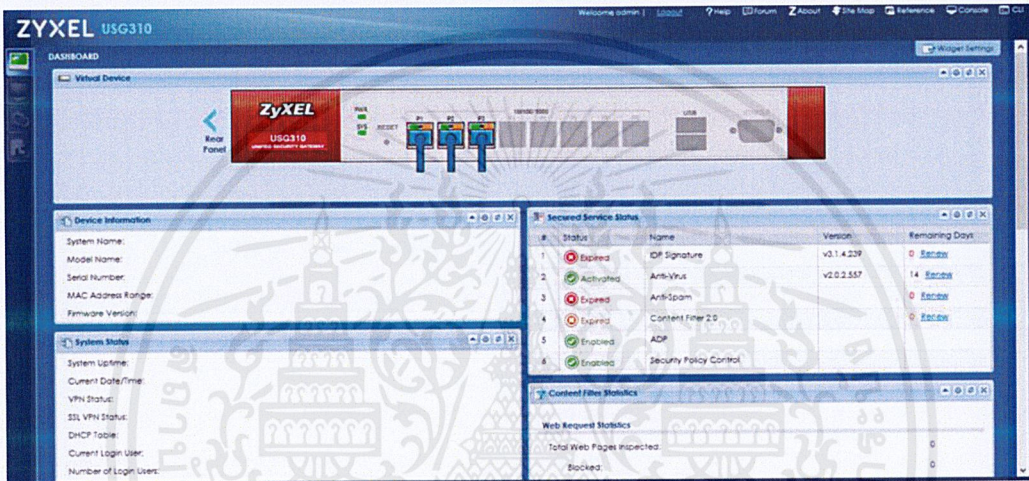


รูปที่ 3.77 แสดงสถานะการสำรองข้อมูล

### 3.9 Config Firewall รุ่น ZyXel USG310

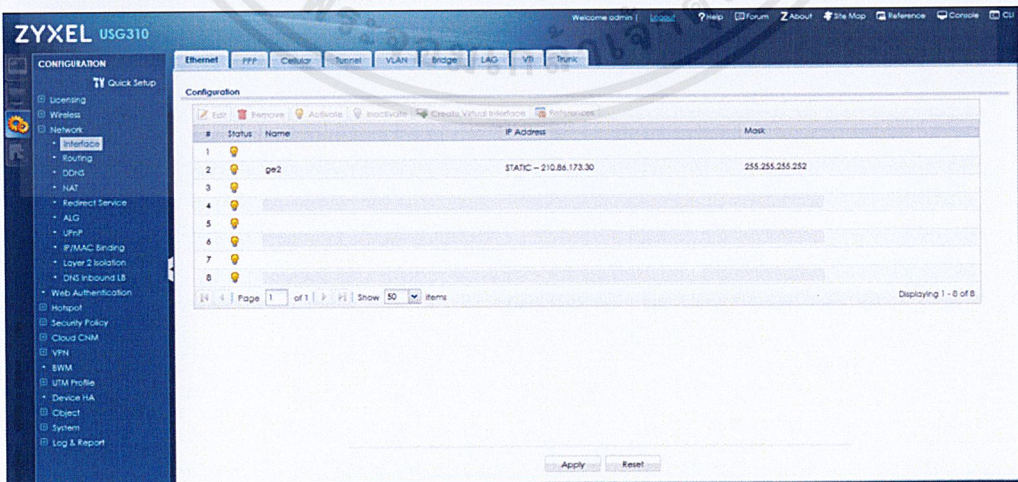
ทำการตั้งค่า Port Forwarding เพื่อให้สามารถเข้าเซิร์ฟเวอร์ VtigerCRM ของบริษัทผ่าน WAN ได้และทำ VPN Client to Site เพื่อให้สามารถ VPN เข้ามาตรวจสอบดูเซิร์ฟเวอร์ VMware ESXi version 6.5 ของบริษัทได้

- 1) เข้าหน้า GUI (Graphical User Interface) ของ firewall โดยใส่เลข IP Address ของตัว firewall



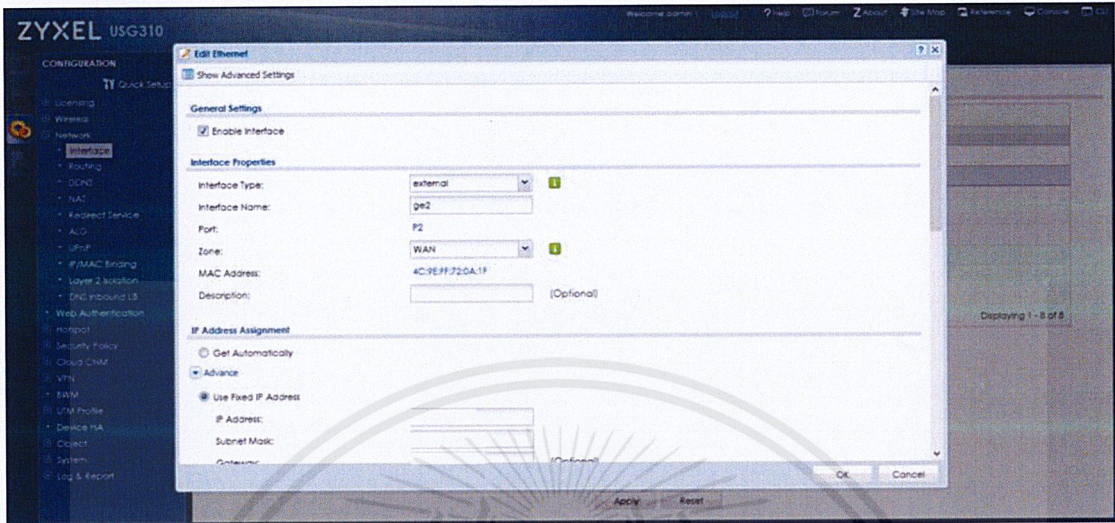
รูปที่ 3.78 หน้า GUI (Graphical User Interface) ของ Firewall รุ่น ZyXel USG310

- 2) เข้าไปหน้า Setting -> Network -> Interface



รูปที่ 3.79 หน้าตั้งค่า interface ของ Firewall

3) คลิก 2 ครั้งที่ Ge2 จะแสดงหน้าต่างดังรูป



รูปที่ 3.80 หน้าการตั้งค่าของแต่ละ Interface (1)

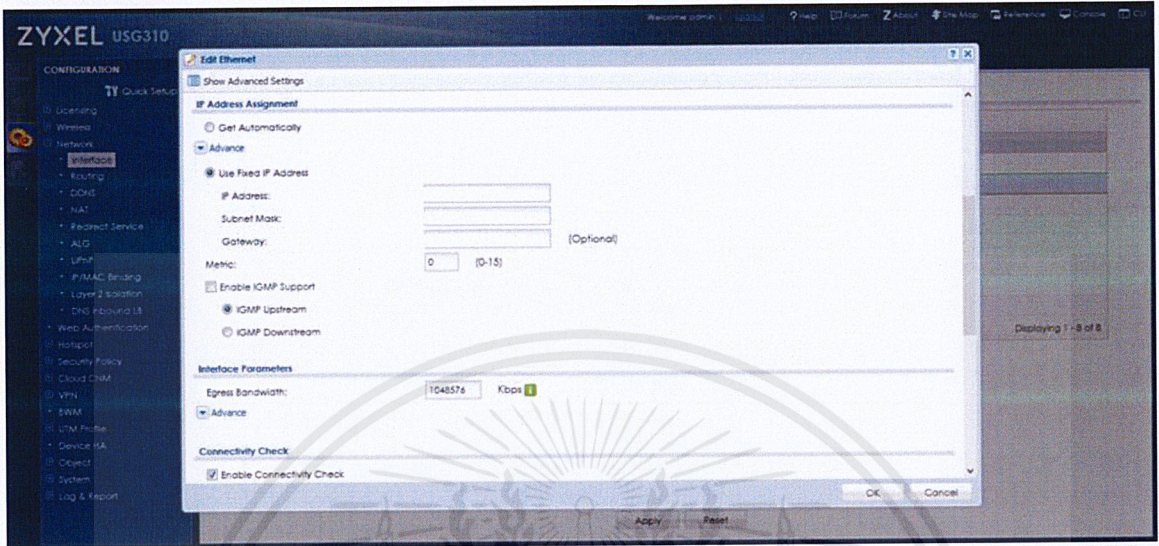
4) ตั้งค่าพอร์ต Ethernet

#### Interface Properties

- Interface Type ตั้งเป็น external
- Interface Name ตั้งเป็น ge2
- Zone เลือกเป็น WAN

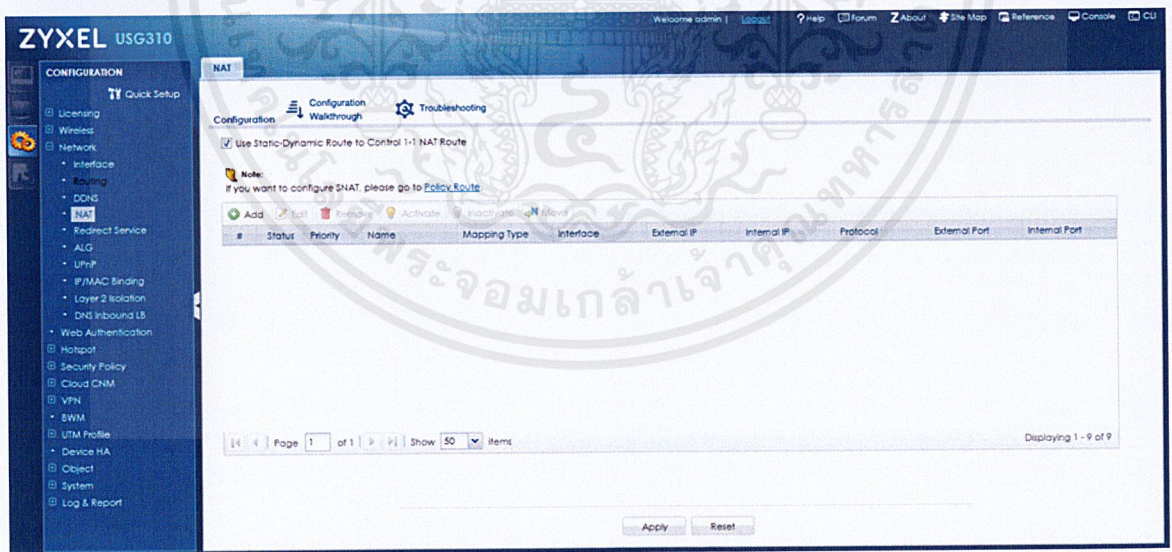
#### IP Address Assignment

- เลือกเป็น Use Fixed IP Address
- กรอก IP Address
- กรอก Subnet Mask
- กรอก Gateway
- กดปุ่ม OK



รูปที่ 3.81 หน้าการตั้งค่าของแต่ละ Interface (2)

5) เข้าไปที่ Network -> NAT

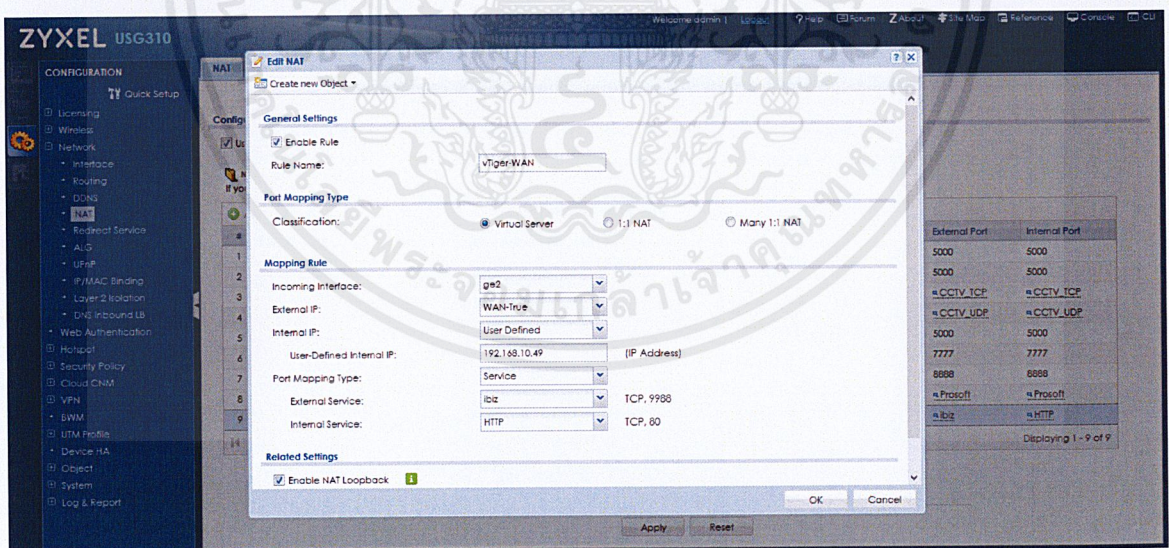


รูปที่ 3.82 หน้าตั้งค่า NAT (Network Address Translation)

6) กดปุ่ม Add แล้วจะขึ้นต่างดังรูปด้าน

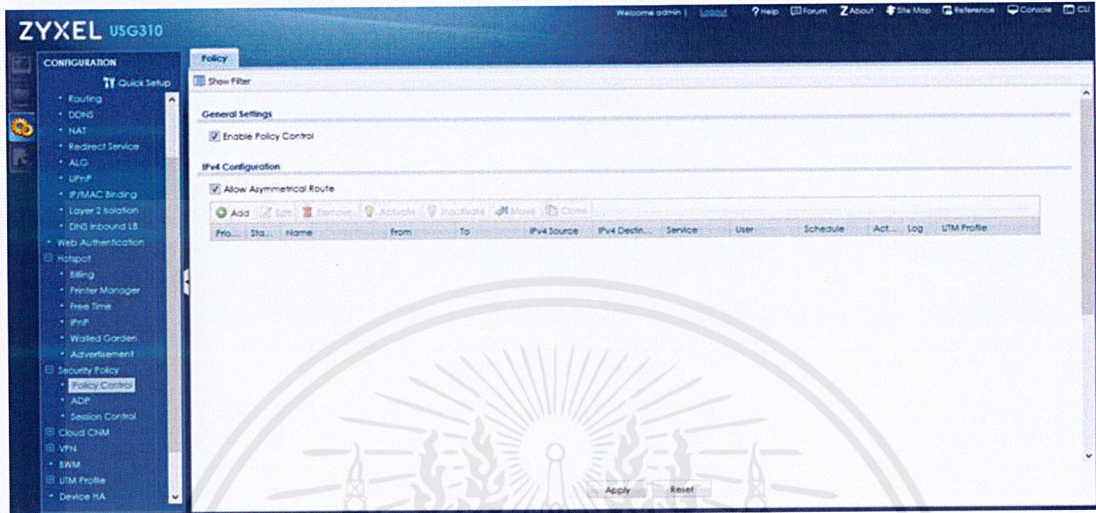
7) การตั้งค่า NAT

- ตั้ง Rule Name ว่า vTiger-WAN
- เลือก Classification เป็น Virtual Server
- เลือก Incoming Interface เป็น ge2
- เลือก External IP เป็น WAN-True
- เลือก Internal IP เป็น User Defined
- ตั้ง User-Defined Internal IP เป็น 192.168.10.49
- เลือก Port Mapping Type เป็น Service
- เลือก External Service เป็น ibiz
- เลือก Internal Service เป็น HTTP
- กดปุ่ม OK



รูปที่ 3.83 หน้าต่างการตั้งค่า NAT

8) เข้าไปที่หัวข้อ Security Policy -> Policy Control

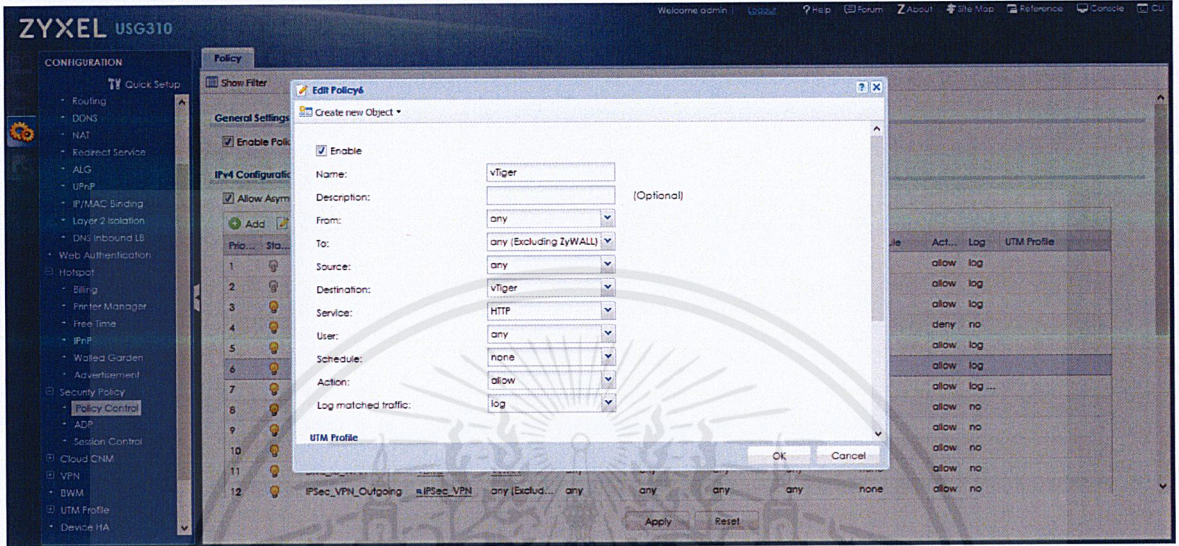


รูปที่ 3.84 หน้าตั้งค่า Policy Control

9) กดปุ่ม Add แล้วจะขึ้นหน้าต่างดังรูป พร้อมกับตั้งค่าดังรูป

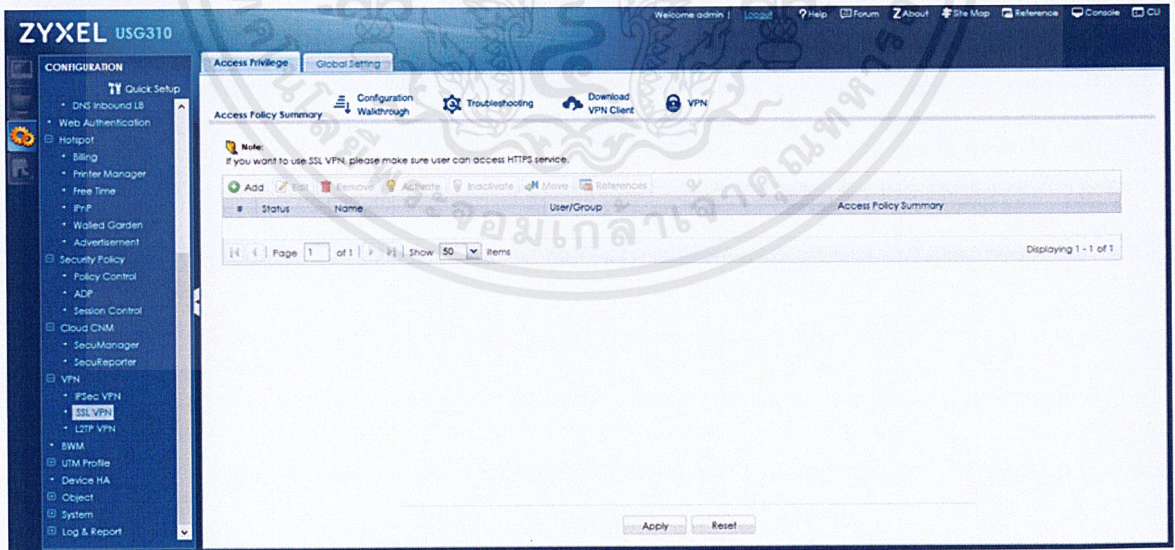
10) ตั้งค่ากำหนด Policy

- ตั้ง Name ว่า vTiger
- เลือก From เป็น any
- เลือก To เป็น any (Excluding ZyWall)
- เลือก Source เป็น any
- เลือก Destination เป็น vTiger
- เลือก Service เป็น HTTP
- เลือก User เป็น any
- เลือก Schedule เป็น none
- เลือก Action เป็น allow
- เลือก Log Matched traffic เป็น log
- กดปุ่ม OK



รูปที่ 3.85 หน้าต่างการตั้งค่า Policy

11) เข้าไปที่หัวข้อ VPN -> SSL VPN

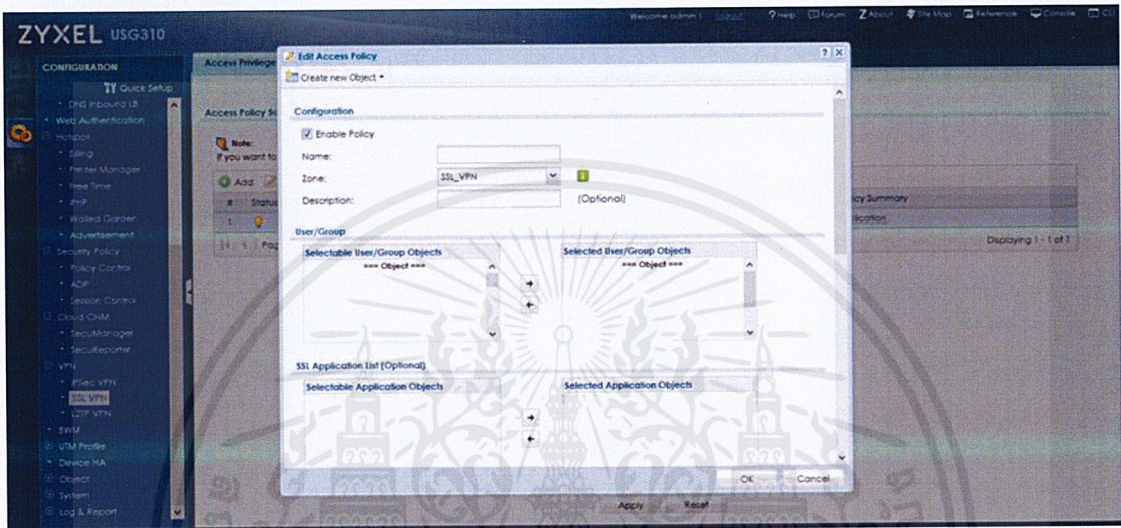


รูปที่ 3.86 หน้าตั้งค่า SSL VPN

12) กดปุ่ม Add แล้วจะขึ้นหน้าต่างดังรูป

13) ตั้งค่า Access Policy

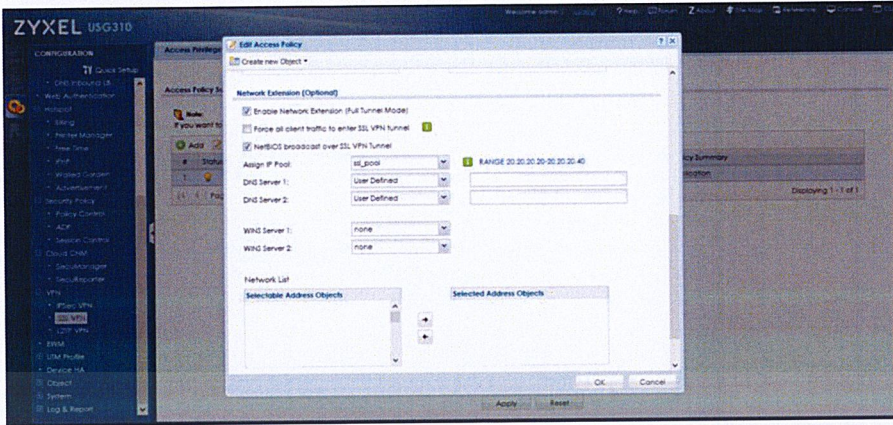
- กรอก Name
- เลือก Zone เป็น SSL\_VPN



รูปที่ 3.87 หน้าต่างการตั้งค่า SSL VPN (1)

ตั้งค่า Network Extension

- เลือก Enable Network Extension (Full Tunnel Mode)
- เลือก NetBIOS Broadcast over SSL VPN Tunnel
- เลือก Assign IP Pool เป็น ssl\_pool
- เลือก DNS Server 1 เป็น User Defined
- กรอก IP Address ของ DNS Server ตัวที่หนึ่ง
- เลือก DNS Server 2 เป็น User Defined
- กรอก IP Address ของ DNS Server ตัวที่สอง
- เลือก WINS Server 1 เป็น none
- เลือก WINS Server 2 เป็น none



รูปที่ 3.88 หน้าต่างการตั้งค่า SSL VPN (2)



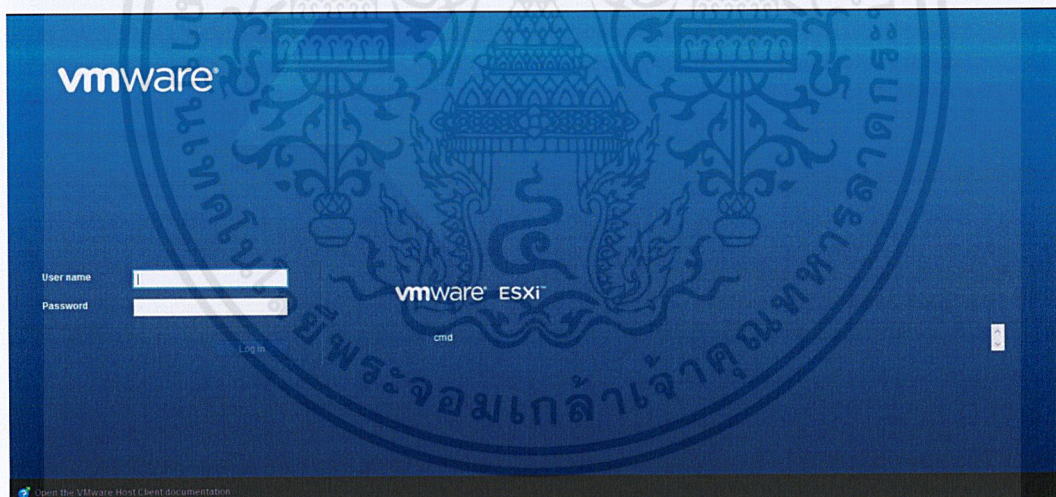
## บทที่ 4

### ผลการทดลอง

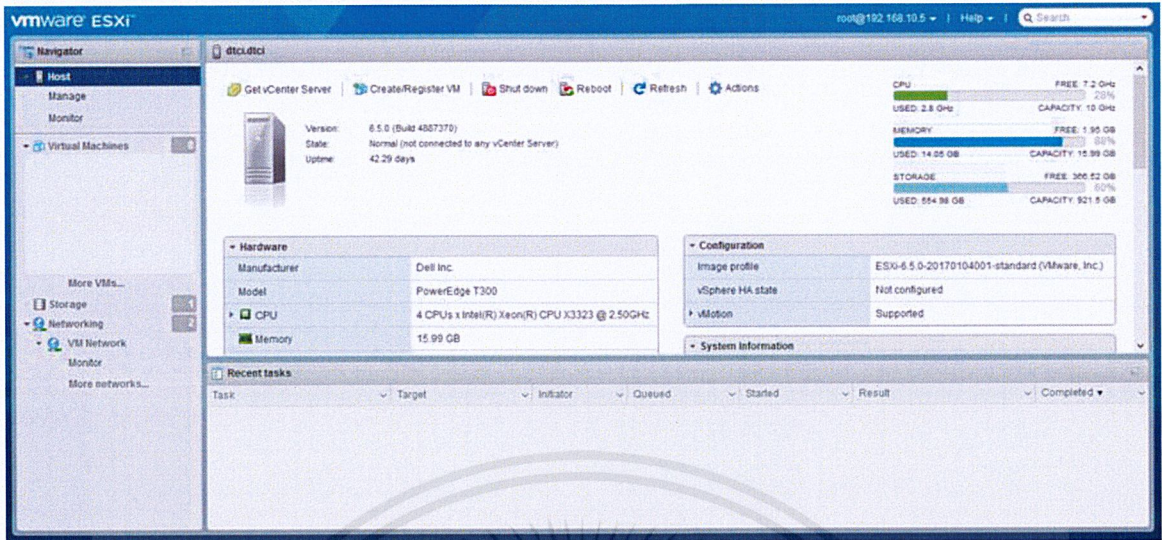
หลังจากที่ได้ทำการติดตั้งโปรแกรม และตั้งค่าระบบให้กับเซิร์ฟเวอร์เรียบร้อยแล้วจึงต้องมีการทดสอบระบบต่าง ๆ ที่ได้ทำการติดตั้งว่าทำงานได้อย่างมีประสิทธิภาพ ตามความต้องการหรือไม่

1. การเข้าใช้งานระบบคลาวด์ส่วนตัวโดยการใช้งาน VPN แบบ Client to Site
2. ตรวจสอบเซิร์ฟเวอร์การทำงานเซิร์ฟเวอร์บนระบบคลาวด์ส่วนตัว
3. ตรวจสอบการทำงานของเซิร์ฟเวอร์สำรองข้อมูลของตัว Virtual Machine
4. ตรวจสอบการใช้งาน VPN
5. ตรวจสอบการเข้าใช้งานเซิร์ฟเวอร์ VtigerCRM ผ่านเครือข่ายภายนอกได้

#### 4.1 การเข้าใช้งานระบบคลาวด์ส่วนตัวโดยการใช้งาน VPN แบบ Client to Site

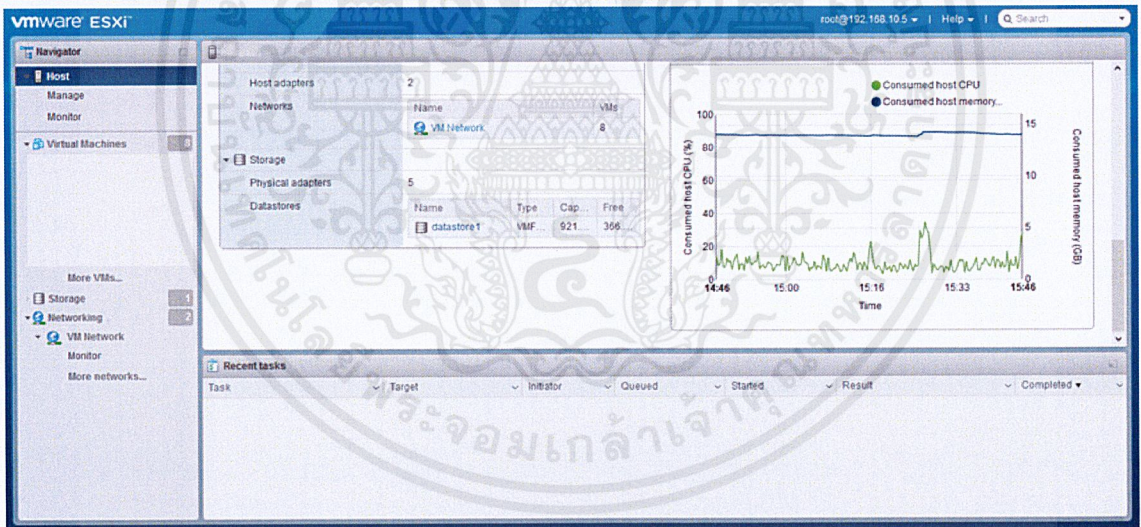


รูปที่ 4.1 หน้าเข้าสู่ระบบของ VMware ESXi version 6.5



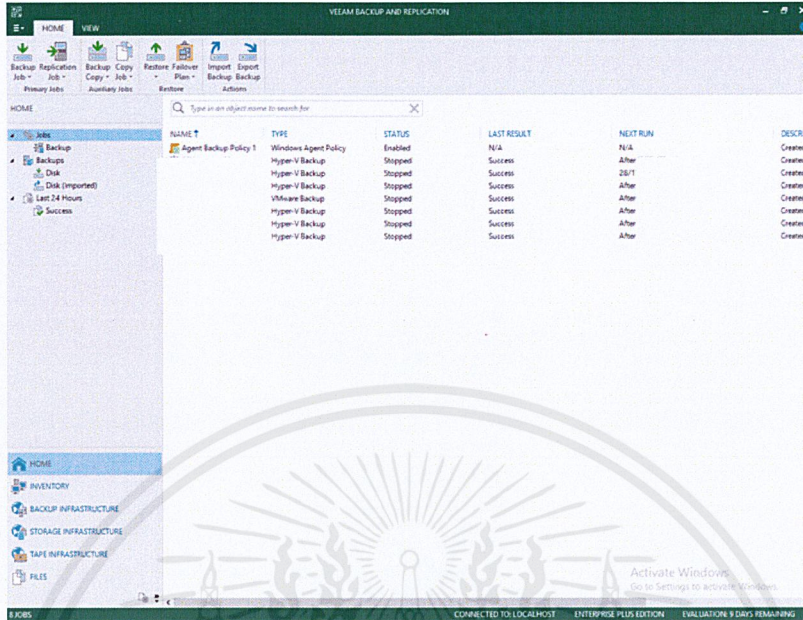
รูปที่ 4.2 หน้าแรกหลังจากการเข้าสู่ระบบ

#### 4.2 ตรวจสอบเซิร์ฟเวอร์การทำงานของเซิร์ฟเวอร์บนระบบคลาวด์ส่วนตัว



รูปที่ 4.3 สถานะของเซิร์ฟเวอร์

### 4.3 ตรวจสอบการทำงานของเซิร์ฟเวอร์สำรองข้อมูลของตัว Virtual Machine

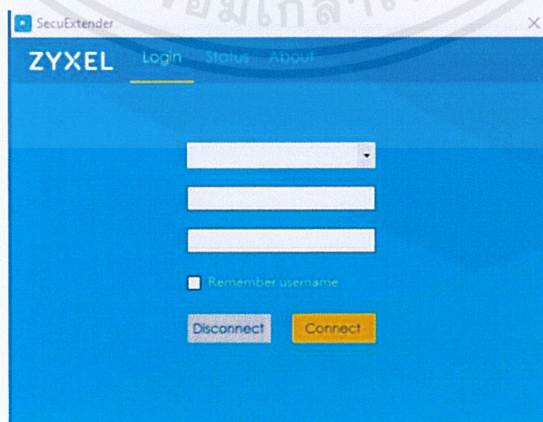


รูปที่ 4.4 สถานการณ์ทำงานของเซิร์ฟเวอร์สำรองข้อมูล

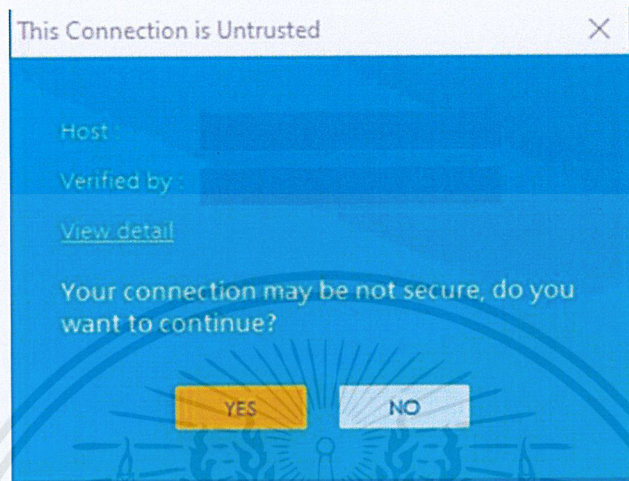
### 4.4 ตรวจสอบการใช้งาน VPN



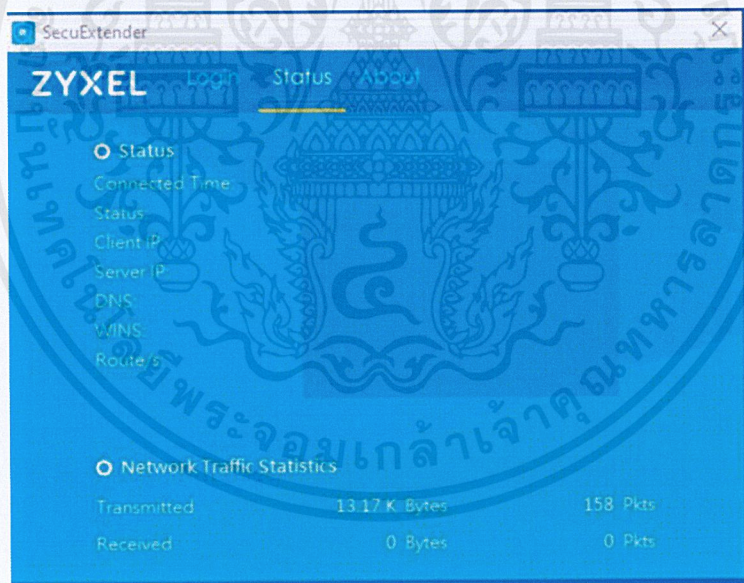
รูปที่ 4.5 ไอคอนซอฟต์แวร์ที่ใช้ในการทำ VPN



รูปที่ 4.6 หน้าเข้าสู่ระบบ VPN แบบ Client to Site

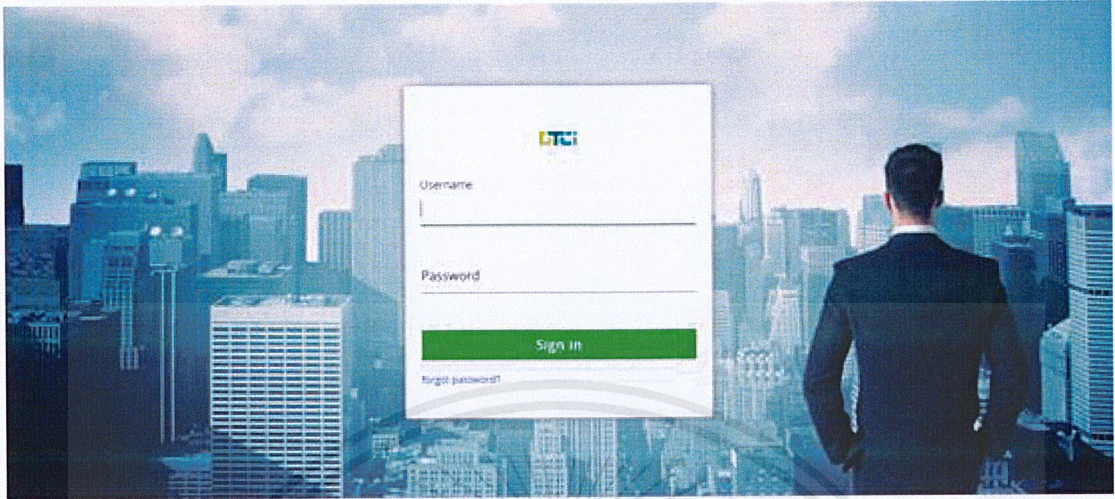


รูปที่ 4.7 หน้ายืนยันการเข้าใช้งาน VPN



รูปที่ 4.8 สถานะของการทำ VPN แบบ Client to Site

#### 4.5 ตรวจสอบการเข้าใช้งานเซิร์ฟเวอร์ VtigerCRM ผ่านเครือข่ายภายนอกได้



รูปที่ 4.9 หน้าเข้าสู่ระบบ VtigerCRM ของบริษัท



## บทที่ 5

### สรุปผลการวิจัย และข้อเสนอแนะ

#### 5.1 สรุปผลการวิจัย

ในปัจจุบันนี้ระบบคลาวด์ส่วนตัวได้ถูกนำมาใช้ภายในองค์กรทั้งขนาดใหญ่และขนาดเล็กเพราะเทคโนโลยีคลาวด์ได้เข้ามาช่วยให้เกิดความสะดวกในการทำงานมากขึ้น ซึ่งระบบคลาวด์ส่วนตัวนั้นจะเน้นหนักในเรื่องความเป็นส่วนตัวของผู้ใช้งานสูง จึงมีระบบรักษาความปลอดภัยในข้อมูลที่เข้มข้นมากกว่า มีขั้นตอนในการจำกัดสิทธิ์การเข้าถึงข้อมูลที่ละเอียดกว่า ซึ่งโครงการนี้ได้จัดทำเพื่อติดตั้งและตั้งค่าระบบคลาวด์ส่วนตัวเพื่อใช้ภายในองค์กรพร้อมกับติดตั้งระบบสำรองข้อมูลอัตโนมัติเพื่อป้องกันความเสียหายให้กับเซิร์ฟเวอร์ขององค์กร ซึ่งการทำงานของระบบคลาวด์ส่วนตัวสามารถใช้งานได้อย่างมีประสิทธิภาพ และผู้ดูแลระบบสามารถดูแลตรวจสอบการทำงานได้ผ่านการสร้างเครือข่ายเสมือนที่ได้ทำการตั้งค่าให้สามารถใช้งานได้ จึงกล่าวได้ว่าระบบคลาวด์ส่วนตัวคือเทคโนโลยีที่สามารถเข้าถึงได้ทุกองค์กรไม่ว่าเล็กหรือใหญ่ก็สามารถมีระบบคลาวด์ส่วนตัวได้ แต่ค่าใช้จ่ายก็จะแตกต่างกันออกไป ยิ่งองค์กรใหญ่จะมีค่าใช้จ่ายค่อนข้างสูงมาก เพราะจะมีค่าใช้จ่ายในการสร้างระบบที่ใหญ่ตามขนาดขององค์กร ซึ่งระบบคลาวด์ส่วนตัวสามารถที่จะสร้างความมั่นใจในการรักษาความเป็นส่วนตัวและให้ความปลอดภัยของข้อมูลได้เป็นอย่างดี

#### 5.2 ปัญหา และอุปสรรคในการดำเนินงาน

- 1) ผู้นิเทศงานไม่ได้จบสายเดียวกับผู้วิจัยจึงทำให้เมื่อเกิดปัญหาในการดำเนินงาน ผู้วิจัยไม่สามารถปรึกษาการทำโครงการกับผู้นิเทศได้ จึงทำให้ผู้วิจัยต้องศึกษาวิธีการเองเกือบทั้งหมด
- 2) ผู้วิจัยได้รับหัวข้องานโครงการจากผู้นิเทศล่าช้า ทำให้การทำวิจัยนี้ต้องทำอย่างเร่งรีบ

#### 5.3 ข้อเสนอแนะ

- 1) บริษัทที่รับนักศึกษาเข้ามาทำสหกิจศึกษาควรมีหัวข้องานวิจัยให้กับนักศึกษาก่อนที่จะรับนักศึกษาเข้ามาทำสหกิจศึกษา

## เอกสารอ้างอิง

- [1] itc.nida. “VMware vCenter Server install and Configuration with SAN fiber Channel”.  
ที่มา: <http://itc.nida.ac.th/main/images/manualbyitc/VMware+vCenter+Server+SAN.pdf>
- [2] microsystems. “มาทำความรู้จักกับ Veeam Backup & Replication”. ที่มา:  
<https://www.microsystems.co.th/news/มาทำความรู้จักกับ-veeam-backup-replication/>
- [3] saixiii. “การทำ Forward Port คือ การเซ็ต router เพื่อ Game Online และ กล้องวงจรปิด”.  
ที่มา: <https://saixiii.com/how-to-forward-port/>
- [4] mindphp. “VPN คืออะไร Virtual Private Network คือเครือข่ายเสมือนส่วนตัว”.ที่มา:  
<https://www.mindphp.com/บทความ/212-network/1824-vpn-คืออะไร.html>
- [5] techtalkthai. “Hillstone: Next Generation Firewall หน้าใหม่ เหนือกว่าด้วยระบบการเรียนรู้  
อัจฉริยะ”. ที่มา:  
<https://www.techtalkthai.com/hillstone-intelligent-next-generation-firewall/>