

การจัดการกำหนดค่าซอฟต์แวร์จากส่วนกลาง  
กรณีศึกษา บริษัทคาลโซนิค คันเซ (ประเทศไทย) จำกัด

วีระพันธ์ ดวงจิตร

งานนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต  
สาขาวิชาเทคโนโลยีสารสนเทศ  
คณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา  
พฤษภาคม 2560  
ลิขสิทธิ์เป็นของมหาวิทยาลัยบูรพา

SYSTEM CENTER CONFIGURATION MANAGER  
CASE STUDY: CALSONIC KANSEI (THAILAND).CO.,LTD.

WEERAPUN DOUNGJIT

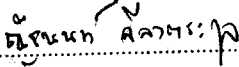
A PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT  
FOR THE MASTER DEGREE OF SCIENCE IN INFORMATION TECHNOLOGY  
FACULTY OF INFORMATICS BURAPHA UNIVERSITY

2017

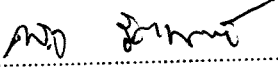
COPYRIGHT OF BURAPHA UNIVERSITY

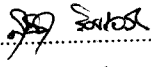
คณะกรรมการควบคุมงานนิพนธ์และคณะกรรมการสอบงานนิพนธ์ได้พิจารณางาน  
นิพนธ์ของ นายวีระพันธ์ ดวงจิตร์ ฉบับนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตาม  
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยบูรพาได้

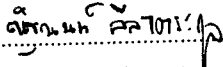
คณะกรรมการควบคุมงานนิพนธ์

 ..... อาจารย์ที่ปรึกษา  
(ผู้ช่วยศาสตราจารย์ ดร.ณัฐนันท์ ลีลาตระกูล)

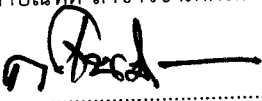
คณะกรรมการสอบงานนิพนธ์

 ..... ประธานกรรมการ  
(ดร.ภารุจ รัตนวรพันธุ์)

 ..... กรรมการ  
(ผู้ช่วยศาสตราจารย์ ดร.สุนิสา รีมเจริญ)

 ..... กรรมการ  
(ผู้ช่วยศาสตราจารย์ ดร.ณัฐนันท์ ลีลาตระกูล)

คณะวิทยาการสารสนเทศ อนุมัติให้รับงานนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม  
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยบูรพา

 ..... คณบดีคณะวิทยาการสารสนเทศ  
(ผู้ช่วยศาสตราจารย์ ดร.กฤษณะ ชินสาร)

วันที่ 31 เดือน พฤศจิกายน พ.ศ. 2560

## กิตติกรรมประกาศ

งานนิพนธ์ฉบับนี้สำเร็จลุล่วงอย่างสมบูรณ์ เนื่องด้วยความเมตตากรุณาและคำแนะนำอันมีค่ายิ่งจากผศ.ดร.ณัฐนนท์ ลีลาตระกูล อาจารย์ที่ปรึกษา ที่กรุณาให้ความรู้ ให้คำปรึกษา ช่วยแก้ไขปัญหาชี้แนะแนวทางที่ถูกต้อง ด้วยความละเอียดถี่ถ้วนและเอาใจใส่ด้วยดีเสมอมา ผู้จัดทำงานนิพนธ์รู้สึกซาบซึ้งเป็นอย่างยิ่ง จึงขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอขอบพระคุณหัวหน้างานและทีมงานแผนกไอที บริษัทคาลโซนิค คันเซ (ประเทศไทย) จำกัด ที่ให้ความร่วมมือในการทดสอบและเก็บรวบรวมข้อมูลการ deploy โปรแกรมประยุกต์เป็นอย่างดี

ขอขอบพระคุณคุณพ่อสวาท ดวงจิตร์ คุณแม่เน้อย ดวงจิตร์ อันเป็นที่รักยิ่ง ที่ให้กำเนิดชีวิตคอยเป็นกำลังใจ อบรมสั่งสอน สนับสนุนการศึกษาแก่ลูกด้วยความรักความหวังใย ขอขอบคุณนายอนันท์ศักดิ์ ดวงจิตร์ นางสาวกัญนาง ดวงจิตร์ นางสาวไพลิน ดวงจิตร์และคุณแม่เน้อย แก้วงาม ที่ช่วยแนะนำ ช่วยหาข้อมูล เป็นกำลังใจและแรงใจให้เสมอมา

ขอขอบพระคุณ พี่ๆ เพื่อนๆ และน้องๆ หลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาเทคโนโลยีสารสนเทศรุ่น 10 ทุกคน ที่ช่วยเป็นแรงผลักดันในการทำงานนิพนธ์ฉบับนี้ให้เสร็จสมบูรณ์

ขอขอบพระคุณ คุณวาริต และคุณเอกพล กรรณสูต ที่ช่วยแนะนำแนวทาง ให้ความรู้เกี่ยวกับระบบ SCCM และ AD เป็นอย่างดี

คุณค่าและประโยชน์ของงานนิพนธ์ฉบับนี้ ขอมอบเป็นกตัญญูกตเวทิตาแต่บุพการีบูรพาจารย์ และผู้มีพระคุณทุกท่านทั้งในอดีตและปัจจุบัน ที่ทำให้ผู้ทำงานนิพนธ์เป็นผู้มีการศึกษาและประสบความสำเร็จมาจนตราบเท่าทุกวันนี้

วีระพันธ์ ดวงจิตร์

57920145: สาขาวิชา: เทคโนโลยีสารสนเทศ; วท.ม. (เทคโนโลยีสารสนเทศ)

คำสำคัญ: การ deploy ระบบปฏิบัติการวินโดวส์ 7/ การกระจายโปรแกรมประยุกต์/ SCCM  
2012 R2

วีระพันธ์ ดวงจิตฺต: การจัดการกำหนดค่าซอฟต์แวร์จากส่วนกลาง กรณีศึกษา บริษัทคาลโซนิค คันเซ (ประเทศไทย) จำกัด. คณะกรรมการควบคุมงานนิพนธ์: ธรรมนูญ ลีลาตระกูล, Ph.D., 190 หน้า. ปี พ.ศ. 2560.

งานนิพนธ์ฉบับนี้เสนอระบบการจัดการกำหนดค่าซอฟต์แวร์จากส่วนกลาง (SCCM) กรณีศึกษา บริษัทคาลโซนิค คันเซ (ประเทศไทย) จำกัด เพื่อควบคุมซอฟต์แวร์ให้เป็นมาตรฐานหรือเป็นรุ่นเดียวกัน โดยเครื่องคอมพิวเตอร์ผู้ใช้ของบริษัทมีทั้งหมดประมาณ 600 เครื่อง ใช้ระบบปฏิบัติการวินโดวส์ 7 ผู้วิจัยได้ deploy ระบบปฏิบัติการวินโดวส์ 7 ไปคอมพิวเตอร์รุ่น HP EliteDesk 705 จำนวน 30 เครื่อง เพื่อทดสอบความเร็วในการติดตั้งระบบปฏิบัติการวินโดวส์ ซึ่งใช้เวลาทั้งหมด 89 นาที และผู้วิจัยได้ deploy โปรแกรมประยุกต์จำนวน 11 ซอฟต์แวร์ ซึ่งสามารถ deploy สำเร็จจำนวน 10 ซอฟต์แวร์ โดยระยะเวลาในการ deploy แล้วเสร็จขึ้นอยู่กับขนาดของซอฟต์แวร์ สำหรับซอฟต์แวร์ที่ไม่สามารถ deploy ได้เนื่องจากระบบ SCCM 2012 R2 ไม่รองรับไฟล์ติดตั้งที่เป็น .exe นอกจากนี้ ผู้วิจัยได้ deploy วินโดวส์อัปเดตจำนวน 326 เครื่อง โดยเครื่องคอมพิวเตอร์สามารถรับการอัปเดตคิดเป็น 85.89% ส่วนที่เหลือไม่สามารถอัปเดตได้เนื่องจากปัญหาของเนื้อที่จัดเก็บของไดรฟ์ C: ไม่เพียงพอ และเครื่องที่ไม่ได้เปิดใช้งาน และ ผู้วิจัยได้ deploy อัปเดตโปรแกรมป้องกันไวรัส SCEP จำนวน 636 เครื่อง พบว่าเครื่องผู้ใช้ได้รับการอัปเดตคิดเป็น 95.3% โดยเครื่องที่ไม่ได้รับการอัปเดตพบว่าสถานะของเครื่องไม่ได้เปิดใช้งานหรือขาดการเชื่อมต่อกับระบบนานเกิน 60 วัน และผู้วิจัยได้ทดสอบควบคุมเครื่องผู้ใช้จากระยะไกลเพื่อช่วยเหลือแก้ไขปัญหาให้กับผู้ใช้ โดยทดสอบได้พบว่าสามารถควบคุมเครื่องผู้ใช้จากระยะไกลได้ทั้งแบบเลือกชื่อเครื่องคอมพิวเตอร์ และไอพีแอดเดรสของเครื่องปลายทางได้

จากการทดสอบพบว่าการทำงานของระบบการจัดการกำหนดค่าซอฟต์แวร์จากส่วนกลางสามารถช่วยลดระยะเวลาในการปรับปรุงซอฟต์แวร์ให้เป็นมาตรฐานและช่วยลดงานของแผนกไอทีในการอัปเดตโปรแกรมวินโดวส์เพื่อปิดช่องโหว่หรือความเสี่ยงจากผู้ไม่ประสงค์ดี และผู้ดูแลระบบสามารถควบคุมเครื่องผู้ใช้จากระยะไกลและเรียกดูรายงานต่าง ๆ จากระบบ SCCM 2012 R2 ได้

57920145: MAJOR: INFORMATION TECHNOLOGY; M.Sc (INFORMATION TECHNOLOGY)

KEYWORDS: SOFTWARE DEPLOYMENT/ SOFTWARE DISTRIBUTION/ SCCM 2012 R2

WEERAPUN DOUNGJIT: SYSTEM CENTER CONFIGURATION MANAGER CASE  
STUDY: CALSONIC KANSEI (THAILAND).CO.,LTD. ADVISORY COMMITTEE: NUTTHANON  
LEELATHAKUL, Ph.D., 190 P. 2017.

In this thesis, we present configuration management using Microsoft System Center Configuration Manager (SCCM 2012) for Calsonic Kansei (Thailand) Co.,Ltd (CKT). The company has issues of time spending on 1) the software installation on client PCs, 2) the software upgrade, 3) the software update / Windows patch deployment, and 4) security risk management.

In experiments, we use about 600 computers located in the CKT's network for testing deployments, done by SCCM 2012. Firstly, we test the deployment of standard OS images on 30 PCs (HP EliteDesk 705 G1). The deployment is completed within 89 min. We found that the finishing deployment time depends heavily on spec of network equipment and hard disk. In the second experiment, we deploy eleven common applications for CKT users. The success rate is 91%, and depends on the installation files' size. Note that SCCM could not deploy the .exe installation file, as we could not deploy LEXITRON Dictionary 2.6. In the third experiment, we deploy Windows security updates and critical patch to the 326 PCs, whose OS is Windows 7 (32 bit) about 326 PCs. It turns out that only 85.89% can get updated successfully, due to various errors, e.g., "not enough storage is available to complete". In the last experiment, we deploy and update the antivirus SCEP on 636 computers. The results show 95.3% SCEP deployment success. The deployment failure might be because there are inactive PCs, of which user is out of office.

## สารบัญ

	หน้า
บทคัดย่อภาษาไทย .....	ง
บทคัดย่อภาษาอังกฤษ .....	จ
สารบัญ .....	ฉ
สารบัญตาราง .....	ฉ
สารบัญภาพ .....	ญ
บทที่	
1 บทนำ.....	1
ความสำคัญและที่มาของปัญหา.....	1
วัตถุประสงค์ของการศึกษา .....	2
ประโยชน์ที่คาดว่าจะได้รับการศึกษา .....	3
ขอบเขตของการศึกษา .....	3
ระยะเวลาในการจัดทำ .....	4
2 ทฤษฎีและความรู้ที่เกี่ยวข้อง .....	5
2.1 ระบบ SCCM 2012 R2 (System center configuration manager .....	5
2.1.1 โครงสร้างลำดับชั้นการทำงาน (System SCCM 2012 R2) .....	7
2.1.2 สเปคเครื่องเซิร์ฟเวอร์ระบบ SCCM 2012 R2 .....	14
2.1.3 จุดให้บริการในลำดับชั้น SCCM 2012 R2 (Site system role placement in hierarchy) .....	15
2.2 ระบบ Active directory (AD) .....	16
2.2.1 Active directory domain service (ADDS) .....	17
2.2.2 ส่วนประกอบของ AD (Active directory components and concepts).....	17
2.3 การกำหนดนโยบายหรือข้อบังคับต่าง ๆ .....	29
2.3.1 การสร้าง Group policy .....	30
2.4 การยืนยันตัวตน Authentication .....	31
2.5 การควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศ (Security control) .....	31
2.5.1 ปัญหาที่ทำให้ระบบสารสนเทศล้มเหลว .....	32
2.5.2 ช่องโหว่ของโปรแกรม (Vulnerabilities) .....	33

## สารบัญ (ต่อ)

บทที่	หน้า
2.6 งานวิจัยที่เกี่ยวข้องกับการ Deploy agent .....	35
3 วิธีการดำเนินโครงการ .....	37
3.1 ขั้นตอนการวางแผนการทำงานนิพนธ์ (System planning) .....	37
3.1.1 การศึกษาระบบงานเดิมและหาแนวทางเพื่อแก้ไขปัญหาต่าง ๆ.....	37
3.1.2 ฝึกอบรมและศึกษาข้อมูลจากอินเทอร์เน็ต (Studying & training) .....	38
3.1.3 แผนงานและระยะเวลาในการดำเนินงาน .....	38
3.2 การออกแบบระบบ (System design) .....	39
3.2.1 การออกแบบระบบเครือข่าย .....	39
3.2.2 การสร้างโครงสร้างของระบบ SCCM .....	41
3.2.3 การตั้งชื่อกลุ่มคอมพิวเตอร์ .....	46
3.2.4 การใช้งานระบบ SCCM 2012 R2 .....	55
3.2.5 กำหนดช่วงไอพีเครือข่ายเครื่องผู้ใช้ใน SCCM boundaries .....	56
3.3 การติดตั้งและตั้งค่าระบบ SCCM 2012 R2 .....	64
3.4 ทดสอบระบบ SCCM 2012 R2 (Testing) .....	66
3.5 สังเกตการณ์ การทำงานระบบ SCCM 2012 R2 (Monitoring) .....	70
4 ผลการดำเนินงาน .....	71
4.1 ผลของการติดตั้งเครื่องเซิร์ฟเวอร์สำหรับระบบ SCCM 2012 R2 ตามสเปคที่กำหนด .....	71
4.2 ผลการสร้างกลุ่ม Security group ใน Active directory .....	72
4.3 สร้าง Collection ใน SCCM 2012 R2 .....	73
4.4 กำหนดช่วงไอพีเครือข่ายของผู้ใช้ใน SCCM 2012 R2 boundaries .....	74
4.5 ผลการทดสอบการทำงานของระบบ SCCM 2012 R2 (Testing) .....	74
4.5.1 การทดสอบการทำงานของระบบฐานข้อมูล .....	74
4.5.2 ผลของการทดสอบ deploy ระบบปฏิบัติการวินโดว (OS) ผ่านระบบ SCCM 2012 R2 .....	77
4.5.3 ผลของการทดสอบ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้งาน 5 กลุ่ม .....	85
4.5.4 ผลการทดสอบอัปเดตวินโดว โดยการกำหนดกลุ่มผู้ใช้งาน 3 กลุ่ม .....	86
4.5.5 การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง ทดสอบจำนวน 3 กลุ่ม .....	90
4.5.6 ทดสอบเรียกดูรายงานสเปคเครื่องผู้ใช้งาน 3 กลุ่ม .....	92



## สารบัญ (ต่อ)

บทที่	หน้า
4.5.7 ผลการทดสอบ Remote control viewer ไปเครื่องผู้ใช้จำนวน 3 เครื่อง .....	94
4.5.8 ผลการทดสอบ deploy ติดตั้งโปรแกรมไวรัส .....	97
4.6 ผลสังเกตการณ์ การทำงานของระบบ SCCM 2012 R2 (Monitoring) .....	102
4.6.1 ผลสังเกตการณ์การ deploy โปรแกรมประยุกต์ที่เป็นกลุ่มซอฟต์แวร์ มาตรฐานของบริษัทจะสามารถ deploy ได้ทุกตัวหรือไม่ และใช้เวลา เท่าไรโดยผู้เขียนงานนิพนธ์เก็บผลการสังเกตการณ์ได้ดังตาราง .....	102
4.6.2 ผลการสังเกตการณ์ deploy OS .....	103
4.6.3 ผลสังเกตการณ์เครื่องที่อยู่ในโปรดักชันจริงสามารถอัปเดตวินโดวส์ได้หรือไม่ .....	105
4.6.4 เครื่องที่อยู่ในโปรดักชันจริงสามารถอัปเดตโปรแกรมป้องกันไวรัสได้กี่เครื่อง .....	106
5 อภิปรายและสรุปผล .....	108
บรรณานุกรม .....	110
ภาคผนวก .....	112
ภาคผนวก ก การติดตั้งระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2012 .....	113
ภาคผนวก ข การสร้าง Boundaries .....	124
ภาคผนวก ค การติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์หลัก (Primary site) .....	126
ภาคผนวก ง ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์ฐานข้อมูล (Database site) .....	134
ภาคผนวก จ ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์สาขาบางนา .....	146
ภาคผนวก ฉ ติดตั้ง Agent ที่เครื่องผู้ใช้ (Client setting) .....	155
ภาคผนวก ช สร้างกลุ่มคอมพิวเตอร์ของผู้ใช้ใน SCCM (Device collections) .....	159
ภาคผนวก ซ ตั้งค่าส่วนการ deploy ระบบปฏิบัติการ .....	169
ภาคผนวก ฌ เปิดใช้ PXE on Distribution Point role .....	174
ภาคผนวก ฎ สร้างโปรแกรมประยุกต์สำหรับ deploy.....	177
ภาคผนวก ฏ การ deploy โปรแกรมประยุกต์ไปที่ Collection เครื่องผู้ใช้.....	181
ภาคผนวก ฐ การควบคุมจากทางระยะไกล (Helpdesk remote assistance) .....	187
ประวัติย่อของผู้ทำงานนิพนธ์ .....	190

## สารบัญตาราง

ตารางที่	หน้า
1-1 ระยะเวลาในการจัดทำโปรเจกต์.....	4
2-1 สเปคเซิร์ฟเวอร์ขั้นต่ำ SCCM 2012 .....	15
2-2 จุดให้บริการในลำดับชั้น SCCM 2012 R2 .....	15
2-3 Group Scope .....	28
3-1 รายละเอียดสเปคของเซิร์ฟเวอร์.....	42
3-2 ชื่อและเครื่องไอพี สำหรับเครื่องเซิร์ฟเวอร์ .....	42
3-3 กำหนดตั้งค่าเครื่องเซิร์ฟเวอร์สำหรับ Domain, Gatewat, DNS และ Subnet mask ....	43
3-4 กำหนดค่าคอนฟิกของแต่ละเครื่อง .....	43
3-5 กำหนดบัญชีผู้ใช้และรหัสผ่าน .....	45
3-6 การตั้งชื่อกลุ่มคอมพิวเตอร์ .....	46
3-7 การตั้งชื่อกลุ่มของ client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection).....	48
3-8 ชื่อกลุ่มของ client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection).....	50
3-9 รายละเอียดกลุ่มผู้ใช้ ที่ใช้ซอฟต์แวร์เดียวกัน (Collection) .....	53
3-10 รายละเอียดช่วงไอพีเครือข่ายของผู้ใช้ใน SCCM boundaries.....	55
3-11 Service point ของ SCCM ที่ต้องเปิดเพื่อให้บริการที่ได้กล่าวถึงในหัวข้อ 3.2 .....	65
3-12 รายละเอียดวิธีการติดตั้งและตั้งค่าระบบ SCCM 2012 R2.....	66
4-1 ผลการกำหนดค่าเครื่องเซิร์ฟเวอร์ระบบ SCCM 2012 R2.....	71
4-2 จำนวน Device Collection.....	73
4-3 ผลการทดสอบระบบฐานข้อมูล SQL cluster.....	77
4-4 การติดตั้งวินโดวส์ผ่าน SCCM 2012 R2.....	83
4-5 ขนาดไฟล์และเวลาในการ deploy OS เครื่องที่ทดสอบได้ผลดังนี้.....	84
4-6 กลุ่มผู้ใช้ที่ทดสอบ deploy โปรแกรมประยุกต์.....	86
4-7 ผลการทดสอบโปรแกรมป้องกันไวรัส .....	102
4-8 ผลการ deploy โปรแกรมประยุกต์ และเวลาที่ใช้ต่อเครื่อง .....	103
4-9 ผลของการทดสอบ deploy OS HP EliteDesk 705 G1 .....	104

## สารบัญภาพ

ภาพที่	หน้า
2-1 SCCM 2012 R2 (System center configuration manager) .....	6
2-2 โครงสร้างลำดับชั้นของ SCCM 2012 R2 .....	8
2-3 รายงานจำนวน Microsoft License .....	11
2-4 การกำหนด SQL server สำหรับ Secondary site .....	14
2-5 Active directory .....	16
2-6 Domain and forest .....	19
2-7 Object Active directory .....	20
2-8 Class โดเมน Calsonickansei.co.th .....	20
2-9 Class organizational unit .....	21
2-10 Class group .....	21
2-11 Attributes ของผู้ใช้ระบบ .....	22
2-12 Container ภายใต้โดเมน calsonickansei.co.th .....	23
2-13 Site โดเมนบริษัทคาลโซนิค คันเซ ประเทศไทย จำกัด .....	23
2-14 OU Computers ของแผนกไอที .....	24
2-15 เครื่องมือช่วย Computer management tool .....	25
2-16 Active directory user and computer .....	25
2-17 Group ที่ชื่อ Remote Desktop Users เป็น Group ชนิด Security .....	26
2-18 กลุ่มรูปแบบชนิด Security ที่ผู้ดูแลระบบสร้างขึ้น .....	27
2-19 การ Replicate โดเมนคอนโทรลเลอร์ .....	29
2-20 Group Policy management .....	30
2-21 อุปกรณ์ Token .....	31
2-22 สเปนเมลล์ (Spam mail) .....	33
2-23 ประกาศจากเว็บไซต์ Adobe Flash Player.....	34
2-24 ช่องโหว่จาก Open SSL.....	35
2-25 สถาปัตยกรรม Software Dock.....	36
3-1 การเชื่อมต่อ Domain แบบ Two-way trust ระหว่าง CKJ-CKT .....	40
3-2 การเชื่อมต่อระบบ SCCM 2012 R2 .....	40
3-3 การออกแบบเซิร์ฟเวอร์เพื่อรองรับระบบ SCCM 2012 R2 .....	41

## สารบัญภาพ (ต่อ)

ภาพที่	หน้า
3-4 การออกแบบตั้งรหัสผ่านของบัญชีผู้ใช้ .....	45
3-5 การตั้งชื่อไฟล์เดอริใน Device collection .....	47
3-6 การตั้งชื่อกลุ่มผู้ใช้ใน Active directory .....	53
3-7 การติดตั้งระบบปฏิบัติการวินโดวส์ผ่าน SCCM 2012 R2 .....	57
3-8 การ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้ .....	58
3-9 การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง .....	59
3-10 การอัปเดตระบบปฏิบัติการวินโดวส์ .....	60
3-11 การอัปเดตโปรแกรมป้องกันไวรัส Endpoint protection point .....	61
3-12 การรีโมทเครื่องผู้ใช้ผ่านระบบ SCCM 2012 R2 .....	62
3-13 การเรียกดูรายงานต่าง ๆ ผ่านระบบ SCCM โดยการเรียกดูรายงานจะทำที่เครื่องหลัก SCCM โดยการเรียกดูรายงานจะทำที่เครื่องหลัก (SCCM primary server) .....	63
3-14 เว็บไซต์ Eicar.org สำหรับการทดสอบโปรแกรมป้องกันไวรัส .....	67
3-15 เว็บไซต์ Support.kaspersky.com สำหรับการทดสอบโปรแกรมป้องกันไวรัส .....	68
3-16 เว็บไซต์ ikarussecurity.com สำหรับการทดสอบป้องกันโปรแกรมไวรัส .....	69
4-1 กลุ่มของผู้ใช้คอมพิวเตอร์ที่ใช้ซอฟต์แวร์เดียวกัน (Security group) .....	72
4-2 ช่วงไอพีเครือข่ายของผู้ใช้ (SCCM 2012 R2 Boundaries) .....	74
4-3 ตรวจสอบสถานะของโน้ตบุ๊คเซิร์ฟเวอร์ฐานข้อมูลทั้งสองเครื่อง .....	75
4-4 ตรวจสอบระบบฐานข้อมูลหลักทำงานที่เครื่องไหน .....	75
4-5 เครื่องฐานข้อมูลตัวที่ 1 CKTSERVER023 ถูกปิดลง .....	76
4-6 สถานะของระบบ Cluster หลังจากปิดเครื่องเซิร์ฟเวอร์ CKTSERVER023 .....	76
4-7 สร้าง package ไดรฟ์เวอร์สำหรับเครื่องที่จะทดสอบ deploy OS .....	78
4-8 ไฟล์ระบบปฏิบัติการวินโดวส์ 7 .....	79
4-9 สร้าง Collection สำหรับการ deploy OS .....	80
4-10 Task Sequence สำหรับการ deploy OS (ในกรอบขาว) .....	81
4-11 deploy task sequence ไปที่ Collection ตามรุ่นที่ได้สร้างไว้ .....	82
4-12 การเชื่อมต่อระบบเครือข่ายในการทดสอบ deploy ระบบปฏิบัติการวินโดวส์ .....	83
4-13 โปรแกรมประยุกต์ java8 Update91 .....	85
4-14 ผลของการ deploy Java 8 Update91 .....	86

## สารบัญภาพ (ต่อ)

ภาพที่	หน้า
4-15 หมวดหมู่ที่ต้องการจะให้มีการอัปเดต (Update classification) .....	87
4-16 ผลของการอัปเดตวินโดว์กลุ่มแผนกออกแบบผลิตภัณฑ์ (R&D) .....	87
4-17 ผลของการอัปเดตวินโดว์กลุ่มแผนกไอที .....	88
4-18 ผลของการตรวจสอบชื่อเครื่องคอมพิวเตอร์ที่มีสถานะอัปเดตวินโดว์เป็น Non-compliant..	88
4-19 ชื่อเครื่องคอมพิวเตอร์ที่มีสถานะ Compliance state unknown ในกลุ่มแผนกไอที.....	89
4-20 ผลการตรวจสอบสถานะเครื่องคอมพิวเตอร์ CKT16B001 .....	89
4-21 ผลของการอัปเดตวินโดว์ของแผนกขาย .....	90
4-22 ติดตั้งโปรแกรมประยุกต์ที่คอมพิวเตอร์ชื่อ TH00NB16OA0001 .....	91
4-23 ติดตั้งโปรแกรมประยุกต์ที่คอมพิวเตอร์ชื่อ TH00NB16OA0002 .....	91
4-24 ติดตั้งโปรแกรมประยุกต์ที่คอมพิวเตอร์ชื่อ TH00NB16OA0003 .....	92
4-25 รายงานสเปคเครื่องของกลุ่มฝ่ายแผนกบุคคล .....	93
4-26 รายงานสเปคเครื่องของกลุ่มแผนกฝ่ายบัญชีต้นทุน .....	93
4-27 รายงานสเปคเครื่องของกลุ่มแผนกฝึกอบรม (VUP) .....	94
4-28 ควบคุมเครื่อง CKT000116 จากระยะไกล .....	95
4-29 รีโมทควบคุมเครื่อง CKTCAD10 .....	96
4-30 รีโมทควบคุมเครื่องไอพี 172.28.129.15 .....	97
4-31 Collection สำหรับทดสอบ deploy ติดตั้งโปรแกรมไวรัส Endpoint protection client .	98
4-32 การติดตั้งโปรแกรมป้องกันไวรัส Endpoint protection client เสร็จสมบูรณ์แล้ว .....	98
4-33 ติดตั้งโปรแกรมป้องกันไวรัส SCEP และอัปเดต Definition เป็นเวอร์ชันปัจจุบัน .....	99
4-34 กำหนดการสแกนโปรแกรมป้องกันไวรัส Endpoint protection client ที่เครื่องผู้ใช้.....	100
4-35 ดาวน์โหลดไฟล์ไวรัสจากเว็บไซต์ <a href="http://www.eicar.org/85-0.Download.html">http://www.eicar.org/85-0.Download.html</a> .....	100
4-36 ดาวน์โหลดไฟล์จากเว็บไซต์ <a href="http://Support.kaspersky.com">Support.kaspersky.com</a> และ <a href="http://ikarussecurity.com">ikarussecurity.com</a> .....	101
4-37 กราฟแสดงผลเวลา deploy OS เครื่อง HP EliteDesk 705 G1 .....	104
4-38 ผลการอัปเดตวินโดว์วันที่ 18 พ.ค. 2559 .....	105
4-39 ผลการอัปเดตวินโดว์ผิดพลาด (ERROR) .....	105
4-40 ผลการอัปเดต Definition โปรแกรมป้องกันไวรัส Endpoint protection client.....	106

# บทที่ 1

## บทนำ

### 1.1 ความสำคัญและที่มาของปัญหา

ฮาร์ดแวร์และซอฟต์แวร์จำนวนมากถูกพัฒนาขึ้นใหม่ เพื่อรองรับการเจริญเติบโตของธุรกิจ ซึ่งจำเป็นต้องนำเทคโนโลยีมาขับเคลื่อนให้สามารถแข่งขันในตลาดอุตสาหกรรมได้ เนื่องจากโรงงานอุตสาหกรรมได้นำอุปกรณ์คอมพิวเตอร์ใหม่ ๆ เข้ามาใช้งานเพื่อช่วยกระบวนการผลิตให้มีประสิทธิภาพที่ดีขึ้น และช่วยจัดทำเอกสารสำหรับส่วนของสำนักงาน เช่น ฝ่ายการตลาด ฝ่ายจัดซื้อ ฝ่ายการผลิต ฝ่ายจัดส่งสินค้า แต่ละฝ่ายจึงมีเครื่องคอมพิวเตอร์สำหรับพนักงานจำนวนมาก ดังนั้นหน่วยงานไอทีจึงจำเป็นต้องควบคุมรุ่นของซอฟต์แวร์ให้เป็นมาตรฐานเพื่อป้องกันระบบและข้อมูลของบริษัทในการดำเนินการผลิตหรือสินค้าต่าง ๆ จากผู้ไม่ประสงค์ดี ไม่ให้รั่วไหลสู่บุคคลภายนอกได้

บริษัทคาลโซนิค คันเซ ได้ประสบปัญหาการบริหารจัดการคอมพิวเตอร์ ทั้งฮาร์ดแวร์และซอฟต์แวร์ต่าง ๆ ที่ติดตั้งให้ผู้ใช้ โดยมีรายละเอียดปัญหาดังนี้

1. ปัญหาการบริหารจัดการรุ่นของซอฟต์แวร์ให้เป็นมาตรฐานทุกเครื่อง เพื่อควบคุมให้ระบบ เป็นมาตรฐานของการใช้งานต่าง ๆ ขององค์กร เช่น เมื่อบริษัทมีการปรับเปลี่ยนมาใช้ ไมโครซอฟต์ ออฟฟิศ 2010 (เปลี่ยนจากรุ่น ไมโครซอฟต์ ออฟฟิศ 2007) โดยหากบางแผนกมีการใช้คำสั่งหรือสูตรต่าง ๆ ลงบนโปรแกรมไมโครซอฟต์ เอ็กเซล และมีการแลกเปลี่ยนข้อมูลระหว่างแผนก หากเอกสารถูกสร้างด้วยไมโครซอฟต์ ออฟฟิศ รุ่นต่างกัน รูปแบบของเอกสารอาจไม่เป็นไปตามแบบหรือผิดเพี้ยนไปจากเดิมได้ ดังนั้นทางแผนกไอทีจึงต้องทำการปรับเปลี่ยนไมโครซอฟต์ ออฟฟิศ ในทุกเครื่องให้เป็น ไมโครซอฟต์ ออฟฟิศ 2010 รุ่นเดียวกันทุกเครื่อง ซึ่งการปรับเปลี่ยนต้องใช้เวลา เนื่องจากบริษัทขาดเครื่องมือหรือซอฟต์แวร์ในการบริหารจัดการ ทำให้บริษัทต้องจัดทำแผนงานที่ให้พนักงานไอทีจำนวน 2 คนเดินไปแต่ละแผนกเพื่อถอนการติดตั้ง ไมโครซอฟต์ ออฟฟิศ 2007 ออกแล้วติดตั้ง ไมโครซอฟต์ ออฟฟิศ 2010 ในเครื่องคอมพิวเตอร์จำนวนประมาณ 600 เครื่อง โดยการติดตั้งแต่ละเครื่องใช้เวลาประมาณ 30-40 นาที จึงทำให้ใช้เวลาในการติดตั้งให้แล้วเสร็จนานกว่า 1 เดือน นอกจากนี้พนักงานต้องเสียเวลาในการทำงานประจำ และทางบริษัทต้องเสียค่าใช้จ่ายในการทำงานล่วงเวลาของพนักงานอีกด้วย

2. ปัญหาการอัพเดทวินโดวส์ล่าช้า ทำให้มีปัญหาเรื่องความเสี่ยงด้านความปลอดภัยของระบบ เนื่องจากมีการค้นพบช่องโหว่ต่าง ๆ ของระบบตลอดเวลา ผู้บริหารของบริษัทคาลโซนิค คันเซ (ประเทศไทย) จำกัด ได้มองเห็นความสำคัญในเรื่องความปลอดภัยของข้อมูลเป็นอย่างมาก จึงให้ฝ่าย

ไอทีทำการควบคุมการอัปเดตวินโดวส์ในทุกเครื่อง ให้ทันสมัยตามมาตรฐานของบริษัท (และต้องผ่านการทดสอบกับทางบริษัทคู่ค้า (นิสสัน) ก่อน)

3. ปัญหาการทำบัญชีสินทรัพย์อุปกรณ์คอมพิวเตอร์ของบริษัท บัญชีดังกล่าวถูกเก็บบันทึกไว้ที่ไฟล์ไมโครซอฟต์ เอ็กเซล แล้วคอมพิวเตอร์มีหลายยี่ห้อ หลายรุ่น จึงทำให้ทำบัญชียาก

4. ปัญหาการควบคุมการติดตั้งซอฟต์แวร์ลิขสิทธิ์ต่างๆของบริษัท บางเครื่องยังให้สิทธิ์แก่ผู้ใช้เป็นสิทธิ์ของแอดมิน ผู้ใช้สามารถติดตั้งซอฟต์แวร์ที่ไม่ได้ซื้อลิขสิทธิ์ถูกต้องได้ด้วยตนเอง ดังนั้นบริษัทจึงต้องการควบคุมและปรับสิทธิ์ของผู้ใช้ให้เป็น Standard User ซึ่งหลังจากสิทธิ์ถูกปรับเปลี่ยนเป็น Standard User แล้ว ผู้ใช้จะไม่สามารถสั่งให้บางโปรแกรมในสสารบบ C:\Program files\ เช่น IFS Application, Mizuho bank, HR payroll, และ Microsoft Office ให้ทำงานได้

5. ปัญหาการร้องขอให้แผนกไอทีติดตั้งซอฟต์แวร์ที่เป็นมาตรฐานที่ทางบริษัทกำหนดไว้ ว่าจะจะเป็นไดรฟ์เวอร์ปริ้นเตอร์ และซอฟต์แวร์อื่น ๆ เช่น การร้องขอให้ติดตั้งโปรแกรม Brava! Reader ซึ่งเป็นโปรแกรมมาตรฐานประเภทแชร์แวร์ ใช้ในการดูไฟล์ .Tiff และมีอายุการใช้งานฟรีเพียง 3 เดือน หากพนักงานต้องการใช้ซอฟต์แวร์ดังกล่าวหลังจากหมดอายุ พนักงานต้องติดต่อให้พนักงานไอทีเพื่อให้ถอนการติดตั้งและติดตั้งให้ใหม่ บริษัทจึงต้องการหาวิธีที่จะช่วยให้ผู้ใช้สามารถเลือกติดตั้งซอฟต์แวร์เหล่านี้ได้เอง

จากปัญหาดังกล่าวข้างต้น ผู้จัดทำงานนิพนธ์จึงได้ศึกษาซอฟต์แวร์ System change management center 2012 (SCCM 2012 R2) ของค่ายไมโครซอฟต์ เข้ามาช่วยบริหารจัดการตามนโยบายของบริษัทแม่ เพื่อให้เป็นมาตรฐานเดียวกันกับทุกบริษัทในเครือ และสนับสนุนการทำงานของแผนกไอทีแต่ละประเทศให้มีความปลอดภัยและมีความถูกต้องของข้อมูล รวมถึงความสามารถควบคุมมาตรฐานต่าง ๆ ของซอฟต์แวร์ให้มีเวอร์ชันการทำงาน และการนำมาใช้งานที่เหมือนกัน เช่น การนำซอฟต์แวร์ ERP มาใช้เหมือนกันทุกสาขาประเทศ การใช้งานโปรแกรมไมโครซอฟต์ ออฟฟิศ เวอร์ชันเดียวกันทุกสาขาประเทศ และฮาร์ดแวร์ที่มีสเปค ยี่ห้อ แบนด์ รุ่น ที่เหมือนกัน เพื่อเป็นการต่อรองราคาซื้อจากบริษัทจำหน่ายให้มีราคาที่ถูกลง และพนักงานสามารถนำเครื่องคอมพิวเตอร์ไปใช้งานได้ทุกสาขาในแต่ละประเทศโดยฮาร์ดแวร์สามารถรองรับการใช้งานได้เหมือนกัน

## 1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อควบคุมซอฟต์แวร์ให้เป็นมาตรฐานหรือมีรุ่นเดียวกัน
2. เพื่อควบคุมฮาร์ดแวร์ คอมพิวเตอร์ที่ใช้งานให้เป็นมาตรฐาน (ยี่ห้อ หรือ รุ่น) เดียวกัน
3. เพื่อเป็นแนวทางให้ผู้ที่สนใจสามารถนำแนวความคิดที่ได้นำเสนอไปทำการพัฒนาหรือประยุกต์ใช้ในงานวิจัยต่าง ๆ

### 1.3 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

1. สามารถควบคุมซอฟต์แวร์และฮาร์ดแวร์ให้เป็นมาตรฐานเดียวกันทั้งระบบ และยังสามารถเรียกดูรายงานการใช้งานของเครื่องผู้ใช้ ได้ตลอดเวลา
2. ลดเวลาที่ใช้ในการปฏิบัติงานของแผนกไอทีในกรณีที่มีการปรับปรุง อัปเดตซอฟต์แวร์ต่าง ๆ ของระบบ
3. สามารถปรับปรุงมาตรฐานการใช้งานให้เป็นไปตามมาตรฐานของบริษัทแม่ได้

### 1.4 ขอบเขตของการศึกษา

การจัดทำ SCCM 2012 R2 โดยมีขอบเขตดังต่อไปนี้

1. การทำงานควบคุมซอฟต์แวร์ของเครื่องคอมพิวเตอร์ที่อยู่ในโดเมน Calsonickansei.co.th
2. การทำงานควบคุมฮาร์ดแวร์คอมพิวเตอร์ที่อยู่ในโดเมน Calsonickansei.co.th โดยมีรายละเอียดคอมพิวเตอร์ ดังนี้
  - คอมพิวเตอร์ส่วนสำนักงาน จำนวน 370 เครื่อง
  - คอมพิวเตอร์โรงงาน 1 จำนวน 50 เครื่อง
  - คอมพิวเตอร์โรงงาน 2 จำนวน 78 เครื่อง
  - คอมพิวเตอร์โรงงาน 3 จำนวน 80 เครื่อง
  - คอมพิวเตอร์โรงงาน 4 จำนวน 32 เครื่อง
  - คอมพิวเตอร์โรงงาน 5 จำนวน 12 เครื่อง
  - Server HQ จำนวน 18 เครื่อง
3. จัดทำระบบควบคุมซอฟต์แวร์ แต่ละแผนกให้เป็นมาตรฐาน และหากมีการร้องขอใช้ซอฟต์แวร์เพิ่มเติมจะต้องมีการร้องขอ และแจ้งกับทางแผนกไอที เพื่อให้ตรวจสอบก่อนทุกครั้ง เนื่องจากทางแผนกไอทีจะทำการควบคุมการติดตั้งซอฟต์แวร์ลิขสิทธิ์ของบริษัททั้งหมด
4. ระบบสามารถควบคุมนโยบายไม่ให้ผู้ใช้สามารถติดตั้งหรือ ถอนการติดตั้งโปรแกรมได้เอง
5. ระบบสามารถทำการปรับปรุงเวอร์ชันของโปรแกรมได้ ด้วยการสั่ง deploy ที่ เครื่อง Server SCCM 2012 R2.
6. ระบบสามารถถอนการติดตั้งโปรแกรมที่เครื่องผู้ใช้ ได้โดยการควบคุมได้จากส่วนกลางของ SCCM Primary server
7. ระบบสามารถ deploy ซอฟต์แวร์อัปเดต และวินโดวส์อัปเดตตามนโยบายบริษัทได้



8. ระบบสามารถ deploy OS เพื่อทำการติดตั้งเครื่องใหม่ได้โดยผ่านสายเคเบิลแลน โดยดึงไฟล์อิมเมจแต่ละรุ่นจากเครื่องเซิร์ฟเวอร์
9. ควบคุมการใช้ และตรวจเช็ครายงานของแต่ละเครื่องได้
10. ทำเอกสารสรุปรายงานของเครื่องต่างๆ รวมถึงชนิดของไฟล์ที่ใช้เก็บในเครื่องคอมพิวเตอร์ได้

### 1.5 ระยะเวลาในการจัดทำ

สำหรับการจัดทำโปรเจกต์นี้ได้กำหนดระยะเวลาในการจัดทำ เพื่อให้สามารถบรรลุตามวัตถุประสงค์ที่ได้กำหนดไว้ ซึ่งมีรายละเอียดดังตารางที่ 1-1

ตารางที่ 1-1 ระยะเวลาในการจัดทำโปรเจกต์

แผนการจัดทำโปรเจกต์ SCCM	เดือน											
	เม.ย. 58	พ.ค. 58	มิ.ย. 58	ก.ค. 58	ส.ค. 58	ก.ย. 58	ต.ค. 58	พ.ย. 58	ธ.ค. 58	ม.ค. 59	ก.พ. 59	มี.ค. 59
ศึกษาทฤษฎีและงานวิจัย ความรู้พื้นฐานที่เกี่ยวข้อง	→											
จัดทำเอกสารและทำการรวบรวม ข้อมูลการติดตั้ง		→										
ติดตั้ง SCCM 2012 R2				→								
จัดทำเอกสารการดำเนินงานนิพนธ์						→						
ทดสอบการใช้งาน ควบคุมให้เป็นไปตามวัตถุประสงค์							→					
จัดทำเอกสารและส่งรายงานฉบับ สมบูรณ์										→		

## บทที่ 2

### ทฤษฎีและความรู้ที่เกี่ยวข้อง

การควบคุมการใช้งานซอฟต์แวร์จากเซิร์ฟเวอร์ส่วนกลาง เป็นส่วนหนึ่งในการช่วยให้การทำงานของแผนกไอที สามารถควบคุมการใช้งานผลิตภัณฑ์ซอฟต์แวร์ลิขสิทธิ์ของบริษัทและการปรับปรุงอัปเดตเวอร์ชันใหม่ ๆ ของซอฟต์แวร์ให้เป็นตามที่องค์กรได้กำหนดนโยบายไว้ เพื่อช่วยลดเวลาในการบริหารจัดการสินทรัพย์ซึ่งเป็นอุปกรณ์คอมพิวเตอร์ และการปรับปรุงอัปเดตวินโดวส์ตามมาตรฐานที่ทางบริษัทได้กำหนดไว้ เนื่องจากเป็นการควบคุมความปลอดภัยของระบบภายในบริษัท รวมถึงข้อมูลที่เป็นความลับหรือข้อมูลสำคัญของบริษัทไม่ให้รั่วไหลออกไปสู่คู่แข่งผ่านช่องโหว่และภาวะคุกคามที่เกิดจากหลายช่องทาง โดยเข้ามาปรับเปลี่ยน แก้ไข ข้อมูลและเอกสารต่าง ๆ ให้ได้รับความเสียหายหรือผิดไปจากรูปแบบเดิม เช่น ไวรัสมัลแวร์ แฮ็กเกอร์

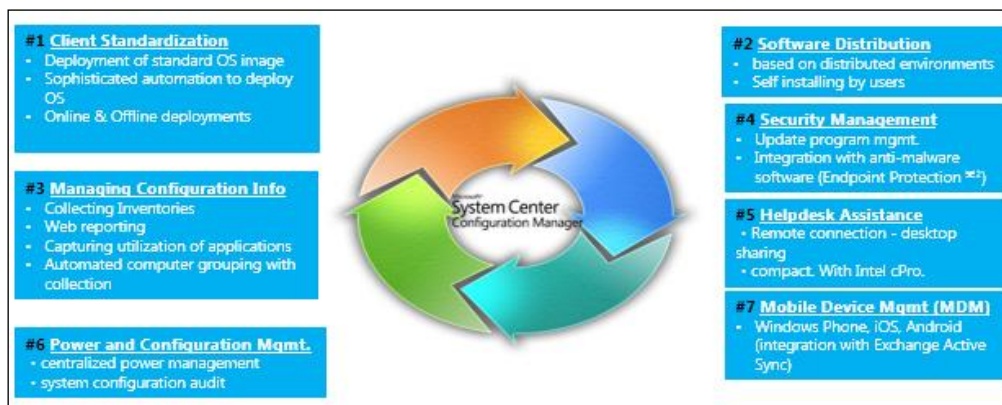
การควบคุมซอฟต์แวร์จากส่วนกลางช่วยให้ผู้ดูแลระบบรู้และตรวจสอบรายการอุปกรณ์คอมพิวเตอร์ได้ว่าการติดตั้งซอฟต์แวร์อะไรบ้าง และชื่อเครื่องเป็นของใครที่ใช้อยู่ในปัจจุบัน ซึ่งการตรวจสอบสามารถทำได้โดยเรียกดูรายงานจากซอฟต์แวร์ส่วนกลางนั่นเอง

ทั้งนี้ในเนื้อหาบทนี้กล่าวถึง ระบบบริหารจัดการฮาร์ดแวร์และซอฟต์แวร์ SCCM 2012 R2 (System center configuration manager) การศึกษาการทำงานของระบบ Active directory การกำหนด Group policy หลักการยืนยันตัวตน (Authentication) ความปลอดภัยของข้อมูล (Security) การศึกษาวิธีการติดตั้งและใช้งานเอเจนต์ (Deploy agent) ไปที่เครื่องของผู้ใช้ ซึ่งในบทนี้จะนำเสนอหลักการและกระบวนการทำงานที่สำคัญของแต่ละขั้นตอนวิธี และศึกษางานวิจัยที่เกี่ยวข้องมีรายละเอียดดังนี้

#### 2.1 ระบบ SCCM 2012 R2 (System center configuration manager)

ระบบ SCCM 2012 R2 เป็นผลิตภัณฑ์ซอฟต์แวร์การจัดการระบบที่พัฒนาโดยไมโครซอฟต์สามารถช่วยเพิ่มประสิทธิภาพขององค์กร สำหรับการจัดการคอมพิวเตอร์, เซิร์ฟเวอร์ ที่ใช้ระบบปฏิบัติการ วินโดวส์(windows), Windows embedded (เป็นระบบปฏิบัติการวินโดวส์ ตัวเล็ก ๆ ที่เอาไว้ลงกับอุปกรณ์ถือได้ เช่น pos station, kios, barcode reader), Mac OS X, Linux หรือ UNIX เช่นเดียวกับระบบปฏิบัติการมือถือต่าง ๆ ที่สามารถคอนโซลการจัดการเดียวได้ในระบบคลาวด์เช่น Windows phone, iOS symbian, และ Android จัดการการตั้งค่าให้สามารถควบคุมจากระยะไกล, จัดการควบคุมซอฟต์แวร์การใช้งานระบบปฏิบัติการ การอัปเดต การติดตั้งใหม่ การถอนการติดตั้ง การจัดการด้านความปลอดภัยในการป้องกันการเข้าถึงเครือข่ายเน็ตเวิร์กภายในโดเมนเดียวกัน การตรวจสอบฮาร์ดแวร์ให้เป็นไปตามมาตรฐานขององค์กร และควบคุมการใช้งานซอฟต์แวร์ลิขสิทธิ์โดย

การเรียกดูรายงานได้จากระบบ SCCM 2012 R2 และช่วยลดค่าใช้จ่ายในการบริหารงานทีมไอที ที่ต้องมีจำนวนมากในการควบคุมฮาร์ดแวร์ ซอฟต์แวร์ ขององค์กรที่มีเครื่องคอมพิวเตอร์จำนวนมากได้ โดยหน้าที่หลักในการทำงาน มีทั้งหมด 7 ส่วน ดังนี้



ภาพที่ 2-1 SCCM 2012 R2 (System center configuration manager)

### 1. การกำหนดมาตรฐานของเครื่องคอมพิวเตอร์ผู้ใช้ (Client standardization)

การกำหนดมาตรฐานของเครื่องคอมพิวเตอร์ผู้ใช้ ให้ได้ตามนโยบายขององค์กรในการควบคุมการใช้งานซอฟต์แวร์ลิขสิทธิ์ การอัปเดตเวอร์ชัน การติดตั้งใหม่ ถอดการติดตั้ง โดยสามารถตรวจเช็คและควบคุมได้จากส่วนกลาง, การ deploy ระบบปฏิบัติการวินโดวส์ (Deployment of standard OS image) การ deploy ซอฟต์แวร์แบบออนไลน์และออฟไลน์ได้ (Online & Offline deployments)

### 2. การกระจายซอฟต์แวร์ (Software distribution)

การกระจายซอฟต์แวร์ไปที่เครื่องของผู้ใช้ หรือเซิร์ฟเวอร์ ที่มีการติดตั้ง Agent ไว้แล้ว สามารถทำได้โดยการสั่ง deploy จาก SCCM เซิร์ฟเวอร์ เพื่อไปทำการติดตั้งใหม่ หรือถอนการติดตั้งซอฟต์แวร์ที่เครื่องผู้ใช้ได้ และยังสร้างเป็นหน้าเว็บ Web Portal สำหรับให้ผู้ใช้งานสามารถทำการเลือกติดตั้งซอฟต์แวร์หรือแอปพลิเคชันต่าง ๆ ได้ คล้ายกับ App Store ของไอโฟน โดยผู้ใช้สามารถเลือกติดตั้งซอฟต์แวร์ได้ด้วยตนเอง (Self-installing by users)

### 3. การจัดการค่าคอนฟิก (Managing configuration info)

การจัดการค่าคอนฟิกของเครื่องผู้ใช้ให้เป็นไปตามมาตรฐานที่ทางองค์กรได้กำหนดไว้ โดยสามารถควบคุมและจัดเก็บข้อมูลของการใช้งานซอฟต์แวร์และฮาร์ดแวร์ (Collecting inventories) สามารถเรียกดูรายงานจาก SCCM server, การจับภาพการใช้ประโยชน์จากการใช้งาน Capturing utilization of applications, การจัดกลุ่มคอมพิวเตอร์อัตโนมัติด้วยคอลเลกชัน โดยการจับกลุ่มของ

ผู้ใช้ที่มีการเชื่อมต่อข้อมูลกับ Active directory (Automated computer grouping with collection) สำหรับการจัดการจัดการค่าคอนฟิกจะทำให้ไอทีสามารถแบ่งกลุ่มของฮาร์ดแวร์และซอฟต์แวร์ออกเป็นส่วน ๆ และสะดวกต่อการจัดทำรายงานเสนอผู้บริหาร

#### 4. การบริหารจัดการด้านความปลอดภัย (Security management)

การบริหารจัดการความปลอดภัยของเครื่องผู้ใช้ ที่มีการติดตั้ง Agent ไปแล้วนั้น ใน SCCM จะมีเครื่องมือซอฟต์แวร์ที่ใช้ในการป้องกันไวรัสมาแล้ว รวมอยู่ด้วย ชื่อโปรแกรม Endpoint protection ซึ่งสามารถเปิดใช้งานและติดตั้งที่เครื่องผู้ใช้ได้โดยสามารถ deploy จากระบบ SCCM สำหรับเครื่องที่มี Agent SCCM หรือสร้างเป็นโปรแกรมประยุกต์ (Software Package) ติดตั้งเครื่องที่ไม่ได้เชื่อมต่อระบบเครือข่ายได้ (Offline)

#### 5. การควบคุมจากทางระยะไกล (Helpdesk Assistance)

การควบคุมจากทางระยะไกลไปที่เครื่องของผู้ใช้ ที่มีการติดตั้ง Agent SCCM ไว้แล้วแล้ว เพื่อช่วยเหลือในการแก้ไขปัญหาที่เกิดขึ้นจากซอฟต์แวร์คอมพิวเตอร์ได้ โดยการควบคุมระยะไกลไปที่เครื่องคอมพิวเตอร์นั้นสามารถกำหนดสิทธิ์ในการควบคุมเครื่องปลายทางได้ เช่นกำหนดให้เครื่องปลายทางตอบตกลงก่อนถึงจะสามารถควบคุมระยะไกลเข้าไปได้ หรือสามารถกำหนดให้ผู้ดูแลระบบสามารถควบคุมระยะไกลเข้าไปที่เครื่องของปลายทางได้ โดยไม่ต้องตอบตกลง ทั้งนี้ขึ้นอยู่กับการตั้งค่าของระบบ และการกำหนดสิทธิ์การใช้งาน

#### 6. การควบคุมตั้งค่าการใช้งานพลังงานคอมพิวเตอร์ (Power and configuration mgmt.)

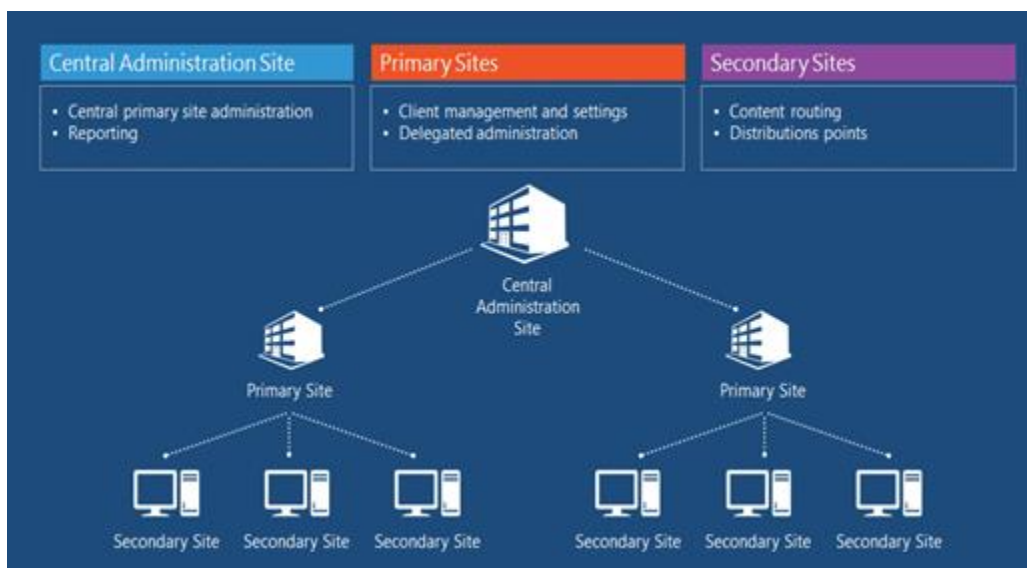
การควบคุมการกำหนดค่าของการใช้พลังงานเครื่องคอมพิวเตอร์เพื่อกำหนดให้ใช้งานตามนโยบายโดยสามารถกำหนดแบบรวมศูนย์ (Centralized power management) เพื่อให้สามารถควบคุมได้จากส่วนกลางและเป็นมาตรฐานเดียวกัน

#### 7. การควบคุมการใช้งานอุปกรณ์มือถือ (Mobile device management (MDM))

การควบคุมการใช้งานปรับตั้งค่าเครื่องมือถือ ให้เป็นไปตามมาตรฐานที่องค์กรกำหนด การควบคุมซอฟต์แวร์ที่ติดตั้งในมือถือ การตั้งค่าโปรแกรม การจัดเก็บข้อมูล การเชื่อมต่อกับเน็ตเวิร์ก โดยระบบโทรศัพท์มือถือที่มีระบบปฏิบัติการ Windows phone, iOS, Android ทำการซิงค์กับระบบ Exchange active sync ที่ใช้งานบนคลาวด์ (cloud) ได้

### 2.1.1 โครงสร้างลำดับชั้นการทำงาน (System SCCM 2012 R2)

การทำงานของ SCCM 2012 R2 สามารถแบ่งออกเป็นระดับของการทำงานระบบได้ 3 ระดับ Central administration site, Primary site, Secondary sites โดยรายละเอียดการทำงานมีดังนี้



ภาพที่ 2-2 โครงสร้างลำดับชั้นของ SCCM 2012 R2 (Adam Gordon. (2559, 6 สิงหาคม))

#### 2.1.1.1 Central administration site 2012 R2

Central administration site (CAS) จะอยู่บนสุดของลำดับชั้น (Hierarchy) ทำหน้าที่ในการบริหารจัดการสิทธิการใช้งานบัญชีผู้ใช้ โดยสามารถกำหนดสิทธิและปรับเปลี่ยนบัญชีผู้ใช้ให้สามารถใช้งาน Primary site ที่อยู่ภายใต้ CAS ได้ทุกตัว และ CAS ยังทำหน้าที่รวบรวมรายงานได้จากส่วนกลางเพื่อลดความยุ่งยากในกรณีที่มี Primary site หลายตัว ที่ผู้ดูแลระบบจะต้องเข้าไปเรียกดูรายงานที่ Primary site ทุกตัว สามารถสำรองค่าติดตั้ง (ค่าคอนฟิก) ต่าง ๆ เพื่อให้ส่วน Site server maintenance task ใน CAS ใช้สำหรับการกู้ Primary site ที่ล่มไปขึ้นมาได้ นอกจากนี้ ผู้ใช้สามารถใช้ CAS เรียกดูค่าการปรับแต่งจากส่วนกลางโดยการเปิดใช้งานส่วน Configuration manager logs, ผู้ใช้สามารถใช้ CAS เปิด-ปิดจุดให้บริการต่าง ๆ (Role, รายละเอียดในตารางที่ 2-2) ใน Primary sites ได้ นอกจากนี้ ผู้ใช้สามารถใช้ CAS เพื่อดูบันทึกเหตุการณ์ (log) ได้

คุณลักษณะของ Central administration site

- ใช้สำหรับการบริหารจัดการสิทธิการใช้งานบัญชีผู้ใช้และรายงาน บนสุดของลำดับชั้น
- ใช้เพื่อวัตถุประสงค์ในการบริหารเท่านั้น
- ใช้ฐานข้อมูล SQL server ในการปรับปรุงฐานข้อมูลให้เหมือนกัน (Replication)
- ไม่สามารถสั่งการไปที่เครื่องผู้ใช้ได้
- เครื่องผู้ใช้ไม่สามารถส่งรายงานมาที่ CAS ได้โดยตรง
- สามารถรองรับได้สูงสุด 25 Primary site พร้อม ๆ กัน
- สามารถรองรับเครื่องผู้ใช้ได้มากกว่า 100,000 เครื่อง

### 2.1.1.2 Primary site

Primary site ให้บริการเครื่องผู้ใช้ในเครือข่ายที่เชื่อมต่อกัน โดย Primary site ยอมให้ CAS มาบริหารจัดการตัวมันได้ แต่ไม่ยอมให้ Primary site ตัวอื่นมาบริหารจัดการกับตัวมัน คุณลักษณะของ Primary site

- Primary site สามารถบริหารจัดการเครื่องผู้ใช้ได้โดยตรง
- Primary site สามารถทำงานได้ด้วยตนเอง (Standalone) หรือ จะถูกจัดการ โดย CAS ก็ได้
- Primary site ไม่สามารถถูกจัดการโดย Primary site ได้
- เมื่อติดตั้ง Primary site ภายใต้ CAS ระบบฐานข้อมูลที่ Primary site จะถูกกำหนดค่าให้มีช่วงเวลาปรับปรุงฐานข้อมูลให้เหมือนกัน (Replication) กับ CAS โดยอัตโนมัติ
- Primary site เมื่อติดตั้งภายใต้ CAS ระบบฐานข้อมูลที่ Primary site จะส่งข้อมูลไปให้ CAS อัตโนมัติ จากนั้น CAS จะทำข้อมูลให้เหมือนกันกับ Primary site (Replication)
- Primary site สามารถดึงข้อมูลของผู้ใช้ (Client) ที่มี Agent SCCM ได้ทั้งหมด
- Primary site สามารถรองรับได้สูงสุด 10 Management point (ผู้ดูแลระบบใช้ Management point หลายตัว เพื่อไม่ให้ตัวใดตัวหนึ่งต้องมีภาระการทำงานมากเกินไป โดยผู้ดูแลระบบสามารถทำ Load balance ให้กับ Management point ได้ด้วย Network load balancing cluster virtual server ใน Windows server 2008
- Primary site สามารถรองรับ Secondary site ได้มากถึง 250 Site
- Primary site รองรับเครื่องผู้ใช้ที่อยู่ภายใต้ไม่เกิน 100,000 เครื่อง เนื่องจากเป็นข้อจำกัดของการปรับปรุงซอฟต์แวร์ไมโครซอฟต์ (WSUS)

Primary site ถูกกำหนดให้มีบริการดังต่อไปนี้

1. Management point เป็นจุดในการบริหารจัดการเครื่องผู้ใช้ โดย Agent จะรับส่งข้อมูลจากเครื่องผู้ใช้ เพื่อเป็นข้อมูลสำหรับการวิเคราะห์และบริหารจัดการ เช่น สถานะการ deploy โปรแกรมประยุกต์, ข้อมูลการติดตั้งซอฟต์แวร์, ข้อมูลฮาร์ดแวร์, ผู้ดูแลระบบสามารถกำหนดนโยบายจาก Management point ในการ deploy โปรแกรมประยุกต์ อัปเดตวินโดวส์ เป็นต้น

2. Distribution point เป็นจุดเก็บไฟล์ซอฟต์แวร์สำหรับแจกจ่ายให้เครื่องผู้ใช้ที่ได้รับนโยบายจากผู้ดูแลระบบ โดย Agent จะดาวน์โหลดไฟล์เพื่อไปติดตั้ง

3. Software update point สามารถเปิดให้บริการได้โดยต้องติดตั้ง WSUS ในระบบเซิร์ฟเวอร์ก่อน เนื่องจาก Software update point จะใช้ความสามารถจาก Library ของ

WSUS ช่วยในการดาวน์โหลดรายการข้อมูลเกี่ยวกับการอัปเดต (Metadata catalog) เช่น ชื่อผลิตภัณฑ์, คำอธิบาย, ผลิตภัณฑ์ที่การอัปเดตสนับสนุน, ประเภทการอัปเดต (Critical, Definition, Driver, Feature packs, Security, Service pack, Tools, Update rollups, Updates ) URL ดาวน์โหลด, กฎบังคับใช้ และอื่น ๆ จากไมโครซอฟต์อัปเดต จากนั้นระบบเซิร์ฟเวอร์ SCCM ที่เปิดใช้งาน Software update point ซึ่งจะปรับปรุงฐานข้อมูลเกี่ยวกับการอัปเดตให้เหมือนกันทุกเซิร์ฟเวอร์ และเมื่อมีข้อมูลการอัปเดตผลิตภัณฑ์จากไมโครซอฟต์แล้ว Software update point จะ deploy update ไปที่เครื่องผู้ใช้ตามนโยบายที่ผู้ดูแลระบบกำหนด

4. System health validator point ให้บริการตรวจสอบค่าต่าง ๆ ในเครื่องผู้ใช้ว่าเป็นไปตามนโยบายการเข้าถึงเครือข่าย (Network access policy) หรือไม่ ซึ่งต้องเปิดใช้งานควบคู่กับ Network policy server โดยผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบตามนโยบายที่ได้กำหนดไว้ เช่น กำหนดนโยบายไว้ว่าเมื่อเครื่องผู้ใช้เชื่อมต่อเครือข่ายให้ตรวจสอบโปรแกรมป้องกันไวรัสได้มีการปรับปรุงอัปเดตเวอร์ชันเป็นวันที่ล่าสุดหรือไม่ ถ้าใช่ ให้สามารถเชื่อมต่อระบบเครือข่ายได้ แต่ถ้าไม่ ให้ทำการอัปเดตก่อนหรือตัดการเชื่อมต่อออกจากระบบเครือข่าย

5. State migration point ทำหน้าที่เก็บข้อมูลโปรไฟล์ของผู้ใช้งาน ในกรณีผู้ใช้ติดตั้งระบบปฏิบัติการวินโดวส์ใหม่ เปลี่ยนเครื่องคอมพิวเตอร์ใหม่ เพื่อให้ได้ข้อมูลและการกำหนดค่าของโปรไฟล์เหมือนเดิม ตัวอย่างเช่น เครื่องผู้ใช้มีการปรับเปลี่ยนระบบปฏิบัติการวินโดวส์จากระบบปฏิบัติการวินโดวส์ 7 เป็น ระบบปฏิบัติการวินโดวส์ 10 จะสำรองข้อมูลโปรไฟล์ไว้ใน State migration point ก่อนที่จะติดตั้งระบบปฏิบัติการวินโดวส์ 10 และเมื่อติดตั้งเสร็จเรียบร้อยแล้ว สามารถเรียกคืนโปรไฟล์จาก State migration point ได้

6. Fallback status point ทำหน้าที่ช่วยผู้ดูแลระบบในการตรวจสอบสถานะการ deploy ว่าสำเร็จหรือไม่สำเร็จ การระบุตัวตนของเครื่องผู้ใช้งาน และเครื่องผู้ใช้งานจะส่งสถานะมาให้ Fallback status point ในกรณีที่ไม่สามารถติดต่อกับ Management Point ได้ เช่น เครื่องผู้ใช้ไม่มีใบรับรอง (Certificate) ที่ถูกต้อง

7. Out-of-band service point ช่วยให้ผู้ดูแลระบบสามารถควบคุมจัดการคอมพิวเตอร์ที่มีชิปเซ็ต Intel vPro และ Intel active management technology (Intel AMT) เช่น ในการ เปิด-ปิด เครื่องคอมพิวเตอร์, ปรับแต่งค่า BIOS, ติดตั้งระบบปฏิบัติการวินโดวส์ผ่านเครือข่ายเน็ตเวิร์ก โดยควบคุมการติดตั้งจากระยะไกลได้, เริ่มต้นเครื่องคอมพิวเตอร์ใหม่ (Restart) กรณีที่ระบบปฏิบัติการวินโดวส์ไม่ตอบสนองการทำงาน

8. Asset Intelligence ทำหน้าที่ต่อไปนี้

1) เป็นคลังที่ใช้เก็บรวบรวมรายการซอฟต์แวร์เครื่องผู้ใช้ทั้งหมดในเครือข่าย โดยเครื่องผู้ใช้จะมี SCCM Agent ทำหน้าที่ส่งข้อมูลซอฟต์แวร์ (เช่น ชื่อของซอฟต์แวร์, ชื่อของผู้

ให้บริการที่พัฒนาซอฟต์แวร์ (Vendor), รุ่นของผลิตภัณฑ์ซอฟต์แวร์ (Versions), ประเภทของซอฟต์แวร์ (Category), และ กลุ่มของซอฟต์แวร์ (Family)) ที่มีในเครื่องผู้ใช้ไปทั่ว Asset intelligence, ผู้ดูแลระบบสามารถจัดการคลังซอฟต์แวร์ได้โดยการเพิ่มประเภทซอฟต์แวร์ (Software categories) และกลุ่มซอฟต์แวร์ (Software families) (เช่น ประเภทของซอฟต์แวร์เป็นบริษัทเกี่ยวกับพลังงาน (Energy companies) กลุ่มซอฟต์แวร์ก็จะเป็น น้ำมัน, แก๊ส, พลังงานน้ำ, หรืออื่น ๆ ) และยังมีป้ายกำกับซอฟต์แวร์ (Software labels) เพื่อให้ผู้ดูแลระบบอธิบายข้อมูลเพิ่มเติมนอกเหนือจากประเภทของซอฟต์แวร์และกลุ่มของซอฟต์แวร์ (เช่น ซอฟต์แวร์ที่เป็นแบบทดลองใช้ (Shareware) หรือ ซอฟต์แวร์ที่ให้ใช้งานได้ฟรี (freeware))

2) เก็บรวบรวมหรือยอมให้ผู้ดูแลระบบระบุข้อมูล Specification ด้านฮาร์ดแวร์ขั้นต่ำที่แต่ละซอฟต์แวร์จำเป็นต้องใช้ (Hardware requirements) เช่น กำหนดความเร็วขั้นต่ำหน่วยประมวลผลกลาง (CPU), กำหนดหน่วยความจำขั้นต่ำ (Memory RAM), กำหนดพื้นที่ว่างขั้นต่ำของฮาร์ดดิสก์ (Hard disk)

3) จัดเตรียมรายงานมากกว่า 60 รายงาน เช่น รายงานซอฟต์แวร์ตามชื่อผลิตภัณฑ์ (Adobe Acrobat reader DC MUI), รายงานชื่อเครื่องที่ติดตั้งซอฟต์แวร์แต่ละชื่อผลิตภัณฑ์ (7Zip, Adobe flash player), รายงานสเปคเครื่อง, รายงานข้อมูลลิขสิทธิ์ซอฟต์แวร์แต่ละเครื่อง

4) ผู้ดูแลระบบสามารถนำเข้าไฟล์รายละเอียดของ License (ซึ่งเป็นรายละเอียดการสั่งซื้อ license ซอฟต์แวร์ของไมโครซอฟต์) มาเก็บใน Asset intelligence เพื่อให้ผู้ดูแลระบบสามารถเรียกดูรายงานจำนวน license ที่มีการสั่งซื้อ และ รายละเอียดที่เกี่ยวข้อง ดังภาพข้างล่างนี้

License 14A - Microsoft Volume Licensing reconciliation report									
Description									
Product Pool	Family Name	Version	Effective Licenses	Unresolved Licenses	Upgrade Licenses	Upgrade with Maintenance Licenses	Inventory Count	Initial Diff	
Applications	Office Professional	Plus 2010	13	0	0	0	74	-61	
Applications	Office Small Business	2007	159	0	0	0	0	159	
Applications	Office Standard	2007	43	0	0	0	0	43	
Applications	Office Standard	XP	1	0	0	0	0	1	
Applications	Office Standard	2010	97	0	0	0	3	94	
Applications	Visio Standard	2007	10	0	0	0	0	10	
Servers	SQL - Device CAL	2008 Release 2	5	0	0	0	0	5	
Servers	SQL Server - Standard	2008 Release 2	1	0	0	0	0	1	
Servers	Windows Server - Device CAL	2003	10	0	0	0	0	10	
Servers	Windows Server - Device CAL	2008	305	0	0	0	0	305	
Servers	Windows Server - Device CAL	2012	5	0	0	0	0	5	
Servers	Windows Server - Standard	2003 Release 2	1	0	0	0	0	1	
Servers	Windows Server - Standard	2008 Release 2	6	0	0	0	0	6	
Servers	Windows Server - Standard	2012	3	0	0	0	0	3	
Systems	Windows	8 Professional Get Genuine	5	0	0	0	0	5	

ภาพที่ 2-3 รายงานจำนวน Microsoft License ที่มีการสั่งซื้อและใช้งานอยู่



9 Reporting Services point ทำหน้าที่จัดทำรายงานต่าง ๆ ที่ผู้ดูแลระบบต้องการเรียกดู โดยจะดึงข้อมูลจากฐานข้อมูลระบบ SCCM เช่น รายงานจำนวนผู้ใช้โปรแกรมประยุกต์ (ไมโครซอฟต์ออฟฟิศ 2013, Java 8.91, Adobe Acrobat Reader), รายงานจำนวนเครื่องผู้ใช้ที่มีการอัปเดตโปรแกรมป้องกันไวรัส Endpoint Protection, รายงานคอมพิวเตอร์เครื่องผู้ใช้ที่มีหน่วยความจำตามสเปคที่ต้องการเรียกดู, รายงานจำนวนเครื่องที่ใช้ระบบปฏิบัติการวินโดวส์ (Windows7, Windows Server 2012)

10. Application Catalog website point เป็นจุดให้บริการหน้าเว็บไซต์แสดงรายชื่อโปรแกรมประยุกต์ ที่ผู้ดูแลระบบอนุญาตให้ผู้ใช้เลือกดาวน์โหลดติดตั้งได้ด้วยตนเองผ่านทางหน้าเว็บไซต์ เช่น ผู้ดูแลระบบอาจกำหนดให้ผู้ใช้เลือกติดตั้งโปรแกรมเหล่านี้เอง Adobe Acrobat Reader, Java 8.91, Microsoft office 2013

11. Application Catalog web service point ทำหน้าที่นำรายชื่อโปรแกรมประยุกต์มาจาก Software library เพื่อตอบคำร้องขอรายชื่อโปรแกรมประยุกต์ของ Application Catalog website point

12. Endpoint protection point ทำหน้าที่เรียกใช้งาน System Center Endpoint Protection ซึ่งเป็นศูนย์กลางในการควบคุมโปรแกรมป้องกันมัลแวร์ (ไวรัส, เวิร์ม, สปายแวร์, โทรจัน, แอดแวร์ และซอฟต์แวร์คุกคามทางคอมพิวเตอร์ประเภทอื่น ๆ) ของบริษัทไมโครซอฟต์ และกำหนดนโยบายความปลอดภัยสำหรับระบบปฏิบัติการไมโครซอฟต์ โดยผู้ดูแลระบบสามารถบริหารจัดการได้ดังนี้

1) เป็นศูนย์กลางสำหรับการติดตั้งและ deploy โปรแกรมป้องกันมัลแวร์ ได้แก่ Windows defender และ Endpoint protection clients

2) กำหนดนโยบายการป้องกันมัลแวร์ที่นำไปใช้กับกลุ่มคอมพิวเตอร์ เช่น กำหนดเวลาเริ่มสแกนหาไวรัสที่เครื่องคอมพิวเตอร์ผู้ใช้, กำหนดเวลาให้โปรแกรมป้องกันมัลแวร์อัปเดต, กำหนดให้โปรแกรมป้องกันมัลแวร์ยกเว้นการสแกนหาไวรัสที่ไฟล์หรือโฟลเดอร์ก็ได้

3) สร้างและปรับตั้งค่า Windows firewall ให้กับเครื่องคอมพิวเตอร์ เช่น เปิด-ปิด Windows Firewall, กำหนดการป้องกันการเชื่อมต่อทั้งหมดกับโปรแกรมที่ไม่ได้อยู่ในรายการของโปรแกรมที่ได้รับอนุญาต

4) ใช้ Configuration manager software updates สำหรับการดาวน์โหลดโปรแกรมป้องกันมัลแวร์เวอร์ชันล่าสุดโดยอัตโนมัติ เพื่อให้โปรแกรมป้องกันมัลแวร์ของคอมพิวเตอร์ผู้ใช้ทันสมัยอยู่ตลอดเวลา

5) ใช้การแจ้งเตือนทางอีเมลเพื่อแจ้งเตือนให้ผู้ดูแลระบบทราบเมื่อคอมพิวเตอร์ถูกคุกคามจากมัลแวร์แล้ว

6) ผู้ดูแลระบบสามารถดูสรุปรายละเอียดข้อมูลการกำหนดค่าและรายงานจากหน้า Configuration manager console ได้ เช่น จำนวนเครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมป้องกันมัลแวร์, จำนวนเครื่องคอมพิวเตอร์ที่มีความเสี่ยงในการถูกคุกคามจากมัลแวร์, 5 อันดับชื่อมัลแวร์ที่โปรแกรมตรวจจับได้มากที่สุด, จำนวนเครื่องคอมพิวเตอร์ที่มีสถานะการอัปเดตโปรแกรมป้องกันมัลแวร์ เช่น เป็นเวอร์ชันล่าสุด, ไม่ได้อัปเดตมา 3 วันแล้ว, อยู่ระหว่าง 3 วันถึง 7 วันแล้ว, และไม่ได้อัปเดตมากกว่า 7 วัน

Primary site ยังมีจุดให้บริการที่ผู้เขียนงานนิพนธ์ไม่ได้นำมาใช้ จึงขอไม่กล่าวถึงรายละเอียดการทำงาน ดังนี้

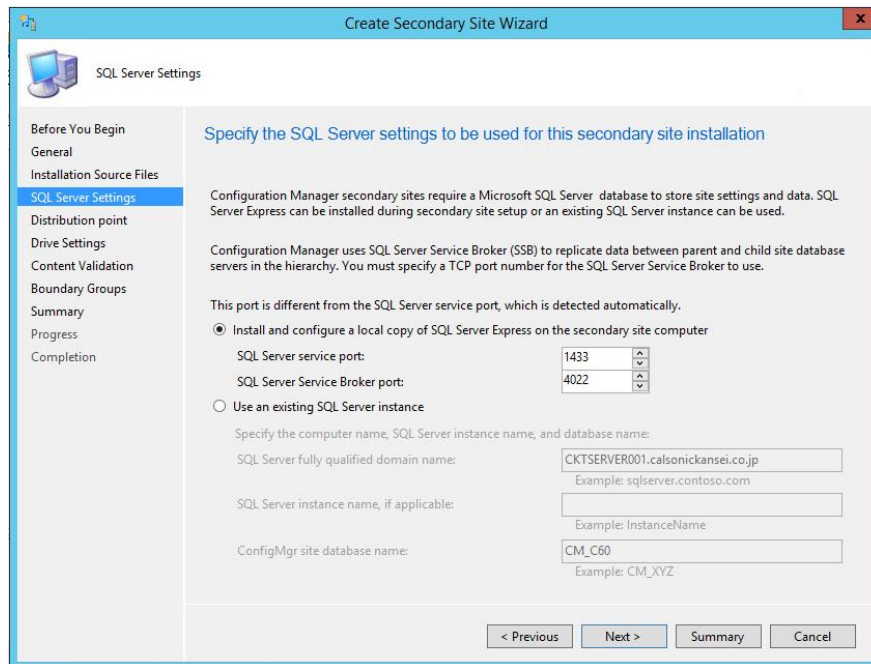
- Certificate registration point
- Enrollment point
- Enrollment proxy point
- Windows Intune connector

#### 2.1.1.3 Secondary site

Secondary site คือ Site ย่อยของ Primary site ที่ให้บริการเครื่องผู้ใช้ในเครือข่ายที่เชื่อมต่อกัน เพื่อช่วยลดเวลาการตอบสนอง (Respond time) และลดปริมาณการรับ-ส่งข้อมูล (Bandwidth) ในกรณีที่ Primary site อยู่ห่างไกล เช่น สาขาหลักตั้งอยู่ที่จังหวัดชลบุรี (Primary site) และสาขาย่อยตั้งอยู่ที่จังหวัดเชียงใหม่ ที่มีเครื่องผู้ใช้จำนวน 500 เครื่อง หากผู้ดูแลระบบ deploy โปรแกรมประยุกต์หรือระบบปฏิบัติการวินโดวส์ที่มีขนาด 750 เมกะไบต์ผ่านเครือข่าย (โดยที่ไม่ติดตั้ง Secondary site ที่สาขาย่อย) เครื่องผู้ใช้ทุกเครื่องจะต้องโหลดไฟล์ขนาด 750 เมกะไบต์จาก Primary site ที่จังหวัดชลบุรี ทำให้ต้องใช้ปริมาณการรับ-ส่งข้อมูล (Bandwidth) มากและใช้เวลาในการดาวน์โหลดนาน ดังนั้นผู้ดูแลระบบควรพิจารณาติดตั้ง Secondary site ที่สาขาจังหวัดเชียงใหม่ เพื่อดาวน์โหลดโปรแกรมประยุกต์หรือระบบปฏิบัติการวินโดวส์มาเก็บไว้ก่อนล่วงหน้า จากนั้นค่อยสั่งให้ Secondary site deploy โปรแกรมประยุกต์หรือระบบปฏิบัติการวินโดวส์ไปยังเครื่องผู้ใช้ในเครือข่ายสาขาจังหวัดเชียงใหม่ ส่งผลให้ความต้องการใช้งานปริมาณการรับ-ส่งข้อมูล (Bandwidth) ระหว่างสาขาหลักกับสาขาย่อยไม่สูงมาก

คุณลักษณะของ Secondary site

- Secondary site จำเป็นต้องมีฐานข้อมูล Microsoft SQL server เพื่อจัดเก็บ การค่า Setting ต่าง ๆ รวมถึงข้อมูลซอฟต์แวร์และฮาร์ดแวร์ของเครื่องผู้ใช้ โดยผู้ดูแลระบบสามารถติดตั้ง SQL Server ก่อนติดตั้ง Secondary site หรือ หากยังไม่มี SQL server ผู้ดูแลระบบก็สามารถติดตั้ง SQL server express ขณะกำลังสร้าง Secondary site ได้ ดังภาพที่ 2-4



ภาพที่ 2-4 การกำหนด SQL server สำหรับ Secondary site

- ระบบฐานข้อมูลที่ Secondary site จะส่งข้อมูลไปให้ Primary site อัตโนมัติ จากนั้น Primary site จะมีข้อมูลบางส่วนเหมือนกันกับข้อมูลที่ Secondary site (Replication)
- Secondary site สามารถรองรับเครื่องผู้ใช้ได้มากที่สุด 5,000 เครื่อง
- เมื่อผู้ดูแลระบบติดตั้ง Secondary site ตัวโปรแกรม Installer จะเปิดใช้งานจุดบริการจัดการเครื่องผู้ใช้ (Management point) และ จุดกระจายโปรแกรมประยุกต์ (Distribution point) ให้อัตโนมัติ

ประเภทของการบริการที่ Secondary site มีเพียง 4 ประเภท (ดังแสดงในตารางที่ 2-2) ดังนี้

1. Distribution point
2. Management point
3. Software update point
4. State migration point

### 2.1.2 สเปคเครื่องเซิร์ฟเวอร์ระบบ SCCM 2012 R2

ไมโครซอฟต์ได้แนะนำฮาร์ดแวร์ในการติดตั้งระบบ SCCM 2012 R2 ควรมีสเปคของเครื่องเซิร์ฟเวอร์ขั้นต่ำ ดังตารางที่ 2-1

ตารางที่ 2-1 สเปคเซิร์ฟเวอร์ขั้นต่ำ SCCM 2012 (Microsoft. (2559, 5 สิงหาคม))

ส่วนประกอบฮาร์ดแวร์	ความต้องการของระบบ SCCM 2012 R2
หน่วยประมวลผลกลาง (CPU)	- ขั้นต่ำ AMD Opteron, AMD Athlon 64, Intel xeon with intel EM64T support, Intel pentium IV with EM64T support
	- ขั้นต่ำ 1.4 GHz
หน่วยความจำหลัก (Memory)	- ขั้นต่ำ 2 GB
พื้นที่ว่างของดิสก์ (Hard disk)	- พื้นที่ว่าง 10 GB
	- เนื้อที่ทั้งหมดประมาณ 50 GB

### 2.1.3 จุดให้บริการในลำดับชั้น SCCM 2012 R2 (Site system role placement in hierarchy)

ตารางที่ 2-2 จุดให้บริการในลำดับชั้น SCCM 2012 (Adam Gordon. (2559, 6 สิงหาคม))

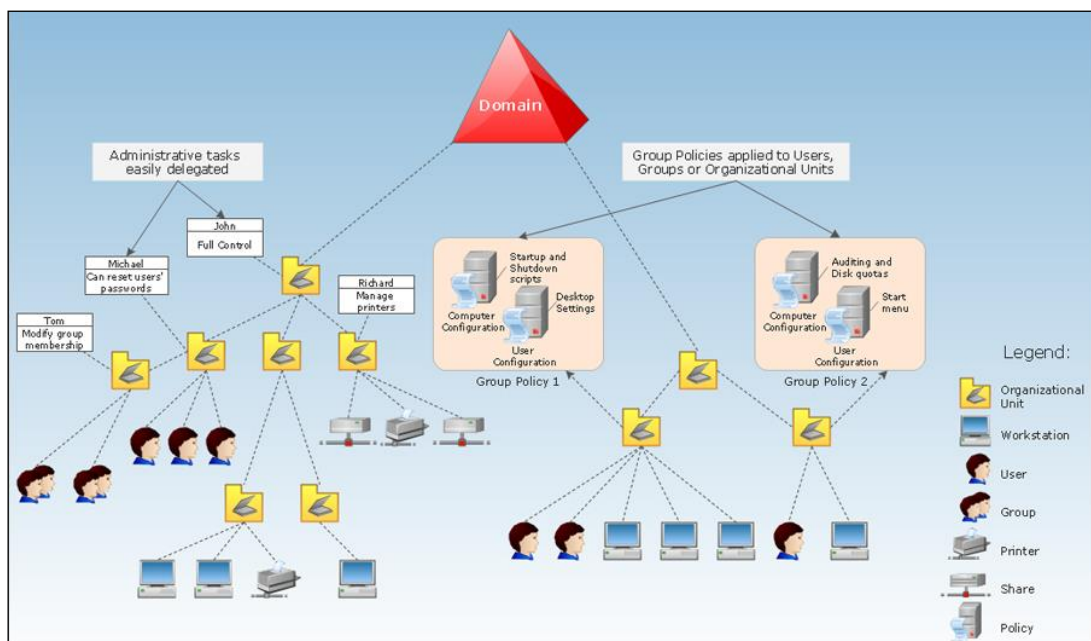
Site System Role	CAS	Child Primary site	Stand-alone primary site	Secondary site
Application catalog web service point	No	Yes	Yes	No
Application catalog website point	No	Yes	Yes	No
Asset Intelligence synchronization point	Yes	No	Yes	No
Certificate registration point	Yes	Yes	Yes	No
Distribution point	No	Yes	Yes	Yes
Fallback status point	No	Yes	Yes	No
Management point	No	Yes	Yes	Yes
Endpoint protection point	Yes	No	Yes	No
Enrollment point	No	Yes	Yes	No
Enrollment proxy point	No	Yes	Yes	No
Out of band service point	No	Yes	Yes	No
Reporting services point	Yes	Yes	Yes	No
Software update point	Yes	Yes	Yes	Yes
State migration point	No	Yes	Yes	Yes
System health validator point	Yes	Yes	Yes	No
Windows intune connector	Yes	No	Yes	No

ตารางที่ 2-2 แสดงให้เห็นว่า Stand-Alone Primary Site สามารถเปิดบริการได้ทุกประเภท โดยหากมีการติดตั้ง Central administration site (CAS) (พร้อมกับ Child Primary Site) Child Primary Site จะไม่สามารถให้บริการได้ 3 ประเภท ดังนี้

1. Asset Intelligence synchronization point
2. Endpoint protection point
3. Windows Intune connector

## 2.2 ระบบ Active directory (AD)

Active directory ช่วยให้ผู้ใช้และระบบจัดการกับบัญชีผู้ใช้, คอมพิวเตอร์, ปริ้นเตอร์ จากจุดศูนย์กลางได้ ผู้ดูแลระบบนิยมนำมาช่วยลดภาระการบริหารจัดการข้อมูลของผู้ใช้ (เช่น ชื่อ-นามสกุล, อีเมล, เบอร์โทรศัพท์) และเป็นประโยชน์ต่อการใช้งานตามนโยบายขององค์กร เช่น ผู้ดูแลระบบสามารถนำไปเป็นเครื่องมือสำหรับกำหนดสิทธิ์การเข้าถึงไฟล์ในเซิร์ฟเวอร์และกำหนดสิทธิ์การใช้งานเครื่องคอมพิวเตอร์ได้



ภาพที่ 2-5 Active directory (CS Odessa. (2559, 17 สิงหาคม))

ภาพที่ 2-5 แสดงให้เห็นถึงไดอะแกรมของ Active directory ซึ่งประกอบด้วยโดเมนอยู่ระดับบนสุด จะมี Organizational unit (OU) ช่วยจัดกลุ่มให้ง่ายต่อการควบคุมและกำหนดสิทธิ์การใช้งาน

ด้านซ้ายของภาพมีการกำหนดสิทธิ์การทำงานดังนี้

- John: มีสิทธิ์ Full control คือ John สามารถกำหนดสิทธิ์ หรือจัดการกับ OU ที่อยู่ภายใต้ ได้ทั้งหมด เช่น สามารถจัดการ OU ภายใต้ได้ (สร้างใหม่, ลบ, แก้ไข), ย้ายบัญชีผู้ใช้ (User), แก้ไขกลุ่ม (Group), เปลี่ยนรหัสผ่านผู้ใช้, บริหารจัดการเครื่องพิมพ์

- Richard: สามารถจัดการเครื่องพิมพ์

- Michael: สามารถเปลี่ยนรหัสผ่านของผู้ใช้

- Tom: สามารถจัดการกลุ่มของผู้ใช้ โดยเพิ่มผู้ใช้เข้าไปในกลุ่ม หรือย้ายออกได้

ด้านขวาของภาพเป็นการจัดการนโยบาย Group policy ดังนี้

- Group policy 1: ผู้ดูแลระบบกำหนดสคริปเพื่อเปิด-ปิดเครื่องคอมพิวเตอร์อัตโนมัติ และกำหนดปรับแต่งหน้าจอ Desktop ของโปรไฟล์ผู้ใช้งาน

- Group policy 2: ผู้ดูแลระบบกำหนดนโยบายให้มีการตรวจสอบโควต้าของฮาร์ดดิสก์ และปรับแต่ง Start Menu ของโปรไฟล์ผู้ใช้งาน

### 2.2.1 Active directory domain services (ADDS)

ADDS คือ ระบบบริหารจัดการ AD ที่ถูกติดตั้งบนและใช้งานบนโดเมนคอนโทรลเลอร์ โดยผู้ดูแลระบบจะบริหาร เข้าถึง จัดการทางด้านเครือข่ายเน็ตเวิร์กได้จากศูนย์กลางทั้งหมด ซึ่ง AD จะเก็บรวบรวมและกำหนดการใช้งานของออบเจกต์ (Objects) ต่าง ๆ ไว้ ยกตัวอย่างฐานข้อมูลประกอบไปด้วยออบเจกต์ต่าง ๆ และไดเรกทอรีเซอร์วิส เช่น Users, Computer, Groups, Share, Printers, Organization Unit (OU) (นพดล สุขศรี บัณฑิต, (2557))

### 2.2.2 ส่วนประกอบของ AD (Active directory components and concepts)

ส่วนประกอบและลักษณะการทำงานของ Active directory มีดังต่อไปนี้

#### 2.2.2.1 โดเมน (Domain)

โดเมน (Domain) คือกลุ่มของ Computer, User, Group, Shared folder, Printer ที่อยู่ในไดเรกทอรีฐานข้อมูลเดียวกัน มีนโยบายความปลอดภัยเดียวกัน และ โดเมนที่มี Trust relationships กับอีกโดเมนหนึ่ง จะสามารถดึงออบเจกต์ต่าง ๆ ของกันและกันไปใช้ได้งานได้

#### 2.2.2.2 Domain controller

Domain controller (DC) คือ เซิร์ฟเวอร์ที่ทำหน้าที่เก็บฐานข้อมูล Active directory ให้บริการและดูแลการให้บริการของ Active directory ด้านการสื่อสารระหว่างผู้ใช้กับ

โดเมน เช่น ขณะที่ผู้ใช้ล็อกออนเข้าสู่ระบบปฏิบัติการวินโดวส์ ผู้ใช้จำเป็นต้องพิสูจน์ตัวตน โดยใช้บัญชีผู้ใช้และรหัสผ่าน ก่อนเข้าถึงคอมพิวเตอร์ที่อยู่ภายใต้โดเมน โดยในแต่ละโดเมนนั้นจะต้องมีเซิร์ฟเวอร์ที่มีหน้าที่เป็น DC อย่างน้อย 1 เครื่อง

#### 2.2.2.3 Root Domain

Root domain คือ โดเมนแรกที่ถูกสร้างขึ้นใน Active directory และไม่มีโดเมนอื่นอยู่ในระดับที่สูงกว่า ตัวอย่าง Root domain เช่น calsonic.com

#### 2.2.2.4 Child domain

Child domain คือ โดเมนย่อยที่ถูกสร้างอยู่ภายใต้ Root domain เป็นการสร้างโดเมนในกรณีที่ต้องการบริหารจัดการแบบรวมศูนย์และแยกขอบเขตการบริหารจัดการ เช่น กำหนดสิทธิ์ให้เครื่องผู้ใช้ไม่สามารถเปิดใช้ Control panel ไว้ที่ Root domain ชื่อ calsonic.com จะส่งผลไปยังโดเมนย่อย th.calsonic.com ด้วยเช่นกัน แต่การปรับแต่งค่านโยบายต่าง ๆ (Policy) ที่โดเมนย่อย th.calsonic.com จะไม่มีผลกระทบต่อโดเมน calsonic.com

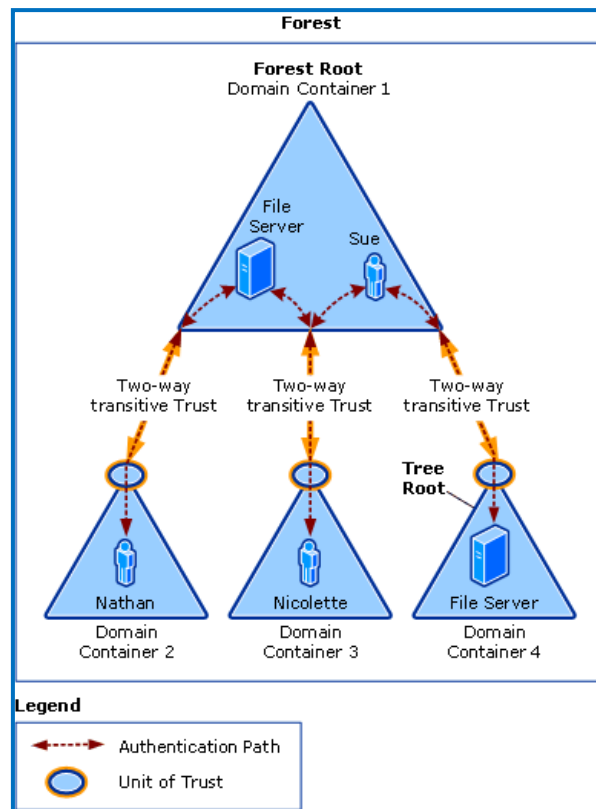
อย่างไรก็ตามผู้ดูแลระบบที่โดเมน calsonic.com จะเป็น Administrator account ในกลุ่ม Enterprise admin groups สามารถเข้ามาปรับเปลี่ยนค่าคอนฟิกต่าง ๆ ที่โดเมนย่อย th.calsonic.com ได้

#### 2.2.2.5 Domain tree (ต้นไม้โดเมน)

Domain tree คือ โครงสร้างโดเมนที่เกิดจากการรวมกันของ Root domain และ Child domain เป็นการจัดเรียงตามลำดับชั้น คล้ายกับระบบชื่อใน DNS

#### 2.2.2.6 Domain forest

Domain forest คือ โครงสร้างของโดเมนที่เกิดจากการรวมกันของต้นไม้โดเมน ตั้งแต่สองต้นไม้โดเมนขึ้นไป โดยแต่ละโดเมนจะมีการเชื่อมโยงกันผ่านทาง Trust relationship แบบสองทาง (2-way trust) ดังภาพที่ 2-6



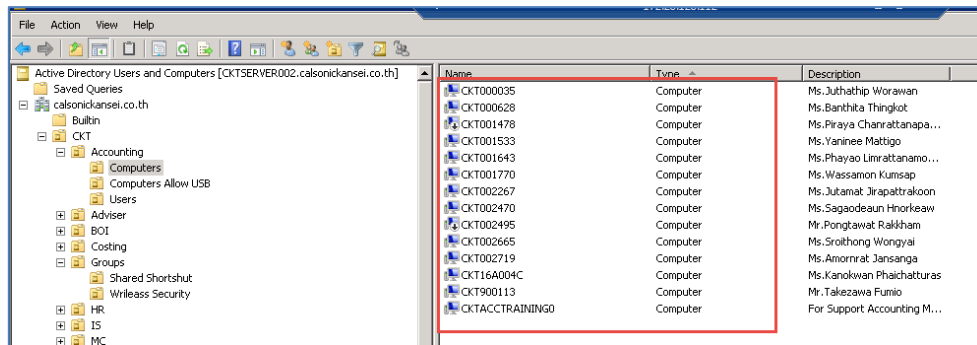
ภาพที่ 2-6 Domain and forest (Microsoft. (2559, 18 สิงหาคม))

### 2.2.2.7 Object

Object เป็นส่วนประกอบต่าง ๆ ที่อยู่ใน Active directory เช่น Organizational unit (OU), Computer, Printer, User, Shared folder, Group ฯลฯ ตัวอย่างการสร้าง Object เช่น เมื่อมีพนักงานเข้ามาใหม่จะมีการสร้างออบเจกต์เพื่อรองรับการใช้งานของพนักงาน เช่น ออบเจกต์ User, Computer ดังภาพที่ 2-7

ชนิด (หรือ Class) ของ Object ที่สามารถเก็บ Object ต่าง ๆ ได้คือ OU และ Container ซึ่งถูกแสดงในส่วน Pane ซ้ายมือของภาพที่ 2-7 ส่วน Object Class อื่น ๆ เช่น Group, Shared folder ไม่สามารถเก็บ Object ใด ๆ ได้ จะถูกแสดงในส่วน Pane ขวามือของภาพที่ 2-7 เท่านั้น จะมาอยู่ซ้ายมือไม่ได้



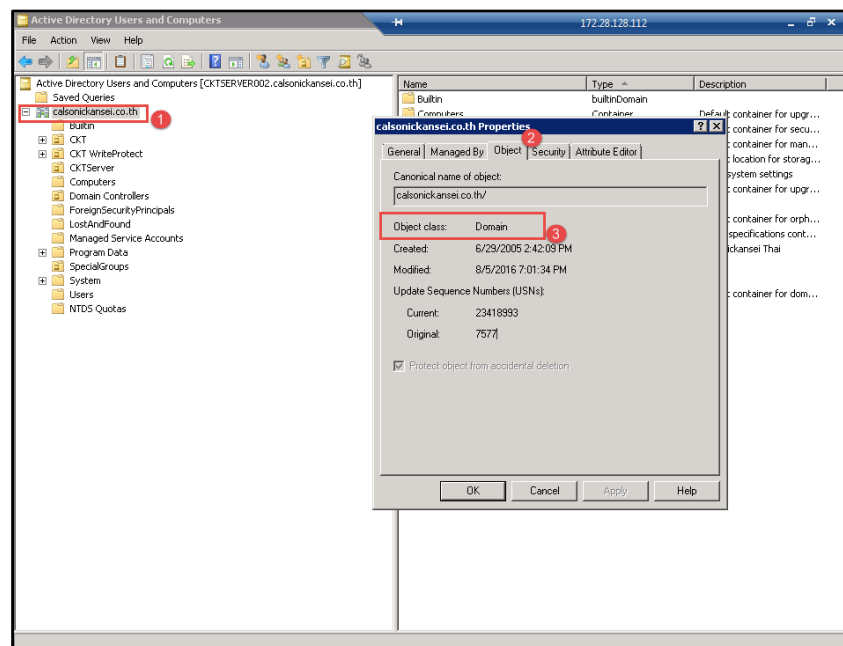


ภาพที่ 2-7 Object Active Directory

ภาพที่ 2-7 แสดง Object computer ใน Active directory ซึ่งผู้ดูแลระบบสร้าง Object computer นี้ขึ้นมาเพื่อเป็นชื่อของเครื่องคอมพิวเตอร์ที่ใช้งานภายใต้โดเมน calsonickansei.co.th และผู้ดูแลระบบได้ใส่ชื่อพนักงานที่ใช้เครื่องคอมพิวเตอร์ไว้ใน Description ด้วย

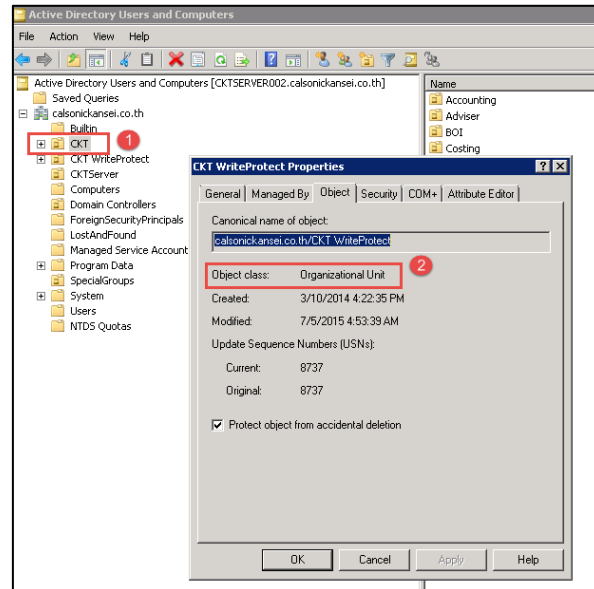
#### 2.2.2.8 Class

Class ทำหน้าที่บอกชนิดของออบเจกต์ ซึ่งมีทั้งหมด 258 ชนิด เช่น Attributes, Containers, Site, Organizational units (OU), User account, Computer account, Group เป็นต้น



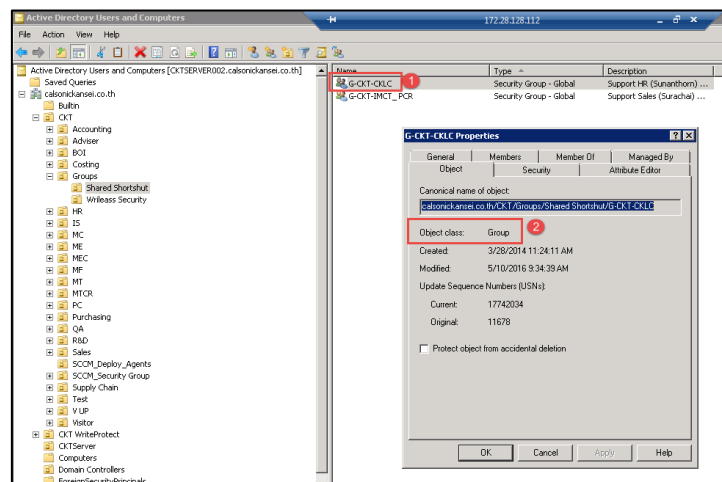
ภาพที่ 2-8 Class โดเมน Calsonickansei.co.th

ภาพที่ 2-8 เมื่อคลิกขวาที่โดเมน calsonickansei.co.th แล้วเลือก Object จะแสดง Object class เป็นค่า Domain ซึ่งหมายความว่าออบเจกต์ calsonickansei.co.th เป็นชนิด Domain



ภาพที่ 2-9 Class organizational unit

ภาพที่ 2-9 เมื่อคลิกขวาที่ Object CKT แล้วเลือก Object จะแสดง Object class เป็นค่า Organizational unit ซึ่งหมายความว่าออบเจกต์ CKT เป็นชนิด Organizational unit (OU)



ภาพที่ 2-10 Class Group

ภาพที่ 2-10 เมื่อคลิกขวาที่ G-KT-CKLC แล้วเลือก Object จะแสดง Object class เป็นค่า Group ซึ่งหมายความว่าออบเจกต์ G-KT-CKLC เป็นชนิด Group

#### 2.2.2.9 Attributes

Attributes คือ คุณลักษณะของแต่ละออบเจกต์ เช่น User object จะมี Attributes ช่วยบอกข้อมูลของ User account ที่เป็น First name, Initials, Last name, Full name, และ User logon name ดังภาพที่ 2-11

The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: HMG.M.COM/HMG.M\_User/HOME'. Below this, there are several input fields:
 

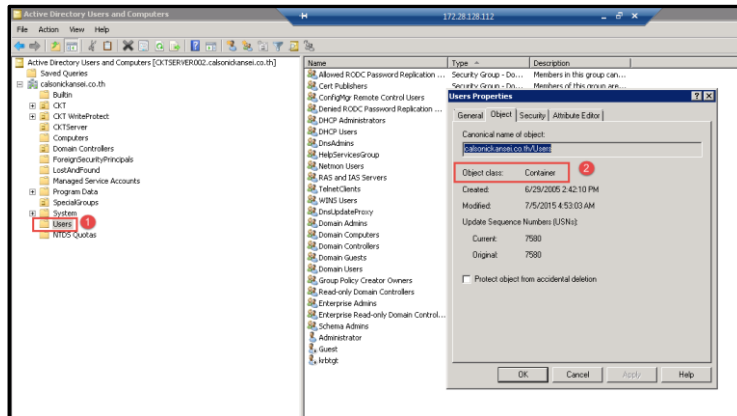
- 'First name:' with the value 'weerapun' and an empty 'Initials:' field.
- 'Last name:' with the value 'dounjit'.
- 'Full name:' with the value 'weerapun dounjit', which is highlighted with a red rectangular box.
- 'User logon name:' with the value 'weerapun' and a dropdown menu showing '@HMG.M.COM'.
- 'User logon name (pre-Windows 2000):' with the value 'HMG\M\weerapun'.

ภาพที่ 2-11 Attributes ของบัญชีผู้ใช้

ภาพที่ 2-11 ผู้ดูแลระบบสร้างบัญชีผู้ใช้โดยกำหนดค่า Attributes Value ที่เป็น Full name คือ weerapun dounjit (ดังแสดงในกรอบสีแดง)

#### 2.2.2.10 Container

Container ทำหน้าที่คล้ายกับโฟลเดอร์ เมื่อติดตั้ง Active directory จะสร้าง Container มาเพื่อเก็บออบเจกต์ต่าง ๆ ของระบบ Active directory ไว้ และผู้ดูแลระบบสามารถสร้าง Container ขึ้นเองได้ด้วย ดังภาพที่ 2-12

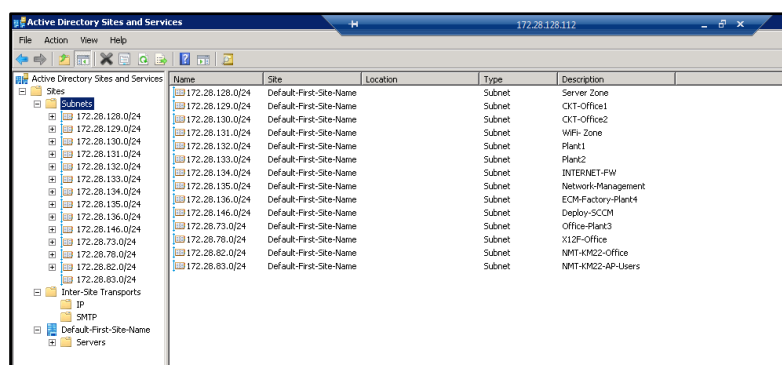


ภาพที่ 2-12 Container ภายใต้โดเมน calsonickansei.co.th

ภาพที่ 2-12 แสดง Container ชื่อ User ในระบบ Active directory โดยเมื่อคลิกขวาที่ Container (ในกรอบสีแดงที่ 1) แล้วเลือก Properties จะสามารถตรวจสอบค่า Object class (ซึ่งก็คือ Container) ได้

2.2.2.11 Site

ไซต์ (Site) คือ การรวบรวมคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่อเข้าหากันในลักษณะที่แน่นนอน (Well-connected) ทั้งหมดไว้ การเพิ่ม Subnets ใน Site ให้ครบถ้วนจะช่วยลดความล่าช้าเมื่อเครื่อง Subnet ต้องการส่งข้อมูลใน Domain ไซต์อาจมีหลาย ๆ Subnets ที่มีการใช้งานร่วมกันและเชื่อมต่อเข้าหากันบนขอบเขตพื้นที่เครือข่ายเน็ตเวิร์กที่เป็น LAN (Local Area Network) โดยไม่ทราบสถานที่ตั้งจริงทางกายภาพ (Physical Locations) ของเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการใช้งานร่วมกันอยู่

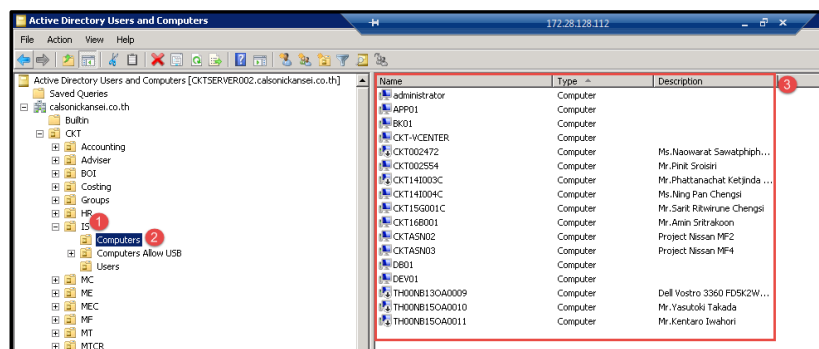


ภาพที่ 2-13 Site โดเมนบริษัทคาลโซนิค คันเซ ประเทศไทย จำกัด

ภาพที่ 2-13 แสดง 14 Subnets ใน Site ชื่อ Default-First-Site-Name ของบริษัทคาลโซนิคคันเซ ประเทศไทย โดยแยกตามสถานที่ของโรงงาน

### 2.2.2.12 Organizational units (OU)

Organizational units (OU) เป็นที่ที่ใช้สำหรับสร้างและจัดเก็บออบเจกต์ที่เป็น Users, Groups, Computers, Organizational Units อื่น ๆ และสามารถใช้ Group Policy ในการกำหนดนโยบายไปยังออบเจกต์ต่าง ๆ จาก OU ระดับบนสุดไปยังระดับล่างสุดได้



ภาพที่ 2-14 OU Computers ของแผนกไอที

ภาพที่ 2-14 แสดง OU ชื่อ IS โดยจะมี OU Computers ที่เก็บออบเจกต์คอมพิวเตอร์ภายใน ดังกรอบสีแดงที่ 3 ขวามือ

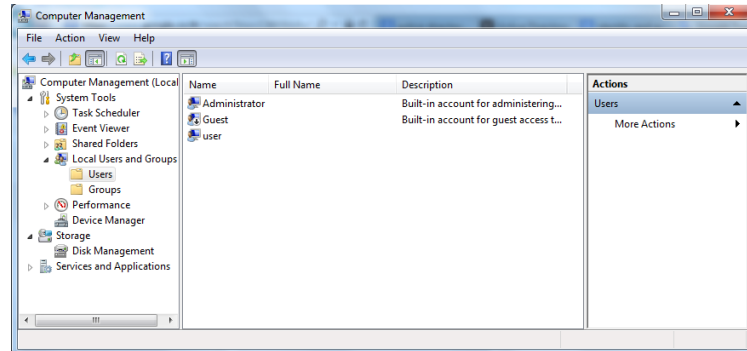
### 2.2.2.13 User account

User account เป็นออบเจกต์ของผู้ใช้ ที่เก็บข้อมูลของผู้ใช้ เช่น user name, password, Full name, Email โดยมี 2 ประเภท ได้แก่ Domain user account และ Local user account

Domain user account เป็น User account ที่ใช้งานได้ภายใต้เครื่องเซิร์ฟเวอร์และคอมพิวเตอร์ที่เข้าร่วมโดเมนนั้น ๆ ทั้งนี้ขึ้นอยู่กับสิทธิ์การใช้งาน โดยจะใช้เครื่องมือ Active directory ในการบริหารจัดการและจัดเก็บบัญชีผู้ใช้ ในฐานข้อมูลของโดเมนในไฟล์ชื่อ NTDS.DIT ซึ่งไฟล์นี้จะเก็บโนโดเมนคอนโทรลเลอร์ทุกตัวของโดเมน

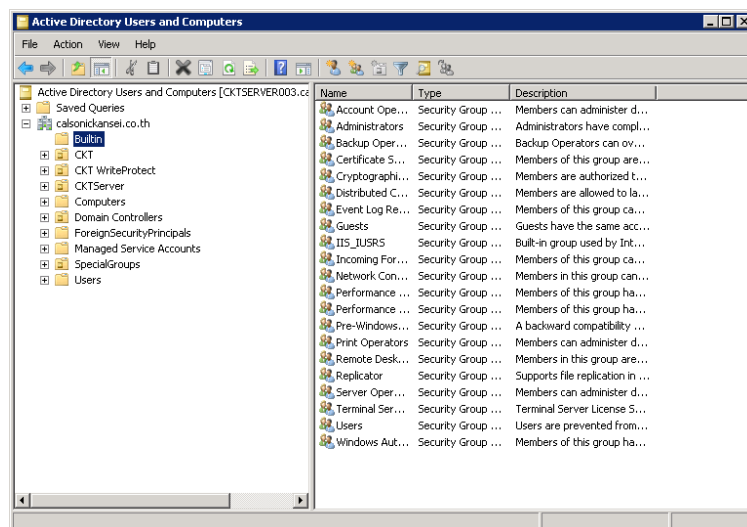
Local user account เป็น User account ในของเครื่องเซิร์ฟเวอร์และคอมพิวเตอร์เฉพาะเครื่องนั้น โดยจะเก็บบัญชีผู้ใช้ ในฐานข้อมูลของระบบปฏิบัติการวินโดวส์ในไฟล์ชื่อ SAM (Security account manager) และไฟล์นี้จะถูกจัดเก็บที่  
%System\root%\Windows\System30\config\

การจัดการ User account นั้น ถ้าเป็น Domain user account จะใช้เครื่องมือที่ชื่อ Active directory users and computers แต่ถ้าเป็น Local user account จะใช้เครื่องมือที่ชื่อ Computers management



ภาพที่ 2-15 เครื่องมือช่วย Computer management tool

ภาพที่ 2-15 แสดงเครื่องมือ Computer management เป็นเครื่องมือที่สามารถจัดการบัญชีผู้ใช้ที่เป็น Local user account ได้



ภาพที่ 2-16 Active directory user and computer

ภาพที่ 2-16 แสดงเครื่องมือ Active directory user and computer ที่มีมาให้พร้อมกับการติดตั้งโดเมนเซิร์ฟเวอร์ และเป็นเครื่องมือที่สามารถจัดการบัญชีผู้ใช้ที่เป็น Domain user account ได้

#### 2.2.2.14 Computer account

Computer account คือ ออบเจกต์ที่เก็บข้อมูลต่าง ๆ ของเครื่องคอมพิวเตอร์ที่เป็นสมาชิกของโดเมน โดยหลังจากเพิ่มเครื่องคอมพิวเตอร์เข้าเป็นสมาชิกของโดเมนแล้ว คอมพิวเตอร์แต่ละเครื่องจะได้รับบัญชีเครื่อง เพื่อใช้ระบุตัวตนของเครื่องนั้น ๆ โดยที่บัญชีที่ได้นั้นจะเป็นชื่อเดียวกันกับชื่อเครื่อง และต้องไม่ซ้ำกับเครื่องอื่น โดย Computer account จะถูกเก็บและจัดการโดย Active directory แบบเดียวกันกับ User account คุณสมบัติต่าง ๆ ของ Computer accounts จะถูกจัดการได้เหมือนกับคุณสมบัติของ User account คือ สามารถเพิ่ม ปิด แก้ว และ ลบได้ โดยใช้เครื่องมือ Active directory users and computers

#### 2.2.2.15 Group

Group คือ ออบเจกต์ที่สามารถมีสมาชิกเป็นผู้ใช้และคอมพิวเตอร์ หรือกลุ่มอื่น ๆ โดย Group ช่วยให้ผู้ใช้และระบบสามารถกำหนดสิทธิ์ และ ส่งอีเมลให้ผู้ใช้ได้ทั้งกลุ่ม Group มี 2 ชนิด ดังนี้

1. Distribution กลุ่มชนิด Distribution เป็น กลุ่มที่ใช้งานอีเมลได้เท่านั้น
2. Security กลุ่มชนิด Security เป็น กลุ่มที่ใช้สำหรับการกำหนดสิทธิ์การกระทำต่าง ๆ ให้กับกลุ่ม และใช้สำหรับการกำหนดอนุญาตใช้งานของบัญชีผู้ใช้หรือคอมพิวเตอร์

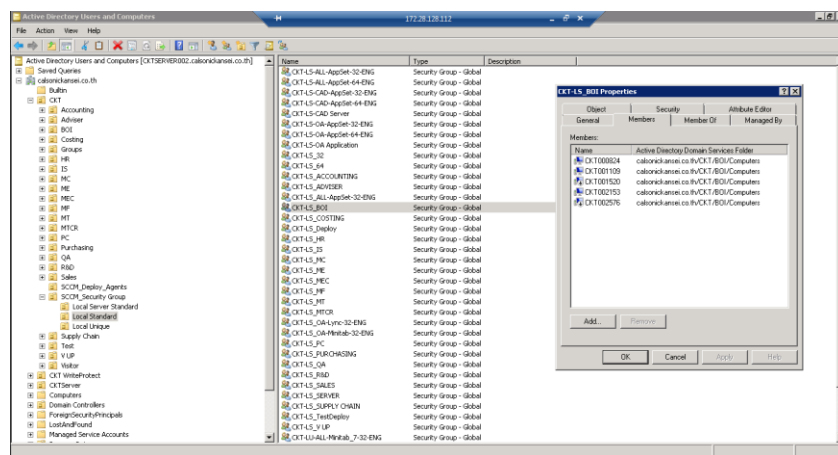
#### 2.1 กลุ่มรูปแบบ Security ที่ไม่โครซอฟท์เตรียมมาให้ในระบบ Active directory

Name	Type	Description
Administrators	Security Group - Domain Local	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Security Group - Domain Local	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Certificate Service DCOM Access	Security Group - Domain Local	Members of this group are allowed to connect to Certification Authorities in the enterprise
Cryptographic Operators	Security Group - Domain Local	Members are authorized to perform cryptographic operations
Distributed COM Users	Security Group - Domain Local	Members are allowed to launch, activate and use Distributed COM objects on the machine
Event Log Readers	Security Group - Domain Local	Members of this group can read event logs from local machine
Guests	Security Group - Domain Local	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
ITIL_SITES	Security Group - Domain Local	Built-in group used by Internal Information Services
Incoming Forest Trust Builders	Security Group - Domain Local	Members of this group can create incoming, one-way trusts to this forest
Network Configuration Operators	Security Group - Domain Local	Members in this group can have some administrative privileges to manage configuration of networking features
Performance Log Users	Security Group - Domain Local	Members of this group have remote access to schedule logging of performance counters on the computer
Performance Monitor Users	Security Group - Domain Local	Members of this group have remote access to monitor the computer
Pre-Windows 2000 Compatible Access	Security Group - Domain Local	A backward compatibility group which allows read access on all users and groups in the domain
Print Operators	Security Group - Domain Local	Members can substitute domain printers
Remote Desktop Users	Security Group - Domain Local	Members in this group are granted the right to login remotely
Replicator	Security Group - Domain Local	Supports file replication in a domain
Server Operators	Security Group - Domain Local	Members can administer domain servers
Terminal Server License Servers	Security Group - Domain Local	Terminal Server License Servers
Users	Security Group - Domain Local	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications
Windows Authentication Access Group	Security Group - Domain Local	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects

ภาพที่ 2-17 Group ที่ชื่อ Remote Desktop Users เป็น Group ชนิด Security

ภาพที่ 2-17 แสดงกลุ่มรูปแบบชนิด Security ชื่อ Remote desktop users ที่มากับระบบ Active directory โดยผู้ใช้ที่เป็นสมาชิกในกลุ่มนี้จะสามารถใช้เครื่องมือ Remote desktop ของระบบปฏิบัติการวินโดวส์ได้

## 2.2 กลุ่มรูปแบบชนิด Security ที่ผู้ดูแลระบบสร้างขึ้น



ภาพที่ 2-18 กลุ่มรูปแบบชนิด Security ที่ผู้ดูแลระบบสร้างขึ้น

ภาพที่ 2-18 แสดงกลุ่มรูปแบบชนิด Security ที่ผู้ดูแลระบบสร้างขึ้น ชื่อ CKT-LS\_BOI เป็นกลุ่มเครื่องคอมพิวเตอร์แผนกส่งเสริมการลงทุน (BOI)

### 2.2.2.16 Group scope

Group Server scope คือ ขอบเขตของกลุ่ม ซึ่งมีอยู่ 3 แบบ ด้วยกันคือ Universal group, Global group และ Domain local group ดังตารางที่ 2-3

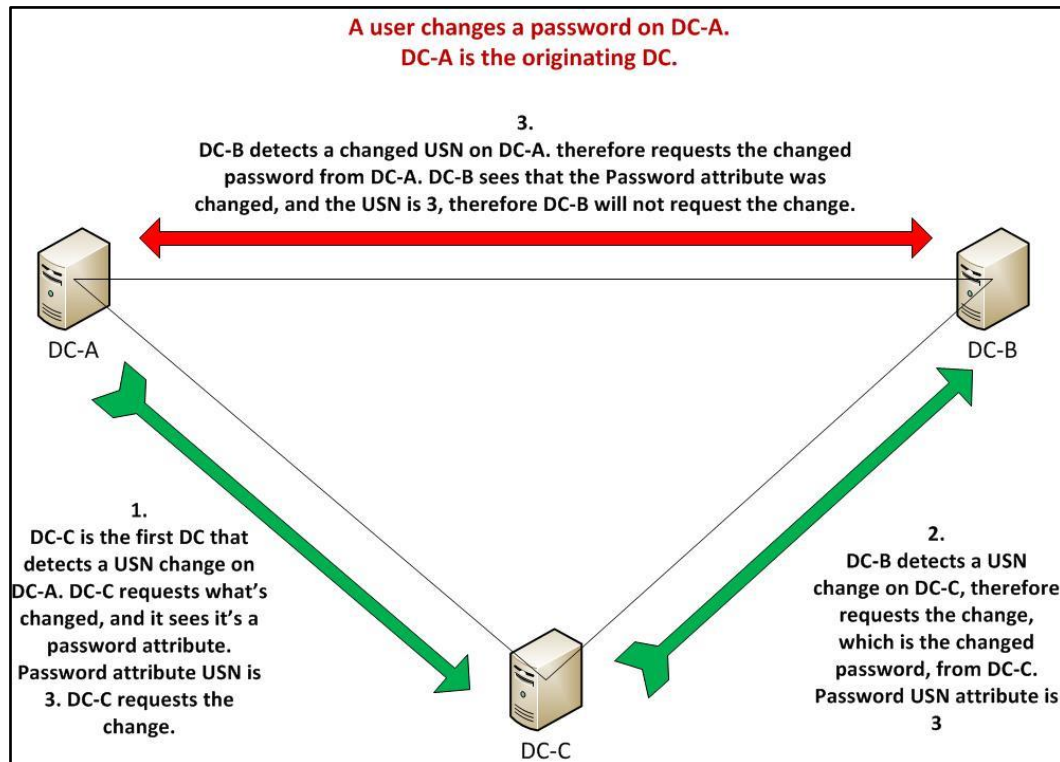


ตารางที่ 2-3 Group Scope (Microsoft. (2559, 20 สิงหาคม))

Scope	Possible Members	Scope Conversion	Can Grant Permissions	Possible Member of
Universal	<p>Accounts from any domain in the same forest</p> <p>Global Groups from any domain in the same forest</p> <p>Other Universal groups from any domain in the same forest</p>	<p>Can be converted to Domain Local scope</p> <p>Can be converted to Global scope if the group does not contain any other Universal group</p>	<p>On any domain in the same forest or trusting forests</p>	<p>Other Universal groups in the same forest</p> <p>Domain Local groups in the same forest or trusting forests</p> <p>Local groups on computers in the same forest or trusting forests</p>
Global	<p>Accounts from the same domain</p> <p>Other global group from the same domain</p>	<p>Can be converted to Universal scope if the group is not a member of any other global group</p>	<p>On any domain in the same forest, or trusting domains or forests</p>	<p>Universal groups from any domain in the same forest</p> <p>Other Global groups from the same domain</p> <p>Domain Local groups from any domain in the same forest, or from any trusting domain</p>
Domain Local	<p>Accounts from any domain or any trusted domain</p> <p>Global groups from any domain or any trusted domain</p> <p>Universal groups from any domain in the same forest</p> <p>Other Domain Local groups from the same domain</p> <p>Accounts, Global groups, and Universal groups from other forests and from external domains</p>	<p>Can be converted to Universal scope if the group does not contain any other Domain Local group</p>	<p>Within the same domain</p>	<p>Other Domain Local groups from the same domain</p> <p>Local groups on computers in the same domain, excluding built-in groups that have well-known SIDs</p>

### 2.2.2.17 การรีพลิเคต (Replication)

การรีพลิเคต (Replication) คือการปรับปรุงข้อมูลระหว่างโดเมนคอนโทรลเลอร์ให้เหมือนกัน ในกรณีที่มีโดเมนคอนโทรลเลอร์ตั้งแต่ 2 ตัวขึ้นไป ดังภาพที่ 2-19



ภาพที่ 2-19 การ Replicate โดเมนคอนโทรลเลอร์ (Ace Fekay. (2559, 20 สิงหาคม))

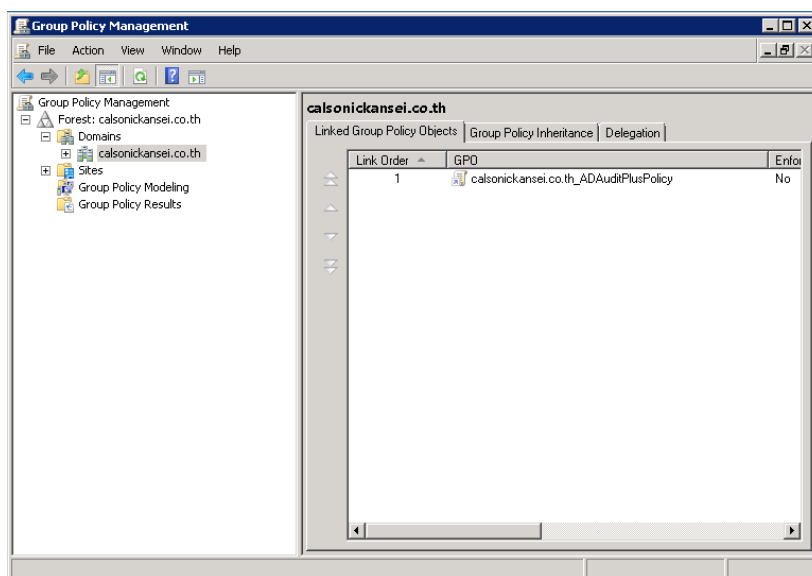
ภาพที่ 2-19 ผู้ใช้ A มีการเปลี่ยนแปลงรหัสผ่านที่โดเมนคอนโทรลเลอร์ DC-A หลังจากนั้นถึงช่วงเวลาโดเมนคอนโทรลเลอร์มีการปรับปรุงข้อมูลให้เหมือนกัน (Replicate) ก็จะมีการปรับปรุงฐานข้อมูลรหัสผ่านใหม่ของผู้ใช้ A ในโดเมนคอนโทรลเลอร์ DC-C และ DC-B ด้วย

## 2.3 การกำหนดนโยบายหรือข้อบังคับต่าง ๆ (Group policy)

Group policy คือ นโยบายหรือข้อบังคับต่าง ๆ ที่ผู้ดูแลระบบต้องการให้ผู้ใช้งานเฉพาะกลุ่มปฏิบัติตาม เช่น กำหนดการควบคุมการใช้งาน Control panel กำหนดนโยบายควบคุมการใช้งานเบราว์เซอร์ (Internet Explorer) กำหนดภาษาบทคำสั่ง (Scripting) กำหนดความมั่นคงปลอดภัย (Security) และอื่น ๆ

### 2.3.1 การสร้าง Group Policy

Group policy management console (GPMC) เป็นเครื่องมือที่มีความสามารถช่วยให้การจัดการและกำหนดนโยบายได้อย่างสะดวก รวดเร็วและมีประสิทธิภาพมากขึ้น นอกจากนี้ยังมีคุณลักษณะพิเศษ (Features) ในส่วนของการจัดการ เช่น การสำรองข้อมูลนโยบาย/การกู้คืนนโยบาย, การทำรายงานเกี่ยวกับนโยบาย และอื่น ๆ ดังภาพที่ 2-20



ภาพที่ 2-20 Group policy management

GPMC สามารถใช้ในการจัดการทุกอย่างที่เกี่ยวข้องกับกำหนดนโยบาย (Policy) เมื่อสร้างนโยบายจะมีออบเจกต์ตัวหนึ่งถูกสร้างขึ้นมาด้วย เรียกว่า “Group Policy Object” หรือเรียกสั้น ๆ ว่า GPO ซึ่งใช้เก็บค่าการกำหนดสิ่งต่าง ๆ ของแต่ละกลุ่มผู้ใช้ โดยค่าดังกล่าวมี 2 ส่วนใหญ่ ๆ คือ

- Computer Configuration กำหนดค่าให้กับเครื่องคอมพิวเตอร์ เช่น กำหนดให้มีการเชื่อมต่อกับเครื่องพิมพ์, กำหนดตั้งค่า Control panel

- User Configuration กำหนดค่าให้กับบัญชีผู้ใช้งานคอมพิวเตอร์ เช่น การกำหนดค่า Profile ของแต่ละบัญชีผู้ใช้งาน, กำหนดค่า Start menu และ Task bar, กำหนดค่าเริ่มต้นโปรแกรมประยุกต์ต่าง ๆ

## 2.4 การยืนยันตัวตน Authentication

Authentication คือ การยืนยันตัวตนของผู้ที่มาใช้งานระบบต่าง ๆ บนเครือข่ายหรือเซิร์ฟเวอร์ โดยระบบจะทำการตรวจสอบจากชื่อผู้ใช้และรหัสผ่าน ซึ่งได้กำหนดค่าไว้ที่ Active Directory ว่าถูกต้องตามที่มีในระบบหรือไม่ จุดประสงค์หลักของการ Authentication คือพิสูจน์ตัวบุคคล ว่าคน ๆ นั้นที่เข้าใช้งานระบบคือใคร? พร้อมทั้งตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบนั้นมีสิทธิ์ทำอะไรบ้าง เช่น การกำหนดสิทธิ์ในการใช้งานอินเทอร์เน็ต

การทำ Authentication นั้นส่วนใหญ่จะต้องใช้รหัสที่เป็นที่รู้จักกันแคระหว่างผู้ให้บริการกับผู้ให้บริการ หรือที่เรียกกันว่ารหัสผ่าน (password) สำหรับระบบที่ต้องการความปลอดภัยสูงกว่านั้น จะมีการใช้สิ่งที่เรียกว่า 2-factor authentication หรือการยืนยันตัวโดยใช้วัตถุสองชนิด ที่เราพบกันบ่อย ๆ ก็คือ OTP (One Time Password) ที่ส่งมาทาง SMS หรือ E-Mail ส่วนระบบที่ต้องการความปลอดภัยมากกว่า OTP จะใช้ Authentication Token ซึ่งเป็นอุปกรณ์ขนาดเล็กที่ทำหน้าที่สร้างรหัสผ่านชุดที่สองและจะเปลี่ยนไปเรื่อย ๆ ตามเวลาที่กำหนด



ภาพที่ 2-21 อุปกรณ์ Token

## 2.5 การควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Control)

ความปลอดภัยของระบบสารสนเทศจะช่วยให้ระบบมีความมั่นคงปลอดภัย ช่วยป้องกันไม่ให้บุคคลภายนอกเข้าสู่ระบบสารสนเทศโดยไม่ได้รับอนุญาต ช่วยควบคุมความปลอดภัยรวมถึงปัญหาอาชญากรรมคอมพิวเตอร์และประเด็นด้านจริยธรรม เมื่อระบบคอมพิวเตอร์เกิดปัญหาไม่สามารถทำงานได้ตามปกติ โดยไม่ว่าจากสาเหตุใดก็ตาม ย่อมกระทบต่อการดำเนินงานขององค์กร โดยเฉพาะองค์กรที่ใช้ระบบคอมพิวเตอร์และระบบสื่อสารต่าง ๆ ในการขับเคลื่อนธุรกิจ เช่น ไวรัสคอมพิวเตอร์ทางอินเทอร์เน็ต ที่เข้ามาทำลายข้อมูล หรือปรับเปลี่ยนแก้ไขไฟล์เอกสารให้ผิดแปลกไปจากเดิม โดยในปัจจุบันก็มีผลกระทบไวรัสชื่อ cryptolocker เป็นมัลแวร์ประเภท "Ransomware" โดยมีกระบวนการเข้ารหัส "ล็อก" ไฟล์เอกสาร ทำให้ไม่สามารถเข้าใช้ไฟล์ได้ จากนั้นจะทิ้งข้อความ

จำนวนเงินพร้อมกับอีเมลเพื่อให้ติดต่อกลับและเรียกค่าไถ่ในการปลดล็อคไฟล์ ซึ่งก่อให้เกิดความเสียหายและการให้บริการต่าง ๆ ขององค์กร

### 2.5.1 ปัญหาที่ทำให้ระบบสารสนเทศล้มเหลว พิจารณาได้ดังนี้

2.5.1.1 ปัญหาที่เกิดจากการกระทำของคน จำแนกได้เป็น อาชญากรรมคอมพิวเตอร์ และปัญหาด้านจริยธรรม ปัจจุบันอาชญากรรมคอมพิวเตอร์ได้แพร่ระบาดไปทั่วโลกจากการที่มีผู้ใช้ อินเทอร์เน็ต อย่างแพร่หลาย และยากแก่การปราบปราม อาชญากรรมคอมพิวเตอร์ที่แอบบุกรุก เจาะ เข้าระบบโดยไม่ถูกกฎหมายเรียกว่า แฮ็คเกอร์ (hacker) หรือแครกเกอร์ (cracker)

- อาชญากรรมคอมพิวเตอร์ แบ่งได้ดังนี้

1) การจารกรรมและขโมยข้อมูล เช่น ความลับทางการค้า ซอฟต์แวร์ ข้อมูลการพัฒนาผลิตภัณฑ์ ข้อมูลหมายเลขบัตรเครดิต ข้อมูลรหัสผ่าน ข้อมูลเงินเดือน ข้อมูลส่วนตัว เป็นต้น

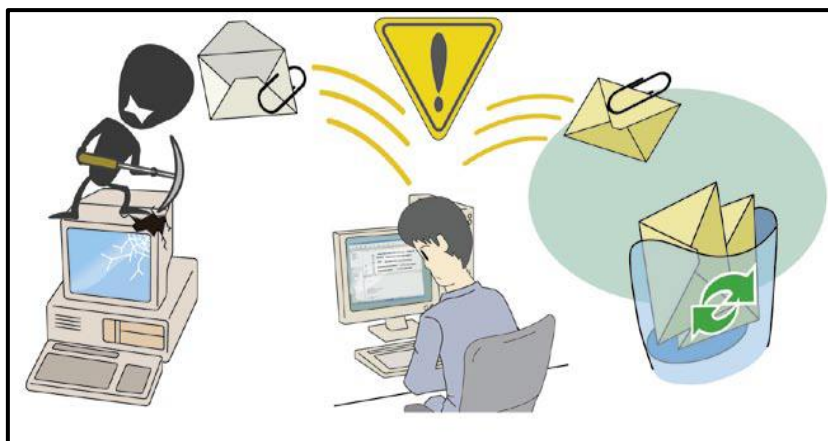
2) การเปลี่ยนแปลงและทำลายข้อมูล เช่น ระบบตัดเศษเงินในธนาคารเพื่อโอนเข้าบัญชีเงินฝากของตน การแพร่ไวรัสหรือหนอนคอมพิวเตอร์ในระบบสารสนเทศเพื่อรบกวนหรือทำลายการทำงานของระบบ ภัยเหล่านี้อาจก่อให้เกิดความเสียหายต่อระบบเครือข่ายและระบบสารสนเทศได้

- ตัวอย่างเครื่องหรือโปรแกรมประยุกต์เพื่อการทำอาชญากรรม มีดังนี้

1. ไวรัสมัลแวร์ (computer virus) เป็นโปรแกรมที่ทำงานร่วมกับโปรแกรมอื่น โดยการแพร่กระจายไปสู่เครื่องอื่นในระบบเครือข่ายได้อย่างรวดเร็ว ไวรัสมัลแวร์หลายประเภท เช่น ทำงานเหมือนระเบิดเวลา หรือวันที่กำหนดได้ (time bomb) การเปลี่ยนแปลงข้อมูลไฟล์หรือโปรแกรมระบบ การทำลายข้อมูล เป็นต้น

2. เวิร์มหรือหนอนคอมพิวเตอร์ (computer worm) เป็นโปรแกรมอิสระที่สามารถจำลองโปรแกรมตัวเองได้ มีลักษณะเป็นหน่วยย่อย ๆ ของไวรัสมัลแวร์ แต่เวิร์มไม่ต้องอาศัยผู้ใช้งานแต่อาศัยไฟล์ หรือคุณสมบัติในการส่งต่อข้อมูลในคอมพิวเตอร์เพื่อกระจายตัวเอง ทำให้เกิดโปรแกรมจำนวนมาก ทำงานในระบบคอมพิวเตอร์ จึงทำให้เครื่องช้า เพราะเครือข่ายเต็มไปด้วยโปรแกรมเหล่านี้

3. สแปมคอมพิวเตอร์หรือสแปมเมล (computer spam) เป็นโปรแกรมที่ส่งข้อมูลหรือภาพในรูปแบบของไปรษณีย์อิเล็กทรอนิกส์จำนวนมากไปยังบุคคลทั่วไป เปรียบได้กับไปรษณีย์ขยะ ซึ่งเป็นการสิ้นเปลืองเวลาของบุคคลากรทั้งในระดับองค์กร ประเทศ หรือนานาชาติ ในการจัดการไปรษณีย์อิเล็กทรอนิกส์โดยไม่จำเป็น ผู้รับบางรายไม่สามารถรับไปรษณีย์ของตนได้ เพราะตู้ไปรษณีย์อิเล็กทรอนิกส์ของตนเต็มไปด้วยเมลที่เป็นสแปม ดังภาพที่ 2-22



ภาพที่ 2-22 สแปมเมล (Spam mail)

ภาพที่ 2-22 แสดงเครื่องผู้ใช้ไม่สามารถรับเมลได้เพราะบัญชีเมลผู้ใช้ได้รับเมลจากระบบสแปมเมลจำนวนมากจึงทำให้เมลเต็ม และไม่สามารถใช้งานได้

### 2.5.2 ช่องโหว่ของโปรแกรม (Vulnerabilities)

การใช้โปรแกรมในการทำงานเชิงธุรกิจขององค์กรนั้นต้องคำนึงถึงช่องโหว่ของโปรแกรมที่เราใช้งานในองค์กรด้วย เนื่องจากผู้ไม่ประสงค์ดีจะหาช่องทางเจาะระบบเข้ามาเอาข้อมูลที่สำคัญได้ เช่น ผู้ใช้มีการใช้โปรแกรมประยุกต์ในการทำงานอินเทอร์เน็ต โดยใช้อินเทอร์เน็ต เบราเซอร์ (IE) ในการทำงานและมีโปรแกรมเสริม Adobe flash player ในการเล่นไฟล์วีดีโอ รูปภาพ ซึ่งมีช่องโหว่ของตัวโปรแกรมเอง โดยบริษัท Adobe ประกาศแจ้งเตือนผู้ใช้ผ่านทางเว็บไซต์ของบริษัท ดังรายละเอียดในภาพที่ 2-23

Adobe Security Bulletin

---

**Security updates available for Adobe Flash Player**

**Release date:** May 12, 2015

**Last updated:** July 3, 2015

**Vulnerability identifier:** APSB15-09

**Priority:** See table below

**CVE number:** CVE-2015-3044, CVE-2015-3077, CVE-2015-3078, CVE-2015-3079, CVE-2015-3080, CVE-2015-3081, CVE-2015-3082, CVE-2015-3083, CVE-2015-3084, CVE-2015-3085, CVE-2015-3086, CVE-2015-3087, CVE-2015-3088, CVE-2015-3089, CVE-2015-3090, CVE-2015-3091, CVE-2015-3092, CVE-2015-3093

**Platform:** All Platforms

**Summary**

Adobe has released security updates for Adobe Flash Player for Windows, Macintosh and Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system. Adobe recommends users update their product installations to the latest versions:

- Users of the Adobe Flash Player desktop runtime for Windows and Macintosh should update to Adobe Flash Player 17.0.0.188.
- Users of the Adobe Flash Player Extended Support Release should update to Adobe Flash Player 13.0.0.289.
- Users of Adobe Flash Player for Linux should update to Adobe Flash Player 11.2.202.460.
- Adobe Flash Player installed with Google Chrome, as well as Internet Explorer on Windows 8.x, will automatically update to version 17.0.0.188.
- Users of the Adobe AIR desktop runtime should update to version 17.0.0.172.
- Users of the Adobe AIR SDK and AIR SDK & Compiler should update to version 17.0.0.172.

**Affected software versions**

- Adobe Flash Player 17.0.0.169 and earlier versions
- Adobe Flash Player 13.0.0.281 and earlier 13.x versions
- Adobe Flash Player 11.2.202.457 and earlier 11.x versions
- AIR Desktop Runtime 17.0.0.144 and earlier versions

ภาพที่ 2-23 ประกาศจากทางเว็บไซต์ Adobe Flash Player (Adobe.com. (2559, 22 สิงหาคม))

ภาพที่ 2-23 เว็บไซต์ Adobe ได้เปิดตัวการปรับปรุงความปลอดภัยโปรแกรม Adobe Flash Player สำหรับระบบปฏิบัติการวินโดวส์, แมคอินทอช และลินุกซ์ ในการปิดช่องโหว่ที่ผู้ไม่ประสงค์ดีอาจจะเข้ามาควบคุมระบบคอมพิวเตอร์ได้ ดังนั้น Adobe แนะนำให้ผู้ใช้ปรับปรุงโปรแกรม Adobe flash player ให้เป็นเวอร์ชันล่าสุด

สำหรับช่องโหว่โปรแกรมคอมพิวเตอร์ยังมีหลายรูปแบบ เช่น ในเดือนเมษายน 2557 มีการประกาศเตือนระวังภัยช่องโหว่ชื่อ Heartbleed ใน OpenSSL ที่ผู้ไม่หวังดีสามารถเข้ามาขโมยข้อมูลจากเครื่องของผู้ใช้ได้ ดังภาพที่ 2-24



ETDA ThaiCERT  
www.etda.or.th Thailand Computer Emergency Response Team a member of ETDA

หน้าแรก > แจ้งเตือนและข้อแนะนำ > สำหรับผู้ดูแลระบบ > ระวังภัย ช่องโหว่ใน OpenSSL ผู้ไม่หวังดีสามารถขโมยข้อมูลใน Memory จากเครื่องของเหยื่อได้ (Heartbleed, CVE-2014-0160)

**ระวังภัย ช่องโหว่ใน OpenSSL ผู้ไม่หวังดีสามารถขโมยข้อมูลใน Memory จากเครื่องของเหยื่อได้ (Heartbleed, CVE-2014-0160)**

วันที่ประกาศ: 9 เมษายน 2557  
ปรับปรุงล่าสุด: 19 เมษายน 2557  
เรื่อง: ระวังภัย ช่องโหว่ใน OpenSSL ผู้ไม่หวังดีสามารถขโมยข้อมูลใน Memory จากเครื่องของเหยื่อได้ (Heartbleed, CVE-2014-0160)

ประเภทภัยคุกคาม: Other

**ข้อมูลทั่วไป**

OpenSSL เป็นไลบรารีสำหรับใช้ในการเข้ารหัสลับข้อมูลผ่านโพรโทคอล SSL และ TLS ซึ่งเป็นไลบรารีแบบ Open source ทำให้ผู้พัฒนาซอฟต์แวร์หลายรายนำไลบรารีดังกล่าวไปใช้ในซอฟต์แวร์ของตนเอง ตัวอย่างโปรแกรมที่ใช้งานไลบรารี OpenSSL เช่น ระบบปฏิบัติการ Linux, เว็บเซิร์ฟเวอร์, โปรแกรมแชท หรือโปรแกรมสำหรับเชื่อมต่อ VPN เป็นต้น

เมื่อวันที่ 7 เมษายน 2557 ทาง OpenSSL ได้แจ้งเตือนช่องโหว่ในซอฟต์แวร์ OpenSSL เวอร์ชัน 1.0.1 ถึง 1.0.1f [1] โดยช่องโหว่ดังกล่าวอยู่ในส่วนของการเชื่อมต่อ TLS/DTLS ในส่วนที่เป็น Heartbeat extension ที่เอาไว้ตรวจสอบว่าโหนดที่เชื่อมต่ออยู่ด้วยนั้นยังทำงานอยู่หรือไม่ [2]

เนื่องจากส่วน Heartbeat extension อนุญาตให้ระบบใด ๆ ก็ตามสามารถส่ง Request เข้ามาเพื่อให้เครื่องปลายทางตอบกลับ แต่กระบวนการนี้มีความผิดพลาดในขั้นตอน

ภาพที่ 2-24 ช่องโหว่จาก Open SSL (ไทยเซิร์ต. (2559, 1 กันยายน))

ภาพที่ 2-24 เป็นการประกาศระวังภัยช่องโหว่ในไลบรารี OpenSSL ที่ผู้ไม่หวังดีสามารถขโมยข้อมูลในหน่วยความจำหลักเครื่องผู้ใช้ได้

## 2.6 งานวิจัยที่เกี่ยวข้องกับการ Deploy Agent

Richard S. Hall, Dennis Heimbigner, Alexander L. Wolf (February: 1997)

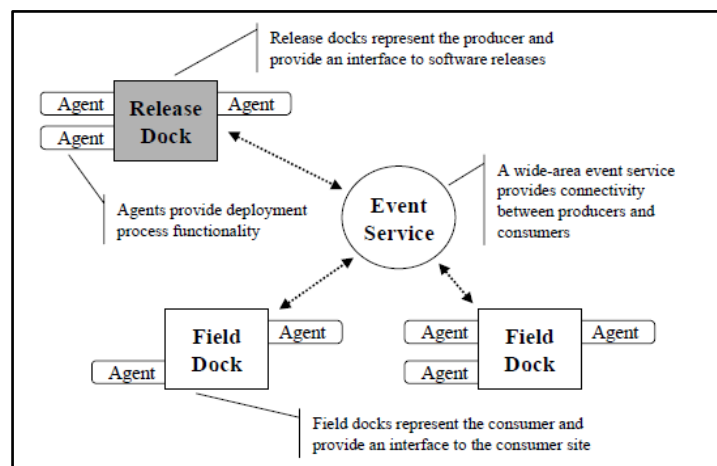
A Cooperative Approach to Support Software Deployment Using the Software Dock

Richard S. Hall, Dennis Heimbigner, Alexander L. Wolf ปรับใช้ซอฟต์แวร์สำหรับพัฒนากระบวนการติดตั้งเอเจนต์ (Agent Deploy) ต่าง ๆ เช่น การเปิดตัว (Release), การติดตั้ง (Install) การดัดแปลงแก้ไข (Adapt), การกำหนดค่าใหม่ (Reconfigure), การอัปเดต, การลงทะเบียน (Activate), การถอนการลงทะเบียน (Deactivate), การถอดออกจากระบบ (Remove), การตั้งอายุการใช้งาน (Retire) และการเชื่อมต่อของเครือข่ายขนาดใหญ่ เช่น อินเทอร์เน็ต มีผลต่อการปรับใช้ซอฟต์แวร์ในการติดตั้งเพราะต้องการแบนด์วิดท์ที่เสถียร ทำให้การ deploy ซอฟต์แวร์มี



ประสิทธิภาพในการใช้งานอย่างเต็มรูปแบบ ในปัจจุบันการติดตั้งซอฟต์แวร์ต่าง ๆ จะถูกดำเนินการติดตั้งผ่านทาง CD-ROM แต่ผู้วิจัยต้องการให้มีทางเลือกในการติดตั้งเพิ่มขึ้น เพื่อสนับสนุนการใช้งานและควบคุมให้เป็นมาตรฐาน และเป็นเวอร์ชันระบบเดียวกันทั้งหมด เทคโนโลยีในการปรับใช้ซอฟต์แวร์ใหม่ต้องสนับสนุนกระบวนการเหล่านี้ Software Dock เป็นโปรเจกต์ในการวิจัยการดำเนินการสร้าง กระจายซอฟต์แวร์ โดยใช้การติดตั้ง Agent สำหรับการสนับสนุน และเจรจาต่อรองกันในหมู่ซอฟต์แวร์ผู้ผลิตและซอฟต์แวร์ลูกค้า สำหรับกรอบการใช้งานคือ การใช้มาตรฐานของการประกาศใช้ซอฟต์แวร์ระบบในรูปแบบที่เรียกว่า Deployable Software Description (DSD) โดย Software dock จะเป็นตัวแทนที่สื่อสารระหว่างซอฟต์แวร์ผู้ผลิตและซอฟต์แวร์ลูกค้า สำหรับโครงสร้าง การเชื่อมต่อและความร่วมมือของ Software Dock นี้จะช่วยให้ผู้ผลิตซอฟต์แวร์ นำเสนอบริการการใช้งานระดับสูงที่ก่อนหน้านี้ไม่สามารถใช้ได้กับลูกค้าของพวกเขา

Software Dock จะมีการติดตั้ง Agent ไว้ที่เครื่องของผู้ใช้ทั้งหมดเพื่อสนับสนุนในการติดตั้งโปรแกรมต่าง ๆ ผ่านตัว Agent ของ Software Dock โดยที่เครื่องแม่หรือตัวเครื่องกลางทำหน้าที่ในการบริหารจัดการจะเชื่อมต่อแลกเปลี่ยนข้อมูลกับ Agent ที่ติดตั้งไปแล้วในเครื่องของผู้ใช้ โดยในการวิจัยนี้สนับสนุนใช้ในการปรับปรุง Java, Mobile agent, configuration เพื่อศึกษาการทำงานและลดเวลาในการติดตั้งแบบเดิม.



ภาพที่ 2-25 สถาปัตยกรรม Software Dock

หลักการการทำงานของ Agent คือ คอยติดต่อกับ Server และทำตามคำสั่งของเซิร์ฟเวอร์ที่ให้ทำงานติดตั้งหรือปรับปรุง ตั้งค่าต่าง ๆ ของซอฟต์แวร์บนเครื่อง Agent รวมทั้งทำการส่งรายงานให้กับเครื่องแม่เพื่อดูสถานะของเครื่องผู้ใช้ได้ เช่น เรียกดูเวอร์ชันของซอฟต์แวร์ เรียกดูสเปคของเครื่อง กำหนดให้สามารถทำการถอดถอนโปรแกรมที่ไม่ต้องการได้ โดยสามารถควบคุมจากส่วนกลาง

## บทที่ 3

### วิธีการดำเนินโครงการ

ในบทนี้ ผู้เขียนงานนิพนธ์จะกล่าวถึงวิธีการดำเนินโครงการ การควบคุมการใช้งานซอฟต์แวร์จากเซิร์ฟเวอร์ส่วนกลาง โดยใช้ซอฟต์แวร์ SCCM 2012 R2 (System center configuration manager) ของบริษัทไมโครซอฟต์ โดยผู้เขียนงานนิพนธ์มีเป้าหมายการดำเนินการ 5 เป้าหมาย ดังนี้

1. การกำหนดมาตรฐานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ผู้ใช้ (Client's operating system standardization)
2. การกระจายซอฟต์แวร์ (Software distribution)
3. การจัดการค่าคอนฟิก (Managing configuration info)
4. การบริหารจัดการด้านความปลอดภัย (Security management)
5. การควบคุมจากทางระยะไกล (Helpdesk remote assistance)

เพื่อบรรลุเป้าหมายการดำเนินโครงการข้างต้น ผู้เขียนงานนิพนธ์ได้ออกแบบและเตรียมแผนการทำงานนิพนธ์ ดังขั้นตอนต่อไปนี้

#### 3.1 ขั้นตอนการวางแผนการทำงานนิพนธ์ (System planning)

ในขั้นตอนนี้ ผู้เขียนงานนิพนธ์ได้ศึกษาระบบงานเดิมที่เกิดปัญหาและหาแนวทาง เพื่อแก้ไขปัญหาต่าง ๆ รวมถึงการศึกษาความเป็นไปได้ ความคุ้มค่าในการพัฒนาระบบงานใหม่ การจัดทำแผนงาน และ ระยะเวลาที่ต้องใช้เพื่อ ติดตั้ง ตั้งค่า ทดสอบ และ ใช้ระบบงานใหม่

##### 3.1.1 การศึกษาระบบงานเดิมและหาแนวทางเพื่อแก้ไขปัญหาต่าง ๆ

ผู้เขียนงานนิพนธ์ได้ศึกษาขั้นตอนการทำงานของพนักงานแผนกไอที ที่เกี่ยวกับการติดตั้งระบบคอมพิวเตอร์และควบคุมการใช้งานซอฟต์แวร์ต่าง ๆ พบว่า การติดตั้งซอฟต์แวร์ (ตั้งแต่การลงระบบปฏิบัติการวินโดวใหม่จนถึงการปรับปรุงซอฟต์แวร์อื่นให้เป็นเวอร์ชันใหม่ล่าสุด การปรับปรุงความปลอดภัยของระบบปฏิบัติการวินโดว เพื่อปิดช่องโหว่และป้องกันการโจมตีหรือการขโมยทำลายข้อมูล จากผู้ไม่ประสงค์ดี) ต้องใช้เวลาติดตั้งนาน เนื่องจากพนักงานไอทีที่ต้องติดต่อผู้ใช้เพื่อขอลงโปรแกรมปรับปรุงต่าง ๆ ทีละเครื่อง จึงทำให้กระทบกับงานที่ทำประจำ และบริษัทต้องเสียค่าใช้จ่ายการทำงานล่วงเวลาให้กับพนักงานไอที เพราะบริษัทมีเครื่องคอมพิวเตอร์มากกว่าห้าร้อยเครื่อง และมีพนักงานไอทีแค่ 3 คนเท่านั้น

จากการศึกษาระบบงานเดิม ผู้เขียนงานนิพนธ์พบว่า พนักงานไอทีอาจลดเวลาที่ใช้ติดตั้งระบบซอฟต์แวร์และปรับปรุงความปลอดภัยวินโดวส์ได้ โดยใช้ซอฟต์แวร์ System center configuration Manager (SCCM 2012 R2) ซึ่งเป็นระบบที่สามารถบริหารจัดการซอฟต์แวร์และควบคุมการปรับปรุงความปลอดภัยของวินโดวส์ได้จากส่วนกลาง และยังสามารถเรียกดูสถานะการติดตั้งซอฟต์แวร์จากหน้าโปรแกรม นอกจากนี้ยังสามารถจัดทำรายงานเสนอผู้บริหารได้ทันที

### 3.1.2 ฝึกอบรมและศึกษาข้อมูลจากอินเทอร์เน็ต (Studying & training)

ผู้เขียนได้ไปฝึกอบรมการติดตั้งระบบ SCCM 2012 R2 และการจัดเตรียมความพร้อมก่อนติดตั้ง กับบริษัทไอโซเน็ต จำกัด ซึ่งเป็นผู้แทนการฝึกอบรมของไมโครซอฟต์ โดยการเรียนจะมีกรณีตัวอย่างให้ฝึกทำ ตั้งแต่ติดตั้งและคอนฟิกค่าต่าง ๆ ที่เป็นพื้นฐานของระบบ SCCM 2012 R2 นอกจากนี้ทางผู้เขียนงานนิพนธ์ยังได้ทำการศึกษาข้อมูลเพิ่มเติมผ่านทางเว็บไซต์ที่เกี่ยวข้อง ยูทูป และเว็บไซต์ของไมโครซอฟต์ เพื่อศึกษาหาข้อมูลและวิธีทำ และ ผู้เขียนงานนิพนธ์ยังได้ทำการทดสอบโดยจำลองการติดตั้งระบบ 2 ครั้งก่อนการติดตั้งจริงอีกด้วย

### 3.1.3 แผนงานและระยะเวลาในการดำเนินงาน

การดำเนินงานการติดตั้งระบบ SCCM 2012 R2 (System center configuration manager) มีกำหนดการประมาณ 9 เดือนดังรายละเอียดข้างล่างนี้

3.1.3.1 ศึกษากระบวนการเดิมและหาแนวทางแก้ไขปัญหา

3.1.3.2 ฝึกอบรมและศึกษาข้อมูลจากอินเทอร์เน็ต

3.1.3.3 ออกแบบระบบ (System design)

1. ออกแบบระบบเครือข่าย

2. ออกแบบโครงสร้างระบบ SCCM

3. การตั้งชื่อกลุ่มของคอมพิวเตอร์ที่ใช้ซอฟต์แวร์เดียวกัน (Collection)

4. ออกแบบการใช้งานของระบบ SCCM 2012 R2

- การติดตั้งระบบปฏิบัติการวินโดวส์ผ่านทางระบบ SCCM

- การ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้

- การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง

- การปรับปรุง (Update) วินโดวส์จากเซิร์ฟเวอร์ SCCM

- การปรับปรุง (Update) โปรแกรมป้องกันไวรัส Endpoint protection point

- การรีโมตไปที่เครื่องผู้ใช้ผ่านระบบ SCCM

- การเรียกดูรายงาน

5. กำหนดช่วงไอพีเครือข่ายเครื่องผู้ใช้ใน SCCM boundaries

3.1.3.4 การติดตั้งและตั้งค่าระบบ SCCM 2012 R2

1. ติดตั้งระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2012
  2. สร้างกลุ่มคอมพิวเตอร์ของผู้ใช้ใน Active directory (Security group)
  3. ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์หลัก (Primary site)
  4. ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์ฐานข้อมูล (Database site)
  5. ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์สาขาบางนา (Distribution point server)
  6. ติดตั้ง Agent ที่เครื่องผู้ใช้ (Client setting)
  7. สร้างกลุ่มคอมพิวเตอร์ของผู้ใช้ใน SCCM (Device collections)
  8. ตั้งค่าส่วนการ Deploy ระบบปฏิบัติการ (Operating system deployment)
  9. ตั้งค่าส่วนคลังข้อมูลอุปกรณ์คอมพิวเตอร์ (Hardware inventory)
  10. ตั้งค่าส่วนคลังข้อมูลซอฟต์แวร์คอมพิวเตอร์ (Software inventory)
  11. ตั้งค่าส่วนการจัดการด้านความปลอดภัย (Security management)
  12. ตั้งค่าส่วนการควบคุมจากทางระยะไกล (Helpdesk remote assistance)
- 3.1.3.5 ทดสอบระบบ SCCM 2012 R2 (Testing)
- 3.1.3.6 สังเกตการณ์ การทำงานระบบ SCCM 2012 R2 (Monitoring)

## 3.2 การออกแบบระบบ (System design)

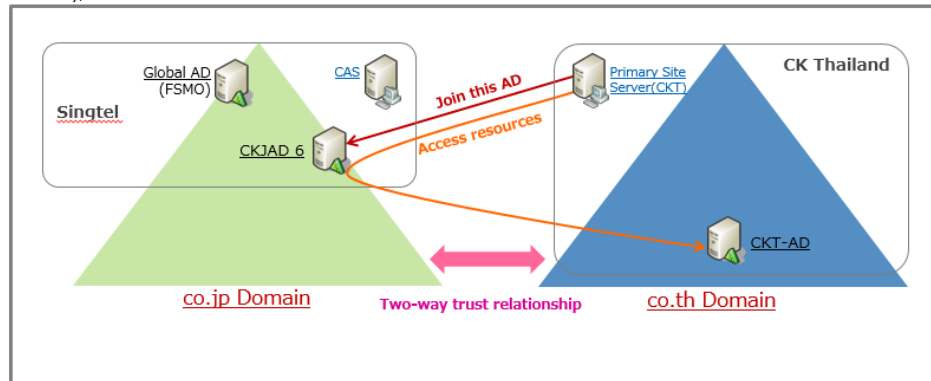
สำหรับการออกแบบระบบ SCCM 2012 R2 นั้น ทางผู้เขียนงานนิพนธ์ได้แบ่งการทำงานออกเป็น 4 ประเภท ดังนี้

1. การออกแบบระบบเครือข่าย
2. การออกแบบโครงสร้างระบบ SCCM
3. การตั้งชื่อกลุ่มของคอมพิวเตอร์ที่ใช้ซอฟต์แวร์เดียวกัน (Collection)
4. การใช้งานระบบ SCCM 2012 R2

### 3.2.1 การออกแบบระบบเครือข่าย

เนื่องจากโดเมนของคาลโซนิคประเทศไทย (Calsonickansei.co.th) และโดเมนของคาลโซนิค ประเทศญี่ปุ่น (Calsonickansei.co.jp) เป็นคนละโดเมน ทั้งสองโดเมนจึงต้องเชื่อมต่อกัน โดยผู้เขียนงานนิพนธ์ได้กำหนดความสัมพันธ์ระหว่างสองโดเมนใน Active directory เป็นแบบเชื่อใจกันแบบ 2 ทาง (two-way trust relationship) ทำให้ทั้งสองฝั่งสามารถมองเห็นทรัพยากรของอีกฝั่งได้ สามารถแลกเปลี่ยนข้อมูลซึ่งกันและกัน และ เข้าไปใช้งานหรือกำหนดสิทธิในการจัดการทรัพยากรใน Active directory ทั้งสองฝั่งได้ ดังภาพที่ 3-1

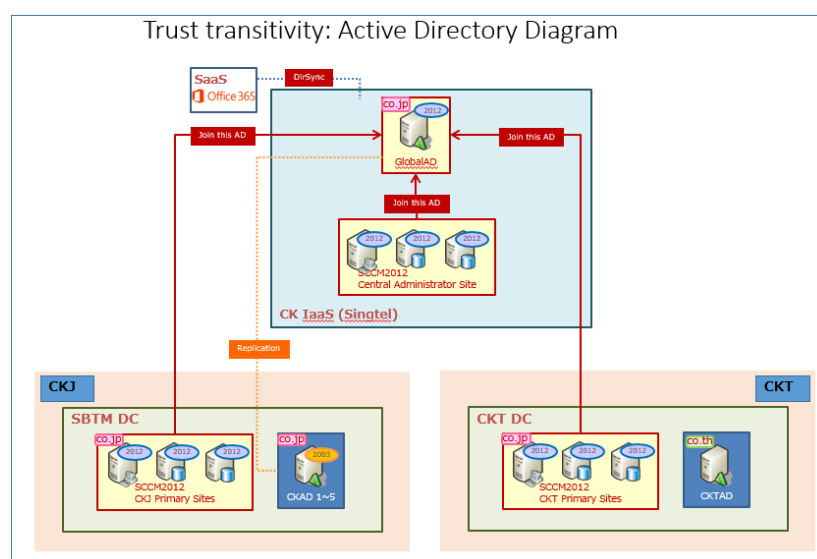
▼Two-way, forest trust for both sides of the trust



ภาพที่ 3-1 การเชื่อมต่อ Domain แบบ Two-way trust ระหว่าง CKJ-CKT

ในอนาคตโดเมนของคาลโซนิคประเทศไทยต้องไปเข้าร่วมกับโดเมนคาลโซนิคญี่ปุ่น ตามนโยบายโดเมนเดียวกันของกลุ่มบริษัทคาลโซนิคทั่วโลก (ทุกเครื่องของบริษัทในกลุ่มจะอยู่ในโดเมน Calsonickansei.co.jp เท่านั้น) ดังนั้น ผู้เขียนงานนิพนธ์จึงติดตั้งระบบ SCCM 2012 R2 (ของคาลโซนิคประเทศไทย) ในส่วน Central access site (CAS, ตัวจัดการระบบ SCCM ระดับบน) และ Primary site (ตัวจัดการระบบ SCCM ระดับกลาง) ในโดเมนคาลโซนิคญี่ปุ่น แต่ ผู้เขียนงานนิพนธ์ติดตั้ง SCCM client ในเครื่องของผู้ใช้ในโดเมนคาลโซนิคประเทศไทย

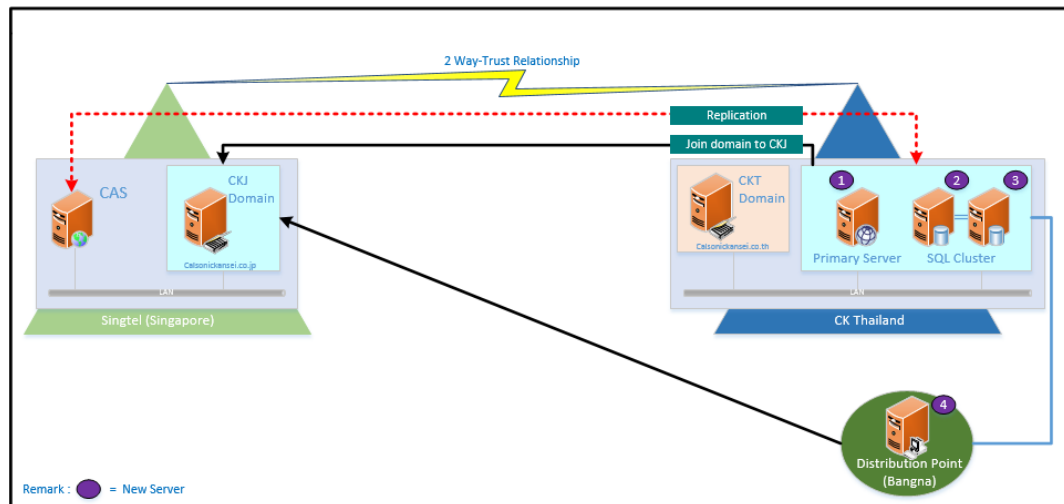
การเชื่อมต่อโดเมนจากคาลโซนิคประเทศไทยไปเชื่อมที่ Cloud ซึ่งเป็นบริการ IaaS ของบริษัท SingTel ซึ่งเป็นบริษัทผู้ให้บริการเครือข่ายรายใหญ่ในประเทศสิงคโปร์ ดังภาพที่ 3-2



ภาพที่ 3-2 การเชื่อมต่อระบบ SCCM 2012 R2

### 3.2.2 การโครงสร้างของระบบ SCCM

ในงานนิพนธ์นี้ ผู้เขียนฯ ใช้เครื่องเซิร์ฟเวอร์จำนวน 4 เครื่องด้วยกัน ดังภาพที่ 3-3



ภาพที่ 3-3 การออกแบบเซิร์ฟเวอร์เพื่อรองรับระบบ SCCM 2012 R2

โดยรายละเอียดของเครื่องเซิร์ฟเวอร์ประกอบไปด้วย

1. Primary server ทำหน้าที่ในการบริหารจัดการคำสั่งและเป็นที่เก็บไฟล์ซอฟต์แวร์ต่าง ๆ ที่จะทำการ deploy ไปที่เครื่องผู้ใช้ นอกจากนี้ Primary site server ยังทำหน้าที่ออกรายงาน เพื่อให้ผู้ดูแลระบบสามารถเรียกดูได้จากหน้าจอโปรแกรมได้

2. เครื่องเซิร์ฟเวอร์ 2 เครื่อง ถูกใช้เป็นฐานข้อมูล (Site database) ที่จัดเก็บรายละเอียดของเครื่องผู้ใช้อย่างเช่น สเปคของเครื่องคอมพิวเตอร์ รุ่น ยี่ห้อ และซอฟต์แวร์อัปเดต เวอร์ชันต่าง ๆ ที่ได้มีการติดตั้งที่เครื่องผู้ใช้ โดยผู้ดูแลระบบสามารถเรียกดูรายละเอียดเหล่านี้ได้จากรายงานต่าง ๆ ผู้เขียนงานนิพนธ์ใช้เครื่องเซิร์ฟเวอร์ 2 เครื่องเพื่อเป็นฐานข้อมูลของ SCCM 2012 R2 เพราะ ข้อมูล SCCM มีความสำคัญ (หากเครื่องเซิร์ฟเวอร์ดาต้าเบสล่ม ระบบทั้งระบบจะไม่สามารถทำงานได้) ดังนั้น ผู้เขียน ฯ จึงออกแบบเพื่อให้ฐานข้อมูลสำรองข้อมูลซึ่งกันและกัน (Active standby) โดยใช้ SQL Server 2012 R2 ทำ Cluster กัน

3. Distribution point server เป็นเซิร์ฟเวอร์ที่อยู่ที่สาขาบางนา ทำหน้าที่คล้ายกับ Primary server (เก็บและแจกจ่ายซอฟต์แวร์ต่าง ๆ ที่จะ deploy ไปเครื่องผู้ใช้ประมาณ 80-100 เครื่อง) Distribution point server ช่วยประหยัดแบนด์วิดท์ที่ต้องใช้ในการแจกจ่ายซอฟต์แวร์ ทำให้การจราจรของเน็ตเวิร์กที่เชื่อมระหว่างสาขาไม่ติดขัด

รายละเอียดสเปคของเซิร์ฟเวอร์ถูกแสดงอยู่ในตารางด้านล่าง

ตารางที่ 3-1 รายละเอียดสเปคของเซิร์ฟเวอร์

Primary server (เครื่องหลักในการบริหารจัดการระบบ SCCM 2012 R2)	
ระบบปฏิบัติการ	ไมโครซอฟต์วินโดวส์เซิร์ฟเวอร์ 2012 R2
หน่วยความจำ	32 GB
ฮาร์ดดิสก์	C : 120 GB D : 500 GB
Site database (ฐานข้อมูล) มีจำนวน 2 เครื่อง	
ระบบปฏิบัติการ	ไมโครซอฟต์วินโดวส์เซิร์ฟเวอร์ 2012 R2
หน่วยความจำ	32 GB
ฮาร์ดดิสก์	C : 120 GB M : 125 GB และ N : 125 GB
Distribution point server (เครื่องกระจายที่สาขาบางนา)	
ระบบปฏิบัติการ	ไมโครซอฟต์วินโดวส์เซิร์ฟเวอร์ 2012 R2
หน่วยความจำ	16 GB
ฮาร์ดดิสก์	C : 120 GB D : 500 GB

ผู้เขียนงานนิพนธ์ได้กำหนดชื่อเครื่องและไอพี สำหรับเครื่องเซิร์ฟเวอร์ ที่ใช้ในการติดตั้งระบบ SCCM ดังตารางที่ 3-2

ตารางที่ 3-2 ชื่อเครื่องและไอพี สำหรับเครื่องเซิร์ฟเวอร์

ชื่อเครื่อง	โดเมน	ไอพี	เซิร์ฟเวอร์
CKTSERVER022	calsonickansei.co.jp	172.xx.aaa.44	Primary site
CKTSERVER023	calsonickansei.co.jp	172.xx.aaa.45	Site database 01
CKTSERVER024	calsonickansei.co.jp	172.xx.aaa.46	Site database 02
CKTSERVER025	calsonickansei.co.jp	172.xx.bb.1	Distribution point

ผู้เขียนงานนิพนธ์ได้กำหนดการตั้งค่าเครื่องเซิร์ฟเวอร์ สำหรับ ชื่อโดเมนที่เข้าร่วม, Gateway, DNS และ Subnet mask ดังตารางที่ 3-3

ตารางที่ 3-3 กำหนดตั้งค่าเครื่องเซิร์ฟเวอร์สำหรับ Domain, Gateway, DNS และ Subnet mask

Domain, Gateway, DNS, Subnet mask	
ชื่อโดเมนที่เข้าร่วม	calsonickensei.co.jp
Gateway	172.xx.aaa.250
DNS1 server	191.xxx.xx.211 (DNS of calsonickensei.co.jp)
DNS2 server	191.xxx.xx.212 (DNS of calsonickensei.co.jp)
Subnet mask	255.255.255.0

จากรายละเอียดการกำหนดตั้งค่าตามตารางที่ 3-2 และ 3-3 ผู้เขียนงานนิพนธ์ได้แสดงการกำหนดค่าคอนฟิกของแต่ละเครื่องเซิร์ฟเวอร์ ดังตารางที่ 3-4

ตารางที่ 3-4 กำหนดค่าคอนฟิกของแต่ละเครื่อง

กำหนดค่าคอนฟิกของแต่ละเครื่อง	
รายละเอียดเครื่อง	เซิร์ฟเวอร์หลัก SCCM 2012 R2 (Primary site)
สถานที่ติดตั้ง	อมตะนคร (CKT HQ)
ชื่อเครื่องเซิร์ฟเวอร์	CKTSERVER022
ไอพีเครื่อง	172.xx.aaa.44
Subnet mask	255.255.255.0
Gateway	172.xx.aaa.250
DNS1 / DNS2	191.xxx.xx.211 / 191.xxx.xx.212
บัญชีผู้ใช้ / รหัสผ่าน	.\Administrator / Xxxxxxxx



ตารางที่ 3-4 กำหนดค่าคอนฟิกของแต่ละเครื่อง (ต่อ)

กำหนดค่าคอนฟิกของแต่ละเครื่อง	
รายละเอียดเครื่อง	เซิร์ฟเวอร์ฐานข้อมูล ตัวที่ 1 (Site database 01)
สถานที่ติดตั้ง	อมตะนคร (CKT HQ)
ชื่อเครื่องเซิร์ฟเวอร์	CKTSERVER023
ไอพีเครื่อง	172.xx.xxx.45
Subnet mask	255.255.255.0
Gateway	172.xx.xxx.250
DNS1 / DNS2	191.xxx.xx.211 / 191.xxx.xx.212
บัญชีผู้ใช้ / รหัสผ่าน	.\Administrator / Xxxxxxxx
รายละเอียดเครื่อง	เซิร์ฟเวอร์ฐานข้อมูล ตัวที่ 2 (Site database 02)
สถานที่ติดตั้ง	อมตะนคร (CKT HQ)
ชื่อเครื่องเซิร์ฟเวอร์	CKTSERVER023
ไอพีเครื่อง	172.xx.aaa.46
Subnet mask	255.255.255.0
Gateway	172.xx.aaa.250
DNS1 / DNS2	191.xxx.xx.211 / 191.xxx.xx.212
บัญชีผู้ใช้ / รหัสผ่าน	.\Administrator / Xxxxxxxx
กำหนดค่าคอนฟิกของแต่ละเครื่อง	
รายละเอียดเครื่อง	เซิร์ฟเวอร์กระจายที่สาขาบางนา (Distribution point)
สถานที่ติดตั้ง	บางนา กม 21
ชื่อเครื่องเซิร์ฟเวอร์	CKTSERVER024
ไอพีเครื่อง	172.xx.xx.1
Subnet mask	255.255.255.0
Gateway	172.xx.xx.250
DNS1 / DNS2	191.xxx.xx.211 / 191.xxx.xx.212
บัญชีผู้ใช้ / รหัสผ่าน	.\Administrator / Xxxxxxxx

ผู้เขียนงานนิพนธ์ได้กำหนดบัญชีผู้ใช้และรหัสผ่านสำหรับติดตั้งระบบ SCCM 2012 R2 ดังตารางที่ 3-5

ตารางที่ 3-5 กำหนดบัญชีผู้ใช้และรหัสผ่าน

บัญชีผู้ใช้	*รหัสผ่าน	รายละเอียด
SCCM_CKT_Admin	xxxxxxxxxxxx	ใช้สำหรับปรับตั้งค่าต่าง ๆ ใน SCCM 2012 R2
SCCM_CKT_PushInstall	xxxxxxxxxxxx	ใช้สำหรับติดตั้งในเครื่องผู้ใช้เพื่อเพิ่ม Agent
SCCM_CKT_SQLAdmin	xxxxxxxxxxxx	ใช้สำหรับปรับตั้งค่าต่าง ๆ ใน SQL Server 2012 R2
SCCM_CKT_SQLAgent	xxxxxxxxxxxx	ใช้สำหรับติดต่อฐานข้อมูลแม่ที่ประเทศญี่ปุ่น Agent
SCCM_CKT_SQLReporting	xxxxxxxxxxxx	ใช้สำหรับดึงรายงานจากฐานข้อมูล
SCCM_CKT_SQLDatabase	xxxxxxxxxxxx	ใช้สำหรับการเชื่อมต่อฐานข้อมูล

\*รหัสผ่าน โดยการใช้การสุ่มรหัสผ่านทางเว็บไซต์ <http://passwordsgenerator.net/> โดยการกำหนดความยาว 16 ตัว ประกอบไปด้วย ตัวเลข ตัวอักษรภาษาอังกฤษ ใหญ่และเล็ก ดังนี้

Password Length:

Include Symbols:  ( e.g. @\$% )

Include Numbers:  ( e.g. 123456 )

Include Lowercase Characters:  ( e.g. abcdefgh )

Include Uppercase Characters:  ( e.g. ABCDEFGH )

Exclude Similar Characters:  ( e.g. i, l, 1, L, o, 0, O )

Exclude Ambiguous Characters:  ( { } [ ] ( ) / \ ' " ~ , ; : . < > )

Generate On The Client Side:  ( do NOT send across the Internet )

Auto-Select:  ( select the password automatically )

Save My Preference:  ( save all the settings above for later use )

Load My Settings Anywhere:

Your New Password:

Remember your password: Apple Shoot SHOOT JACK Zero Visa ROPE Four APPLE KOREAN Washington Drip JACK TECHNOLOGY Technology Seven

ภาพที่ 3-4 การออกแบบตั้งรหัสผ่านของบัญชีผู้ใช้

### 3.2.3 การตั้งชื่อกลุ่มคอมพิวเตอร์

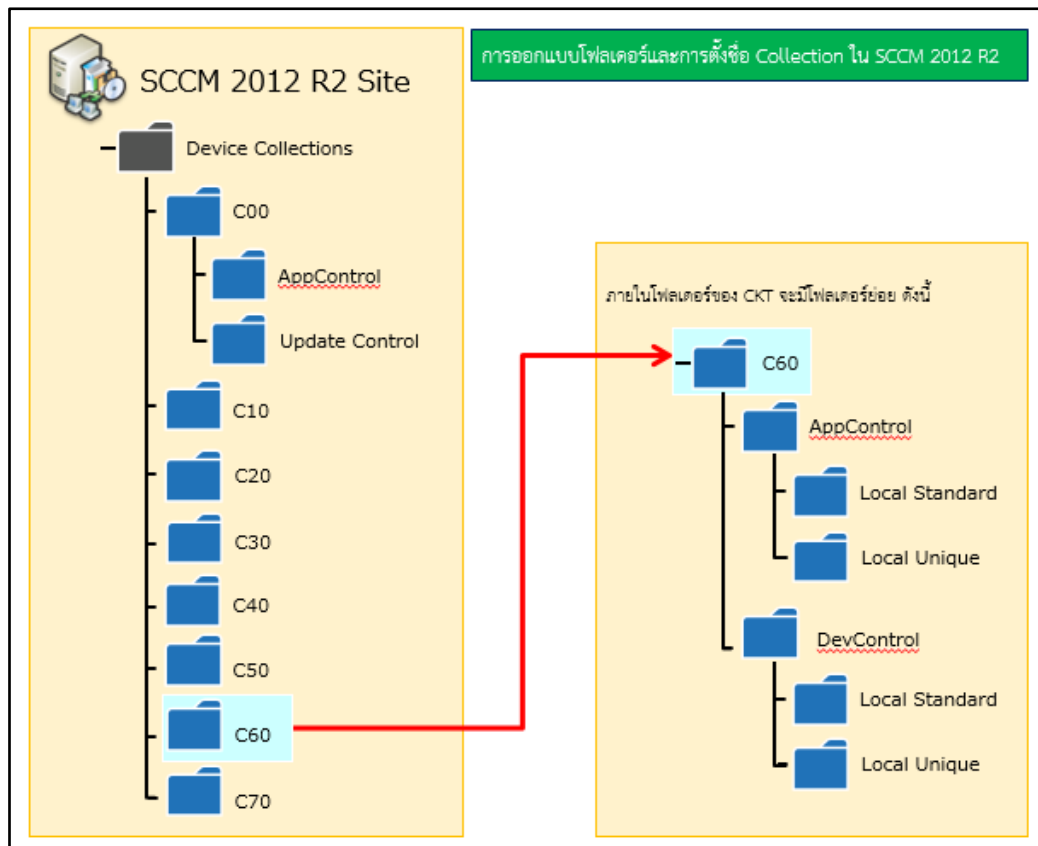
เจ้าหน้าที่จากบริษัทแม่ที่ญี่ปุ่น ได้ตั้งชื่อกลุ่มคอมพิวเตอร์ตามที่ตั้งของแต่ละประเทศ ดังนี้

ตารางที่ 3-6 การตั้งชื่อกลุ่มคอมพิวเตอร์

ชื่อที่ตั้ง (Site)	ชื่อย่อ (Site code)
Global Central Administration Site	C00
CKJ Primary Site	C10
CKAUS Primary Site	C20
CKAMX Primary Site	C30
CKC Primary Site	C40
CKEX Primary Site	C50
CKT Primary Site	C60
CKMY Primary Site	C70

จากตาราง 3-6 ได้แสดงการตั้งชื่อกลุ่มคอมพิวเตอร์ของแต่ละประเทศ โดยชื่อที่ตั้ง (Site) ประเทศไทยได้ชื่อย่อเป็น C60

เพื่อให้เป็นมาตรฐานเดียวกันและสามารถใช้งานระบบ SCCM ร่วมกันได้ ทางบริษัทแม่ที่ญี่ปุ่นจึงได้มีการกำหนดสิทธิการใช้งานเครื่องในแต่ละประเทศ (ใน Device collection) โดยแบ่งตามชื่อรหัสของที่ตั้งประเทศนั้น ๆ และผู้ดูแลระบบจะสามารถจัดการอุปกรณ์ที่อยู่ภายในโพลเดอร์ตัวเองเท่านั้น สำหรับของคอลไลซอนิคประเทศไทยจะเป็นรหัสจะเป็น C60 ดังภาพข้างล่างนี้



ภาพที่ 3-5 การตั้งชื่อไฟลเตอร์ใน Device collection

จากภาพที่ 3-5 ไฟลเตอร์ C60 จะเป็นรหัสของประเทศไทย ซึ่งจะมีไฟลเตอร์ย่อย 2 ไฟลเตอร์ คือ

1. AppControl จะเป็นไฟลเตอร์ที่เกี่ยวกับการควบคุมโปรแกรมประยุกต์ ซึ่งโปรแกรมที่ใช้งานในบริษัทจะมีทั้งที่เป็นมาตรฐานของบริษัทกาลโซนิคเอง เรียกว่า Local standard (เช่น โปรแกรมไมโครซอฟต์ออฟฟิต 2013, Adobe reader, Java, Internet explorer) ซึ่งทุกประเทศใช้เหมือนกัน และ โปรแกรมที่แต่ละประเทศใช้งานไม่เหมือนกันหรือไม่เป็นมาตรฐานของบริษัทกาลโซนิคแต่ได้มีการจดทะเบียนว่าเป็นโปรแกรมที่มีการใช้งานในปัจจุบัน เรียกว่า Local unique (เช่น โปรแกรม Brava!, โปรแกรมตัดต่อภาพ Faststone, โปรแกรมการบริหารจัดการบุคคลากร, และ โปรแกรมเงินเดือนของฝ่ายทรัพยากรมนุษย์)

ดังนั้น ใน AppControl จึงมีไฟลเตอร์ Local standard และ Local unique เพื่ออำนวยความสะดวกในการจัดการและควบคุมให้เป็นมาตรฐานของระบบ ผู้เขียนงานนิพนธ์ต้องกำหนดให้เครื่อง Client ที่ใช้ซอฟต์แวร์เดียวกันอยู่ในกลุ่ม Client เดียวกัน (หรือเรียกอีกอย่างว่า อยู่ใน Collection เดียวกัน) โดยที่เครื่อง Client อยู่ในกลุ่มของ Client หลาย ๆ กลุ่มได้

2. DevControl จะเป็นโพลเตอร์เกี่ยวกับการควบคุมไดรเวอร์ของอุปกรณ์ต่าง ๆ เช่น ไดรเวอร์ของเครื่องคอมพิวเตอร์, ปริ้นเตอร์ สำหรับโพลเตอร์ย่อย ได้แก่ Local standard และ Local unique ซึ่งคล้ายกับที่กล่าวมาแล้วในข้อ 1

- การตั้งชื่อกลุ่มของ Client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection)

การตั้งชื่อกลุ่มของ Client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection) ใน folder Local standard และ Local unique ของ SCCM 2012 R2 ต้องเป็นไปตามกฎของการตั้งชื่อ Collection (Naming Rules) ตามนโยบายของบริษัท โดยชื่อต้องประกอบไปด้วยส่วนย่อย ดังแสดงด้านล่าง  
[Site Code]-[Scope]-[Application name]-[Word size]-[Language(Abbrev)]

ตารางที่ 3-7 การตั้งชื่อกลุ่มของ Client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection)

หัวข้อ	เงื่อนไข	ตัวอย่าง
รหัสสถานที่ [Site code]	ตัวย่อ 3 ตัว	C00
ขอบข่าย [Scope]	ตัวย่ออักษรจำนวน 2 ตัว	GS (Global standard) - OA/CAD/ALL
		LS (Local standard) - OA/CAD/ALL
		LU (Local unique) - OA/CAD/ALL
ชื่อโปรแกรมประยุกต์ [Application name]	ตัวอักษรและตัวเลข	Office 2013
บิตโปรแกรม [Word size]	ตัวเลขจำนวน 2 ตัว	32/64/00
ภาษาตัวย่อ [Language(Abbrev)]	ตัวย่ออักษร 3 ตัวอักษร	MUI/JPN/ENG/CHA
<u>ตัวอย่าง</u>	กรณี : Office 2013 (MUI, ไม่มีความแตกต่างของขนาดบิต)	
→ C60-GS-ALL-Office2013-00-MUI		

[Site code] รหัสสถานที่ที่ตั้ง โดยมีเงื่อนไขให้ใช้ตัวอักษรย่อจำนวน 3 ตัว โดยเอาตัวย่อที่ตั้งแต่ละประเทศมาใส่ เพื่อให้รู้ว่า Collection ประเทศอะไรเป็นผู้สร้าง [Scope] ขอบข่าย โดยมีเงื่อนไขให้ใช้ตัวอักษรย่อจำนวน 2 ตัว ได้แก่

1. Global standard เป็นขอบข่ายของโปรแกรมและอุปกรณ์ที่ใช้เหมือนกันทั่วโลก

2. Local standard เป็นขอบข่ายของโปรแกรมและอุปกรณ์ที่ใช้ด้วยกันบางประเทศ แต่ไม่ได้ใช้เหมือนกันทุกประเทศ

3. Local unique เป็นขอบข่ายที่ใช้แต่ละประเทศ กล่าวคือเป็นโปรแกรมส่วนตัวของแต่ละประเทศนั่นเอง

เมื่อกำหนดตัวอักษรย่อ 2 ตัวแล้วยังกำหนดขอบข่ายประเภทของโปรแกรมและอุปกรณ์ด้วย โดยมีความหมายดังนี้

OA: Office area คือคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ภายในสำนักงาน

CAD: CAD design คือคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการออกแบบผลิตภัณฑ์

ALL: Office area + CAD design คือทั้งสองอย่างรวมกัน

[Application name] ชื่อโปรแกรมประยุกต์ โดยมีเงื่อนไขให้ใช้ตัวเลขและตัวอักษร เช่น Office2013, FlashPlayer21.0.0.213, Java8.1 เป็นต้น

[Word size] บิตโปรแกรมระบบปฏิบัติการ โดยมีเงื่อนไขให้ใช้ตัวเลขจำนวน 2 ตัว ดังนี้

1. 32 คือ มีการระบุบิตของโปรแกรมระบบปฏิบัติการที่ใช้ได้คือ 32 บิต

2. 64 คือ มีการระบุบิตของโปรแกรมระบบปฏิบัติการที่ใช้ได้คือ 64 บิต

3. 00 คือ ไม่ได้มีการระบุบิตของโปรแกรมระบบปฏิบัติการ สามารถใช้ได้ทั้ง 32 บิต

และ 64 บิต

[Language(Abbrev)] ภาษาตัวย่อ เป็นภาษาที่ใช้ในการแสดงหน้าต่างโปรแกรมประยุกต์ หรือไทรเวอร์อุปกรณ์ โดยมีเงื่อนไขในการใช้ตัวย่อตัวอักษร 3 ตัวอักษร ดังนี้

ENG (English) คือ ภาษาอังกฤษ

JPN (Japanese) คือ ภาษาญี่ปุ่น

CHA (China) คือ ภาษาจีน

MUI (Multilanguage user interface) คือ สามารถใช้ได้ทั้ง 3 ภาษา (ENG/JPN/CHA)

จากการกำหนดกฎการตั้งชื่อของ Collection ทางผู้ออกแบบได้ตั้งชื่อกลุ่มของเครื่อง Client (Collection) ดังตารางที่ 3-8

ตารางที่ 3-8 ชื่อกลุ่มของ Client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection)

ซอฟต์แวร์มาตรฐานของบริษัทคาลโซนิค (Local standard software)			
ชื่อซอฟต์แวร์	ภาษา	บิต	ชื่อ Collection
[ซอฟต์แวร์]			
Office2013 Professional Plus	ENG	32	C60-LS_ALL-Office2013-32-ENG
Office2013 Professional Plus	ENG	64	C60-LS_ALL-Office2013-64-ENG
Internet Explorer 11	ENG	32	C60-LS_OA-IE11-32-ENG
Internet Explorer 11	ENG	64	C60-LS_OA-IE11-64-ENG
Firefox 30	MUI	32	C60-LS_OA-Firefox30-32-MUI
Adobe Flash Player Ver 17	ENG	32	C60-LS_OA-FlashPlayer17-32-ENG
Adobe Flash Player Ver 17	ENG	64	C60-LS_OA-FlashPlayer17-64-ENG
7-ZIP Ver 9.20	ENG	32	C60-LS_OA-7Zip9_20-32-ENG
Adobe Reader 17Z5.0	MUI	00	C60-LS_ALL-AdobeReader15-32-MUI
Java Ver 8	ENG	00	C60-LS_ALL-Java8-32-ENG
Lync 2010	ENG	00	C60-LS_OA-Lync2010-32-ENG
[ไดร์เวอร์]			
H/W Driver HP 645 Laptop	ENG	32	C60-LS-OA-HP645_DriverSet-32-ENG
H/W Driver HP 645 Laptop	ENG	64	C60-LS-OA-HP645_DriverSet-64-ENG
H/W Driver HP 725 Laptop	ENG	32	C60-LS-OA-HP725_DriverSet-32-ENG
H/W Driver HP 725 Laptop	ENG	64	C60-LS-OA-HP725_DriverSet-64-ENG
H/W Driver HP 705 Laptop	ENG	32	C60-LS-OA-HP705_DriverSet-32-ENG
H/W Driver HP 705 Desktop	ENG	64	C60-LS-OA-HP705_DriverSet-64-ENG

ตารางที่ 3-8 ชื่อกลุ่มของ Client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection) (ต่อ)

ซอฟต์แวร์ท้องถิ่นที่ใช้สำหรับบริษัทคาสิโนประเทศไทย (Local unique software)			
ชื่อซอฟต์แวร์	ภาษา	บิต	ชื่อ Collection
[ซอฟต์แวร์]			
Cisco NAC Agent (VPN)	ENG	00	C60-LU_OA-Cisco-00-ENG
IFS	ENG	32	C60-LU_OA-IFS-32-ENG
Oracle	ENG	32	C60-LU_OA-Oracal-32-ENG
HR Payroll Program	ENG	32	C60-LU_OA-Payroll-32-ENG
TiffViwer	ENG	32	C60-LU_OA-Tiffviwer-32-ENG
MacAfee SP2	ENG	32	C60-LU_OA-Macafee-32-ENG
Lotus Note	ENG	32	C60-LU_OA-LotusNote-32-ENG
Compu Program	ENG	32	C60-LU_OA-Compu-32-ENG
[ไดร์เวอร์]			
Printer Driver FUJI Xerox 5575	MUI	32	C60-LU-ALL-FijiDriver_5575-32-MUI
Printer Driver FUJI Xerox 5575	MUI	64	C60-LU-ALL-FujiDriver_5575-64-MUI
Printer Driver FUJI Xerox 4112	MUI	32	C60-LU-ALL-FujiDriver_4112-32-MUI
Printer Driver FUJI Xerox 4112	MUI	64	C60-LU-ALL-FujiDriver_4112-64-MUI
H/W Driver DELL V130 Laptop	ENG	32	C60-LU-OA-DELLV130_DriverSet-32-ENG
H/W Driver DELL V131 Laptop	ENG	32	C60-LU-OA-DELLV131_DriverSet-32-ENG
H/W Driver DELL 3360 Laptop	ENG	32	C60-LU-OA-DELL3360_DriverSet-32-ENG
H/W Driver DELL E6330 Laptop	ENG	32	C60-LU-OA-DELLE6330_DriverSet-32-ENG

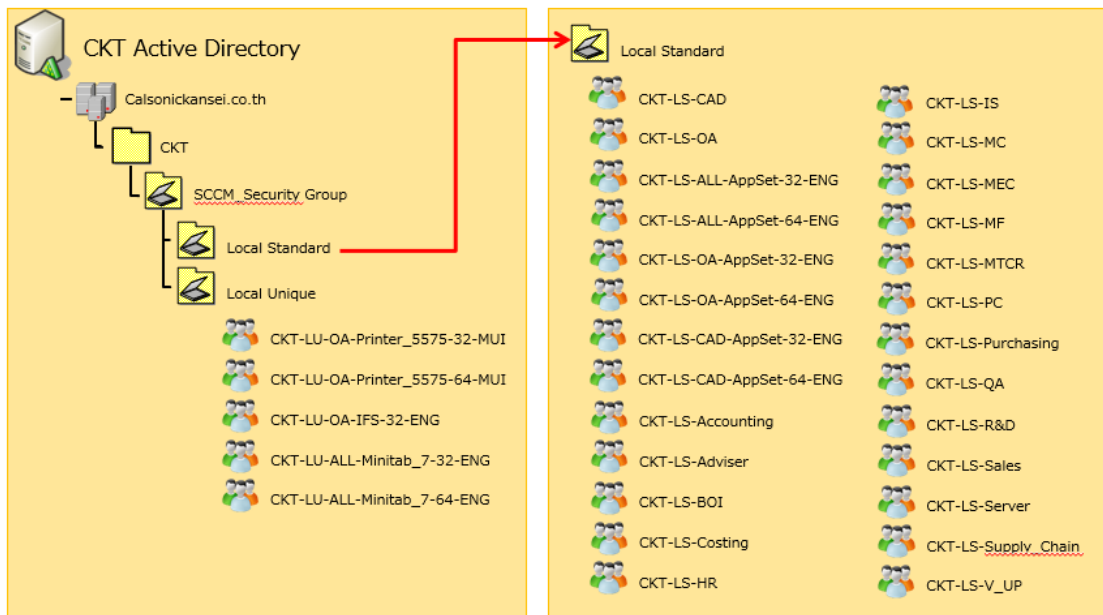


ตารางที่ 3-8 ตารางที่ 3-8 ชื่อกลุ่มของ Client ที่ใช้ซอฟต์แวร์เดียวกัน (Collection) (ต่อ)

ซอฟต์แวร์ท้องถิ่นที่ใช้สำหรับบริษัทคาสิโนประเทศไทย (Local unique software)			
ชื่อซอฟต์แวร์	ภาษา	บิต	ชื่อ Collection
[ไดร์เวอร์]			
H/W Driver DELL E6430 Laptop	ENG	32	C60-LU-OA-DELLE6430_DriverSet-32-ENG
H/W Driver DELL E5430 Laptop	ENG	32	C60-LU-OA-DELL5430_DriverSet-32-ENG
H/W Driver HP 645 Laptop	ENG	32	C60-LU-OA-HP645_DriverSet-32-ENG
H/W Driver HP 725 Laptop	ENG	32	C60-LU-OA-HP725_DriverSet-32-ENG
H/W Driver HP DC5800 Desktop	ENG	32	C60-LU-OA-HPDC5800_DriverSet-32-ENG
H/W Driver HP 6000 Desktop	ENG	32	C60-LU-OA-HP6000_DriverSet-32-ENG
H/W Driver DELL 3011 Desktop	ENG	32	C60-LU-OA-HP3011_DriverSet-32-ENG
H/W Driver DELL 9010 Desktop	ENG	32	C60-LU-OA-HP9010_DriverSet-32-ENG

- การออกแบบการตั้งชื่อใน Active directory 2012 R2

เพื่อทำการเชื่อมกันระหว่าง Collection ใน SCCM กับ Active directory ผู้เขียนงานนิพนธ์จึงต้องตั้งชื่อใน Active directory ให้สื่อความหมายเหมือนกับชื่อใน SCCM โดยใน Active directory นั้นเราจะสร้างเป็นกลุ่มของคอมพิวเตอร์ผู้ใช้ (Security group) ดังภาพด้านล่างนี้



ภาพที่ 3-6 การตั้งชื่อกลุ่มผู้ใช้ใน Active directory (Security group)

คำอธิบายรายละเอียดของกลุ่มต่าง ๆ ดังนี้

ตารางที่ 3-9 รายละเอียดกลุ่มผู้ใช้ ที่ใช้ซอฟต์แวร์เดียวกัน (Collection)

กลุ่มผู้ใช้ซอฟต์แวร์ที่ใช้สำหรับบริษัทคาลโซนิคประเทศไทย (Local unique software)	
ชื่อกลุ่มผู้ใช้	รายละเอียด
CKT-LU-OA-Printer_5575-32-MUI	กลุ่มผู้ใช้เครื่องปริ้นเตอร์ Fuji Xerox 5575 โดยใช้ระบบปฏิบัติการวินโดว์ 32 บิต เฉพาะส่วนสำนักงาน
CKT-LU-OA-Printer_5575-64-MUI	กลุ่มผู้ใช้เครื่องปริ้นเตอร์ Fuji Xerox 5575 โดยใช้ระบบปฏิบัติการวินโดว์ 64 บิต เฉพาะส่วนสำนักงาน
CKT-LU-OA-IFS-32-ENG	กลุ่มผู้ใช้โปรแกรมประยุกต์ IFS โดยใช้ระบบปฏิบัติการวินโดว์ 32 บิต เฉพาะส่วนสำนักงาน
CKT-LU-ALL-Minitab_7-32-ENG	กลุ่มผู้ใช้โปรแกรมประยุกต์ Minitab โดยใช้ระบบปฏิบัติการวินโดว์ 32 บิต ทั้งหมด
CKT-LU-ALL-Minitab_7-64-ENG	กลุ่มผู้ใช้โปรแกรมประยุกต์ Minitab โดยใช้ระบบปฏิบัติการวินโดว์ 64 บิต ทั้งหมด

ตารางที่ 3-9 รายละเอียดกลุ่มผู้ใช้ ที่ใช้ซอฟต์แวร์เดียวกัน (Collection) (ต่อ)

กลุ่มผู้ใช้ซอฟต์แวร์มาตรฐานของบริษัทคาลโซนิค (Local standard software)	
ชื่อกลุ่มผู้ใช้	รายละเอียด
CKT-LS-CAD	กลุ่มผู้ใช้เครื่องออกแบบผลิตภัณฑ์ของบริษัท
CKT-LS-OA	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ในส่วนสำนักงาน
CKT-LS-ALL-AppSet-32-ENG	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ระบบปฏิบัติการวินโดวส์ 32 บิต ทั้งหมด
CKT-LS-ALL-AppSet-64-ENG	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ระบบปฏิบัติการวินโดวส์ 64 บิต ทั้งหมด
CKT-LS-OA-AppSet-32-ENG	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ระบบปฏิบัติการวินโดวส์ 32 บิต เฉพาะส่วนสำนักงาน
CKT-LS-OA-AppSet-64-ENG	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ระบบปฏิบัติการวินโดวส์ 64 บิต เฉพาะส่วนสำนักงาน
CKT-LS-CAD-AppSet-32-ENG	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ระบบปฏิบัติการวินโดวส์ 32 บิต เฉพาะเครื่องออกแบบ
CKT-LS-CAD-AppSet-64-ENG	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ระบบปฏิบัติการวินโดวส์ 64 บิต เฉพาะเครื่องออกแบบ
CKT-LS-Accounting	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกบัญชี
CKT-LS-Adviser	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์ที่ปรึกษาจากต่างประเทศ
CKT-LS-BOI	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกบีโอไอ
CKT-LS-Costing	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกต้นทุนบัญชี
CKT-LS-HR	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกทรัพยากรบุคคล
CKT-LS-IS	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกไอที
CKT-LS-MC	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนก MC
CKT-LS-MEC	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนก MEC
CKT-LS-MF	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกในส่วนโรงงาน
CKT-LS-MTCR	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนก MTCR
CKT-LS-PC	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกวางแผนการผลิต
CKT-LS-Purchasing	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกจัดซื้อจัดจ้าง

ตารางที่ 3-9 รายละเอียดกลุ่มผู้ใช้ ที่ใช้ซอฟต์แวร์เดียวกัน (Collection) (ต่อ)

กลุ่มผู้ใช้ซอฟต์แวร์มาตรฐานของบริษัทเทคโนโลยี (Local standard software)	
ชื่อกลุ่มผู้ใช้	รายละเอียด
CKT-LS-QA	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกคุณภาพ
CKT-LS-R&D	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนก R&D
CKT-LS-Sales	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกขาย
CKT-LS-Server	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์เซิร์ฟเวอร์
CKT-LS-Supply_Chain	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนกSupply_Chain
CKT-LS-V-UP	กลุ่มผู้ใช้เครื่องคอมพิวเตอร์แผนก V-UP

### 3.2.4 กำหนดช่วงไอพีเครือข่ายเครื่องผู้ใช้ใน SCCM boundaries

ตาราง 3-10 แสดงรายละเอียดของช่วงไอพีเครือข่ายเครื่องผู้ใช้ ที่มีการใช้งานอยู่ภายใต้โดเมนของบริษัทเทคโนโลยีประเทศไทย

ตารางที่ 3-10 รายละเอียดช่วงไอพีเครือข่ายของผู้ใช้ใน SCCM boundaries

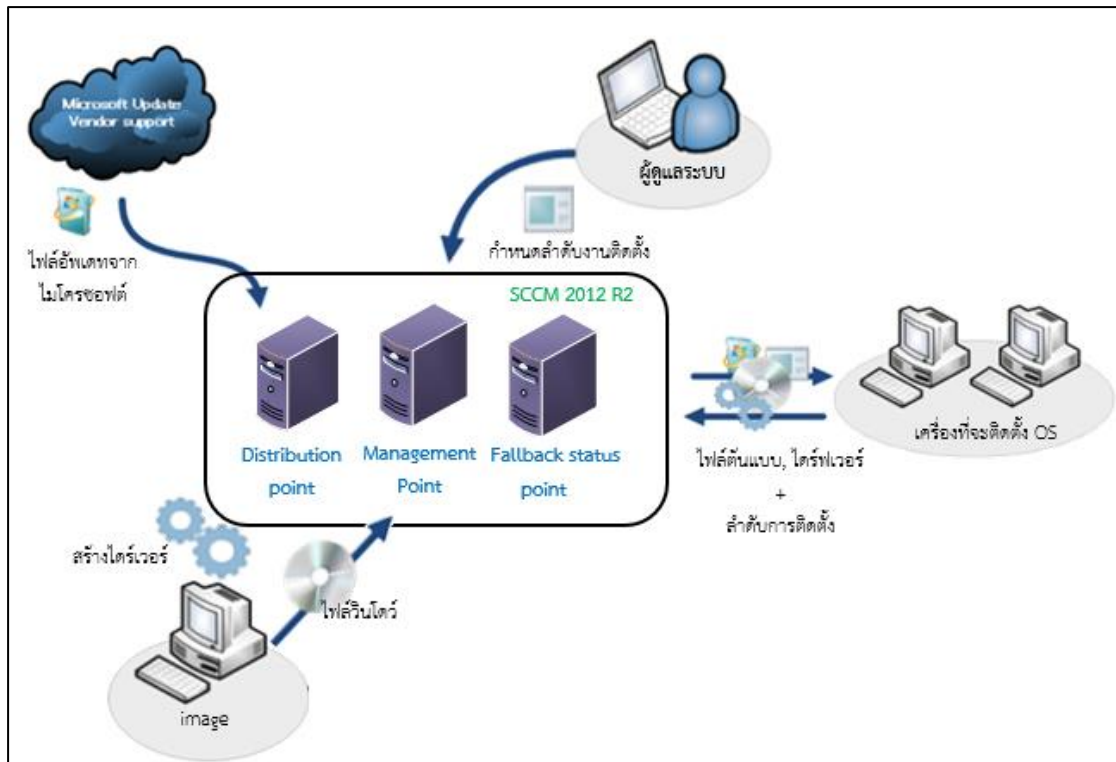
ช่วงเครือข่าย (Range network)	รายละเอียด (Description)
172.xx.aaa.1-172.xx.aaa.254	เครื่องเซิร์ฟเวอร์ VLanaaa
172.xx.bbb.1-172.xx.bbb.254	เครื่องผู้ใช้ ส่วนสำนักงานใหญ่ 1 VLanbbb
172.xx.ccc.1-172.xx.ccc.254	เครื่องผู้ใช้ ส่วนสำนักงานใหญ่ 2 VLanccc
172.xx.ddd.1-172.xx.ddd.254	เครื่องผู้ใช้งานสัญญาณเครือข่ายไร้สาย (Wi-Fi) VLandddd
172.xx.eee.1-172.xx.eee.254	เครื่องผู้ใช้ ส่วนโรงงาน 1 VLaneeee
172.xx.fff.1-172.xx.fff.254	เครื่องผู้ใช้ ส่วนโรงงาน 2 VLanffff
172.xx.ggg.1-172.xx.ggg.254	เครื่องผู้ใช้ ส่วนโรงงาน 4 VLannggg
172.xx.hhh.1-172.xx.hhh.254	เครื่องผู้ใช้ ส่วนโรงงาน 3 กม.22 VLanhhhh
172.xx.ii.1-172.xx.iii.254	เครื่องทดสอบระบบ SCCM และ CCTV VLaniii
172.xx.jjj.1-172.xx.jjj.254	เครื่องผู้ใช้งานสัญญาณเครือข่ายไร้สาย (Wi-Fi) VLanjjjj
172.xx.kkk.1-172.xx.kkk.254	เครื่อง deploy ระบบปฏิบัติการ VLankkkk
172.xx.ll.1-172.xx.ll.254	เครื่องผู้ใช้ ส่วนสำนักงานโรงงาน 3 กม.21 VLanllll

ตารางที่ 3-10 รายละเอียดช่วงไอพีเครือข่ายของผู้ใช้ใน SCCM boundaries (ต่อ)

ช่วงเครือข่าย	รายละเอียด
172.xx.mm.1-172.xx.mm.254	เครื่องผู้ใช้ ส่วนโรงงาน 3 กม.21 CPM Vlanmm
172.xx.nn.1-172.xx.nn.254	เครื่องผู้ใช้ ส่วนสำนักงานโรงงาน 3 กม.22 VLannn
172.xx.oo.1-172.xx.oo.254	เครื่องผู้ใช้งานสัญญาณเครือข่ายไร้สาย (Wi-Fi) VLanoo

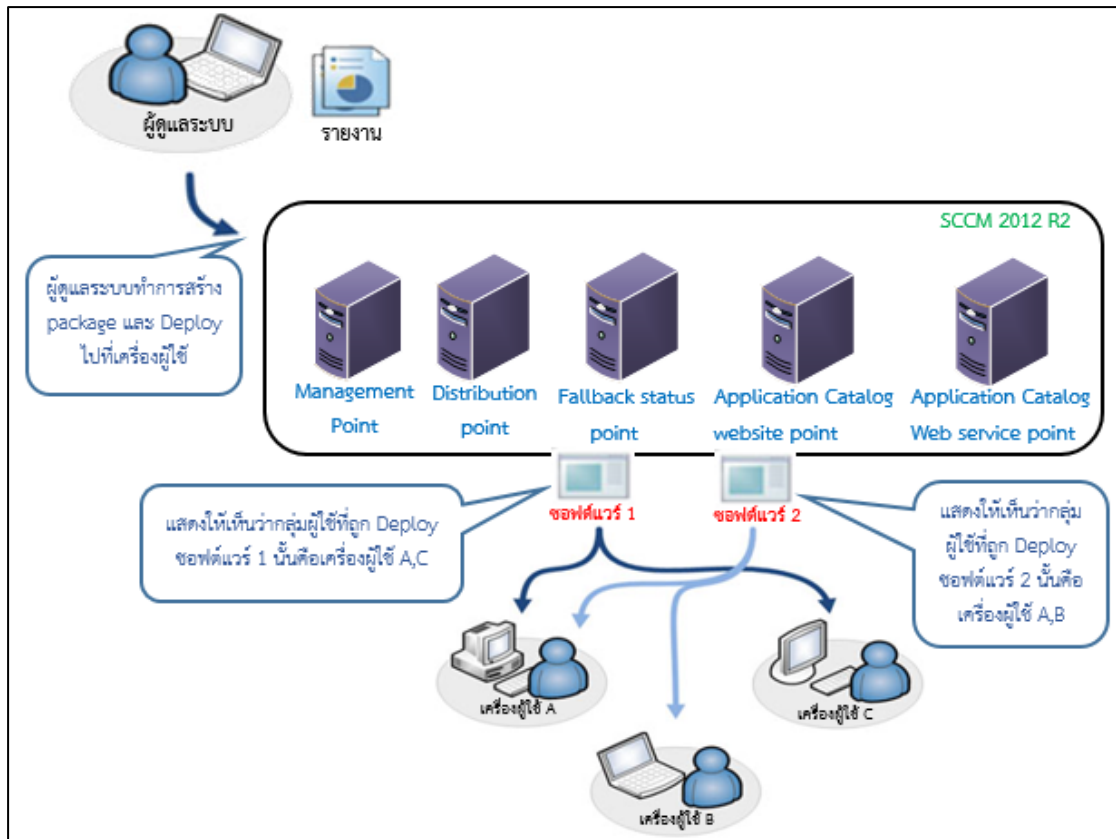
### 3.2.5 การใช้งานระบบ SCCM 2012 R2 จะประกอบไปด้วยการทำงานดังนี้

1. การติดตั้งระบบปฏิบัติการวินโดวส์ผ่านทางระบบ SCCM 2012 R2
  2. การ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้
  3. การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง
  4. การปรับปรุง (Update) วินโดวส์จากเซิร์ฟเวอร์ SCCM 2012 R2
  5. การปรับปรุง (Update) โปรแกรมป้องกันไวรัส Endpoint protection point เครื่องเซิร์ฟเวอร์และเครื่องผู้ใช้
  6. การรีโมทไปที่เครื่องผู้ใช้ผ่านระบบ SCCM 2012 R2
  7. การเรียกดูรายงาน
    - การติดตั้งระบบปฏิบัติการวินโดวส์ผ่านระบบ SCCM 2012 R2
- การติดตั้งระบบปฏิบัติการวินโดวส์ผ่าน SCCM 2012 R2 นั้น ผู้ดูแลระบบจะต้องสร้างไฟล์ต้นแบบก่อน โดยการนำเครื่องต้นแบบพร้อมไดร์เวอร์ที่เกี่ยวข้องมาทำเป็นไฟล์ในระบบ SCCM 2012 R2 แล้วจากนั้น สั่ง deploy ไปที่เครื่องที่ต้องการ โดยระบุ Mac address และต่อ VLAN ที่เตรียมไว้สำหรับการ deploy ระบบปฏิบัติการวินโดวส์ด้วย ดังภาพที่ 3-7



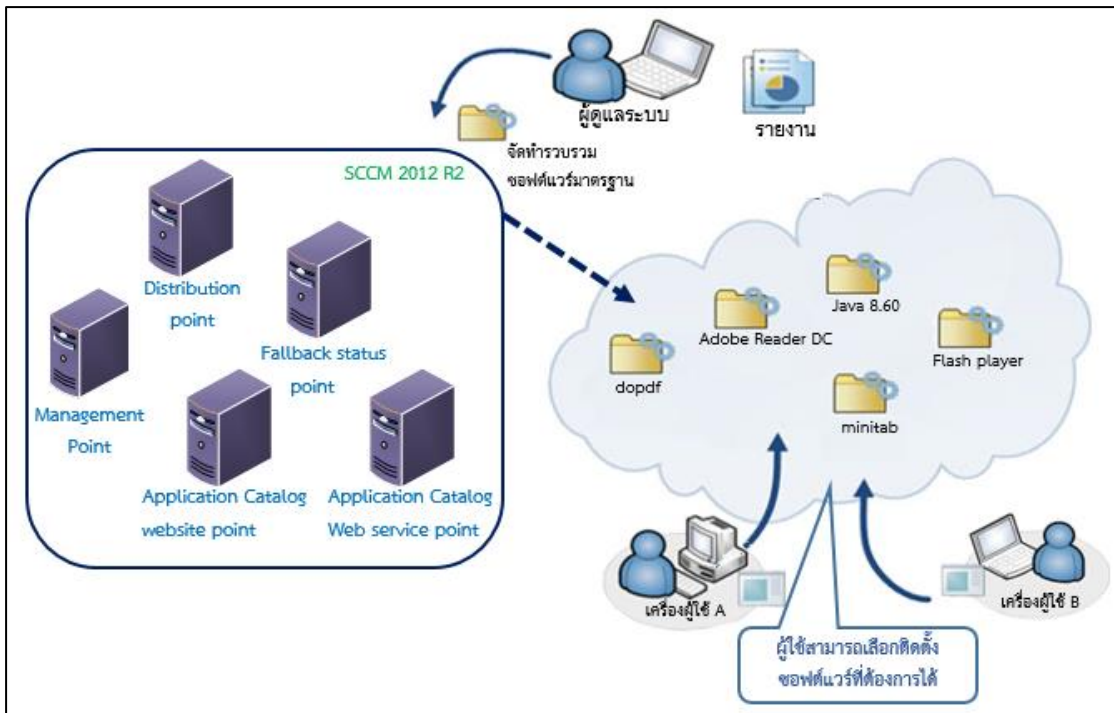
ภาพที่ 3-7 การติดตั้งระบบปฏิบัติการวินโดวส์ผ่าน SCMM 2012 R2

- การ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้
- การกระจายโปรแกรมประยุกต์โดยผ่านระบบ SCCM ไปที่เครื่องผู้ใช้งาน โดยการกระจายตามกลุ่มของผู้ใช้งานซอฟต์แวร์แต่ละประเภท ดังภาพที่ 3-8



ภาพที่ 3-8 การ Deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้

- การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง  
 การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งได้เอง และสามารถเลือกติดตั้งโปรแกรมที่ทางผู้ดูแลระบบได้จัดเตรียมไว้ให้แล้ว ดังภาพที่ 3-9

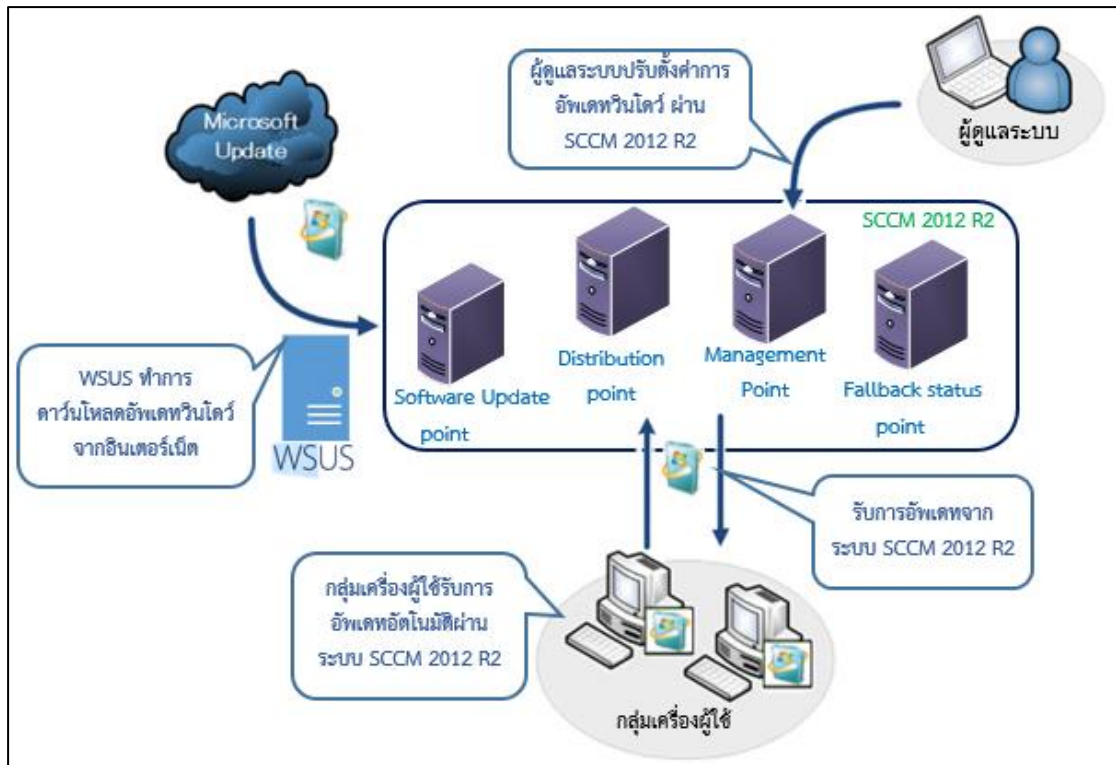


ภาพที่ 3-9 การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง

- การอัปเดตระบบปฏิบัติการวินโดวส์

การอัปเดตระบบปฏิบัติการวินโดวส์ ผู้ดูแลระบบกำหนดค่าการอัปเดต โดยให้เซิร์ฟเวอร์ SCCM ไปดาวน์โหลดอัปเดตโดยตรงกับเว็บไซต์ไมโครซอฟต์ ผ่านทางอินเทอร์เน็ต โดย ผู้เขียนงาน นิพนธ์ได้กำหนดนโยบายโปรแกรม SCCM (Primary server) ให้อัปเดตเครื่องผู้ใช้ทุก ๆ วันพุธ เวลาบ่ายโมงตรง ดังแสดงในภาพที่ 3-10

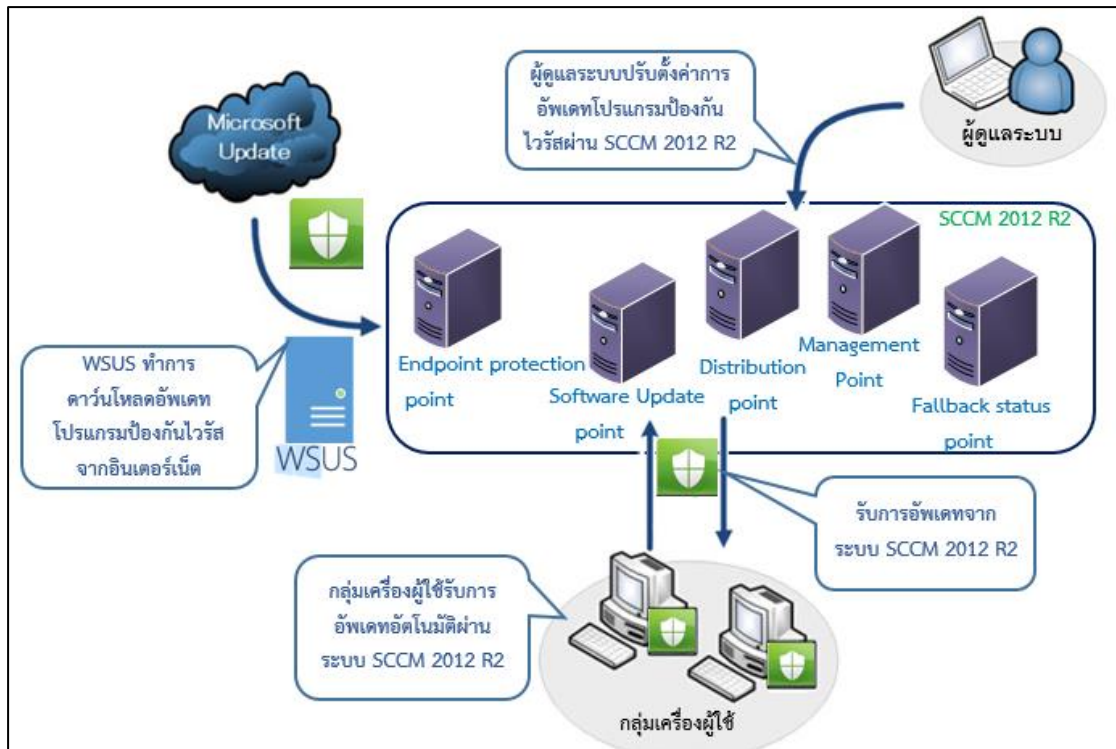




ภาพที่ 3-10 การอัปเดตระบบปฏิบัติการวินโดวส์

- การอัปเดตซอฟต์แวร์ป้องกันไวรัส Endpoint protection point

การอัปเดตโปรแกรมป้องกันไวรัสไมโครซอฟต์ Endpoint protection point ผู้ดูแลระบบ กำหนดค่าการอัปเดต โดยให้เซิร์ฟเวอร์ SCCM ไปดาวน์โหลดอัปเดตโดยตรงกับเว็บไซต์ไมโครซอฟต์ ผ่านทางอินเทอร์เน็ต โดยผู้เขียนงานนิพนธ์ได้กำหนดนโยบายให้โปรแกรม SCCM (Primary server) อัปเดตเครื่องผู้ใช้ทุก ๆ วันเวลาบ่ายโมงตรง ดังแสดงในภาพที่ 3-11



ภาพที่ 3-11 การอัปเดตโปรแกรมป้องกันไวรัส Endpoint protection point

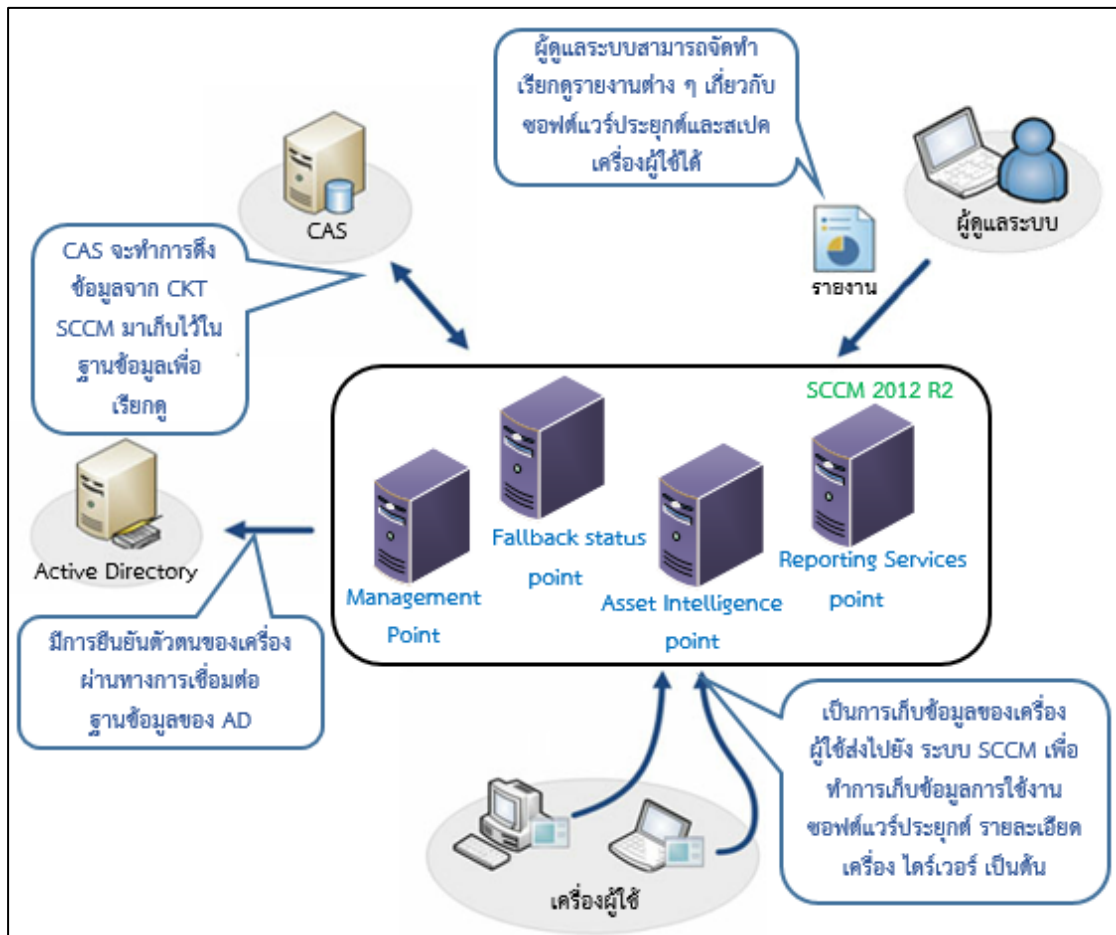
- การรีโมทไปที่เครื่องผู้ใช้ผ่านระบบ SCCM 2012 R2
- การรีโมทไปที่เครื่องผู้ใช้เพื่อช่วยเหลือหรือตรวจสอบการทำงานของโปรแกรมจากผู้ที่มีสิทธิ์ในการรีโมท โดยแสดงการรีโมทดังภาพด้านล่าง



ภาพที่ 3-12 การรีโมทเครื่องผู้ใช้ผ่านระบบ SCCM 2012 R2

ภาพที่ 3-12 แสดงการรีโมทจากเครื่องผู้ที่มีสิทธิ์รีโมทเครื่องผู้ใช้ ผ่านระบบ SCCM โดยการรีโมท จะต้องเปิดโปรแกรมที่หน้าจอ (Desktop) เพื่อทำการรีโมทไปที่เครื่องผู้ใช้งาน และระบบ จะทำการตรวจสอบสิทธิ์ หากมีสิทธิ์ SCCM จะยอมให้ผู้ร้องขอรีโมทไปที่เครื่องของผู้ใช้ได้ (โดยการรีโมทเครื่องผู้ใช้นั้น ผู้ร้องขอสามารถระบุเครื่องปลายทาง โดยใช้บัญชีของผู้ใช้ที่อยู่ใน AD หรือ ใช้ไอพีเครื่องคอมพิวเตอร์ก็ได้)

ผู้ดูแลระบบสามารถเรียกดูรายงานต่าง ๆ จากระบบ SCCM ได้ โดยแสดงรายละเอียดดังภาพด้านล่าง



ภาพที่ 3-13 การเรียกดูรายงานจากระบบ SCCM 2012 R2

ภาพที่ 3-13 แสดงการเรียกดูรายงานต่าง ๆ ผ่านระบบ SCCM โดยการเรียกดูรายงานจะทำที่เครื่องหลัก (SCCM primary server) ผู้ดูแลระบบสามารถเรียกดูรายงานต่อไปนี้

- เรียกดูรายงานอุปกรณ์คอมพิวเตอร์ (สเปคเครื่อง, รุ่น, ยี่ห้อ)
- เรียกดูรายงานโปรแกรมประยุกต์
- เรียกดูรายงานการอัปเดตวินโดวส์ (Patch windows update)
- เรียกดูรายงานการอัปเดตโปรแกรมป้องกันไวรัส
- เรียกดูรายงานการตรวจสอบสถานะการ deploy โปรแกรมประยุกต์

### 3.3 การติดตั้งและตั้งค่าระบบ SCCM 2012 R2

ก่อนการติดตั้ง SCCM ผู้เขียนงานนิพนธ์ต้องเข้าไปใน Service manager ของ วินโดว์เซิร์ฟเวอร์ (ที่เป็น Primary site) เพื่อเปิดใช้งาน service ต่าง ๆ ดังต่อไปนี้

Web Server (IIS)

- WebDAV Publishing
- Health and Diagnostics

.Net Framework 3.5 Features

- HTTP Activation
- Non-HTTP Activation

.Net Framework 4.5 Features

- ASP.Net.4.5
- HTTP Activation
- Message Queuing (MSMQ) Activation
- TCP Activation
- TCP Port Sharing

Background Intelligent Transfer Service (BITS)

Remote Differential Compression

Remote Server Administration Tools

SMB 1.0

CIFS File Sharing support

Windows Server Update Services

- WSUS Services
- Database

User Interfaces and Infrastructure

Management Tools

- IIS 6 Scripting Tools
- IIS 6 WMI Compatibility

Security

- Windows Authentication

การติดตั้งและตั้งค่าระบบ SCCM 2012 R2 นั้น ผู้เขียนงานนิพนธ์ได้จัดทำและรวบรวม วิธีการติดตั้งและปรับแต่งค่าต่าง ๆ ไว้ในภาคผนวก ดังรายละเอียดข้างล่างนี้

ตารางที่ 3-11 Service point ของ SCCM ที่ต้องเปิดเพื่อให้บริการที่ได้กล่าวถึงในหัวข้อ 3.2 (ภาพที่ 3-7 ถึง 3-14)

รายละเอียดการใช้งานระบบ SCCM 2012 R2	*บริการที่ต้องเปิดใช้งาน									
	1	2	3	4	5	6	7	8	9	10
การติดตั้งระบบปฏิบัติการวินโดวส์ผ่านทางระบบ SCCM 2012 R2	<input type="checkbox"/>		✓	✓			✓	<input type="checkbox"/>		
การ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้	✓	✓	✓	✓			✓			
การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง	✓	✓	✓	✓			✓			
การปรับปรุง (Update) วินโดวส์จากเซิร์ฟเวอร์ SCCM 2012 R2			✓	✓	✓		✓		<input type="checkbox"/>	✓
การปรับปรุง (Update) โปรแกรมป้องกันไวรัส Endpoint protection point			✓	✓	✓		✓	✓		✓
การรีโมทไปที่เครื่องผู้ใช้ผ่านระบบ SCCM 2012 R2				✓			✓			
การเรียกดูรายงาน				✓		✓	✓			✓

\*บริการที่ต้องเปิดใช้งาน อธิบายตามหมายเลข ดังนี้

1. Application Catalog web service point
2. Application Catalog website point
3. Distribution point
4. Fallback status point
5. Software update point
6. Asset Intelligence point
7. Management point
8. Endpoint protection point
9. Reporting services point
10. Windows Server Update Services

ตารางที่ 3-12 รายละเอียดวิธีการติดตั้งและตั้งค่าระบบ SCCM 2012 R2

รายละเอียด	หน้า
ติดตั้งระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2012	113
สร้าง Boundary	124
ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์หลัก (Primary site)	126
ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์ฐานข้อมูล (Database site)	134
ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์สาขาบางนา (Distribution point server)	146
ติดตั้ง Agent ที่เครื่องผู้ใช้ (Client setting)	155
สร้างกลุ่มคอมพิวเตอร์ของผู้ใช้ใน SCCM (Device collections)	159
ตั้งค่าส่วนการ deploy ระบบปฏิบัติการ (Operating system deployment)	169
เปิดใช้ PXE on Distribution Point	174
สร้างโปรแกรมประยุกต์สำหรับ deploy (Application Management)	177
การ deploy โปรแกรมประยุกต์ไปที่ Collection เครื่องผู้ใช้	181
การควบคุมจากทางระยะไกล (Helpdesk remote assistance)	187

### 3.4 ทดสอบระบบ SCCM 2012 R2 (Testing)

ก่อนการใช้งานจริง ผู้เขียนงานนิพนธ์ได้ทดสอบระบบ SCCM 2012 R2 ดังนี้

1. ทดสอบการทำงานของฐานข้อมูล ในกรณีเครื่องฐานข้อมูลตัวหลักเกิดปัญหาในระบบปฏิบัติการวินโดวส์ หรือ เครื่องหยุดการทำงาน เครื่องที่เป็นตัวสำรองจะต้องทำหน้าที่แทนตัวหลักทันที

2. ทดสอบการติดตั้งระบบปฏิบัติการวินโดวส์ โดยทำการติดตั้งจำนวน 3 โมเดล

3. ทดสอบ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้ โดยกำหนดผู้ใช้จำนวน 5 Collections

4. ทดสอบการอัปเดตวินโดวส์ โดยเรียกดูผลการอัปเดตจำนวน 3 กลุ่ม

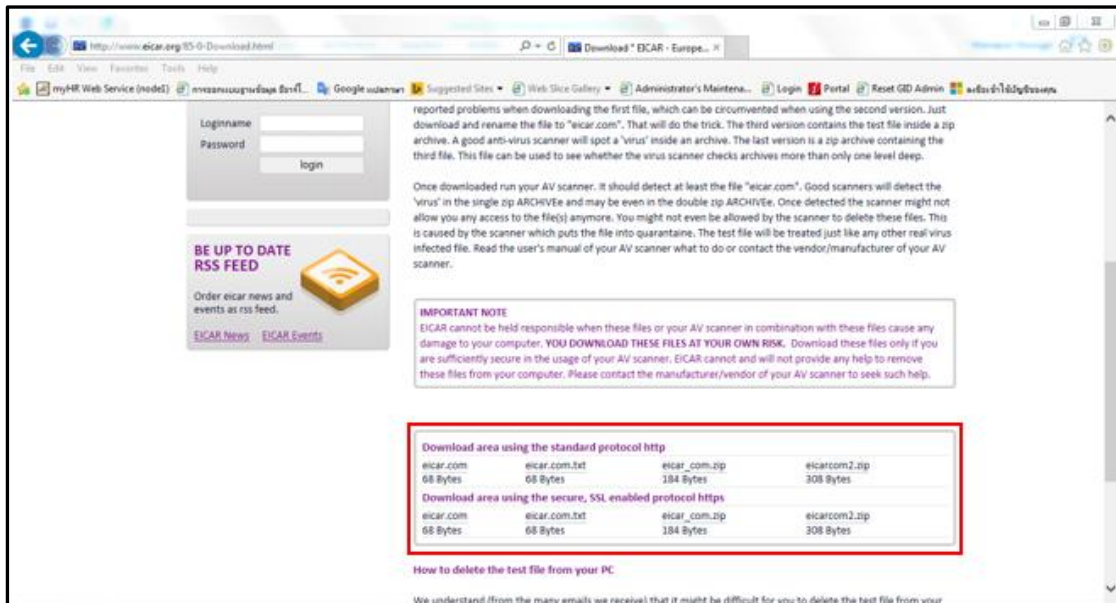
5. การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง โดยทดสอบจำนวน 3 เครื่อง

6. ทดสอบเรียกดูรายงานสเปคเครื่องผู้ใช้จำนวน 3 กลุ่ม

7. ทดสอบ Remote control viewer ไปที่เครื่องผู้ใช้จำนวน 3 เครื่อง

8. ทดสอบติดตั้งโปรแกรมป้องกันไวรัส Endpoint protection point โดยติดตั้งกลุ่มผู้ใช้จำนวน 3 เครื่อง และทดสอบการทำงานของโปรแกรมป้องกันไวรัส Endpoint protection point โดยการดาวน์โหลดไวรัสจากเว็บไซต์ 3 เว็บ ดังนี้

1. <http://www.eicar.org/85-0-Download.html>

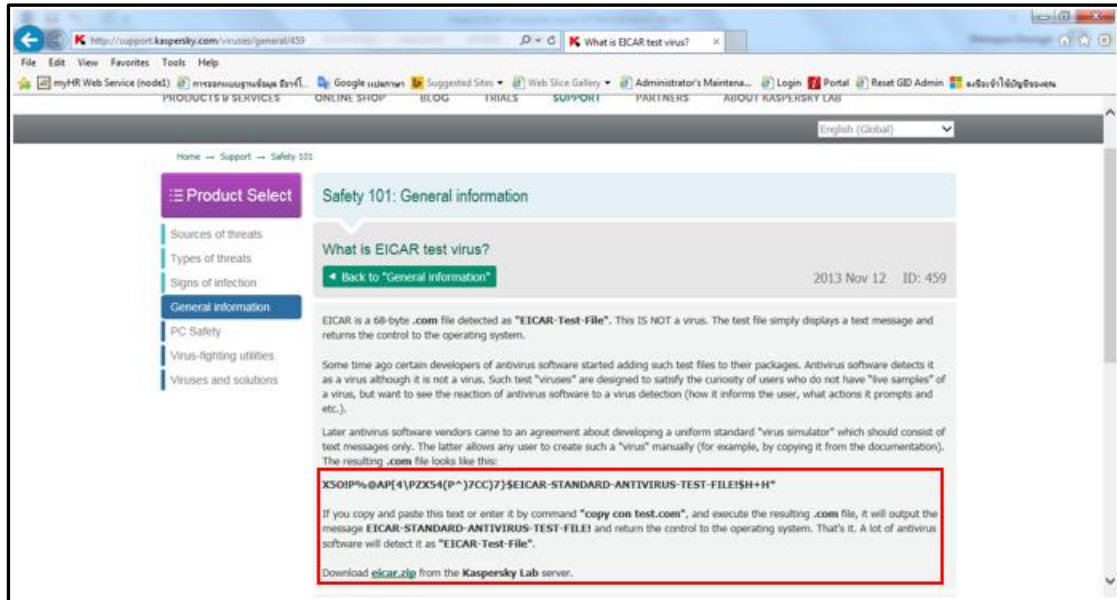


ภาพที่ 3-14 เว็บไซต์ Eicar.org สำหรับการทดสอบโปรแกรมป้องกันไวรัส

จากภาพที่ 3-14 เข้าสู่หน้าเว็บแล้ว <http://www.eicar.org/85-0-Download.html> และดาวน์โหลดไฟล์ตามกรอบสี่เหลี่ยมสีแดง เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส ว่าจะสามารถป้องกันหรือลบไฟล์ที่เป็นไวรัสได้ทันทีเลยหรือไม่



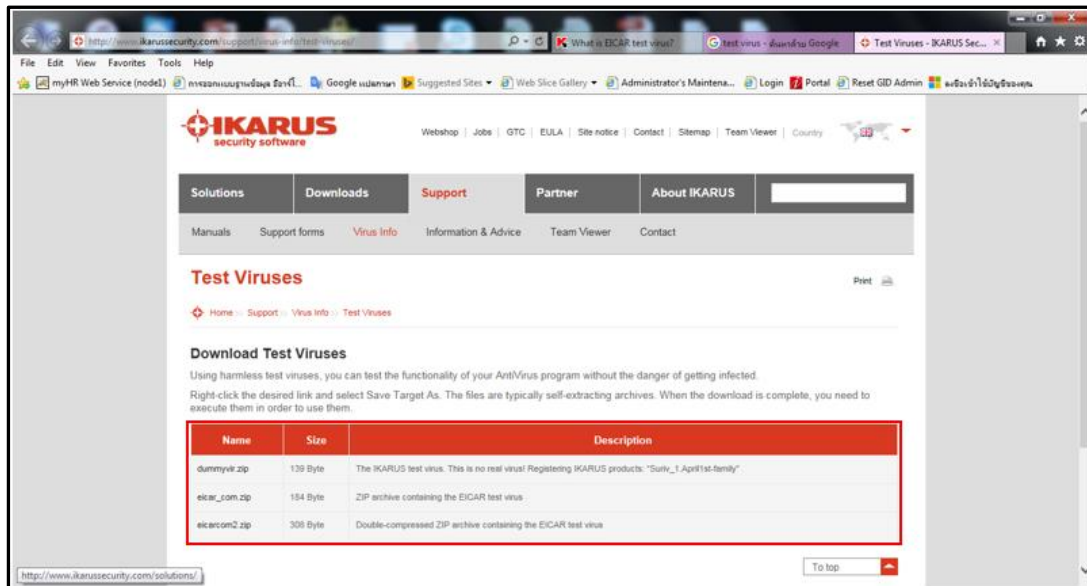
## 2. <http://support.kaspersky.com/viruses/general/459>



ภาพที่ 3-15 เว็บไซต์ [support.kaspersky.com](http://support.kaspersky.com) สำหรับการทดสอบโปรแกรมป้องกันไวรัส

จากภาพที่ 3-15 เข้าสู่หน้าเว็บ <http://support.kaspersky.com/viruses/general/459> แล้วดาวน์โหลดไฟล์ตามกรอบสี่เหลี่ยมสีแดง เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส ว่าจะสามารถป้องกันหรือลบไฟล์ที่เป็นไวรัสได้ทันทีเลยหรือไม่

3. <http://www.ikarussecurity.com/support/virus-info/test-viruses/>



ภาพที่ 3-16 เว็บไซต์ ikarussecurity.com สำหรับการทดสอบโปรแกรมป้องกันไวรัส

จากภาพที่ 3-16 เข้าสู่หน้าเว็บ <http://www.ikarussecurity.com/support/virus-info/test-viruses/> แล้วดาวน์โหลดไฟล์ตามกรอบสี่เหลี่ยมสีแดง เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส ว่าจะสามารถป้องกันหรือลบไฟล์ที่เป็นไวรัสได้ทันทีเลยหรือไม่

### 3.5 สังเกตการณ์ การทำงานระบบ SCCM 2012 R2 (Monitoring)

ผู้เขียนงานนิพนธ์ได้จัดทำแผนสำหรับสังเกตการณ์ทำงานของระบบ SCCM ในการ deploy โปรแกรมประยุกต์ต่าง ๆ โดยเฝ้าระวังสังเกตการณ์เพื่อต้องการตอบคำถาม 5 ข้อต่อไปนี้

1. ซอฟต์แวร์ที่เป็นกลุ่มมาตรฐานของบริษัทสามารถ deploy ได้ทุกตัวไหม และใช้เวลาเท่าไร โดยโปรแกรมประยุกต์ที่เป็นมาตรฐานของบริษัทมีดังนี้

- 7zip
- IE11
- Firefox 46.0
- Acrobat Reader DC MUI
- Flash player
- Java 8 Update 91
- MS Office 2013
- doPDF
- Antivirus Endpoint protection point
- LEXiTRON Dictionary 2.6

2. ความเร็วในการ Deploy OS เครื่อง HP EliteDesk 705 G1 โดยทดสอบ deploy ทีละ 1, 5, 10, 20 และ 30 เครื่อง

3. เครื่องที่อยู่ในโปรดักชั่นจริงสามารถอัปเดตวินโดวส์ได้หรือไม่

4. เครื่องที่อยู่ในโปรดักชั่นจริงสามารถอัปเดตโปรแกรมป้องกันไวรัสได้กี่เครื่อง

## บทที่ 4

### ผลการดำเนินงาน

ในบทนี้ ผู้เขียนงานนิพนธ์จะกล่าวถึงผลการดำเนินงานการจัดการและการกำหนดค่าซอฟต์แวร์จากส่วนกลาง โดยใช้ซอฟต์แวร์ SCCM 2012 R2 (System Center Configuration Manager) ของบริษัทไมโครซอฟต์ ซึ่งเป็นผลที่ได้จากการดำเนินงานออกแบบระบบในบทที่ 3 ดังนี้

#### 4.1 ผลการติดตั้งเครื่องเซิร์ฟเวอร์สำหรับระบบ SCCM 2012 R2 ตามสเปคที่กำหนด

จากการออกแบบในบทที่ 3 ผู้เขียนงานนิพนธ์ได้ติดตั้งระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2012 R2, กำหนดชื่อเครื่องคอมพิวเตอร์, เข้าร่วมโดเมน calsonickansei.co.jp และกำหนดไอพีสำหรับเครื่องเซิร์ฟเวอร์ระบบ SCCM 2012 R2 ดังตารางที่ 4-1

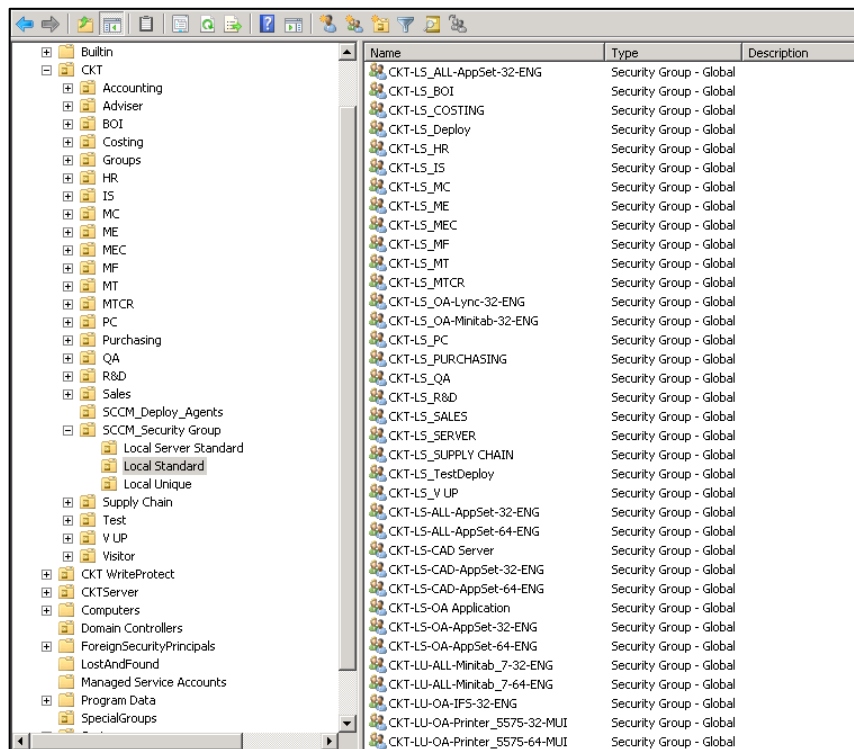
ตารางที่ 4-1 ผลการกำหนดค่าเครื่องเซิร์ฟเวอร์ระบบ SCCM 2012 R2

เซิร์ฟเวอร์	ชื่อเครื่อง	ไอพี	ระบบปฏิบัติการ	หน่วยความจำ	ฮาร์ดดิสก์ (c:)
Primary site	CKTSERVER022	172.xx.xxx.44	Windows server 2012 R2	32 GB	120 GB
Site database 01	CKTSERVER023	172.xx.xxx.45	Windows server 2012 R2	32 GB	120 GB
Site database 02	CKTSERVER024	172.xx.xxx.46	Windows server 2012 R2	32 GB	120 GB
Distribution point	CKTSERVER025	172.xx.xx.1	Windows server 2012 R2	16 GB	120 GB

ตารางที่ 4-1 แสดงผลการกำหนดค่าเครื่องเซิร์ฟเวอร์สำหรับระบบ SCCM 2012 R2 โดยค่าต่าง ๆ ในตารางได้มาจากการออกแบบในบทที่ 3 และผู้เขียนงานนิพนธ์ได้ลงทะเบียนเปิดใช้งานลิขสิทธิ์วินโดวส์เรียบร้อยแล้ว

## 4.2 ผลการสร้างกลุ่ม Security group ใน Active directory

ผู้เขียนงานนิพนธ์ได้สร้างกลุ่มของคอมพิวเตอร์ (ชนิดของกลุ่มเป็น Security group) ใน Active directory โดยแบ่งตามแผนกหรือซอฟต์แวร์ที่ใช้งาน ดังภาพที่ 4-1



Name	Type	Description
CKT-LS_ALL-AppSet-32-ENG	Security Group - Global	
CKT-LS_BOI	Security Group - Global	
CKT-LS_COSTING	Security Group - Global	
CKT-LS_Deploy	Security Group - Global	
CKT-LS_HR	Security Group - Global	
CKT-LS_IS	Security Group - Global	
CKT-LS_MC	Security Group - Global	
CKT-LS_ME	Security Group - Global	
CKT-LS_MEC	Security Group - Global	
CKT-LS_MF	Security Group - Global	
CKT-LS_MT	Security Group - Global	
CKT-LS_MTCR	Security Group - Global	
CKT-LS_OA-Lync-32-ENG	Security Group - Global	
CKT-LS_OA-Minitab-32-ENG	Security Group - Global	
CKT-LS_PC	Security Group - Global	
CKT-LS_PURCHASING	Security Group - Global	
CKT-LS_QA	Security Group - Global	
CKT-LS_R&D	Security Group - Global	
CKT-LS_SALES	Security Group - Global	
CKT-LS_SERVER	Security Group - Global	
CKT-LS_SUPPLY CHAIN	Security Group - Global	
CKT-LS_TestDeploy	Security Group - Global	
CKT-LS_V UP	Security Group - Global	
CKT-LS-ALL-AppSet-32-ENG	Security Group - Global	
CKT-LS-ALL-AppSet-64-ENG	Security Group - Global	
CKT-LS-CAD Server	Security Group - Global	
CKT-LS-CAD-AppSet-32-ENG	Security Group - Global	
CKT-LS-CAD-AppSet-64-ENG	Security Group - Global	
CKT-LS-OA Application	Security Group - Global	
CKT-LS-OA-AppSet-32-ENG	Security Group - Global	
CKT-LS-OA-AppSet-64-ENG	Security Group - Global	
CKT-LU-ALL-Minitab_7-32-ENG	Security Group - Global	
CKT-LU-ALL-Minitab_7-64-ENG	Security Group - Global	
CKT-LU-OA-IFS-32-ENG	Security Group - Global	
CKT-LU-OA-Printer_5575-32-MUI	Security Group - Global	
CKT-LU-OA-Printer_5575-64-MUI	Security Group - Global	

ภาพที่ 4-1 กลุ่มของผู้ใช้คอมพิวเตอร์ที่ใช้ซอฟต์แวร์เดียวกัน (Security group)

ภาพที่ 4-1 แสดงผลการสร้างกลุ่มของคอมพิวเตอร์ที่ใช้ซอฟต์แวร์เดียวกัน โดยผู้เขียนได้สร้างกลุ่มชนิด Security สำหรับกลุ่มผู้ใช้ซอฟต์แวร์มาตรฐานที่บริษัทกำหนด จำนวน 67 กลุ่ม และกลุ่มผู้ใช้ซอฟต์แวร์ท้องถิ่นที่ถูกใช้ในเครื่องภายในบริษัทในประเทศไทย (Local unique) จำนวน 26 กลุ่ม ทั้งนี้ผู้จัดทำงานนิพนธ์จะตั้งค่าใน SCCM 2012 R2 ให้อัปเดตข้อมูล Collection คอมพิวเตอร์ให้สอดคล้องกับข้อมูลกลุ่มใน AD สัปดาห์ละ 1 ครั้ง ทุกวันเสาร์ เวลาเที่ยงคืน

### 4.3 สร้าง Collection ใน SCCM 2012 R2

ในขั้นตอนนี้ ผู้จัดทำงานนิพนธ์ได้สร้าง Collection ใน SCCM 2012 R2 ทั้งหมด 130 Collection (โดย Collection คือ กลุ่มของคอมพิวเตอร์ที่ถูกออกแบบมาให้ใช้ซอฟต์แวร์เดียวกัน) จากนั้น กำหนดกลุ่มคอมพิวเตอร์ใน Active directory ให้มาอยู่ใน Collection ที่ได้สร้างไว้ ตามการออกแบบดังนี้

1. จากการออกแบบและตั้งชื่อ Device collection ใน SCCM 2012 R2 ผู้เขียนงานนิพนธ์ได้สร้างโพลเดอร์ C60 (รหัสของประเทศไทย) และ สร้างโพลเดอร์ย่อย 2 โพลเดอร์ในโพลเดอร์ C60 เพื่อแยก Collection ระหว่างโปรแกรมประยุกต์ (AppControl) และไดร์ฟเวอร์อุปกรณ์ต่าง ๆ (DevControl) ผู้เขียนงานนิพนธ์ได้สร้างกลุ่ม Device collection ตามการออกแบบในบทที่ 3 ตามตารางที่ 4-2

ตารางที่ 4-2 จำนวน Device collection

โพลเดอร์	จำนวน Device Collection
AppControl	104
DevControl	26

ตารางที่ 4-2 แสดงให้เห็นได้ว่าโพลเดอร์ AppControl มีจำนวน 104 Collection ซึ่งเป็น Collection ของแผนกและใช้ซอฟต์แวร์เดียวกัน ส่วน DevControl จะเป็น Collection ไดร์ฟเวอร์ต่าง ๆ มีทั้งหมด 26 กลุ่ม

#### 4.4 กำหนดช่วงไอพีเครือข่ายของผู้ใช้ใน SCCM 2012 R2 boundaries

ผู้เขียนงานนิพนธ์ได้กำหนดช่วงไอพีที่ใช้งานสำหรับกลุ่มของผู้ใช้คอมพิวเตอร์ที่ใช้ซอฟต์แวร์เดียวกัน ดังภาพที่ 4-2

Icon	Boundary	Type	Description	Group Count	Date Created
	172.1.0.0	IP subnet	C60-Server_Vlan128	1	6/23/2015 4:08 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office 1	2	3/24/2015 5:57 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office 2	2	3/24/2015 6:01 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office Wifi...	2	3/24/2015 6:02 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office Plan...	2	3/24/2015 6:02 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office Plan...	2	3/24/2015 8:31 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office Plan...	2	3/24/2015 8:32 PM
	172.1.0.0	IP subnet	C60-CKT LCB Office 1	2	3/24/2015 9:00 PM
	172.1.0.0	IP address range	C60-CKT HQ Test	1	7/21/2015 10:45 PM
	172.1.0.0	IP subnet	C60-CKT HQ Office Wifi...	2	3/24/2015 8:32 PM
	172.1.0.0	IP subnet	C60-CKT-Deploy OS	1	6/4/2015 11:48 AM
	172.1.0.0	IP subnet	C60-CKT NMT Office K...	2	3/24/2015 8:33 PM
	172.1.0.0	IP subnet	C60-CKT NMT Office X1...	2	3/24/2015 8:34 PM
	172.1.0.0	IP subnet	C60-CKT NMT Office K...	2	3/24/2015 8:36 PM
	172.1.0.0	IP subnet	C60-CKT NMT Office Wi...	2	3/24/2015 8:35 PM

ภาพที่ 4-2 ช่วงไอพีเครือข่ายของผู้ใช้ (SCCM 2012 R2 Boundaries)

ภาพที่ 4-2 แสดงการกำหนดช่วงไอพีเครือข่ายของผู้ใช้ ผู้เขียนงานนิพนธ์ได้ระบุรายละเอียดแต่ละช่วงไอพี ที่ใช้งานในแต่ละพื้นที่ด้วย

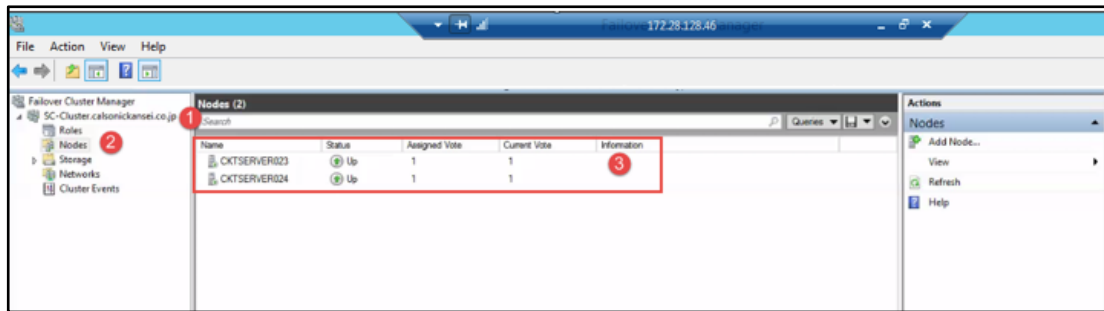
#### 4.5 ผลการทดสอบการทำงานของระบบ SCCM 2012 R2 (Testing)

ผู้เขียนงานนิพนธ์ได้ทดสอบประสิทธิภาพการทำงานของระบบจากการออกแบบในบทที่ 3 ซึ่งมีรายละเอียดในการทดสอบ ดังนี้

##### 4.5.1 การทดสอบการทำงานของระบบฐานข้อมูล

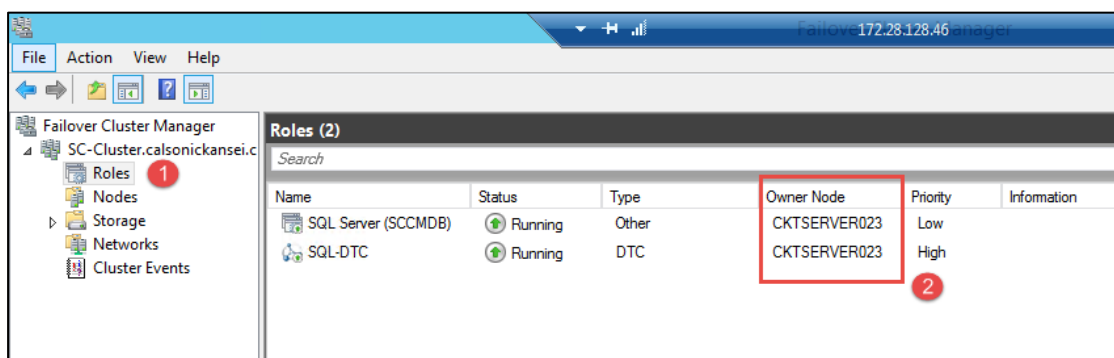
ผู้เขียนงานนิพนธ์ได้ทดสอบการสำรองข้อมูลซึ่งกันและกัน (Active standby) ของ SQL Server 2012 R2 ที่ทำ Cluster กัน ซึ่งเครื่องที่ทำหน้าที่ Active คือฐานข้อมูลตัวที่ 1 (ชื่อเครื่อง CKTSERVER023) และเครื่องที่ทำหน้าที่ Standby คือฐานข้อมูลตัวที่ 2 (ชื่อเครื่อง CKTSERVER024) โดยขั้นตอนการทดสอบดังนี้

ผู้เขียนงานนิพนธ์ล็อกอินเข้าเครื่องเซิร์ฟเวอร์ฐานข้อมูล ตัวที่ 2 (CKTSERVER024) จากนั้นเปิดโปรแกรม failover cluster manager และคลิกเลือกที่ SC- Cluster. calsonickansei.co.jp จากนั้นคลิกเลือก Nodes (โหนด) จะได้ดังภาพ 4-3



ภาพที่ 4-3 ตรวจสอบสถานะของโหนดเซิร์ฟเวอร์ฐานข้อมูลทั้งสองเครื่อง

ภาพที่ 4-3 แสดงให้เห็นว่าเครื่องฐานข้อมูลทั้งสองเครื่อง มีสถานะ การออนไลน์ปกติ ผู้เขียนงานนิพนธ์ได้ตรวจสอบดูว่าเครื่องฐานข้อมูลที่ทำหน้าที่เป็นฐานข้อมูลหลัก (Active) คือเครื่องเซิร์ฟเวอร์ตัวไหน โดยเข้าไปที่ Roles จะได้ดังภาพที่ 4-4

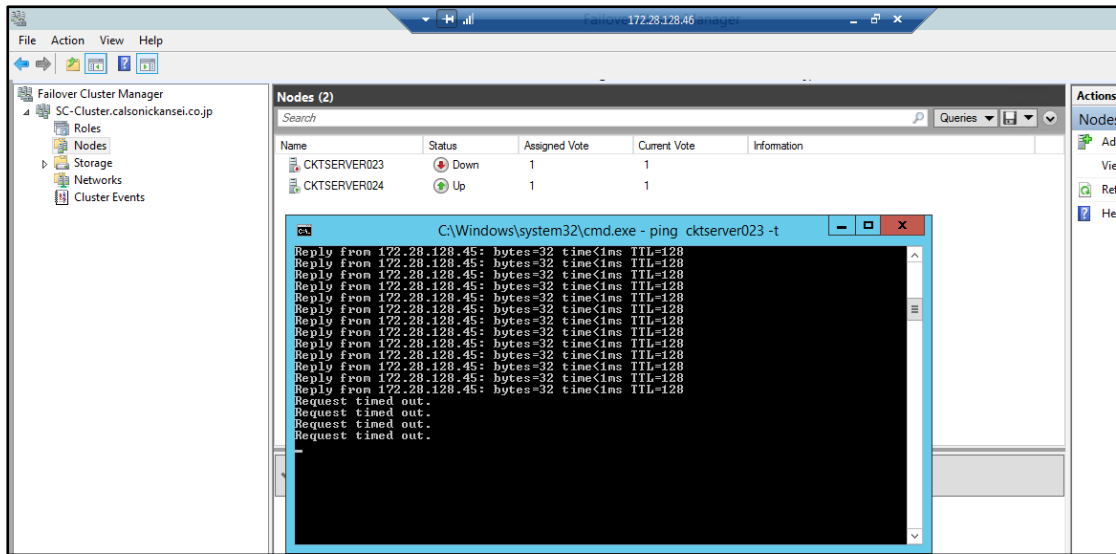


ภาพที่ 4-4 ตรวจสอบระบบฐานข้อมูลหลักทำงานที่เครื่องไหน

ภาพที่ 4-4 ในกรอบสี่เหลี่ยมสีแดงที่หมายเลข 2 แสดงชื่อเครื่องเซิร์ฟเวอร์ที่ทำหน้าที่เป็นฐานข้อมูลหลัก (Active) คือเครื่องเซิร์ฟเวอร์ที่เป็น Owner Node (CKTSERVER023)

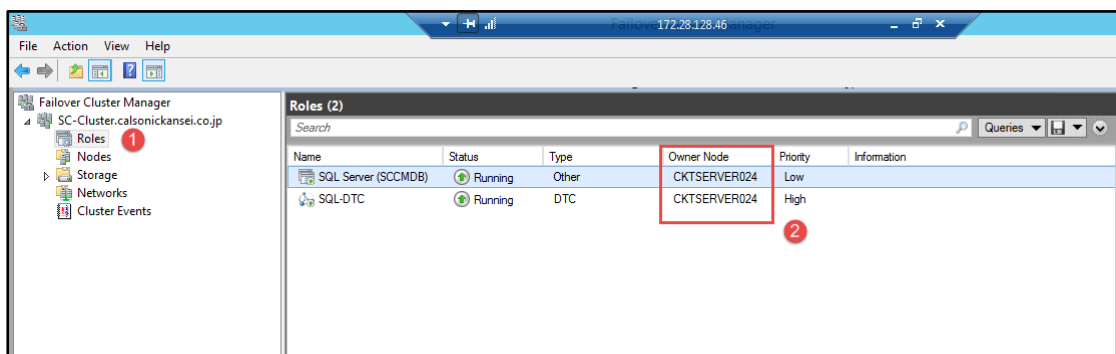
จากนั้นผู้เขียนงานนิพนธ์ได้ปิดเครื่อง CKTSERVER023 เพื่อทดสอบว่าระบบการทำงานของ Cluster จะทำงานหลังจากที่เครื่องฐานข้อมูลที่ Active อยู่ถูกปิดลงหรือไม่ดังภาพที่ 4-5





ภาพที่ 4-5 เครื่องฐานข้อมูลตัวที่ 1 CKTSERVER023 ถูกปิดลง

ภาพที่ 4-5 หลังจากที่มีการสั่งปิดเครื่องเซิร์ฟเวอร์ฐานข้อมูลตัวที่ 1 CKTSERVER023 สถานะของโหนดจะขึ้นสถานะเป็น Down ทั้งนี้จากนั้นผู้เขียนงานนิพนธ์ได้ตรวจสอบสถานะของการทำงานที่เมนู Roles ดังภาพที่ 4-6



ภาพที่ 4-6 สถานะของระบบ Cluster หลังจากปิดเครื่องเซิร์ฟเวอร์ CKTSERVER023

ภาพที่ 4-6 หลังจากปิดเครื่องเซิร์ฟเวอร์ฐานข้อมูลตัวที่ 1 (CKTSERVER023) ไปแล้วนั้นใช้เวลาโดยเฉลี่ย 16 วินาที เครื่องที่ Standby จะทำหน้าที่ Active แทน โดยผู้เขียนงานนิพนธ์ได้ทดสอบปิดเครื่องเซิร์ฟเวอร์สลับกันไปมาระหว่างเซิร์ฟเวอร์ CKTSERVER023 และ CKTSERVER024 จำนวน 10 ครั้ง ได้ผลดังตารางที่ 4-3

ตารางที่ 4-3 ผลการทดสอบระบบฐานข้อมูล SQL cluster

ทดสอบระบบฐานข้อมูล SQL Cluster		
ครั้งที่	เซิร์ฟเวอร์ที่ปิดเครื่อง	เวลาที่เครื่องสำรอง Active (วินาที)
1	CKTSERVER023	15
2	CKTSERVER024	16
3	CKTSERVER023	18
4	CKTSERVER024	16
5	CKTSERVER023	15
6	CKTSERVER024	14
7	CKTSERVER023	18
8	CKTSERVER024	17
9	CKTSERVER023	15
10	CKTSERVER024	17
เฉลี่ย :		16

ผลของตารางที่ 4-3 แสดงให้เห็นว่าระบบฐานข้อมูล SQL cluster สามารถทำงานแทนกันได้ปกติ หากระบบเซิร์ฟเวอร์ฐานข้อมูลตัวใดตัวหนึ่งเสียหาย โดยใช้เวลาในการย้ายไปใช้งานเซิร์ฟเวอร์ฐานข้อมูลอีกตัวหนึ่งประมาณ 14-18 วินาที เฉลี่ยในจำนวน 10 ครั้ง ประมาณ 16 วินาที

#### 4.5.2 ผลของการทดสอบ deploy ระบบปฏิบัติการวินโดวส์ (OS) ผ่านระบบ SCCM 2012 R2

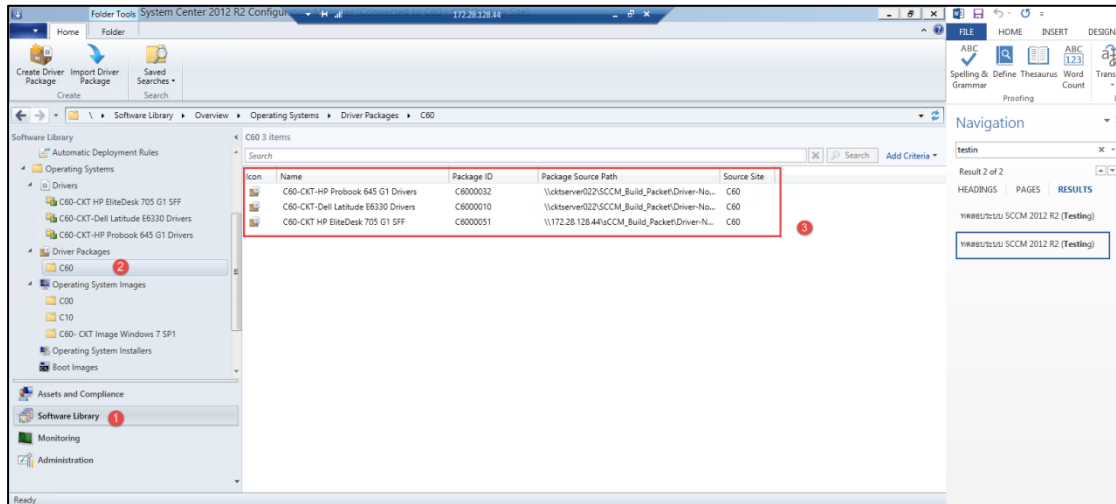
ผู้เขียนงานนิพนธ์ทดสอบ deploy ติดตั้งระบบปฏิบัติการวินโดวส์โดยเชื่อมต่อระบบเน็ตเวิร์กจากห้องเซิร์ฟเวอร์ไปที่แผนกไอทีซึ่งผ่านสวิตช์มีอัตราความเร็วในการส่งข้อมูล 10 Mbps และ 100 Mbps (10/100) โดยทดสอบ deploy ระบบปฏิบัติการวินโดวส์ 7 ลงในคอมพิวเตอร์ 3 โมเดล ดังนี้

1. Dell Latitude E6330
2. HP Probook 645 G1
3. HP EliteDesk 705 G1

การ deploy ระบบปฏิบัติการวินโดวส์จะมีกระบวนการ deploy ดังนี้

### 1. เตรียมไดรฟ์เวอร์คอมพิวเตอร์ (Driver packages)

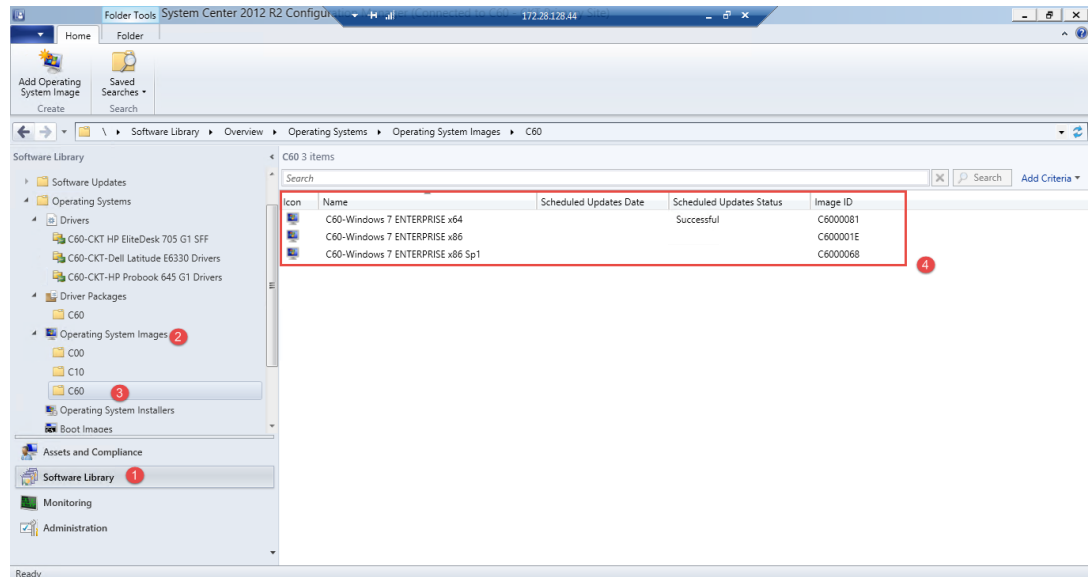
ผู้เขียนงานนิพนธ์ได้เตรียมไดรฟ์เวอร์คอมพิวเตอร์ของรุ่นที่จะทดสอบ จำนวน 3 โมเดล ซึ่งเป็นไดรฟ์เวอร์ของระบบปฏิบัติการวินโดว 7 ดังภาพที่ 4-7



ภาพที่ 4-7 สร้าง package ไดรฟ์เวอร์สำหรับเครื่องที่จะทดสอบ deploy OS

ภาพที่ 4-7 ผู้เขียนงานนิพนธ์ใช้ SCCM สร้าง packages ที่รวมไดรฟ์เวอร์ต่าง ๆ ของคอมพิวเตอร์รุ่น HP EliteDesk 705 G1, Dell latitude E6330, และ HP Probook 645 G1 สำหรับระบบปฏิบัติการวินโดว 7

## 2. เตรียมไฟล์ติดตั้งระบบปฏิบัติการวินโดวส์ 7

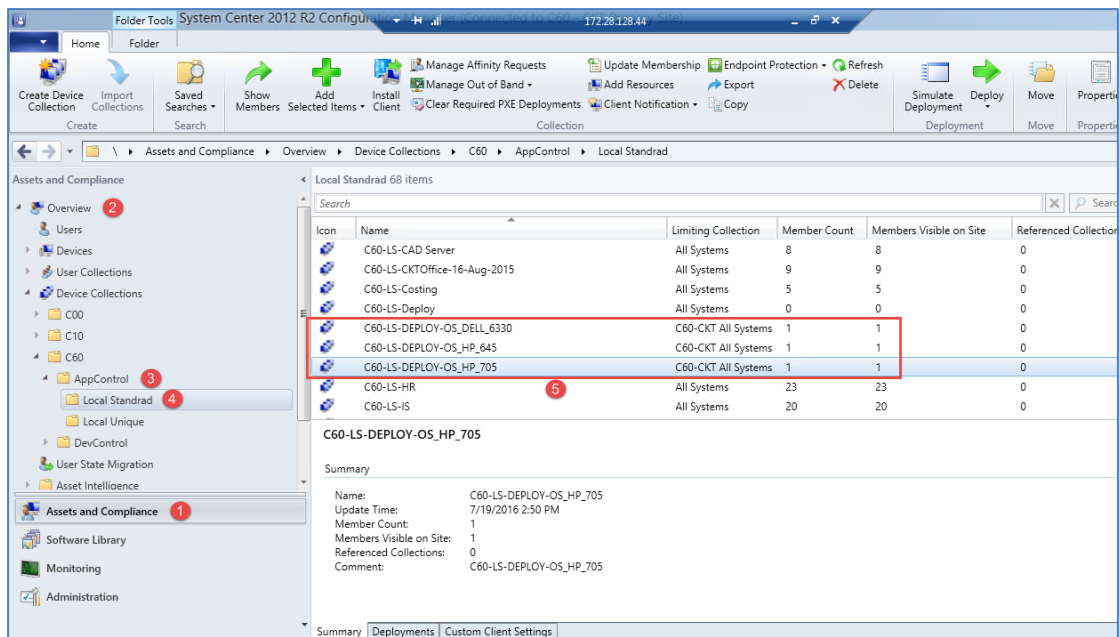


ภาพที่ 4-8 ไฟล์ระบบปฏิบัติการวินโดวส์ 7

จากภาพที่ 4-8 ผู้เขียนงานนิพนธ์ใช้ SCCM สร้างไฟล์ระบบปฏิบัติการวินโดวส์ 7 ทั้งหมด 3 ชนิด คือ ระบบปฏิบัติการวินโดวส์ 7 32 บิต, 32 บิต SP1 และ 64 บิต โดยเปิดหน้าต่าง Add operating system image wizard ก่อนเลือกไฟล์ install.wim ที่อยู่บนแผ่นติดตั้งระบบปฏิบัติการวินโดวส์

### 3. สร้าง Collection คอมพิวเตอร์

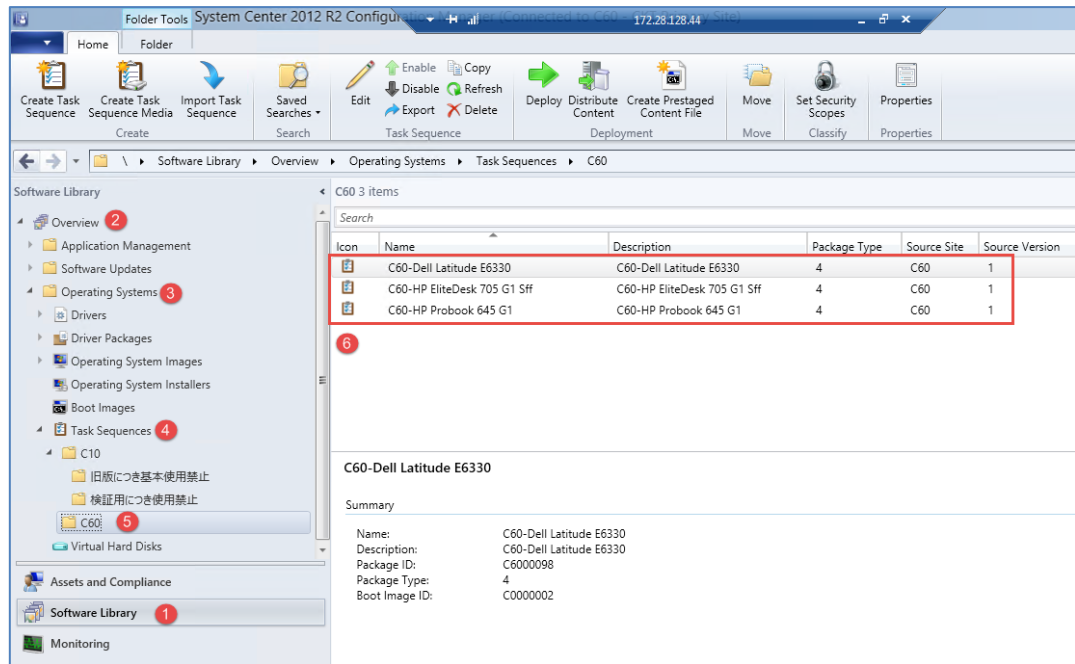
สำหรับการทดลองนี้ ผู้เขียนงานนิพนธ์ได้สร้าง Collection ขึ้นมาใหม่ (1 Collection ต่อ 1 โมเดลเครื่องคอมพิวเตอร์ ใน Device collections>>C60>>AppControl>>Local Standard) โดย Collection นี้มีสมาชิกเป็นคอมพิวเตอร์ที่จะถูกติดตั้งระบบปฏิบัติการวินโดวส์ 7 ดังภาพที่ 4-9



#### ภาพที่ 4-9 สร้าง Collection สำหรับการ deploy OS

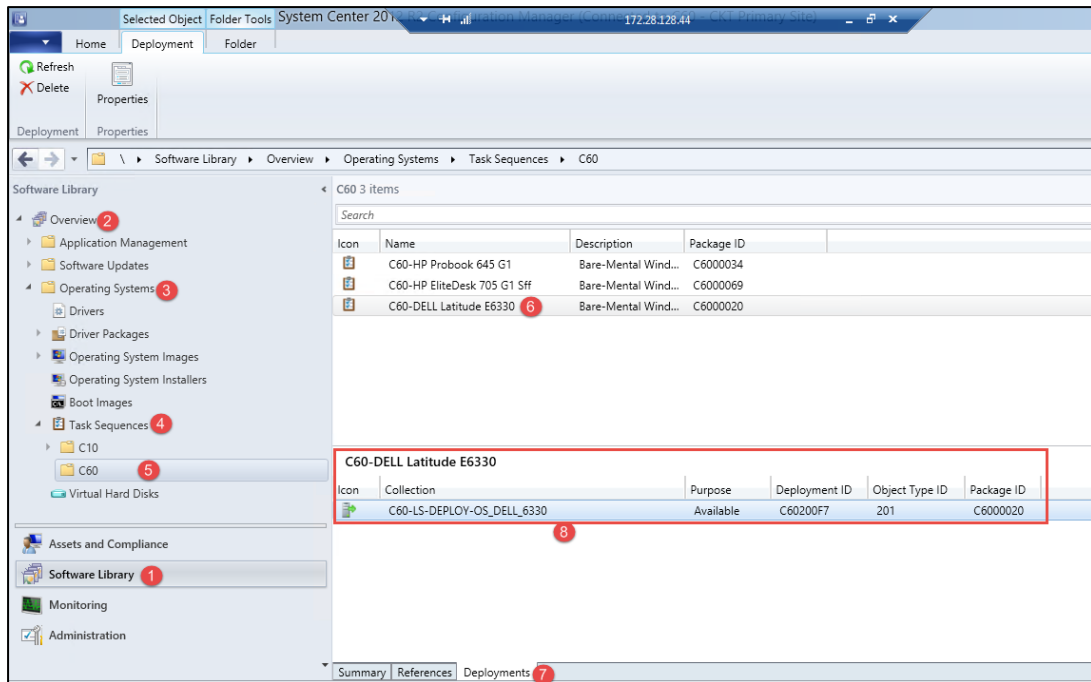
ภาพที่ 4-9 ในกรอบสี่เหลี่ยมสีแดงหมายเลข 5 แสดง Collection ของคอมพิวเตอร์ทั้ง 3 โมเดลที่ผู้เขียนงานนิพนธ์ได้สร้างไว้เพื่อ deploy ระบบปฏิบัติการวินโดวส์

4. สร้าง Task sequence, แล้ว deploy OS ไปที่ Collection ที่จะติดตั้งระบบปฏิบัติการวินโดวส์ ผู้เขียนงานนิพนธ์ได้สร้าง Task sequence เพื่อกำหนดการ deploy ระบบปฏิบัติการวินโดวส์แต่ละรุ่นและกำหนดค่าต่าง ๆ เช่น ตั้งชื่อ Task sequence, เลือกไฟล์ระบบปฏิบัติการวินโดวส์, เลือกไดรฟ์เวอร์คอมพิวเตอร์ (Driver packages), และเลือกโปรแกรมประยุกต์ที่ต้องการ deploy



ภาพที่ 4-10 Task Sequence สำหรับการ deploy OS (ในกรอบขาว)

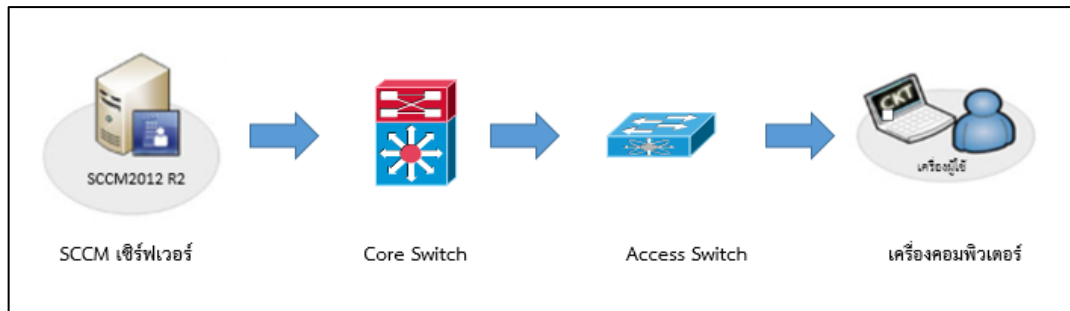
ภาพที่ 4-10 แสดง Task sequences สำหรับ deploy ระบบปฏิบัติการวินโดวส์ 7 (เลขในวงกลมแสดงถึงลำดับการเลือกเมนูก่อนที่ผู้ใช้จะสามารถคลิกขวาที่ Task Sequence ได้) โดยผู้เขียนงานนิพนธ์ได้คลิกขวาที่ Task sequence ชื่อ C60-Dell Latitude E6330 แล้วเลือก deploy ไปที่ Collection C60-LS-DEPLOY-OS\_DELL\_6330 ดังภาพที่ 4-11



ภาพที่ 4-11 deploy task sequence ไปที่ Collection ตามรุ่นที่ได้สร้างไว้

จากภาพที่ 4-11 แสดงการ deploy task sequence ชื่อ C60-Dell\_Latitude E6330 ไปที่ Collection ชื่อ C60-LS-DePLOY\_OS\_DELL\_6330



โดยหากต้องการ deploy ระบบปฏิบัติการวินโดวส์สำหรับเครื่องคอมพิวเตอร์ Dell 6330 ผู้ดูแลระบบจะต้องเพิ่มคอมพิวเตอร์ที่มีข้อมูลชื่อเครื่องและ Mac address เข้าไปใน Collection (ในที่นี้ชื่อ C60-LS-DePLOY\_OS\_DELL\_6330) หลังจากนั้นผู้เขียนงานนิพนธ์ได้เชื่อมต่อคอมพิวเตอร์เข้าสู่ระบบเครือข่ายเน็ตเวิร์กบริษัทคาลโซนิค ภาพที่ 4-12 แสดงให้เห็นถึงการเชื่อมโยงของเครือข่ายจากเซิร์ฟเวอร์ SCCM ผ่านอุปกรณ์ Core switch และ Access switch จนไปถึง เครื่องคอมพิวเตอร์ที่กำลังรอรับการ deploy (ผู้วิจัยจะใช้การเชื่อมดังกล่าวสำหรับทุก ๆ การทดลองในงานนิพนธ์นี้)



ภาพที่ 4-12 การเชื่อมต่อระบบเครือข่ายในการทดสอบ deploy ระบบปฏิบัติการวินโดวส์

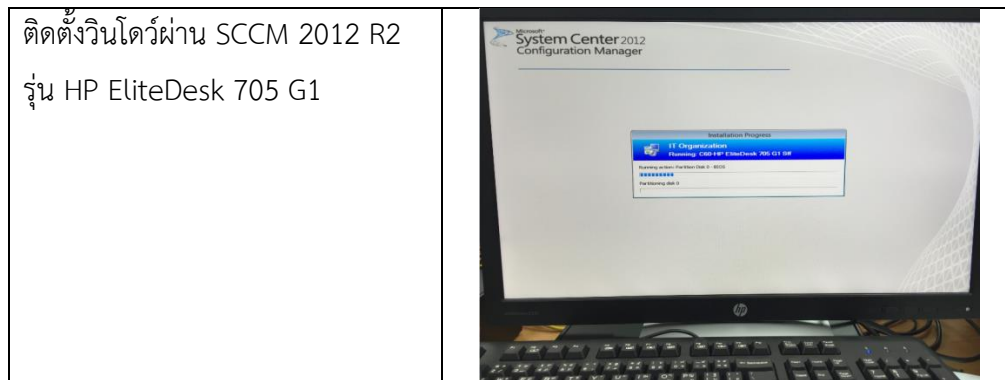
หลังจากเชื่อมต่อระบบเครือข่ายเน็ตเวิร์กเสร็จเรียบร้อยแล้ว ผู้เขียนงานนิพนธ์ได้ทดสอบติดตั้งระบบปฏิบัติการวินโดวส์ทั้ง 3 รุ่น ดังตารางที่ 4-4

ตารางที่ 4-4 การติดตั้งวินโดวส์ผ่าน SCCM 2012 R2

<p>ติดตั้งวินโดวส์ผ่าน SCCM 2012 R2 รุ่น Dell Latitude E6330</p>	
<p>ติดตั้งวินโดวส์ผ่าน SCCM 2012 R2 รุ่น HP Probook 645 G1</p>	



ตารางที่ 4-4 การติดตั้งวินโดวส์ผ่าน SCCM 2012 R2 (ต่อ)



จากตารางที่ 4-4 เป็นการติดตั้งระบบปฏิบัติการวินโดวส์ 7 จากระบบ SCCM 2012 R2 จำนวน 3 รุ่น โดยให้เครื่องคอมพิวเตอร์ทำการทดสอบบูตเครื่องคอมพิวเตอร์ผ่านระบบเน็ตเวิร์กหรือกด F12 เลือก PXE (Boot-on-LAN) จากนั้นจะเข้าสู่การติดตั้งระบบปฏิบัติการวินโดวส์จาก SCCM 2012 R2 ได้

ตารางที่ 4-5 ขนาดไฟล์และเวลาในการ deploy OS เครื่องที่ทดสอบได้ผลดังนี้

รุ่นที่ทำการทดสอบ	ขนาดไฟล์ ไดร์ฟเวอร์ (KB)	ขนาดไฟล์วินโดวส์ 7 32 บิต (KB)	รวมขนาดไฟล์ ทั้งหมด (KB)	ใช้เวลา (นาที)
Dell Latitude E6330	207,937	2,071,675	2,279,612	34
HP Probook 645 G1	1,292,113	2,071,675	3,363,788	46
HP EliteDesk 705 G1	681,379	2,071,675	2,753,054	41

ผลของการทดสอบ deploy ทั้ง 3 รุ่น ใช้เวลาต่างกัน ดังนี้

- Dell LatitudeE6330 มีหน่วยประมวลผลกลาง (CPU) Core i5 2.70 GHz.  
ใช้เวลา 34 นาที
- HP Probook 645 G1 มีหน่วยประมวลผลกลาง (CPU) A8-4500M 1.90GHz  
ใช้เวลา 46 นาที
- HP EliteDesk 705 G1 มีหน่วยประมวลผลกลาง (CPU) A4-7300B 3.80GHz  
ใช้เวลา 41 นาที

สรุปจากการทดสอบ deploy ระบบปฏิบัติการวินโดวส์ทั้ง 3 รุ่น พบว่าเครื่อง Dell Latitude 6330 มีความสามารถในการ deploy ได้เร็วกว่ารุ่นอื่นที่ทำการทดสอบ ซึ่งผู้เขียนงานนิพนธ์พอจะสรุปได้ว่าอาจจะมีผลกับขนาดของไฟล์ที่ทำการติดตั้ง, สเปคของอุปกรณ์เน็ตเวิร์กที่สามารถรองรับปริมาณการรับ-ส่งข้อมูล (Bandwidth) จาก SCCM เซิร์ฟเวอร์ไปที่เครื่องผู้ใช้ และความเร็วของการเขียน Hard disk โดยเครื่อง Dell Latitude E6330 มีขนาดรวมไฟล์ในการ deploy ทั้งหมด 2,279,612 KB ซึ่งน้อยกว่ารุ่นอื่น

#### 4.5.3 ผลการทดสอบ deploy โปรแกรมประยุกต์ไปที่เครื่องผู้ใช้ จำนวน 5 กลุ่ม

ผู้เขียนงานนิพนธ์ได้ทดสอบ deploy โปรแกรมประยุกต์ โดยโปรแกรมที่ใช้ทดสอบครั้งนี้คือ Java 8 Update 91 x86 ดังภาพที่ 4-13

Icon	Name	Deployment Types	Deployments	Status
	Java 8 Update 91 x86	1	5	Active

Java 8 Update 91 x86							
Icon	Collection	Compliance %	Action	Number Errors	Number Success	Package ID	Summary Type
	C60-LS-MEC	100.0	Install	0	14	C600008D	1
	C60-LS-Sale	100.0	Install	0	16	C600008D	1
	C60-LS-R&D	100.0	Install	0	29	C600008D	1
	C60-CKT-TestSECP-Desktop	100.0	Install	0	3	C600008D	1
	C60-LS-BOI	100.0	Install	0	6	C600008D	1

ภาพที่ 4-13 โปรแกรมประยุกต์ Java 8 Update 91

จากภาพที่ 4-13 ผู้เขียนงานนิพนธ์ใช้ SCCM ในหน้า Create application wizard ในการสร้างไฟล์ติดตั้งโปรแกรมประยุกต์ Java 8 Update 91 จากนั้น deploy ไปที่ Collection ทั้ง 5 ที่ได้สร้างขึ้น (C60-LS-MEC, C60-LS-Sale, C60-LS-R&D, C60-CKT-TestSECP-Desktop และ C60-LS-BOI) โดยในแต่ละ Collection มีจำนวนสมาชิกคอมพิวเตอร์ ดังตารางที่ 4-6

ตารางที่ 4-6 กลุ่มผู้ใช้ที่ทดสอบ deploy โปรแกรมประยุกต์

ลำดับ	ชื่อ Collection	แผนก	จำนวนเครื่อง	หมายเหตุ
1	C60-LS-MEC	MEC	14	
2	C60-LS-Sale	Sale	16	
3	C60-LS-R&D	R&D	29	
4	C60-CKT-TestSECP-Desktop	IT Test	3	กลุ่มแผนกไอที
5	C60-LS-BOI	BOI	6	

ผู้เขียนงานนิพนธ์ได้ทดสอบ deploy ไปที่เครื่องผู้ใช้ใน 5 Collection ดังตารางที่ 4-6 หลังจากนั้น 1 สัปดาห์ได้ตรวจสอบผลของการ deploy ดังภาพที่ 4-14

Icon	Software	Collection	Action	Feature Type	Compliance %	Number Errors	Number Success	Number Unknown
	Java 8 Update 91 x86	C60-CKT-TestSECP-Desktop	Install	Application	100.0	0	3	0
	Java 8 Update 91 x86	C60-LS-BOI	Install	Application	100.0	0	6	0
	Java 8 Update 91 x86	C60-LS-R&D	Install	Application	100.0	0	29	0
	Java 8 Update 91 x86	C60-LS-Sale	Install	Application	100.0	0	16	0
	Java 8 Update 91 x86	C60-LS-MEC	Install	Application	100.0	0	14	0

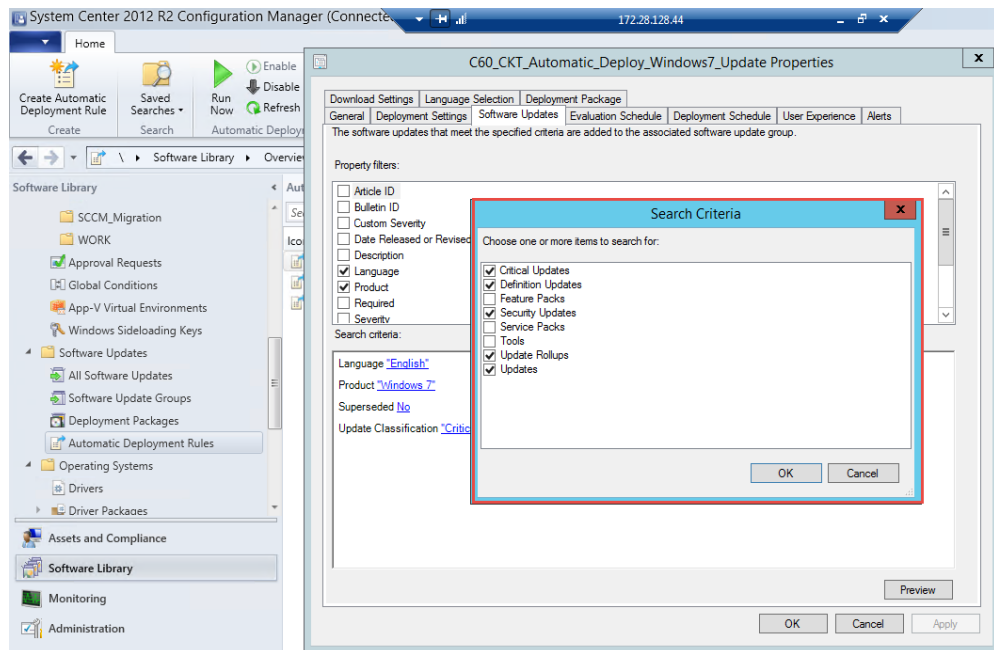
ภาพที่ 4-14 ผลของการ deploy Java 8 Update 91

ภาพที่ 4-14 แสดงผลของการ deploy โปรแกรมประยุกต์ Java 8 Update 91 โดยพบว่าสามารถ deploy ทุกเครื่องโดยไม่เกิดข้อผิดพลาด (Error) จากนั้นผู้เขียนงานนิพนธ์ได้ตรวจสอบเครื่องผู้ใช้เพื่อให้มั่นใจว่าเครื่องผู้ใช้ได้รับการติดตั้งโปรแกรมประยุกต์จริง โดยทำการสุ่มเช็ค ซึ่งปรากฏว่าเครื่องที่ได้ deploy ติดตั้งโปรแกรมประยุกต์ Java 8 Update 91 ได้รับการติดตั้งทุกเครื่อง

#### 4.5.4 ผลการทดสอบอัปเดตวินโดวส์ โดยการกำหนดกลุ่มผู้ใช้จำนวน 3 กลุ่ม

ผู้เขียนงานนิพนธ์ได้เปิดใช้บริการ Software update point ใน SCCM และ deploy ไปที่ Collection 3 Collection ของแผนกต่อไปนี้

- แผนกออกแบบผลิตภัณฑ์ (R&D)
- แผนกไอที (IT)
- แผนกขาย (Sales)



ภาพที่ 4-15 หมวดหมู่ที่ต้องการจะให้มีการอัปเดต (Update classification)

จากภาพที่ 4-15 ผู้เขียนงานนิพนธ์ได้เลือกหมวดหมู่ในการอัปเดต ได้แก่ Critical Update, Definition updates, Security Updates, Update Rollups และ Updates ของระบบปฏิบัติการ วินโดว์ 7

1. แผนกออกแบบผลิตภัณฑ์ (R&D) มีเครื่องคอมพิวเตอร์ทั้งหมด 27 เครื่อง จากการตรวจสอบผลการอัปเดตวินโดว์ ปรากฏว่าเครื่องคอมพิวเตอร์ที่ยินยอมให้อัปเดตได้สมบูรณ์ (Compliant) จำนวน 27 เครื่อง (100.00%)

Update Group:	C60_CKT_Automatic_Deploy_Windows7_Updates 2016-05-18 09:00:31	Values...
Collection:	C6000018 - C60-CKT R&D Department	Values... 1
Microsoft System Center 2012 R2 Configuration Manager		
<b>Compliance 1 - Overall compliance</b>		
Description		
Collection Name	Clients in Collection	
C60-CKT R&D Department	27	
State	Count of Computers	% of Total
Compliant	27	100.00

ภาพที่ 4-16 ผลของการอัปเดตวินโดว์กลุ่มแผนกออกแบบผลิตภัณฑ์ (R&D)

ภาพที่ 4-16 แสดงจำนวนเครื่องที่ยินยอมให้อัพเดทวินโดว์ได้สำเร็จ โดยสามารถคลิกเข้าไปตรงสถานะ Compliant ก็จะสามารถตรวจสอบดูชื่อเครื่องคอมพิวเตอร์และชื่อผู้ใช้ได้

2. แผนกไอที มีเครื่องคอมพิวเตอร์ทั้งหมด 15 เครื่อง จากการตรวจสอบผลการอัปเดตวินโดว์ ปรากฏว่าเครื่องคอมพิวเตอร์ที่ยินยอมให้อัพเดทได้สมบูรณ์ (Compliant) จำนวน 12 เครื่อง (80.00%) และเครื่องที่ไม่สามารถอัปเดตได้จำนวน 3 เครื่อง (20.00%)

Update Group: C60\_CKT\_Automatic\_Deploy\_Windows7\_Updates 2016-05-18 09:00:31 Values...

Collection: C600000A - C60-CKT IS Department Values...

Microsoft System Center 2012 R2 Configuration Manager

### Compliance 1 - Overall compliance

Description

Collection Name	Clients in Collection
C60-CKT IS Department	15

State	Count of Computers	% of Total
Compliant	12	80.00
Non-compliant	2	13.33
Compliance state unknown	1	6.67

ภาพที่ 4-17 ผลของการอัปเดตวินโดว์กลุ่มแผนกไอที

ภาพที่ 4-17 แสดงผลของการอัปเดตวินโดว์กลุ่มแผนกไอที ซึ่งสถานะอัปเดตวินโดว์ (State) Non-compliant จำนวน 2 เครื่อง คือเครื่องที่ไม่ยินยอมให้อัปเดตวินโดว์ โดยผู้เขียนงานนิพนธ์ได้คลิกเข้าไปที่ Non-Compliant เพื่อตรวจสอบว่า 2 เครื่องที่ไม่ได้รับการอัปเดตคือเครื่องไหนบ้าง ดังภาพที่ 4-18

Update Group: C60\_CKT\_Automatic\_Deploy\_Windows7\_Updates 2016-05-18 09:00:31 Values...

Collection: C600000A - C60-CKT IS Department Values...

State Name: Non-compliant Values...

Microsoft System Center 2012 R2 Configuration Manager

### Compliance 7 - Computers in a specific compliance state for an update group (secondary)

Description

Device Name	Last Logged on User	Assigned Site	Client Version
BK01_CKTHAI		C60	5.00.7958.1000
TH00NB150A0011_C_KTHAI	CKTHAI\ckt16d001c	C60	5.00.7958.1000

ภาพที่ 4-18 ผลการตรวจสอบชื่อเครื่องคอมพิวเตอร์ที่มีสถานะอัปเดตวินโดว์เป็น Non-Compliant

ภาพที่ 4-18 แสดงชื่อเครื่องที่สถานะอัปเดตวินโดว์เป็น Non-Compliant จำนวน 2 เครื่องคือ BK01 และ TH00NB15OA0011 ซึ่งจากการตรวจสอบสถานะของเครื่องพบว่าเครื่องไม่ได้เปิดใช้งานจึงไม่ได้มีการเชื่อมต่อระบบเครือข่ายเน็ตเวิร์กอยู่ ดังนั้นหากเปิดใช้งานเครื่องคอมพิวเตอร์และเชื่อมต่อระบบเครือข่ายเน็ตเวิร์กก็จะสามารถได้รับการอัปเดตวินโดว์จากระบบ SCCM ได้

จากภาพที่ 4-17 ผู้เขียนงานนิพนธ์ได้คลิกเข้าไปเพื่อตรวจสอบสถานะ การอัปเดตวินโดว์ Compliance state unknown ดังภาพด้านล่างนี้

Update Group: C60\_CKT\_Automatic\_Deploy\_Windows7\_Updates 2016-05-18 09:00:31 Values...

Collection: C600000A - C60-CKT IS Department Values...

State Name: Compliance state unknown Values...

Microsoft System Center 2012 R2 Configuration Manager

**Compliance 7 - Computers in a specific compliance state for an update group (secondary)**

Description

Device Name	Last Logged on User	Assigned Site	Client Version
CKT16B001.CKTHAI	CKTHAI\ckt16b001c	C60	5.00.7958.1000

ภาพที่ 4-19 ชื่อเครื่องคอมพิวเตอร์ที่มีสถานะ Compliance state unknown ในกลุ่มแผนกไอที

ภาพที่ 4-19 แสดงชื่อเครื่องที่มีสถานะอัปเดตวินโดว์ compliance state unknown จำนวน 1 เครื่องคือ CKT16B001 จากการตรวจสอบพบว่าสถานะของเครื่อง Inactive อยู่ ดังภาพที่ 4-20

Icon	Name	Client	Site Code	Client Activity	Endpoint Protection Enabled
	CKT16B001	Yes	C60	Inactive	Enabled

ภาพที่ 4-20 ผลการตรวจสอบสถานะเครื่องคอมพิวเตอร์ CKT16B001

ภาพที่ 4-20 แสดงสถานะของเครื่อง CKT16B001 มีสถานะ Inactive ผู้เขียนงานนิพนธ์จึงได้ตรวจสอบพบว่าเครื่องถูกปิดไว้ไม่ได้ใช้งานตั้งแต่พนักงานลาออกไป

3. แผนกขาย มีเครื่องคอมพิวเตอร์ทั้งหมด 16 เครื่อง โดยจากการตรวจสอบผลการอัปเดตวินโดว์ ปรากฏว่ามีเครื่องคอมพิวเตอร์ที่ยินยอมให้อัปเดตได้สมบูรณ์ (Compliant) จำนวน 15 เครื่อง (93.75%) และเครื่องที่ไม่ยินยอมให้อัปเดตได้จำนวน 1 เครื่อง (6.25%) ดังภาพที่ 4-21

Update Group: C60\_CKT\_Automatic\_Deploy\_Windows7\_Updates 2016-05-18 09:00:31 Values...

Collection: C6000019 - C60-CKT Sales Department Values...

Microsoft System Center 2012 R2 Configuration Manager

**Compliance 1 - Overall compliance**

Description

Collection Name	Clients in Collection
C60-CKT Sales Department	16

State	Count of Computers	% of Total
Compliant	15	93.75
Compliance state unknown	1	6.25

ภาพที่ 4-21 ผลของการอัปเดตวินโดว์กลุ่มแผนกขาย

ภาพที่ 4-21 แสดงผลของการอัปเดตวินโดว์กลุ่มแผนกขาย ซึ่งสถานะอัปเดตวินโดว์ (State) Compliant state unknown จำนวน 1 เครื่อง คือเครื่องที่ไม่ยินยอมให้อัปเดตวินโดว์ จากการตรวจสอบพบว่าเครื่องนี้เป็นเครื่องของพนักงานญี่ปุ่นที่เดินทางกลับประเทศเพื่อประชุมกับลูกค้า จึงทำให้เครื่องคอมพิวเตอร์อัปเดตวินโดว์ไม่ได้

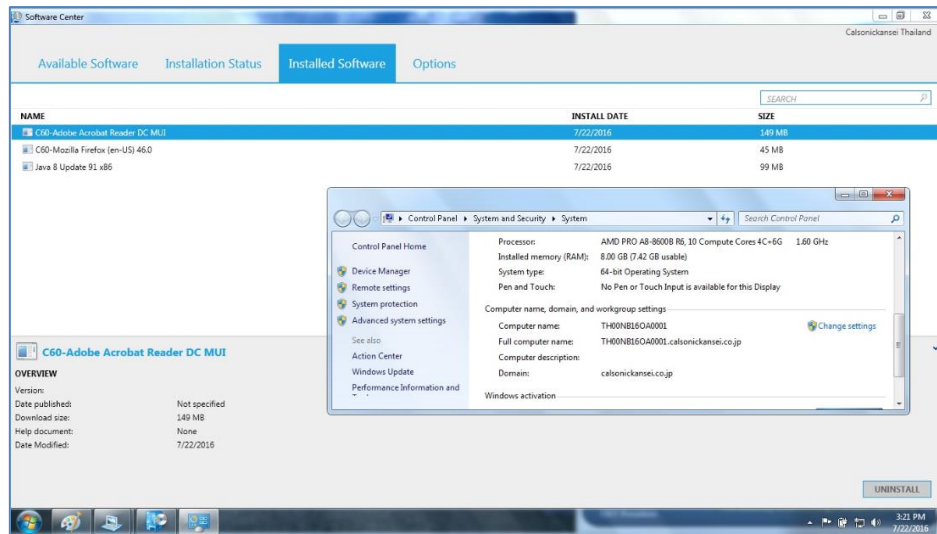
#### 4.5.5 การติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง ทดสอบจำนวน 3 เครื่อง

ผู้เขียนงานนิพนธ์ ได้ทดสอบให้เครื่องคอมพิวเตอร์ผู้ใช้สามารถเลือกติดตั้งโปรแกรมประยุกต์ได้ด้วยตนเอง โดยผู้ใช้สามารถเลือกติดตั้งได้จากโปรแกรม SCCM Software Center จำนวน 3 เครื่องโดยเลือกติดตั้งโปรแกรมประยุกต์จำนวน 3 โปรแกรมดังนี้

- Adobe Acrobat Reader DC      ขนาดไฟล์      149 MB
- Mozilla Firefox 46.0            ขนาดไฟล์      99 MB
- Java 8 Update 91                ขนาดไฟล์      45 MB

1. ติดตั้งที่เครื่องคอมพิวเตอร์ชื่อ TH00NB16OA0001

เปิดเครื่องคอมพิวเตอร์และเชื่อมต่อระบบเน็ตเวิร์ก จากนั้นเปิดโปรแกรม SCCM software center และเลือกติดตั้งโปรแกรม (ที่ Menu Available Software)

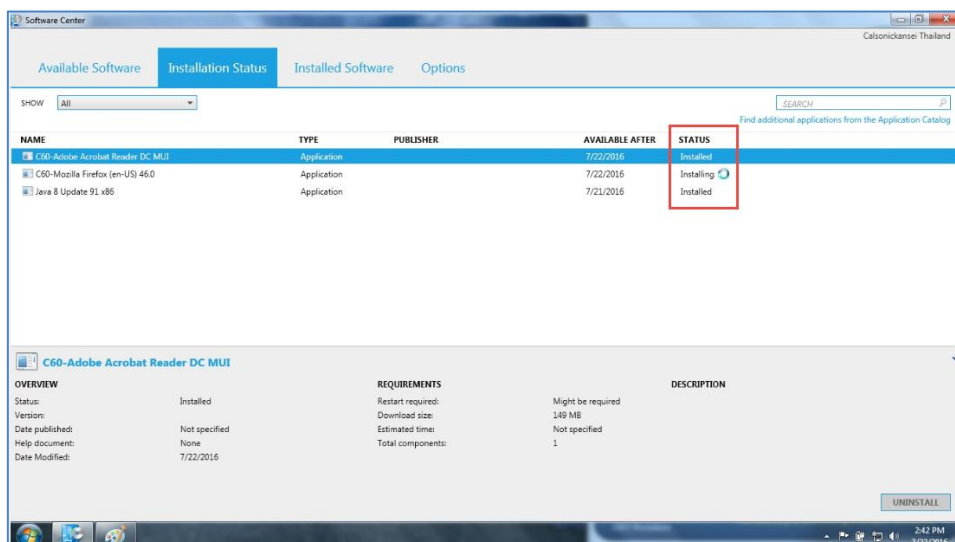


ภาพที่ 4-22 ติดตั้งโปรแกรมประยุกต์ที่คอมพิวเตอร์ชื่อ TH00NB16OA0001

จากภาพที่ 4-22 แสดงผลการติดตั้งโปรแกรมประยุกต์ โดยผู้เขียนงานนิพนธ์เลือกติดตั้งเองผ่านระบบ SCCM software center และสามารถติดตั้งได้สำเร็จ

2. ติดตั้งที่เครื่องคอมพิวเตอร์ชื่อ TH00NB16OA0002

เปิดเครื่องคอมพิวเตอร์และเชื่อมต่อระบบเน็ตเวิร์ก จากนั้นเปิดโปรแกรม SCCM software center และเลือกติดตั้งโปรแกรมประยุกต์



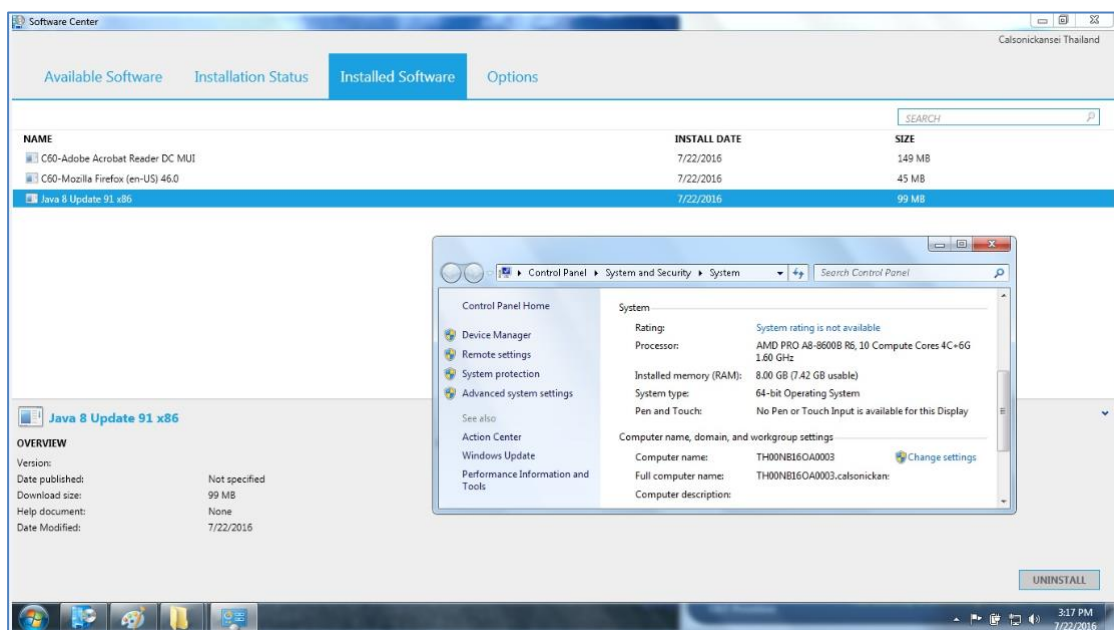
ภาพที่ 4-23 ติดตั้งโปรแกรมประยุกต์ที่คอมพิวเตอร์ชื่อ TH00NB16OA0002



ภาพที่ 4-23 แสดงสถานะ การติดตั้งโปรแกรมประยุกต์ทั้ง 3 โปรแกรม โดยจากภาพแสดงสถานะกำลังติดตั้งโปรแกรม Mozilla Firefox อยู่ และสามารถติดตั้งโปรแกรมประยุกต์ได้สำเร็จทั้ง 3 โปรแกรม

### 3. ติดตั้งที่เครื่องคอมพิวเตอร์ชื่อ TH00NB16OA0003

เปิดเครื่องคอมพิวเตอร์และเชื่อมต่อระบบเน็ตเวิร์ก จากนั้นเปิดโปรแกรม SCCM software center และเลือกติดตั้งโปรแกรมประยุกต์



ภาพที่ 4-24 ติดตั้งโปรแกรมประยุกต์ที่คอมพิวเตอร์ชื่อ TH00NB16OA0003

ภาพที่ 4-24 แสดงผลการติดตั้งโปรแกรมประยุกต์ที่เครื่อง TH00NB16OA0003 โดยผู้เขียนงานนิพนธ์เลือกติดตั้งเองผ่านระบบ SCCM software center และสามารถติดตั้งโปรแกรมประยุกต์ทั้ง 3 โปรแกรมได้สำเร็จ

สรุปจากการทดสอบข้างต้นในการติดตั้งโปรแกรมประยุกต์ด้วยตนเองทั้ง 3 โปรแกรมโดยทดสอบ คอมพิวเตอร์จำนวน 3 เครื่อง พบว่าสามารถติดตั้งได้สำเร็จทั้ง 3 เครื่องคอมพิวเตอร์

#### 4.5.6 ทดสอบเรียกดูรายงานสเปคเครื่องผู้ใช้งานจำนวน 3 กลุ่ม

ผู้เขียนงานนิพนธ์ได้ทดสอบการเรียกดูรายงานสเปคอุปกรณ์ฮาร์ดแวร์ของเครื่องผู้ใช้งานจำนวน 3 กลุ่มได้แก่ แผนกฝ่ายบุคคล, แผนกบัญชีต้นทุนและแผนกฝึกอบรม (VUP) โดยจากรายงานสามารถบอกชื่อเครื่อง, รหัสเครื่อง, โมเดล, รุ่น, หน่วยความจำ, ระบบปฏิบัติการ และอื่น ๆ ได้ ผลการเรียกดูรายงานแผนกฝ่ายบุคคล

Microsoft System Center 2012 R2 Configuration Manager											
Hardware 01A - Summary of computers in a specific collection											
Computer Name	Top Console User	Operating System	Service Pack Level	Serial Number	Asset Tag	Manufacturer	Model	Memory (KBytes)	Processor (GHz)	Total Disk Space (MB)	Free Disk Space (MB)
CKT000294	okthaick24591	Microsoft Windows 7 Enterprise	Service Pack 1	5CG60932F3	THJH00838	Hewlett-Packard	HP EliteBook 725 G2	7282983	1900	476836	325236
CKT000277	okthaick000377	Microsoft Windows 7 Enterprise	Service Pack 1	D4LFP0I		Dell Inc.	Latitude E5230	3580300	2900	476837	304123
CKT000629	th00ws12a0033local_us	Microsoft Windows 7 Enterprise Professional	Service Pack 1	CCVFBG1		Dell Inc.	Vostro 360	3056732	3200	460056	342467
CKT000683	okthaick000683	Microsoft Windows 7 Enterprise	Service Pack 1	5CG5304Y7B	THLH250429	Hewlett-Packard	HP ProBook 645 G1	2319760	2100	476836	388703
CKT000959	Unknown	Microsoft Windows 7 Enterprise	Service Pack 1	9KMTX2I		Dell Inc.	Latitude E5440	3919700	2500	476837	381986
CKT001279	okthaick001279	Microsoft Windows 7 Enterprise	Service Pack 1	5CG53003J5	THLH250643	Hewlett-Packard	HP ProBook 645 G1	2319760	2100	476836	358283
CKT001324	calsoniakensehok001334	Microsoft Windows 7 Enterprise	Service Pack 1	S3VFFH2I		Dell Inc.	OptiPlex 3011 AIO	3601488	2800	953885	900644
CKT002486	okthaick002486	Microsoft Windows 7 Professional	Service Pack 1	7DFBQI		Dell Inc.	Vostro 360	3056732	3200	460056	390434
CKT002579	okthaick002579	Microsoft Windows 7 Enterprise	Service Pack 1	3F5K2V1		Dell Inc.	Vostro 3360	3010580	1700	476836	407700
CKT002689	okthaick002689	Microsoft Windows 7 Enterprise	Service Pack 1	J63PNI		Dell Inc.	Vostro V131	3575912	2500	476837	354085
CKT002697	ok1002807administrator	Microsoft Windows 7 Enterprise	Service Pack 1	BQ79NV1		Dell Inc.	OptiPlex 9000	3580464	2900	476836	390328
CKT002711	okthaick002711	Microsoft Windows 7 Enterprise	Service Pack 1	74VFFH2I		Dell Inc.	OptiPlex 3011 AIO	3601488	2900	953786	902942
CKT002932	okthaick002932	Microsoft Windows 7 Enterprise	Service Pack 1	4F5K2V1		Dell Inc.	Vostro 3360	3010588	1700	476836	430897
IH00MB1D0A0077	ok1001280administrator	Microsoft Windows 7 Enterprise	Service Pack 1	G8JTNRI		Dell Inc.	Vostro V131	3575912	2500	476837	48475
IH00MB1D0A0000	Unknown	Microsoft Windows 7 Enterprise	Service Pack 1	2F5K2V1		Dell Inc.	Dell System Vostro 3360	3010580	1700	476836	448293
IH00SID0A0075	okthaick001877	Microsoft Windows 7 Enterprise	Service Pack 1	SD3PNI		Dell Inc.	Vostro V131	3575912	2500	476837	419358
IH00SID0A0044	ok1002283administrator	Microsoft Windows 7 Enterprise	Service Pack 1	DK3FNV1		Dell Inc.	OptiPlex 9010 AIO	3568904	2900	476836	234543
IH00SID0A0045	ok1002056administrator	Microsoft Windows 7 Enterprise	Service Pack 1	DST9NV1		Dell Inc.	OptiPlex 9000	3580464	2900	476836	341893
IH00SR0A0000	th00ws15o4000local_us	Microsoft Windows 7 Enterprise	Service Pack 1	SGH601Q5DC	THDH001368	Hewlett-Packard	HP EliteDesk 705 G1 SFF	32749576	3800	476836	322250

ภาพที่ 4-25 รายงานสเปคเครื่องของกลุ่มแผนกฝ่ายบุคคล

ภาพที่ 4-25 แสดงรายงานสเปคเครื่องของกลุ่มแผนกฝ่ายบุคคลซึ่งมีการใช้งานระบบปฏิบัติการเป็นวินโดว 7 ทุกเครื่อง โดยมีทั้งหมด 19 เครื่อง และมีการใช้สเปคเครื่องคอมพิวเตอร์แต่ละรุ่นต่างกัน สำหรับพนักงานจะใช้เครื่องที่เป็นรุ่น All in one หรือเครื่องโน้ตบุ๊ก ส่วนผู้บริหารจะใช้เครื่องโน้ตบุ๊กในการทำงาน

- ผลการเรียกดูรายงานแผนกฝ่ายบัญชีต้นทุน

Service Pack Level	Serial Number	Asset Tag	Manufacturer	Model	Memory (KBytes)	Processor (GHz)	Total Disk Space (MB)	Free Disk Space (MB)
Service Pack 1	6K9FNW1		Dell Inc.	OptiPlex 9010 AIO	3568904	2900	476836	264230
	FMGCF25		Dell Inc.	OptiPlex 9010	3576500	2800	476836	386453
Service Pack 1	C9JTNRI		Dell Inc.	Vostro V131	3575912	2500	476837	391018
Service Pack 1	5CG5304YFN	THLH250419	Hewlett-Packard	HP ProBook 645 G1	2319760	2100	305142	84811
Service Pack 1	SGH535580J	THDH001360	Hewlett-Packard	HP EliteDesk 705 G1 SFF	3619580	3800	476836	418668

ภาพที่ 4-26 รายงานสเปคเครื่องของกลุ่มแผนกฝ่ายบัญชีต้นทุน

ภาพที่ 4-26 แสดงรายงานสเปคเครื่องของกลุ่มแผนกฝ่ายบัญชีต้นทุน ซึ่งมีเครื่องทั้งหมด 5 เครื่อง ในกรอบสีแดงหมายเลข 1 เป็นเครื่อง All in one OptiPlex 9010 จำนวน 2 เครื่อง และในกรอบสีน้ำเงินเป็นเครื่องโน้ตบุ๊กจำนวน 2 เครื่อง ได้แก่รุ่น Vostro V131, HP Probook 645 G1

อย่างละ 1 โมเดลและกรอบสีแดงหมายเลข 3 เป็นเครื่องคอมพิวเตอร์ HP EliteDesk705 จำนวน 1 เครื่อง

- ผลการเรียกดูรายงานแผนกฝึกอบรม (VUP)

Computer Name	Domain/Workgroup	ConfigMgr Site Name	Top Console User	Operating System	Service Pack Level	Serial Number	Asset Tag	Manufacturer	Model	Memory (KByte)	Processor (G)
QKTRABNK05	OXTHAI	OXT Primary Site	Unknown	Microsoft Windows 7 Enterprise	Service Pack 1	586LSPI		Dell Inc.	Vostro V130	1956348	1330
QKTRABNK07	OXTHAI	OXT Primary Site	ddhai\cltraining07	Microsoft Windows 7 Enterprise	Service Pack 1	F96LSPI		Dell Inc.	Vostro V130	1956348	1330
TRABNK06	OXTHAI	OXT Primary Site	training06\local_users	Microsoft Windows 7 Enterprise	Service Pack 1	62VXTPI		Dell Inc.	Vostro V130	1956348	1330
TRABNK08	OXTHAI	OXT Primary Site	Unknown	Microsoft Windows 7 Enterprise	Service Pack 1	01VXTPI		Dell Inc.	Vostro V130	1956348	1330

ภาพที่ 4-27 รายงานสเปคเครื่องของกลุ่มแผนกฝึกอบรม (VUP)

ภาพที่ 4-27 แสดงรายงานสเปคเครื่องของกลุ่มแผนกฝึกอบรม (VUP) ซึ่งมีทั้งหมด 4 เครื่อง โดยเป็นเครื่องโน้ตบุ๊กรุ่น Vostro 130 ทั้งหมด และทั้ง 4 เครื่องใช้ระบบปฏิบัติการวินโดวส์ 7 SP1

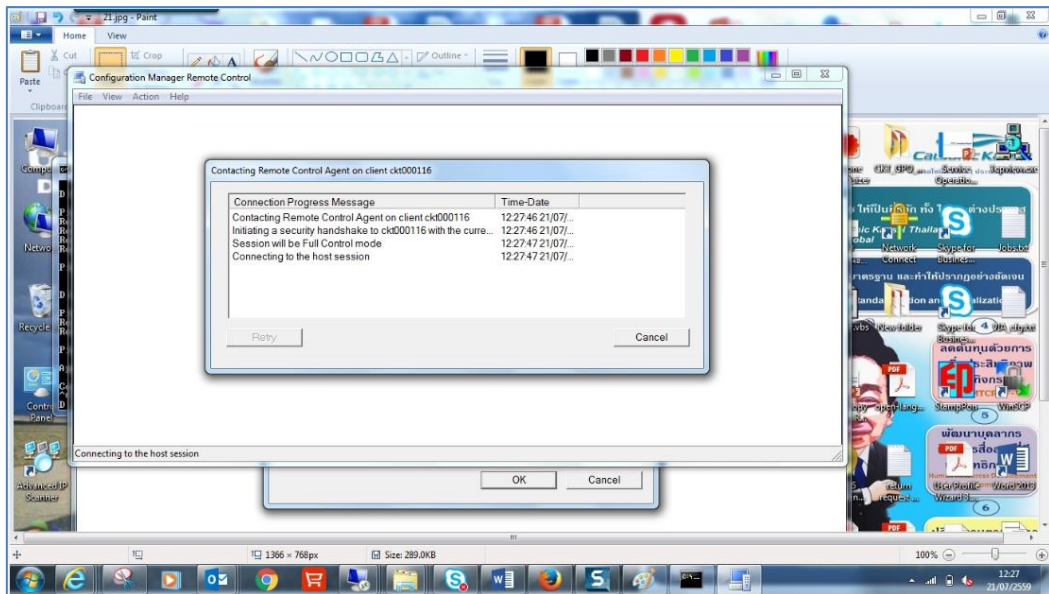
สรุปการทดสอบเรียกดูรายงานทั้ง 3 แผนก ปรากฏว่าสามารถเรียกดูข้อมูลสเปคฮาร์ดแวร์คอมพิวเตอร์ได้ตรงกับเครื่องที่มีการใช้งานอยู่จริง

#### 4.5.7 ผลการทดสอบ Remote control viewer ไปเครื่องผู้ใช้งานจำนวน 3 เครื่อง

ผู้เขียนงานนิพนธ์ได้ทดสอบ Remote control ไปที่เครื่องผู้ใช้ โดยกำหนดเครื่องผู้ใช้งานจำนวน 3 เครื่อง ดังนี้

1. เครื่องคอมพิวเตอร์ชื่อ CKT000116

ผู้เขียนงานนิพนธ์ได้ทดสอบควบคุมเครื่องผู้ใช้งานระยะไกล โดยใช้โปรแกรม SCCM remote control viewer แล้วระบุเครื่องคอมพิวเตอร์ปลายทาง ดังภาพที่ 4-28

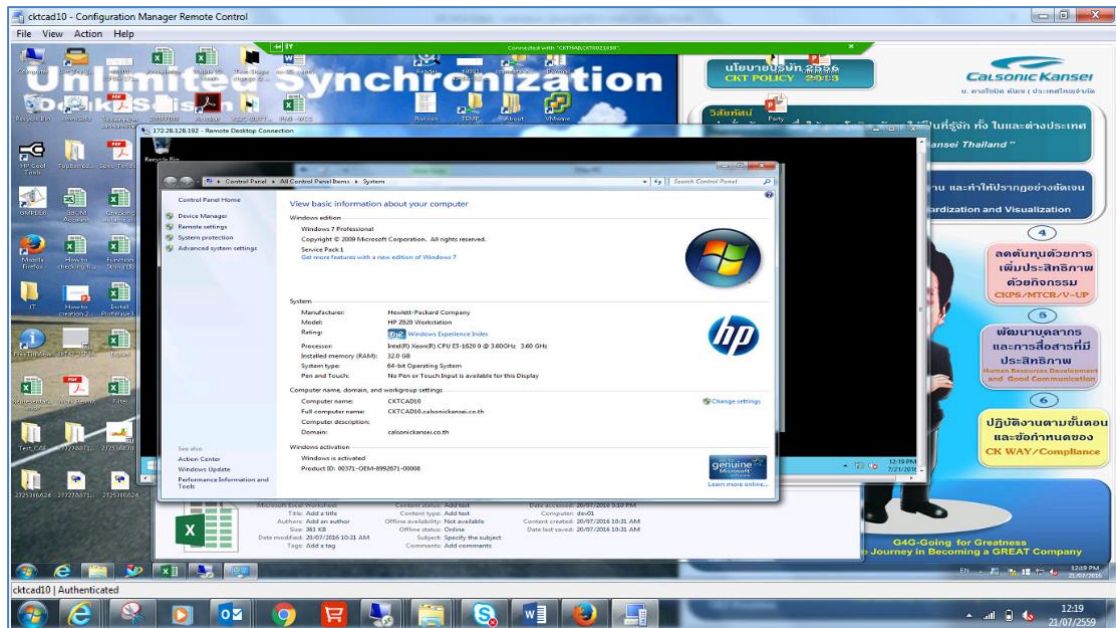


ภาพที่ 4-28 ควบคุมเครื่อง CKT000116 จากระยะไกล

ภาพที่ 4-28 แสดงการเชื่อมต่อควบคุมเครื่องผู้ใช้ CKT000116 จากระยะไกล โดยจะปรากฏข้อมูลการเชื่อมต่อและเวลาในการเชื่อมต่อ เมื่อกดเชื่อมต่อแล้วจะใช้เวลาแสดงผลจอภาพของเครื่องผู้ใช้ประมาณ 3-5 วินาที

## 2. เครื่องคอมพิวเตอร์ชื่อ CKTCAD10

ทดสอบควบคุมเครื่องผู้ใช้ CKTCAD10 จากระยะไกล โดยใช้โปรแกรม SCCM Remote control viewer ดังภาพที่ 4-29

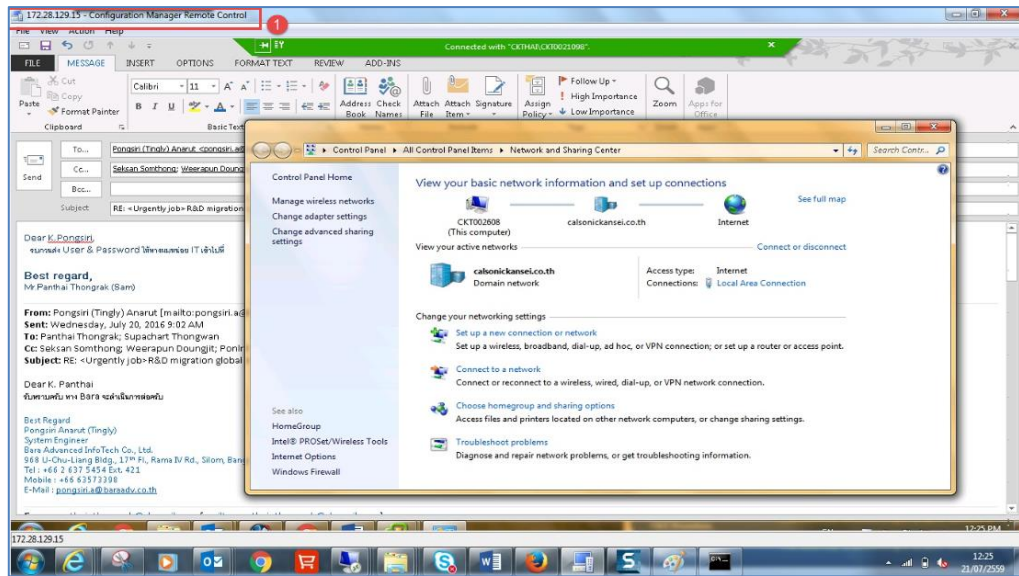


ภาพที่ 4-29 รีโมทควบคุมเครื่อง CKTCAD10

จากภาพที่ 4-29 แสดงผลหลังจากเชื่อมต่อไปเครื่องคอมพิวเตอร์ปลายทางได้เรียบร้อยแล้ว หลังจากนั้นผู้ที่ควบคุมเครื่องผู้ใช้จากระยะไกลจะสามารถควบคุมการทำงานของเครื่องคอมพิวเตอร์ปลายทางได้ โดยสามารถใช้เมาส์และคีย์บอร์ดของเครื่องต้นทางควบคุมเครื่อง CKTCAD10 ได้

3. เครื่องคอมพิวเตอร์ชื่อ CKT002608 (IP 172.28.129.15)

ทดสอบควบคุมเครื่องผู้ใช้จากระยะไกล โดยระบุเครื่องเป็นไอพี 172.28.129.15 ใช้โปรแกรม SCCM remote control viewer ดังภาพที่ 4-30



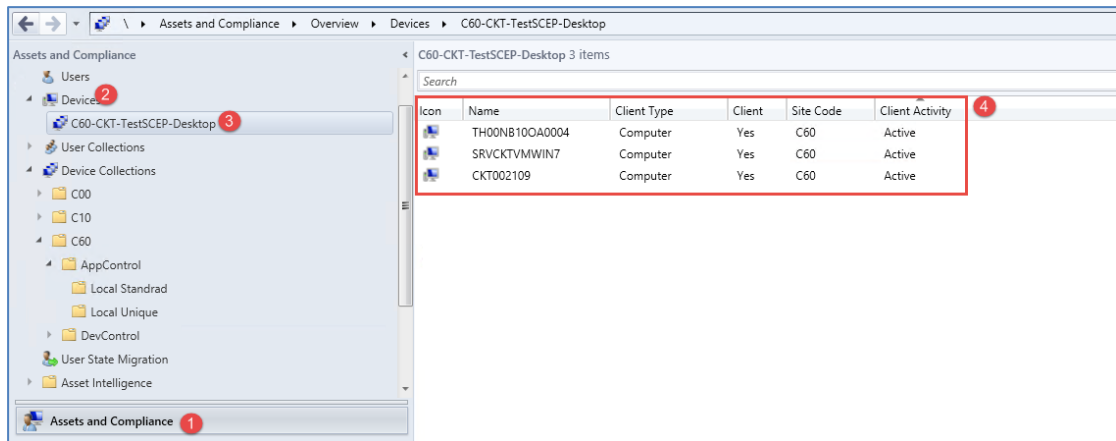
ภาพที่ 4-30 รีโมทควบคุมเครื่องไอพี 172.28.129.15

ภาพที่ 4-30 แสดงการควบคุมเครื่องผู้ใช้จากระยะไกลโดยระบบไอพีแอดเดรส 172.28.129.15

สรุปการควบคุมเครื่องผู้ใช้จากระยะไกลผ่านซอฟต์แวร์ SCCM remote control viewer สามารถทำได้ 2 ทางคือชื่อเครื่องคอมพิวเตอร์ และไอพีแอดเดรส โดยผู้เขียนงานนิพนธ์ได้ทดสอบควบคุมเครื่องผู้ใช้ทั้งสองแบบจำนวน 10 เครื่อง ปรากฏว่าสามารถควบคุมเครื่องผู้ใช้ปลายทางได้ ทั้งนี้ผู้ที่ทำการควบคุมเครื่องผู้ใช้ได้ จะต้องมียุติสิทธิ์ในการควบคุมจากระบบ SCCM ก่อน

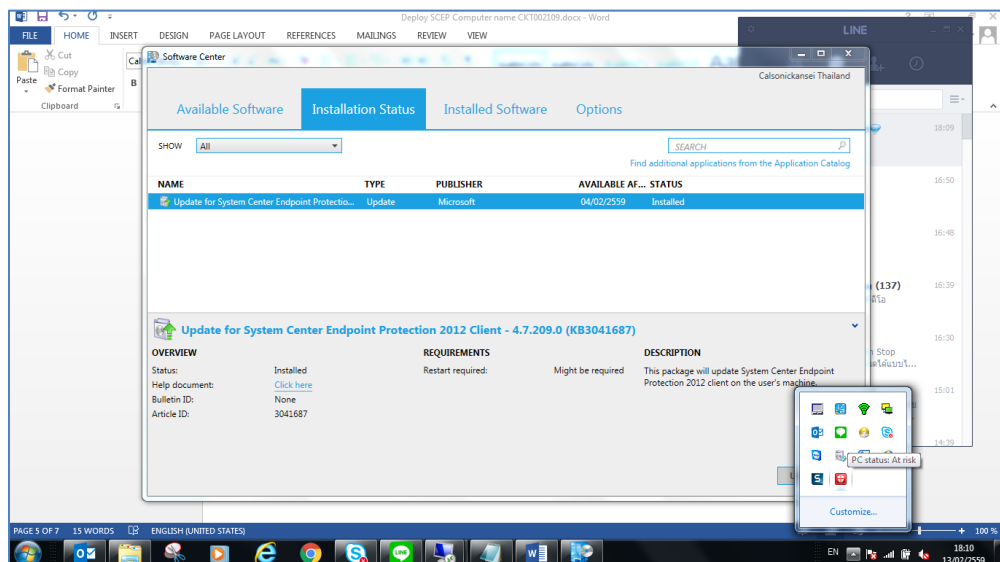
#### 4.5.8 ผลการทดสอบ deploy ติดตั้งโปรแกรมป้องกันไวรัส

ผู้เขียนงานนิพนธ์ได้เปิดใช้บริการ Endpoint protection point ใน SCCM ที่ทำหน้าที่เรียกใช้งาน System Center Endpoint Protection (SCEP) ซึ่งเป็นศูนย์กลางในการควบคุมโปรแกรมป้องกันมัลแวร์ (ไวรัส, เวิร์ม, โทรจัน, สปายแวร์, แอดแวร์ และซอฟต์แวร์คุกคามทางคอมพิวเตอร์ประเภทอื่น ๆ) ผู้เขียนงานนิพนธ์ได้ทดสอบ deploy ติดตั้งโปรแกรมป้องกันไวรัส Endpoint protection client จากระบบ SCCM แทนตัวเดิม (McAfee) โดยหลังจาก deploy ติดตั้งเสร็จสมบูรณ์แล้วผู้เขียนงานนิพนธ์ได้ดาวน์โหลดไฟล์ไวรัสจากเว็บไซต์เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัสด้วย



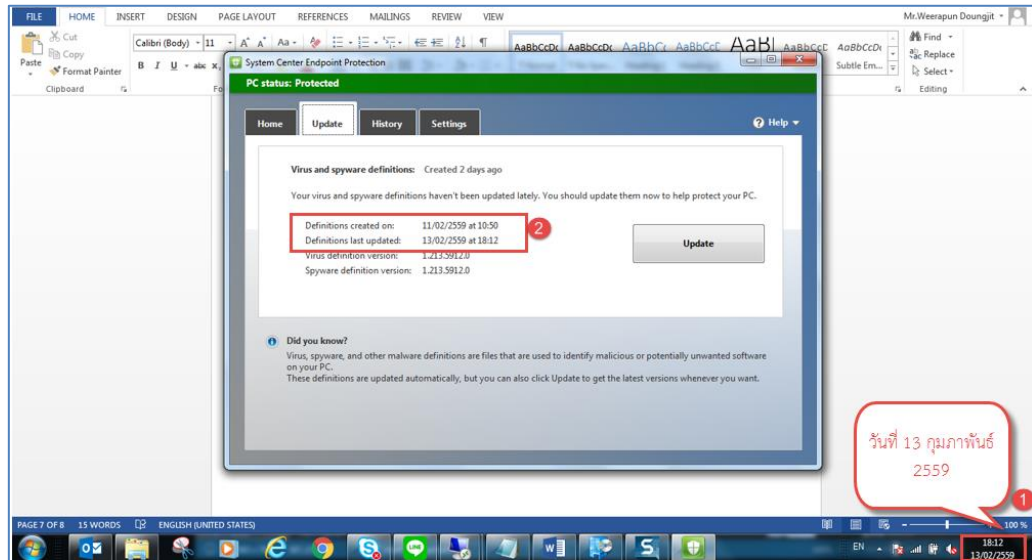
ภาพที่ 4-31 Collection สำหรับทดสอบ deploy ติดตั้งโปรแกรมป้องกันไวรัส Endpoint Protection client

ภาพที่ 4-31 แสดง Collection ที่จะทดสอบ deploy โปรแกรมป้องกันไวรัส Endpoint protection client โดยในกรอบสี่เหลี่ยมสีแดงหมายเลข 4 มีเครื่องคอมพิวเตอร์ทั้งหมดจำนวน 3 เครื่องด้วยกัน



ภาพที่ 4-32 การติดตั้งโปรแกรมป้องกันไวรัส Endpoint protection client เสร็จสมบูรณ์แล้ว

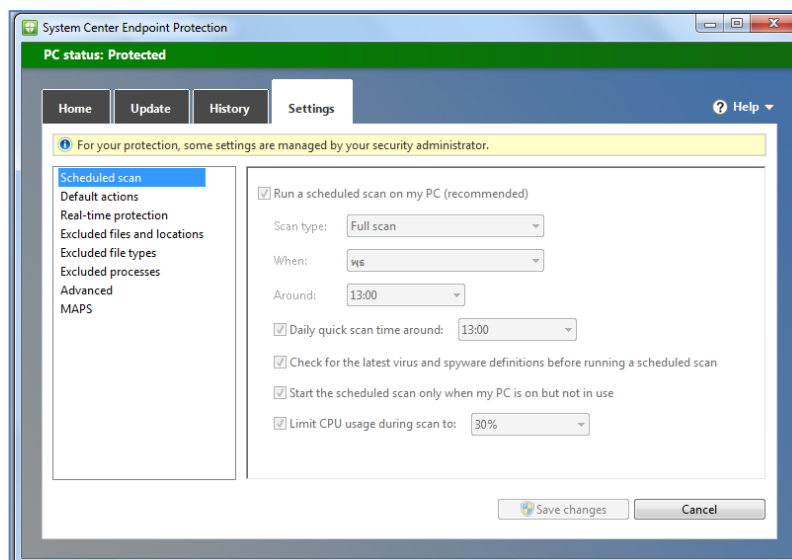
ภาพที่ 4-32 แสดงผลการติดตั้งโปรแกรมป้องกันไวรัส Endpoint protection client เสร็จสมบูรณ์แล้ว จากนั้นจะเชื่อมต่อกับเซิร์ฟเวอร์ SCCM เพื่ออัปเดต Definition โปรแกรมป้องกันไวรัสให้เป็นเวอร์ชันปัจจุบันดังภาพที่ 4-33



ภาพที่ 4-33 ติดตั้งโปรแกรมป้องกันไวรัส SCEPและอัปเดต Definition เป็นเวอร์ชันปัจจุบัน

ภาพที่ 4-33 แสดงผลการอัปเดตโปรแกรมป้องกันไวรัส Endpoint protection client เป็นวันที่ปัจจุบันกับวันที่ทดสอบคือวันที่ 13 กุมภาพันธ์ 2559 (เวอร์ชันล่าสุด) ผู้เขียนงานนิพนธ์ได้กำหนดให้สแกนไวรัสทุก ๆ วันพุธเวลาบ่ายโมงตรง ดังภาพด้านล่างนี้

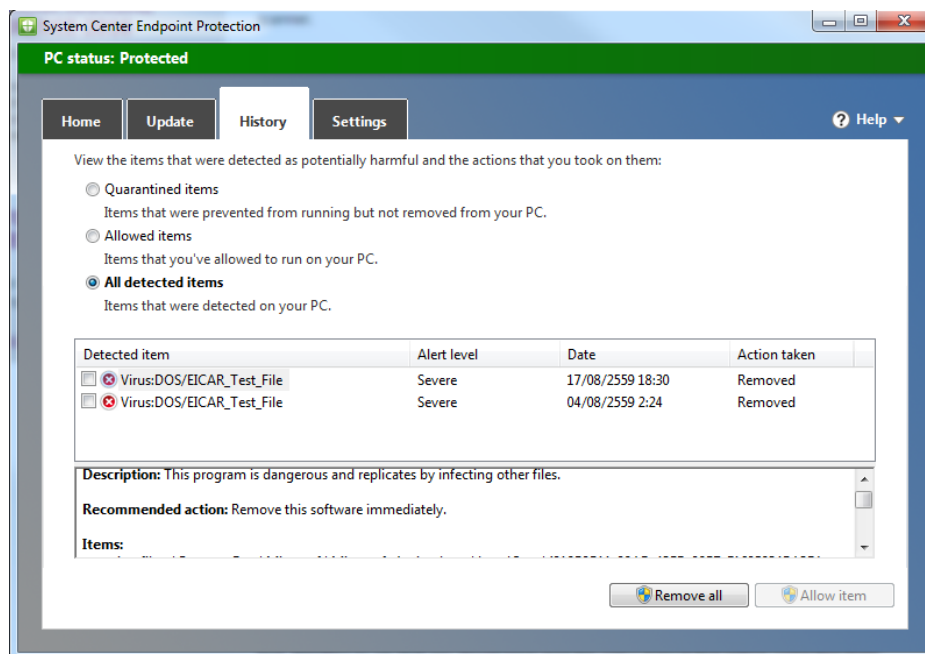




ภาพที่ 4-34 กำหนดการสแกนโปรแกรมป้องกันไวรัส Endpoint protection client ที่เครื่องผู้ใช้

หลังจากติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องทดสอบเสร็จแล้วผู้เขียนงานนิพนธ์ได้ทดสอบดาวน์โหลดไฟล์ไวรัสจากเว็บไซต์ 3 เว็บ ดังนี้

1. ทดสอบดาวน์โหลดไฟล์จากเว็บ <http://www.eicar.org/85-0-Download.html>

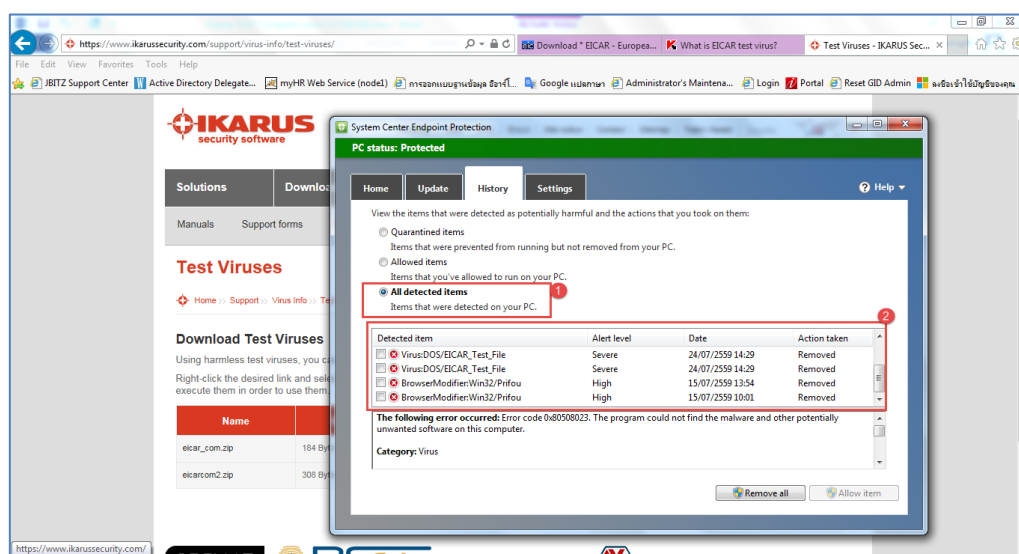


ภาพที่ 4-35 ดาวน์โหลดไฟล์ไวรัสจากเว็บไซต์ <http://www.eicar.org/85-0-Download.html>

ภาพที่ 4-35 ดาวน์โหลดไฟล์จากเว็บไซต์ <http://www.eicar.org/85-0-Download.html> เสร็จแล้วโปรแกรมป้องกันไวรัส Endpoint protection client ตรวจสอบเจอ จึงลบไฟล์ที่ดาวน์โหลดทันที เนื่องจากไฟล์ที่ดาวน์โหลดมาเป็นไฟล์ไวรัสนั่นเอง

## 2. ทดสอบดาวน์โหลดไฟล์จากเว็บ



- <http://support.kaspersky.com/viruses/general/459>
- <http://www.ikarussecurity.com/support/virus-info/test-viruses/>



ภาพที่ 4-36 ดาวน์โหลดไฟล์จากเว็บไซต์ [Support.kaspersky.com](http://Support.kaspersky.com) และ [ikarussecurity.com](http://ikarussecurity.com)

ภาพที่ 4-36 หลังจากดาวน์โหลดไฟล์ไวรัสจากเว็บไซต์ [Support.kaspersky.com](http://Support.kaspersky.com) และ [ikarussecurity.com](http://ikarussecurity.com) แล้ว โปรแกรมป้องกันไวรัส Endpoint protection client ตรวจสอบเจอและลบไฟล์ที่ดาวน์โหลดมาทันที

ตารางที่ 4-7 ผลการทดสอบโปรแกรมป้องกันไวรัส

ชื่อเครื่อง	ดาวน์โหลดไฟล์ไวรัสจากเว็บไซต์	ผลการทดสอบ	
		ป้องกัน ไม่ได้	ป้องกัน ได้
TH00NB10OA0004	<a href="http://www.eicar.org/85-0-Download.html">http://www.eicar.org/85-0-Download.html</a>		
SRVCKTVMWIN7	<a href="http://support.kaspersky.com/viruses/genera/459">http://support.kaspersky.com/viruses/genera/459</a>		
CKT002109	<a href="http://www.ikarussecurity.com/support/virus-info/test-viruses/">http://www.ikarussecurity.com/support/virus-info/test-viruses/</a>		

สรุปตารางที่ 4-7 ผลการทดสอบโปรแกรมป้องกันไวรัส Endpoint protection client ทั้ง 3 เครื่อง สามารถป้องกันไวรัสและลบไฟล์ไวรัสเมื่อดาวน์โหลดจากเว็บไซต์ได้ทันที

#### 4.6 ผลสังเกตการณ์ การทำงานระบบ SCCM 2012 R2 (Monitoring)

จากการออกแบบเพื่อสังเกตการณ์ การทำงานของระบบ SCCM 2012 R2 ผู้เขียนงานนิพนธ์ได้เก็บผลการสังเกตการณ์ ดังนี้

4.6.1 ผลสังเกตการณ์ การ deploy โปรแกรมประยุกต์ที่เป็นกลุ่มซอฟต์แวร์มาตรฐานของบริษัทจะสามารถ deploy ได้ทุกตัวหรือไม่ และใช้เวลาเท่าไรโดยผู้เขียนงานนิพนธ์เก็บผลการสังเกตการณ์ได้ดังตารางที่ 4-8

ตารางที่ 4-8 ผลการ deploy โปรแกรมประยุกต์ และเวลาที่ใช้ต่อเครื่อง

ซอฟต์แวร์	ขนาดไฟล์ (MB)	Deploy	เวลาดำเนินการ: เครื่อง	รายละเอียด
7zip	2.15		1	
IE11	185.63		5	ต้องการ Restart
Firefox 46.0	45.26		2	
Acrobat Reader DC MUI	149.18		3	
Flash player	36.93		2	
Java 8 Update 91	99.86		2	
MS Office 2013	759.55		10	ต้องการ Restart
MS Lync2013	389.31		7	
doPDF	44.43		1	
Antivirus SCEP	577.22		4	
LEXITRON Dictionary 2.6	49.065		-	SCCM ไม่รองรับ

\*หมายเหตุ = สามารถ Deploy ได้

= ไม่สามารถ Deploy ได้

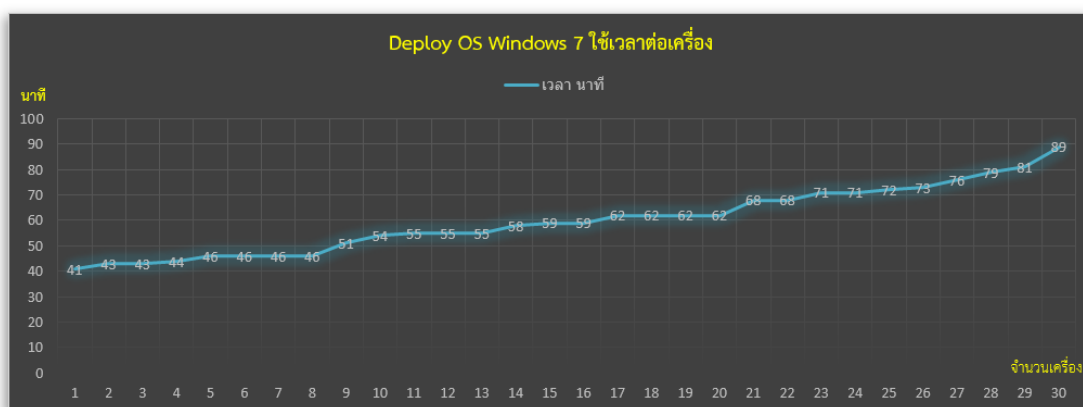
ตารางที่ 4-8 แสดงผลการ deploy โปรแกรมประยุกต์ได้สำเร็จคิดเป็น 91% ของโปรแกรมที่ทดสอบทั้งหมด ซึ่งผลของการสังเกตการณ์ได้พบที่สามารถ deploy โปรแกรมประยุกต์ที่มีไฟล์นามสกุล.msi ได้ทุกตัวที่ทำการทดสอบ และไฟล์ที่ไม่สามารถ deploy ได้คือโปรแกรมแปลภาษา LEXITRON Dictionary 2.6 ซึ่งโปรแกรมเป็นไฟล์ .exe และไม่สามารถสร้างให้เป็นไฟล์.msi ได้ ดังนั้นการ deploy จึงไม่สามารถทำผ่านระบบ SCCM ได้ และผู้เขียนงานนิพนธ์ยังได้พบว่าขนาดของไฟล์มีผลต่อการ deploy ด้วย โดยหากไฟล์ที่มีขนาดใหญ่ก็จะใช้เวลาในการ deploy มากขึ้น

4.6.2 ผลการสังเกตการณ์ deploy OS โดยทดสอบครั้งละ 1 เครื่อง, 5 เครื่อง, 10 เครื่อง และ 30 เครื่อง โดยทดสอบคอมพิวเตอร์รุ่น HP EliteDesk 705 G1

ตารางที่ 4-9 ผลของการทดสอบ deploy OS HP EliteDesk 705 G1

ครั้งที่	ทดสอบ Deploy OS จำนวน	ใช้เวลา:นาที	เฉลี่ยนาที : ต่อเครื่อง
1	1	41	41.00
2	5	46	9.20
3	10	54	5.40
4	20	62	3.10
5	30	89	2.97

ตารางที่ 4-9 แสดงผลการสังเกตการณ์ deploy OS เครื่องคอมพิวเตอร์ HP EliteDesk 705 G1 โดยผลการ deploy จำนวนมากขึ้นพบว่าเวลาในการ deploy ต่อเครื่องลดลงเรื่อย ๆ ซึ่งผู้เขียนงานนิพนธ์ได้ทดสอบ deploy สูงสุด 30 เครื่อง ใช้เวลาทั้งหมด 89 นาที และเฉลี่ยเวลาต่อเครื่อง 2.97 นาทีดังภาพที่ 4-37



ภาพที่ 4-37 กราฟแสดงผลเวลา deploy OS เครื่อง HP EliteDesk 705 G1

ภาพที่ 4-37 แสดงกราฟเวลาในการ deploy OS เครื่อง HP EliteDesk 705 G1 ซึ่งหาก deploy OS จำนวน 1 เครื่องจะใช้เวลาต่อเครื่อง 41 นาที แต่ถ้าหาก deploy จำนวนมากขึ้นจะสามารถลดเวลาดำเนินการต่อเครื่องลงได้ ทั้งนี้ขึ้นอยู่กับความสามารถของระบบเครือข่ายด้วยเนื่องจากการ deploy ที่ผู้เขียนงานนิพนธ์ทดสอบนั้น ได้เตรียมไว้เฉพาะทดสอบ deploy OS ผ่านระบบ SCCM เท่านั้นไม่ได้มีการแชร์การใช้งานอุปกรณ์เครือข่ายกับส่วนงานอื่น ๆ

4.6.3 ผลการสังเกตการณ์เครื่องที่อยู่ในโปรดักชันจริงสามารถอัปเดตวินโดวส์ได้หรือไม่  
จากการสังเกตการณ์อัปเดตวินโดวส์จำนวน 326 เครื่องซึ่งเป็นเครื่องคอมพิวเตอร์ที่ติดตั้ง  
ระบบปฏิบัติการวินโดวส์ 7 32 บิต ได้ผลดังภาพที่ 4-38

Collection Name	Clients in Collection
C60-LS_32	326

State	Count of Computers	% of Total
Compliant	280	85.89
Compliance state unknown	43	13.19
Non-compliant	3	0.92

ภาพที่ 4-38 ผลการอัปเดตวินโดวส์วันที่ 18 พ.ค.2559

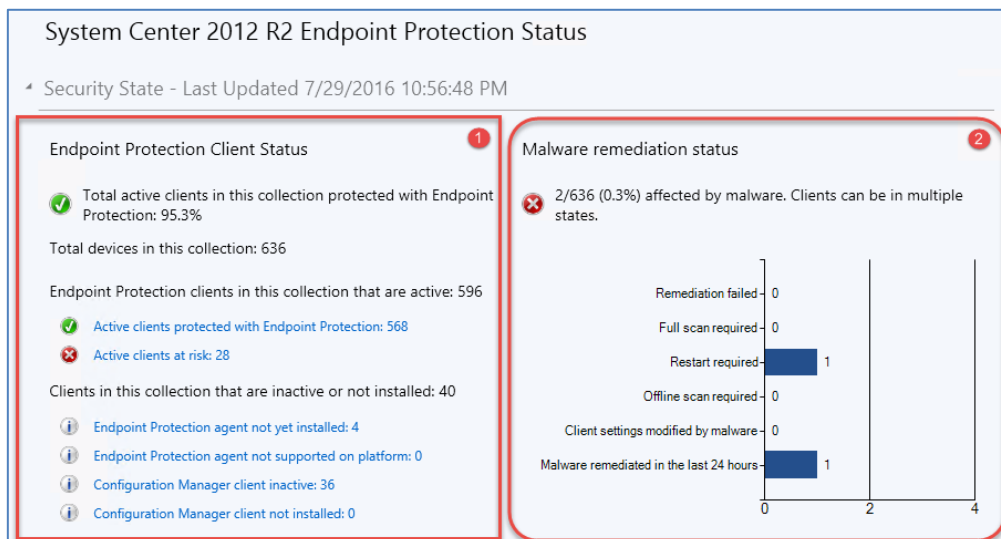
ภาพที่ 4-38 แสดงผลการอัปเดตวินโดวส์ 326 เครื่อง พบว่าสามารถอัปเดตได้สำเร็จจำนวน 280 เครื่อง คิดเป็น 85.89% และเครื่องที่ไม่สำเร็จจำนวน 46 เครื่องคิดเป็น 14.11% โดยจากการตรวจสอบพบว่าเครื่องที่ไม่สามารถรับการอัปเดตวินโดวส์ได้ เนื่องจากคอมพิวเตอร์เป็นรุ่นเก่าและไดรฟ์ c: ใกล้เต็มแล้ว จึงติดปัญหาเรื่องเนื้อที่ของฮาร์ดดิสก์คอมพิวเตอร์ไม่เพียงพอ ดังภาพที่ 4-39

Total Assets	Status	Error Code	Error Description	Summarization Time	Collection
28	Failed to install update(s)	0XB007000E	Not enough storage is available to complete this operation.	7/27/2016 11:51 PM	C60-LS_32
4	Failed to install update(s)	0XC80003F3	Unknown Error (-939523085)	7/27/2016 11:51 PM	C60-LS_32
2	Failed to install update(s)	0XC8000222	Unknown Error (-939523550)	7/27/2016 11:51 PM	C60-LS_32
2	Failed to install update(s)	0XB0004005	Unspecified error	7/27/2016 11:51 PM	C60-LS_32
1	Failed to install update(s)	0XD0000000	Success	7/27/2016 11:51 PM	C60-LS_32
1	Failed to install update(s)	0XB0070308	The client of a component requested an operation which is not valid given the st...	7/27/2016 11:51 PM	C60-LS_32

ภาพที่ 4-39 ผลการอัปเดตวินโดวส์ผิดพลาด [Error]

ภาพที่ 4-39 แสดงผลการอัปเดตวินโดวส์ที่เกิดความผิดพลาดจากเนื้อที่ของฮาร์ดดิสก์ไม่เพียงพอจำนวน 28 เครื่อง และบางเครื่องเกิดความผิดพลาดจากการอัปเดตแล้วขาดการเชื่อมต่อระบบเครือข่ายหลุดจากเน็ตเวิร์ก หรือผู้ใช้ปิดเครื่องคอมพิวเตอร์ก่อนการอัปเดตจะเสร็จสิ้น จึงทำให้เกิดข้อผิดพลาดดังกล่าว

4.6.4 เครื่องที่อยู่ในโปรดักชันจริงสามารถอัปเดตโปรแกรมป้องกันไวรัสได้ก็เครื่อง การอัปเดตโปรแกรมป้องกันไวรัสคอมพิวเตอร์ เครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่าย บริษัทกาลโซนิคประเทศไทยมีเครื่องโดยประมาณ 636 เครื่อง



ภาพที่ 4-40 ผลการอัปเดต Definition โปรแกรมป้องกันไวรัส Endpoint protection client

ภาพที่ 4-40 ในสี่เหลี่ยมกรอบที่ 1 แสดงคอมพิวเตอร์ผู้ใช้งานโปรแกรมป้องกันไวรัส Endpoint protection client มีจำนวนเครื่องผู้ใช้ทั้งหมด 636 เครื่อง โดยแยกเป็นเครื่องที่กำลังใช้งานและได้รับการเชื่อมต่อกับระบบเซิร์ฟเวอร์ส่วนกลางในระยะไม่เกิน 7 วัน จำนวน 596 เครื่องและเครื่องที่ไม่ได้มีการใช้งานหรือขาดการเชื่อมต่อกับระบบเซิร์ฟเวอร์ส่วนกลางเกิน 7 วัน จำนวน 40 เครื่อง

เครื่องที่กำลังใช้งาน 596 เครื่องมีเครื่องที่ได้รับการอัปเดตและป้องกันไวรัสโดยโปรแกรม Endpoint protection client จากเซิร์ฟเวอร์ส่วนกลางจำนวน 568 เครื่อง (95.3%) และเครื่องที่มีความเสี่ยงจำนวน 28 เครื่อง (4.7%) ซึ่งจากการตรวจสอบพบว่าเครื่องที่มีความเสี่ยงคือเครื่องที่ยังไม่สามารถอัปเดต Definition โปรแกรมป้องกันไวรัสเป็นเวอร์ชันปัจจุบันและยังมีบางเครื่องที่รอการอัปเดต Definition ให้สมบูรณ์โดยการเริ่มต้นเครื่องคอมพิวเตอร์ใหม่อีกครั้งนั่นเอง (Restart)

เครื่องคอมพิวเตอร์ที่ไม่ได้มีการใช้งานจำนวน 40 เครื่อง พบว่าเป็นเครื่องที่ยังไม่ได้ติดตั้ง agent จำนวน 4 เครื่อง และเครื่องที่ขาดการเชื่อมต่อกับระบบ SCCM จะขึ้นสถานะเป็น Inactive จำนวน 36 เครื่อง

จากภาพที่ 4-40 ในสี่เหลี่ยมกรอบที่ 2 แสดงผลการป้องกันไวรัส ซึ่งมี 2 เครื่องที่ถูกตรวจพบไวรัส จากนั้นผู้เขียนงานนิพนธ์ได้ตรวจสอบพบว่าโปรแกรมป้องกันไวรัสได้ลบไฟล์ keygen ซึ่งเป็นไฟล์ของโปรแกรมปลอมคีย์ (Crack) ผลลัพธ์โปรแกรมประยุกต์ ซึ่งโปรแกรมป้องกันไวรัส Endpoint protection client พบโปรแกรมดังกล่าวมีความเสี่ยงและอาจจะเป็นไวรัสคอมพิวเตอร์จึงได้ลบไฟล์นั้นทิ้งไป

สรุปจากการตรวจสอบพบว่าโปรแกรมป้องกันไวรัส Endpoint protection client สามารถใช้งานและป้องกันไวรัสคอมพิวเตอร์ได้โดยมีบางไวรัสหรือความเสี่ยงที่โปรแกรม Endpoint protection client ไม่สามารถป้องกันได้ เช่นไวรัส autorun ที่มาจากแฟลชไดรฟ์ ไวรัสที่มาในรูปแบบสแปมเมล และอื่น ๆ ซึ่งอาจจะต้องใช้โปรแกรมเฉพาะสำหรับการป้องกัน



## บทที่ 5

### อภิปรายและสรุปผล

ในงานนิพนธ์นี้ ผู้วิจัยได้จัดทำระบบการจัดการกำหนดค่าซอฟต์แวร์จากส่วนกลาง (SCCM 2012 R2) กรณีศึกษา บริษัทคาลโซนิค คันทเซ (ประเทศไทย) จำกัด โดยเครื่องคอมพิวเตอร์ของบริษัท มีทั้งหมดประมาณ 600 เครื่อง ซึ่งผลการทดสอบสรุปได้ดังนี้

1. ผลการทดสอบการทำงานของฐานข้อมูล ในกรณีเครื่องฐานข้อมูลตัวหลักเกิดปัญหาในระบบปฏิบัติการวินโดว์ หรือ เครื่องหยุดการทำงาน โดยใช้เวลาในการย้ายไปใช้งานเซิร์ฟเวอร์ฐานข้อมูลอีกตัวหนึ่งประมาณ 14-18 วินาที เฉลี่ยในจำนวน 10 ครั้ง ประมาณ 16 วินาที

2. ผลการทดสอบ deploy ระบบปฏิบัติการวินโดว์ 7 โดยทดสอบ deploy เครื่องคอมพิวเตอร์รุ่น HP EliteDesk 705 G1 จำนวน 30 เครื่อง ซึ่งผลที่ได้สามารถ deploy สำเร็จในเวลา 89 นาที และได้ทำการทดสอบเครื่องรุ่นอื่น ๆ ที่มีสเปคต่างกันโดยผลการทดสอบพบว่าเวลาในการ deploy ขึ้นอยู่กับสเปคของอุปกรณ์เน็ตเวิร์กที่สามารถรองรับปริมาณการรับ-ส่งข้อมูล (Bandwidth) จาก SCCM เซิร์ฟเวอร์ไปที่เครื่องผู้ใช้, ความเร็วของการเขียน Hard disk และหน่วยความจำหลัก (Memory RAM) ของเครื่องคอมพิวเตอร์ด้วย

3. ผลการทดสอบ deploy โปรแกรมประยุกต์ซึ่งเป็นซอฟต์แวร์มาตรฐานของบริษัท จำนวน 11 ซอฟต์แวร์ ซึ่งสามารถ deploy ได้ทั้งหมด 10 ซอฟต์แวร์ โดยระยะเวลาในการ deploy แล้วเสร็จขึ้นอยู่กับขนาดของซอฟต์แวร์ด้วย สำหรับซอฟต์แวร์ที่ไม่สามารถ deploy ได้ เนื่องจากระบบ SCCM ไม่รองรับการทำงานชื่อโปรแกรม LEXITRONDictionary 2.6

4. ผลทดสอบ deploy วินโดว์อัปเดตจำนวน 326 เครื่อง ซึ่งเป็นเครื่องที่ใช้ระบบปฏิบัติการวินโดว์ 7 โดยเครื่องคอมพิวเตอร์สามารถรับการอัปเดตคิดเป็น 85.89% ส่วนที่เหลือไม่สามารถอัปเดตได้เนื่องจากปัญหาของเนื้อที่จัดเก็บของไดรฟ์ C: ไม่เพียงพอ และเครื่องที่ไม่ได้เปิดใช้งาน

5. ผลทดสอบติดตั้งโปรแกรมประยุกต์โดยผู้ใช้เลือกติดตั้งเอง โดยจากการทดสอบผู้ใช้สามารถเลือกติดตั้งได้จากโปรแกรม SCCM Software Center ทั้งนี้ขึ้นอยู่กับขนาดของไฟล์และการเชื่อมต่ออุปกรณ์เน็ตเวิร์กด้วย

6. ผลการทดสอบเรียกดูรายงานสเปคเครื่องคอมพิวเตอร์ทั้ง 3 แผนก ปรากฏว่าสามารถเรียกดูข้อมูลสเปคฮาร์ดแวร์คอมพิวเตอร์ได้ตรงกับเครื่องที่มีการใช้งานอยู่จริง

7. ผลทดสอบ deploy อัปเดตโปรแกรมป้องกันไวรัส SCEP จำนวน 636 เครื่อง พบว่าเครื่องผู้ใช้ได้รับการอัปเดตคิดเป็น 95.3% โดยเครื่องผู้ใช้ที่ไม่ได้รับการอัปเดตพบว่าสถานะของเครื่องไม่ได้เปิดใช้งานหรือขาดการเชื่อมต่อกับระบบนานเกิน 60 วัน

8. ผลทดสอบควบคุมเครื่องผู้ใช้จากระยะไกลเพื่อช่วยเหลือแก้ไขปัญหาให้กับผู้ใช้ โดยการทดสอบได้พบว่าสามารถควบคุมเครื่องผู้ใช้จากระยะไกลได้ทั้งแบบเลือกซื้อเครื่องคอมพิวเตอร์ และไอพีแอดเดรสของเครื่องปลายทางได้

จากการทดสอบพบว่าการทำงานของระบบการจัดการกำหนดค่าซอฟต์แวร์จากส่วนกลางสามารถช่วยลดระยะเวลาในการปรับปรุงซอฟต์แวร์ให้เป็นมาตรฐานและช่วยลดงานของแผนกไอทีในการอัปเดตโปรแกรมวินโดวส์เพื่อปิดช่องโหว่หรือความเสี่ยงจากผู้ไม่ประสงค์ดี และผู้ดูแลระบบสามารถควบคุมเครื่องผู้ใช้จากระยะไกลได้ด้วย

## บรรณานุกรม

- ไทยเซิร์ต. (2559, 1 กันยายน). *ระวังภัย ช่องโหว่ใน OpenSSL ผู้ไม่หวังดีสามารถขโมยข้อมูลใน Memory จากเครื่องของเหยื่อได้ (Heartbleed, CVE-2014-0160)*. เข้าถึงได้จาก <https://www.thaicert.or.th/alerts/admin/2014/al2014ad002.html>
- นพดล สุขศรี บีทีเตอร์. (2557). *คู่มือติดตั้งและเทคนิคการใช้งาน Windows Server 2012 R2*. กรุงเทพมหานคร, บริษัทซีไอทียูเคชั่น จำกัด (มหาชน).
- Ace Fekay. (2559, 20 สิงหาคม). *Windows Server 2012 AD Cloning, Snapshot Support & Preventing USN Rollbacks*. เข้าถึงได้จาก [http://blogs.ms\\_mvps.com/acefekay/category/usn-active-directory-replication/](http://blogs.ms_mvps.com/acefekay/category/usn-active-directory-replication/)
- Adam Gordon. (2559, 6 สิงหาคม). *SCCM 2012 R2 Upgrade Checklist/Guide*. เข้าถึงได้จาก <https://www.linkedin.com/pulse/20141105163714-5177136-sccm-2012-r2-upgrade-checklist-guide>
- Adobe.com. (2559, 22 สิงหาคม). *Security updates available for Adobe Flash Player*. เข้าถึงได้จาก <https://helpx.adobe.com/security/products/flash-player/apsb15-09.html>
- CS Odessa. (2559, 17 สิงหาคม). *Active Directory Domain Services Diagram*. เข้าถึงได้จาก <http://www.conceptdraw.com/solution-park/computer-active-directory>
- Microsoft. (2559, 5 สิงหาคม). *Recommended hardware for System Center Configuration Manager*. เข้าถึงได้จาก <https://msdn.microsoft.com/en-gb/library/mt589500.aspx>
- Microsoft. (2559, 17 สิงหาคม). *Logical structure of Active Directory*. เข้าถึงได้จาก <https://msdn.microsoft.com/en-us/library/bb742592.aspx>
- Microsoft. (2559, 18 สิงหาคม). *Domain and Forest*. เข้าถึงได้จาก <https://i-msdn.sec.msft.com/dynimg/IC197060.gif>
- Microsoft, (2559, 18 สิงหาคม). *Review the Existing Physical Structure*. เข้าถึงได้จาก [https://technet.microsoft.com/cs-cz/library/dd734784\(v=ws.10\).aspx](https://technet.microsoft.com/cs-cz/library/dd734784(v=ws.10).aspx)
- Microsoft. (2559, 20 สิงหาคม). *Active Directory Security Groups*. เข้าถึงได้จาก [https://technet.microsoft.com/en-us/library/dn579255\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx)

Ned Pyle. (2559, 22 สิงหาคม). *Fail to log Security Settings from Default Domain Policy*.

เข้าถึงได้จาก <https://blogs.technet.microsoft.com/askds/2008/09/22/fail-to-log-security-settings-from-default-domain-policy/>

Tarek Majdalani. (2559, 20 สิงหาคม). *How to Raise the Forest and Domain Functional*

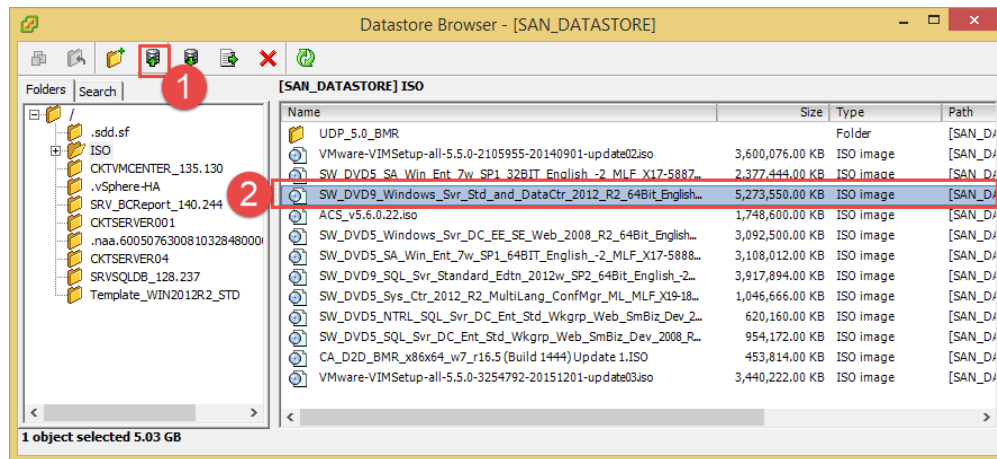
*Levels in Windows Server 2008/R2*. เข้าถึงได้จาก [http://www.elmajdal.net/win2k8/How\\_To\\_Raise\\_the\\_Forest\\_and\\_Domain\\_Functional\\_Levels\\_in\\_Windows\\_Server\\_2008\\_R2.aspx](http://www.elmajdal.net/win2k8/How_To_Raise_the_Forest_and_Domain_Functional_Levels_in_Windows_Server_2008_R2.aspx)

ภาคผนวก

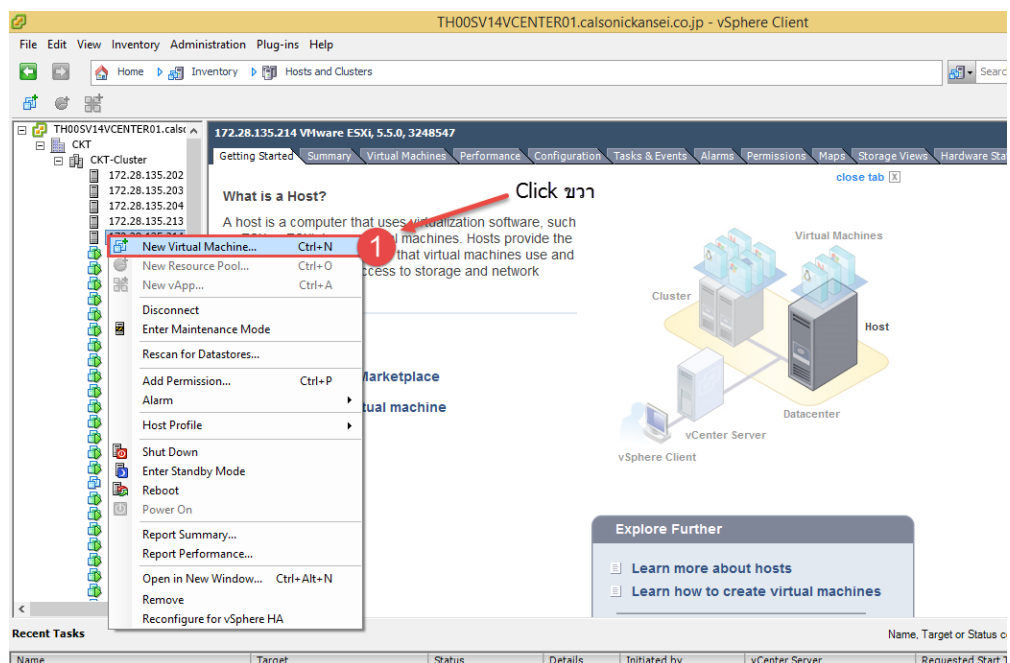
ภาคผนวก ก  
ติดตั้งระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2012

## ติดตั้งระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2012

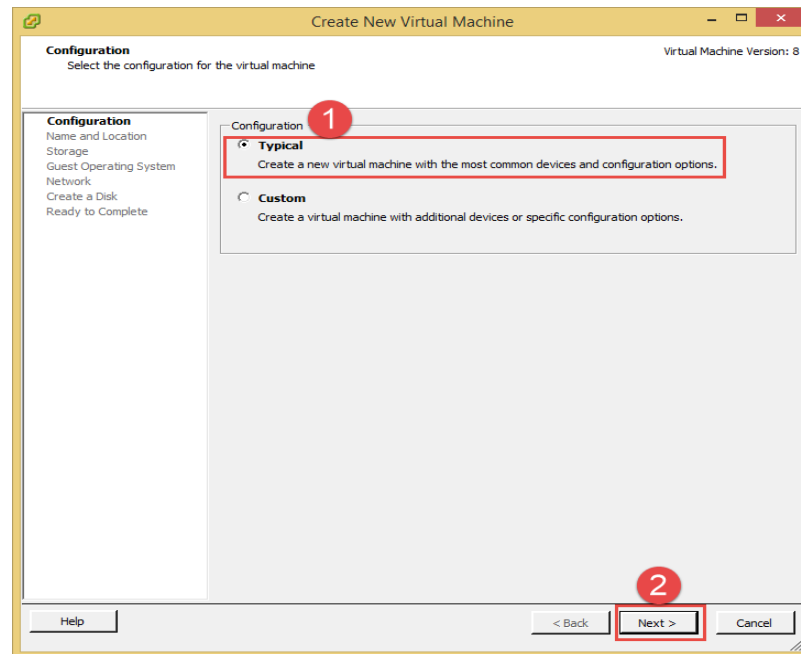
- 1.) Load CD หรือ file iso เข้าไปใน Data store ของ Vmware (กรณีเราใช้ Vmware ในการติดตั้ง Windows)



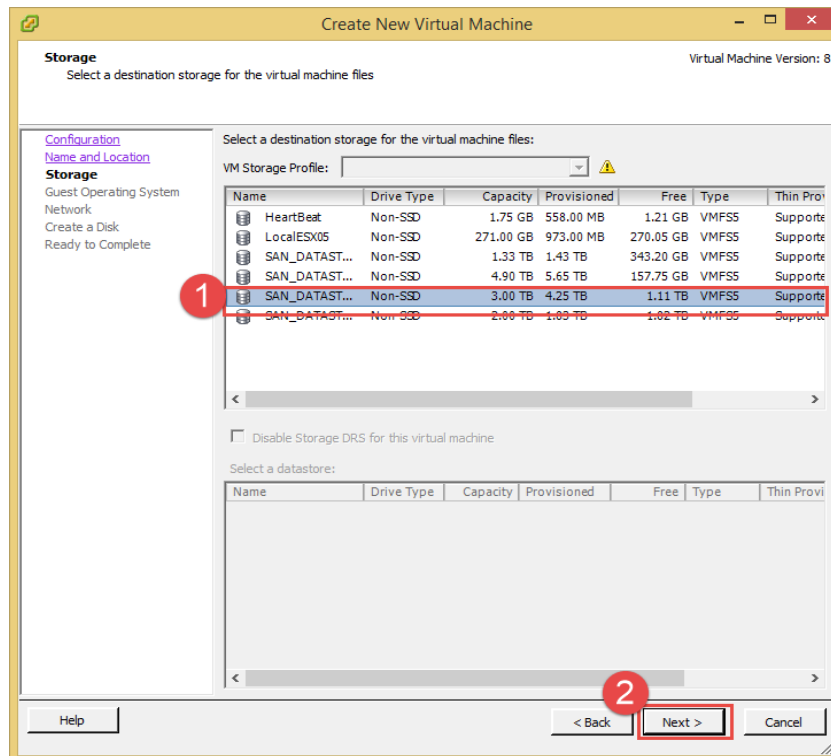
- 2.) หลังจาก LOAD ISO file เรียบร้อยแล้วให้ไป Create Guest บน VMware ตามรูปด้านล่าง



3.) ทำการเลือก Configuration เป็น Typical แล้ว กด Next

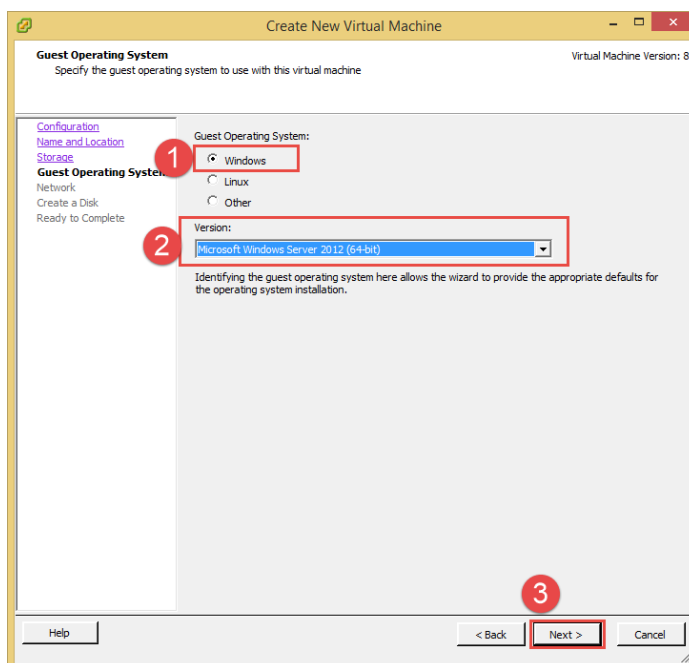


4.) จากนั้นเลือก Disk ที่จะติดตั้งลงไป จากนั้นกด Next

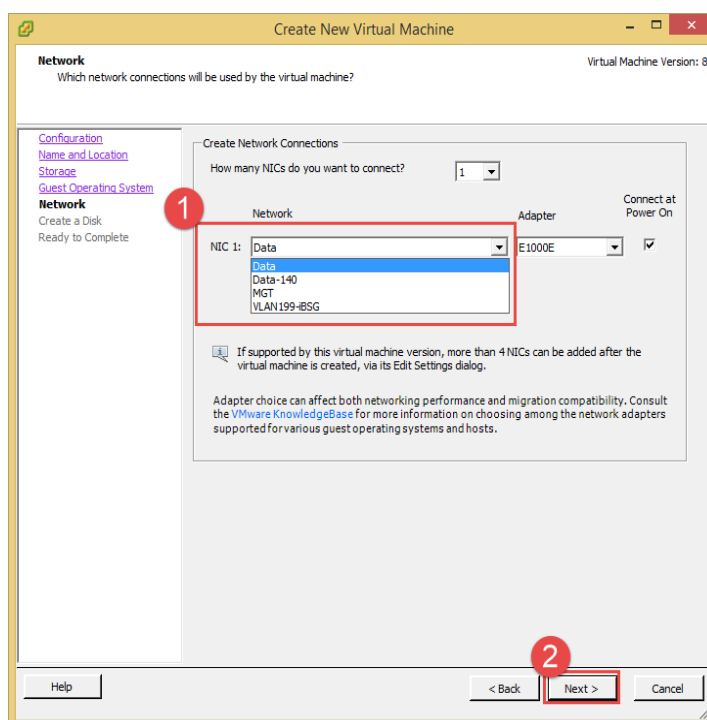




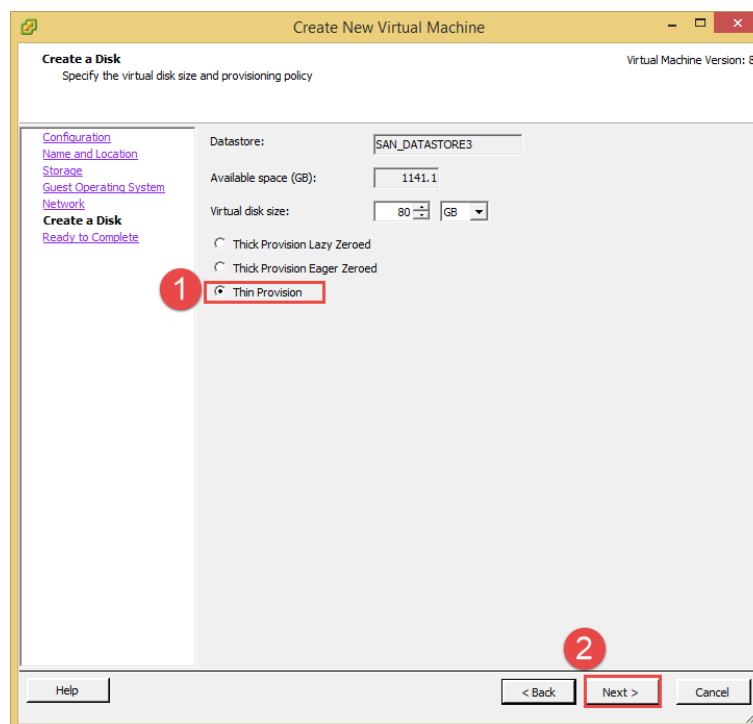
- 5.) จากนั้นทำการเลือก Operation System เป็น Windows แล้วเลือก version “Microsoft Windows Server 2012 (64bit)”



- 6.) จากนั้นเลือก Network Card ตามที่ได้มีการแบ่ง Network ไว้ ตามรูปด้านล่างนี้ แล้วกด Next

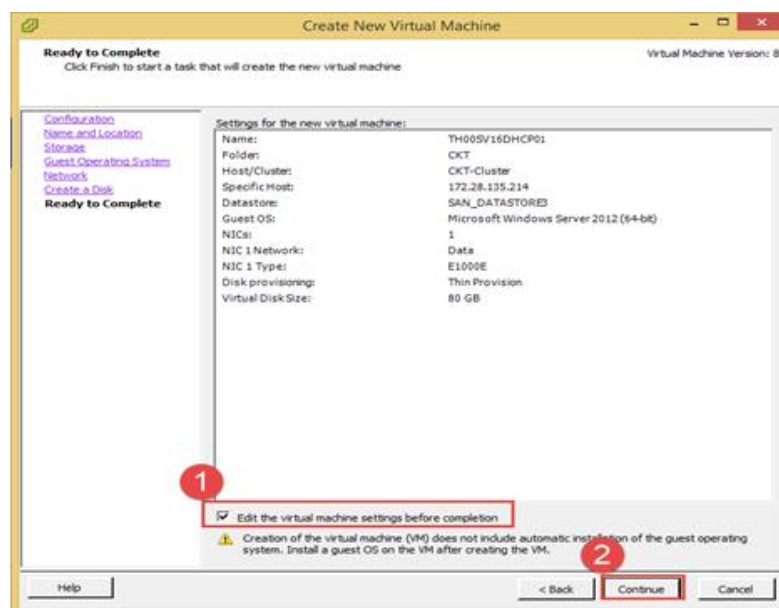


- 7.) จากนั้นกำหนดขนาด Disk ของ Drive ให้กับ Windows ตามรูปด้านล่าง แล้วกด Next

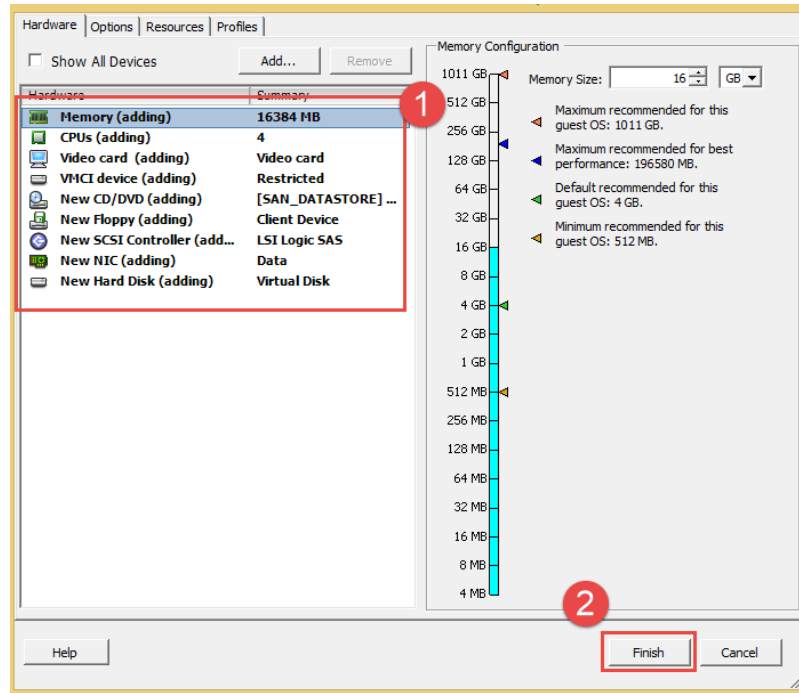


Thin Provisioning หมายถึง การจองพื้นที่ตามการใช้งาน เช่น หากทำการจองพื้นที่ 100GB แล้วมีการใช้งาน เพียงแค่ 30GB บน storage ก็จะมีพื้นที่ถูกใช้ไปแค่ 30GB

- 8.) Summary ในการ Create Guest จากกด “Continue”



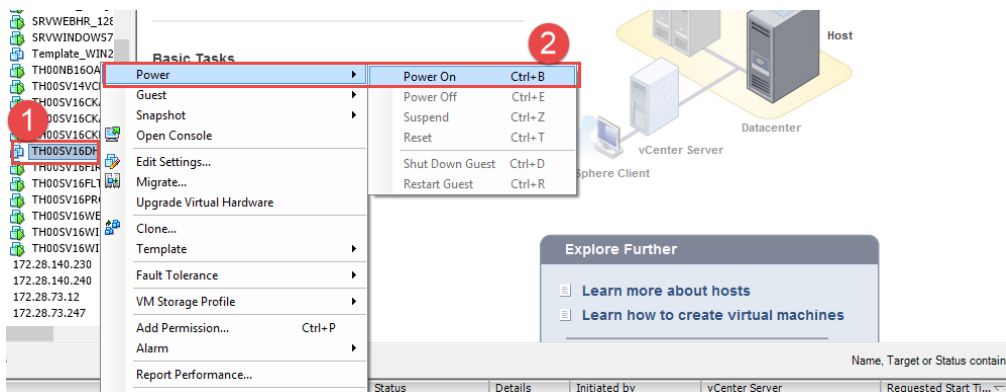
- 9.) จากนั้นกำหนด CPU, RAM, Boot CDROM ตามรูปด้านล่างนี้



ระบบจะทำการ Create Guest จากนั้นทำการ ติดตั้ง Windows 2012 R2

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed
Create virtual machine	CKT	Completed	CKTHA1 ckt-infra	TH00SV14VCENTER01.ca...	TH00SV14VCENTER01.ca...	4/8/2016 20:29:06	4/8/2016 20:29:06	4/8/2016

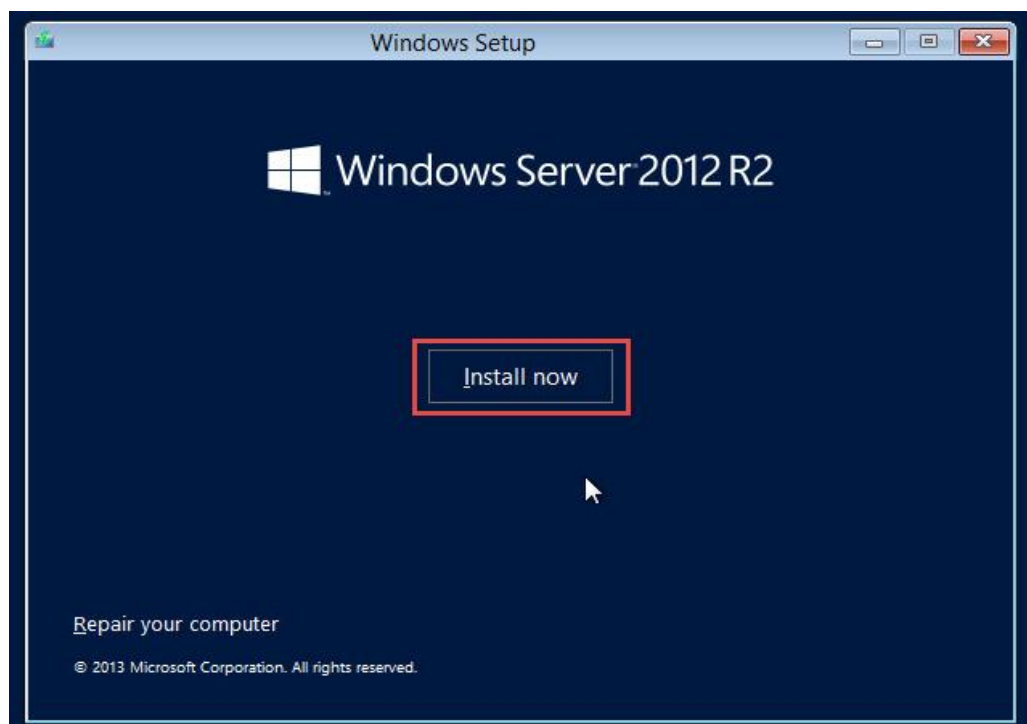
10.) ทำการ start เปิด Power Guest



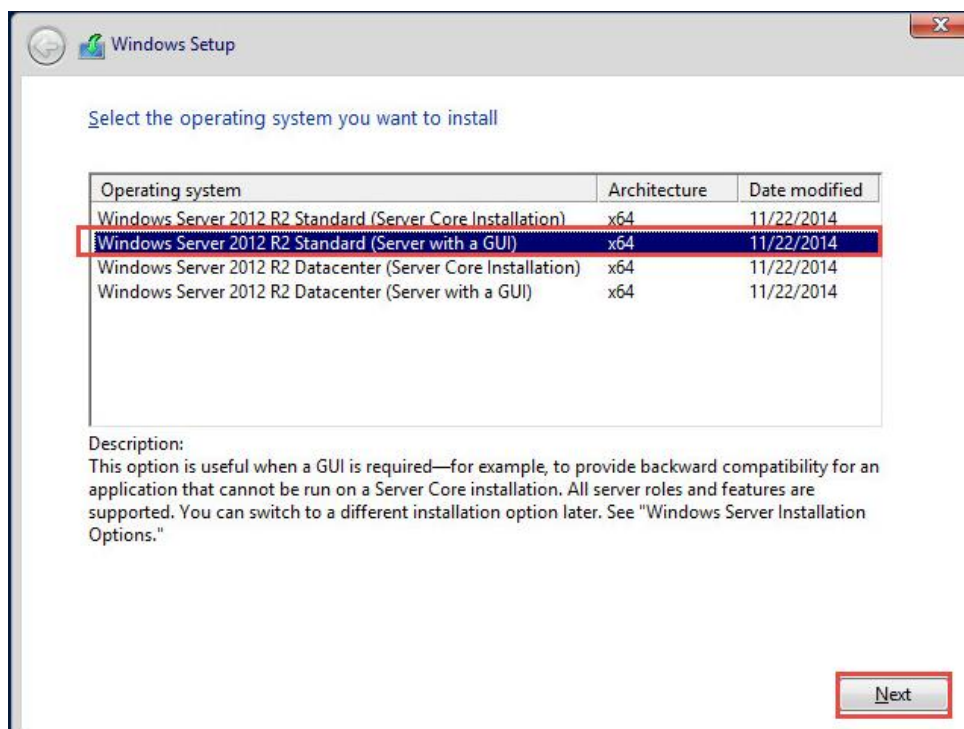
11.) จากนั้นเริ่มทำการติดตั้ง Windows Server 2012 R2



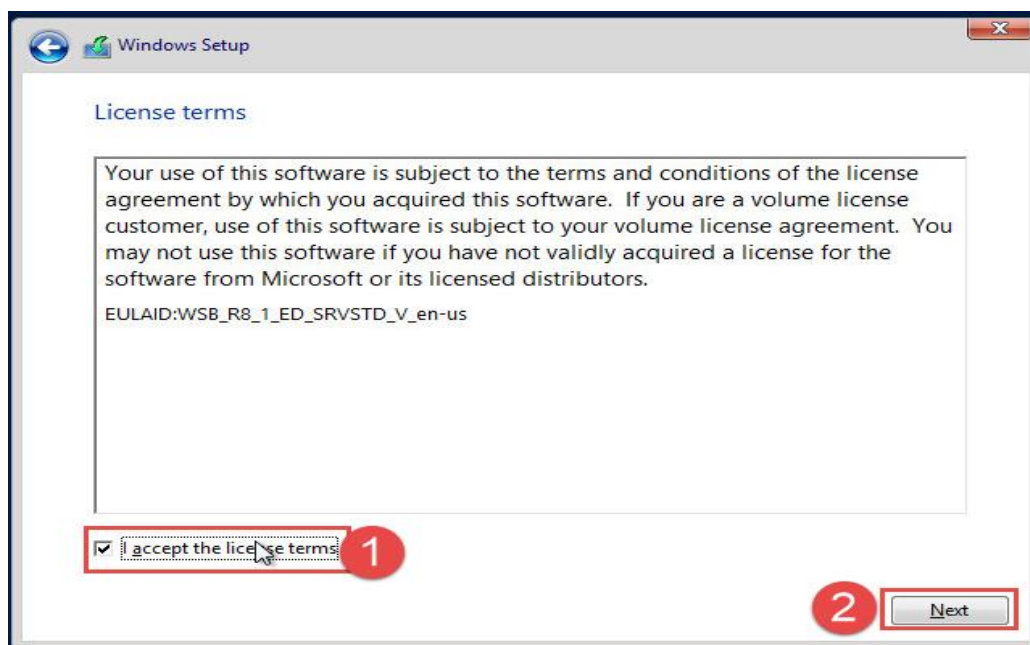
12.) หลังจากนั้นจากเลือก Install



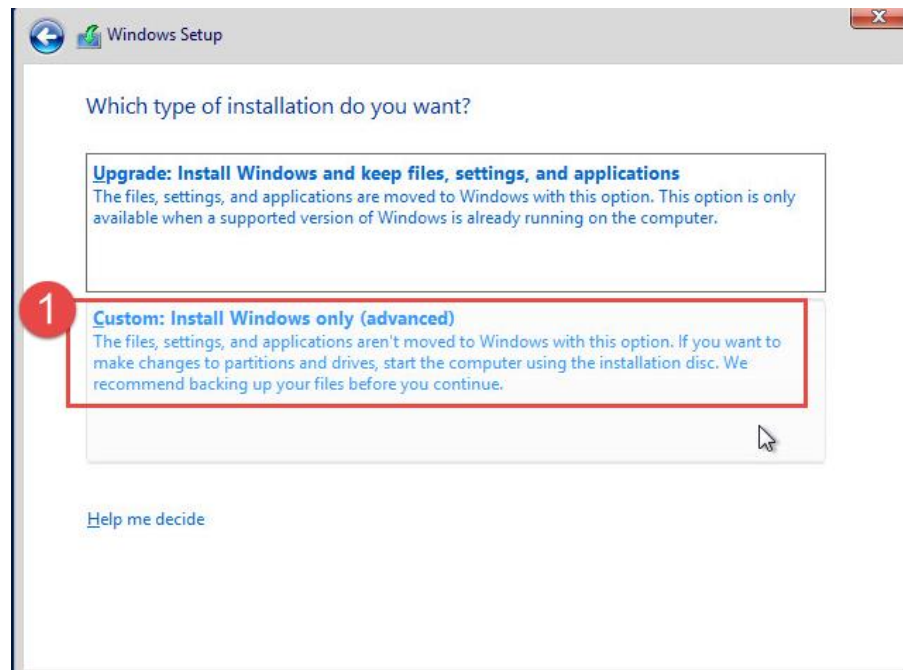
13.) ทำการเลือก Windows 2012 STD GUI



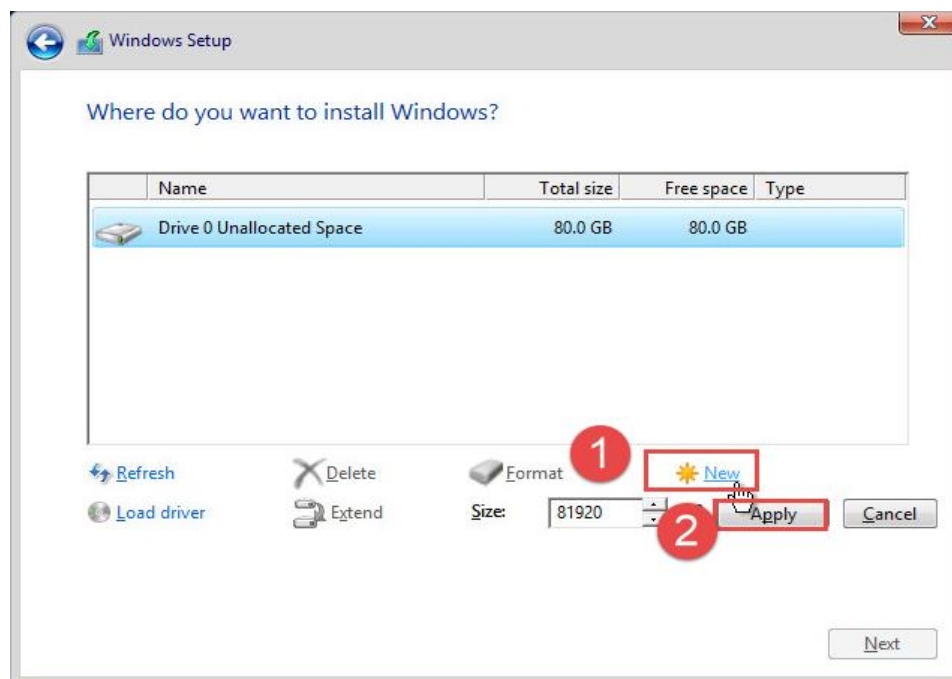
- 14.) จากนั้นทำการเลือก “I accept the license terms” เพื่อตกลงเรื่อง License



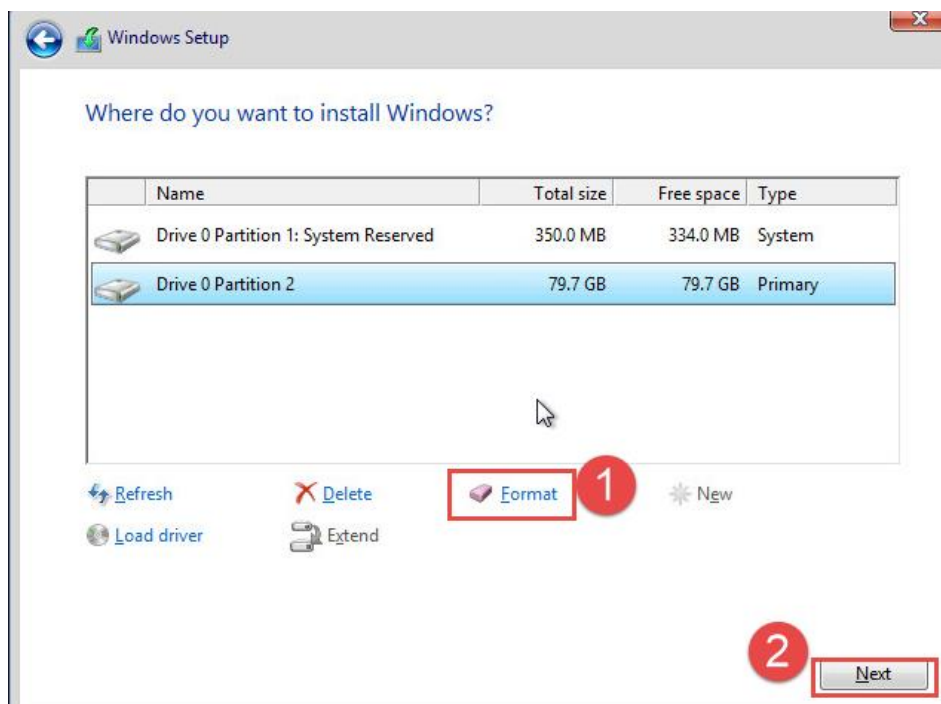
- 15.) เลือก “Custom: Install Windows only” เพื่อจะเข้าไป Create Disk และ format



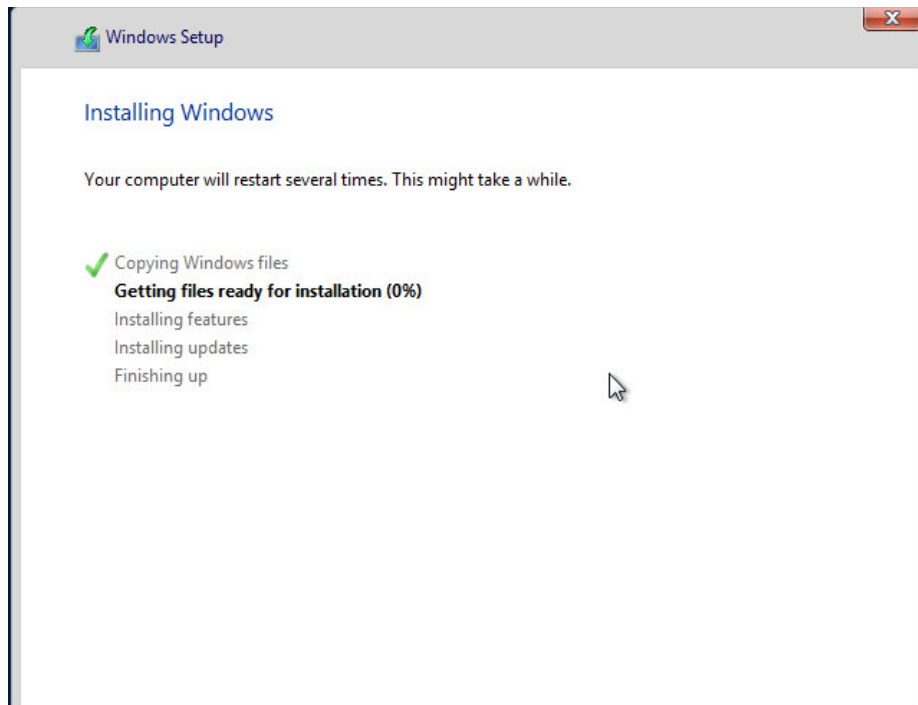
16.) ทำการเลือก “New” แล้วเลือก “Apply” เพื่อเลือกขนาด disk



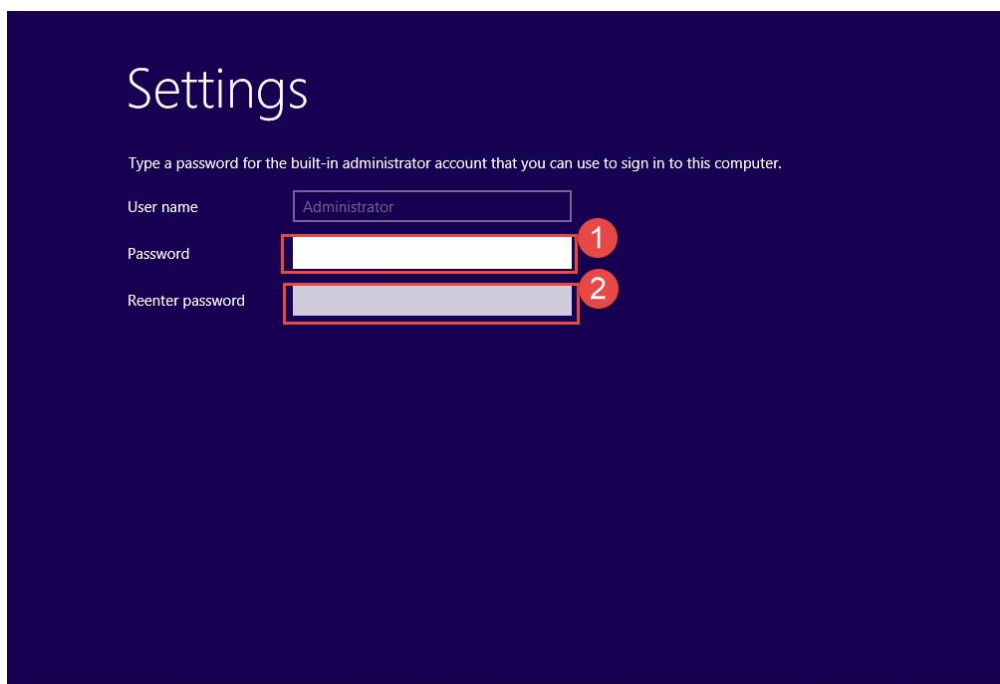
17.) ทำการ Format disk ที่เราเลือกไว้ จากนั้น กด “Next”



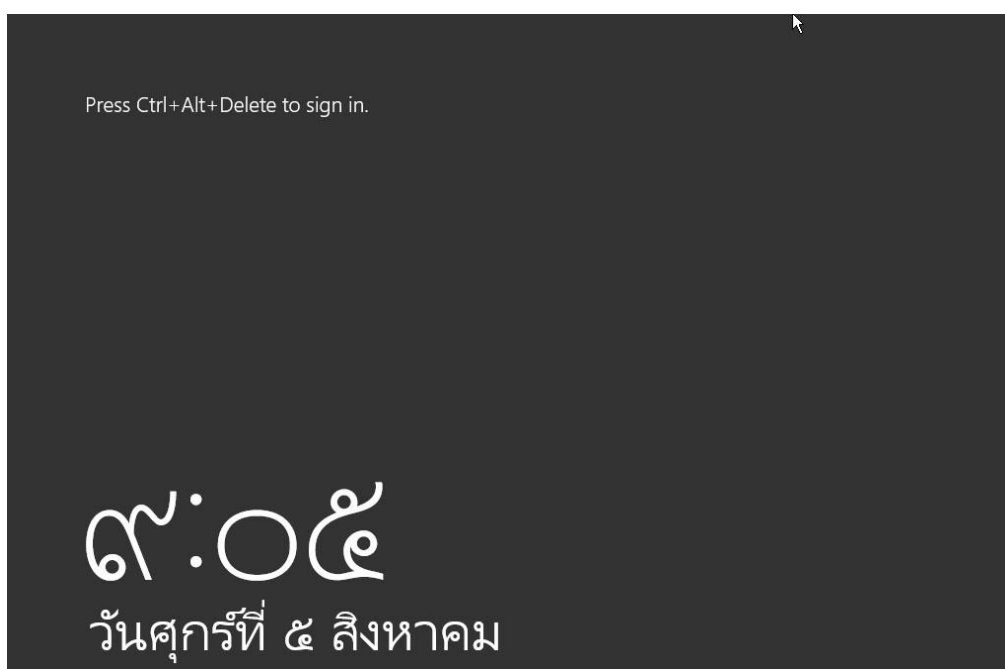
18.) จากนั้นทำการรอ Install Windows



19.) หลังจากทำการ Install Windows เสร็จแล้วจะทำการ reboot เครื่อง 1 ครั้งจากนั้นจะให้ใส่ Password ของ Administrator ของเครื่อง ดังรูปด้านล่างนี้ แล้วเลือก “Finish”



20.) จากนั้นก็จะขึ้นหน้า login ก็เป็นอันเสร็จในการ install



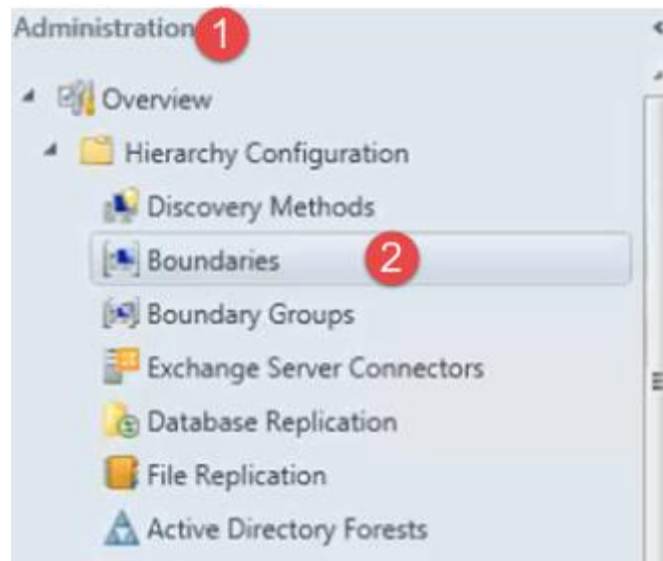


## ภาคผนวก ข

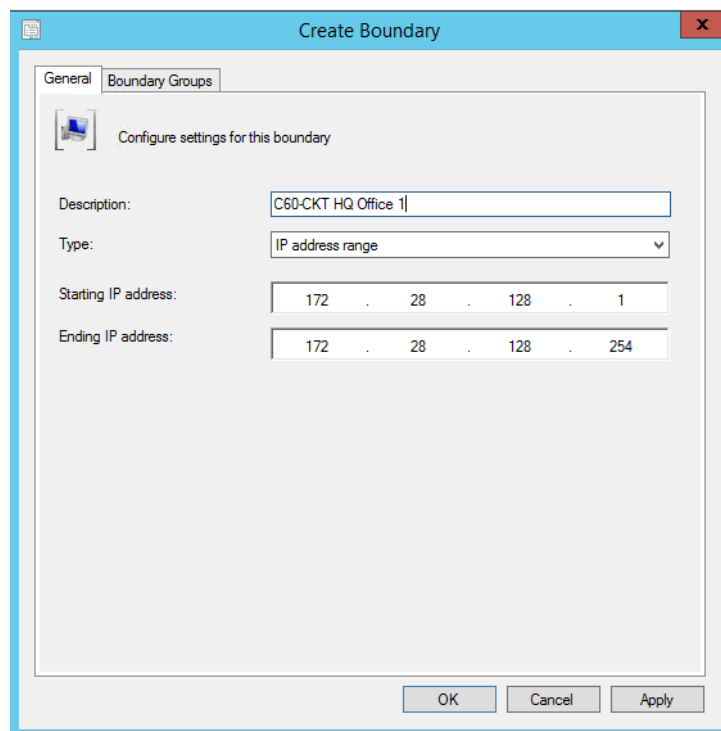
### สร้าง Boundaries

สร้าง Boundaries

1. เปิด โปรแกรม SCCM แล้วเข้าไปที่ Administration>Boundaries ดังรูป



2. จากนั้นคลิกขวาที่ Boundaries แล้วเลือก **Create Boundary** แล้วกำหนดชื่อในช่อง Description เลือก Type เป็น IP address range และใส่ IP Address ดังรูป



ภาคผนวก ค

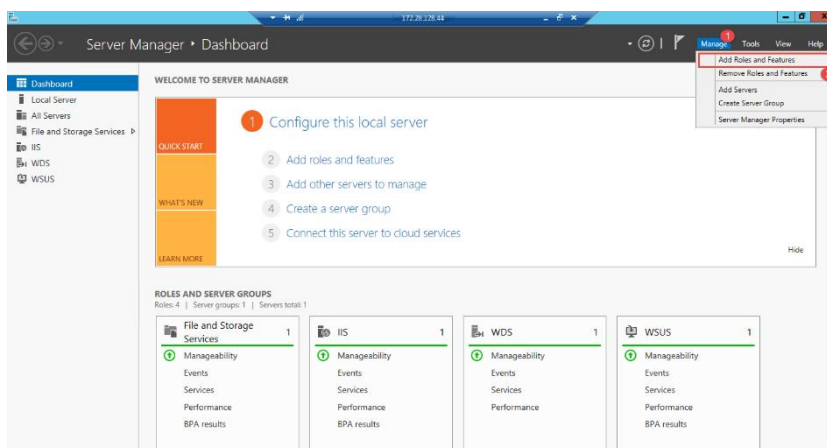
ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์หลัก (Primary site)

ติดตั้ง Primary Site.

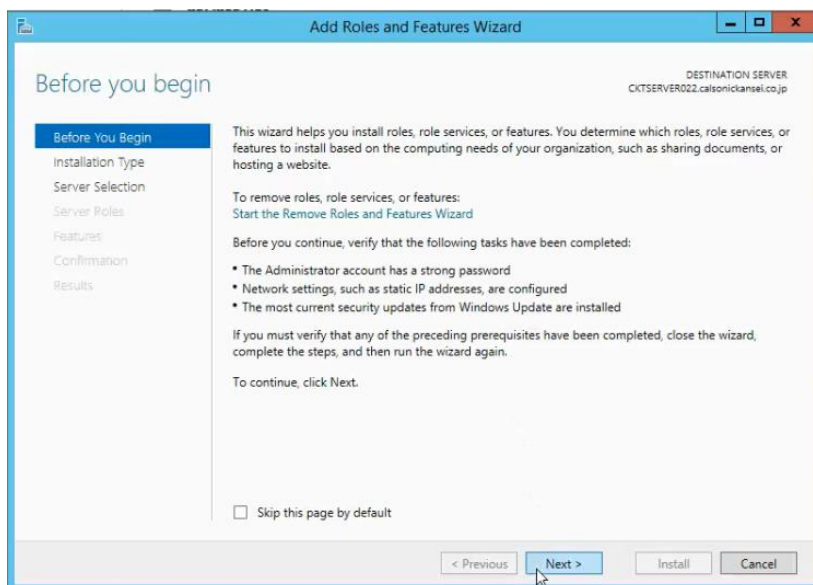
การติดตั้ง – Roles and Features (SCCM 2012 R2 – Configuration Manager)

เปิดเครื่อง Primary site (CKTSERVER022.calsonickansei.co.jp)

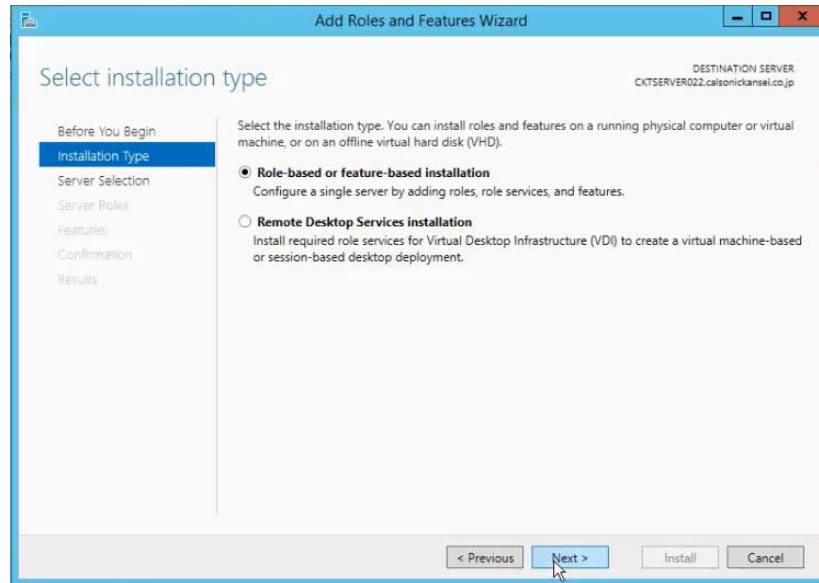
1. เข้าไปที่ Server Manager แล้วเลือก Manage>>Add rules and features



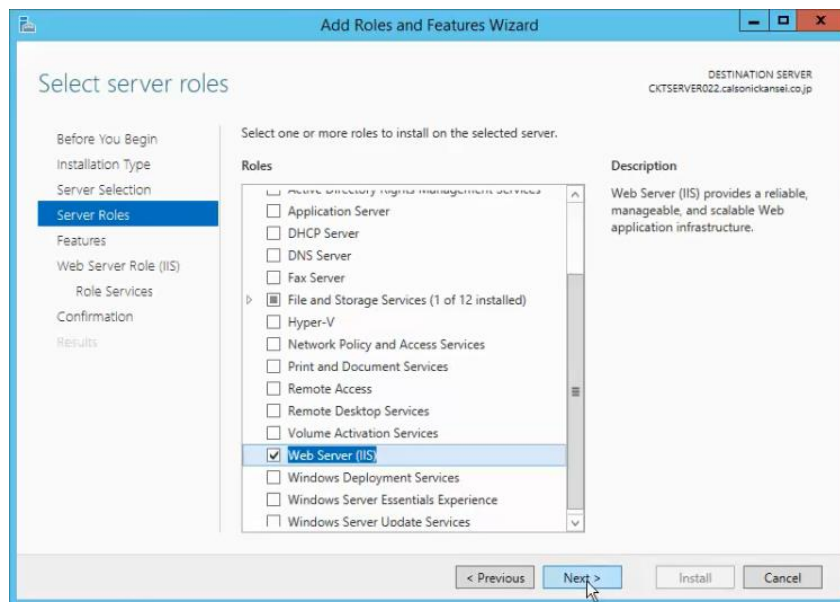
2. คลิก Next



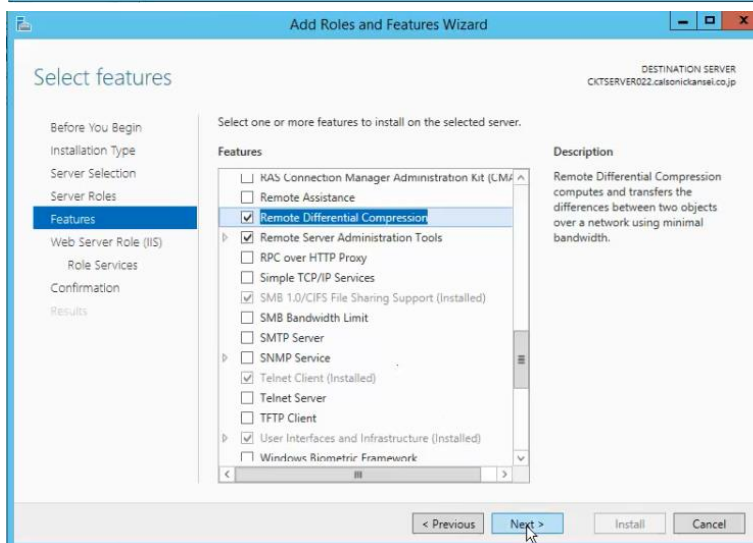
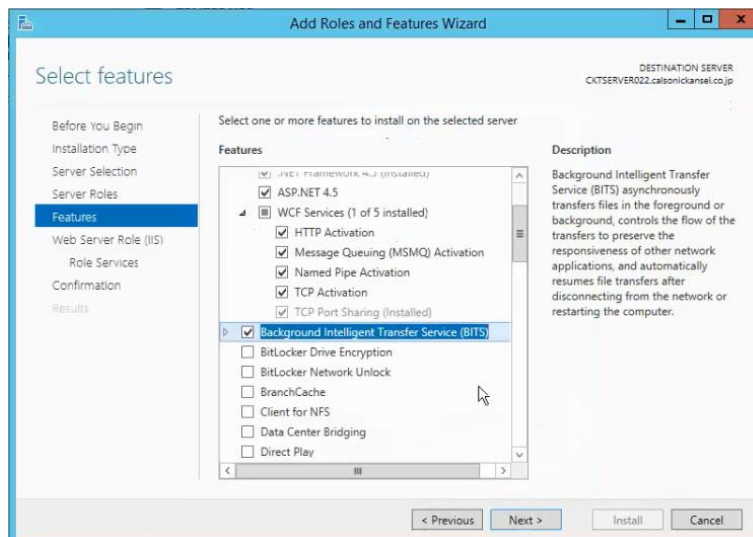
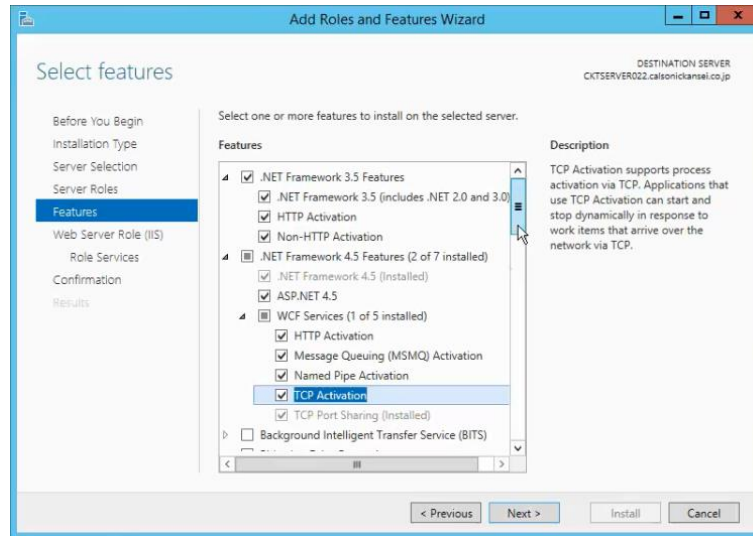
## 3. คลิก Next



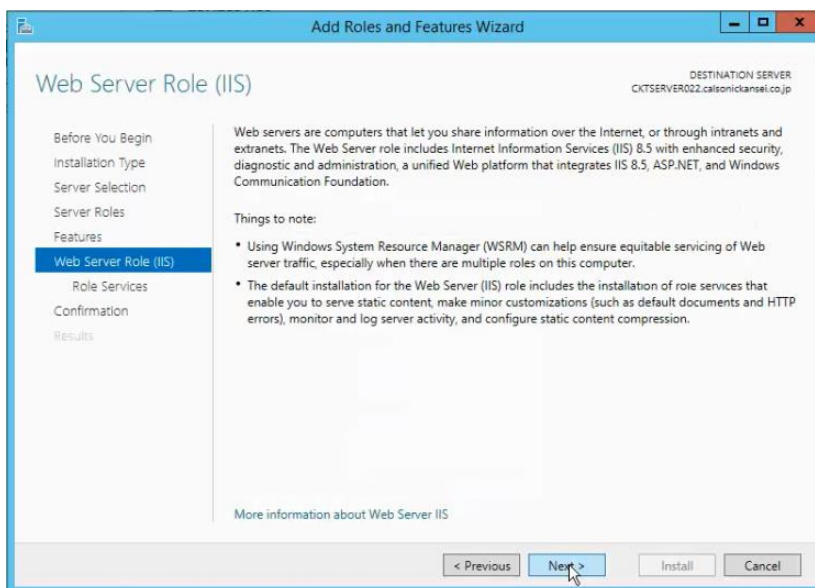
## 4. เลือก (IIS) จากนั้นคลิก Next.



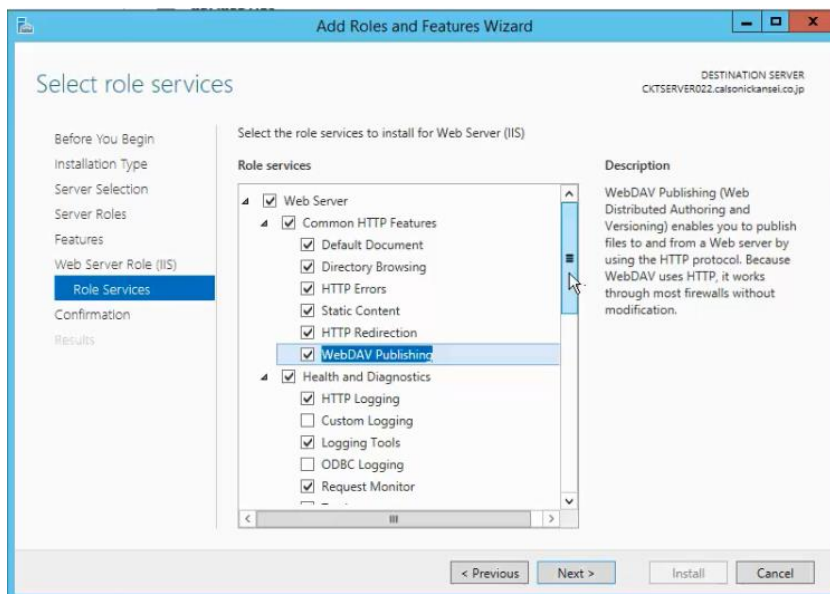
## 5. เปิดใช้งานคุณลักษณะ (features) ตามเอกสารติดตั้งไมโครซอฟต์

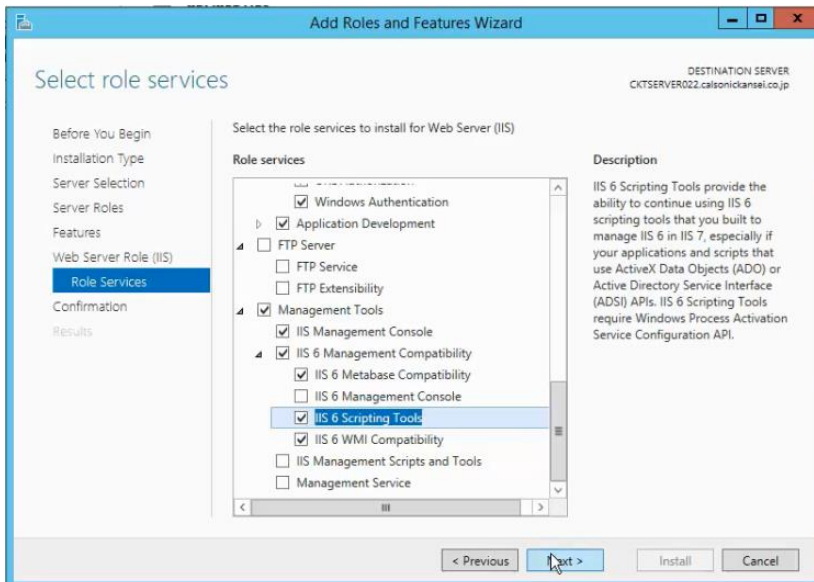
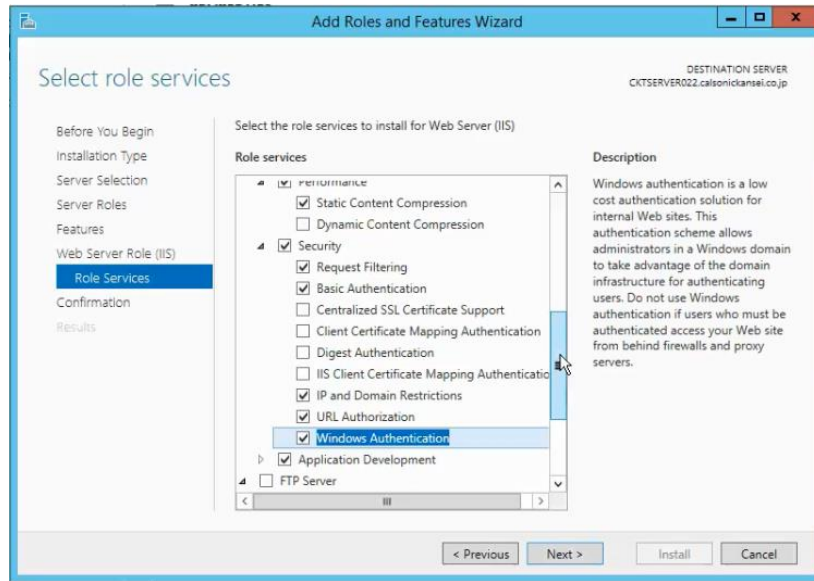


## 6. กด Next



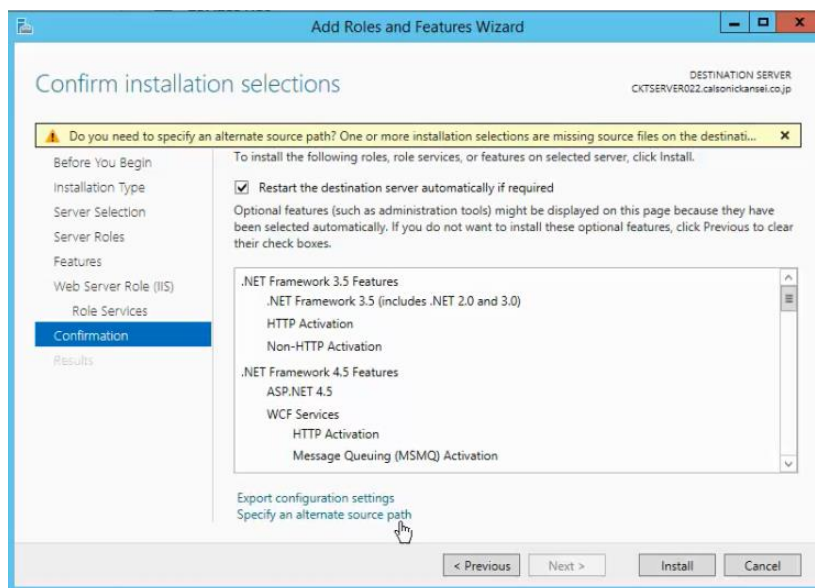
## 7. เปิดใช้งาน role services ตามภาพข้างล่างนี้



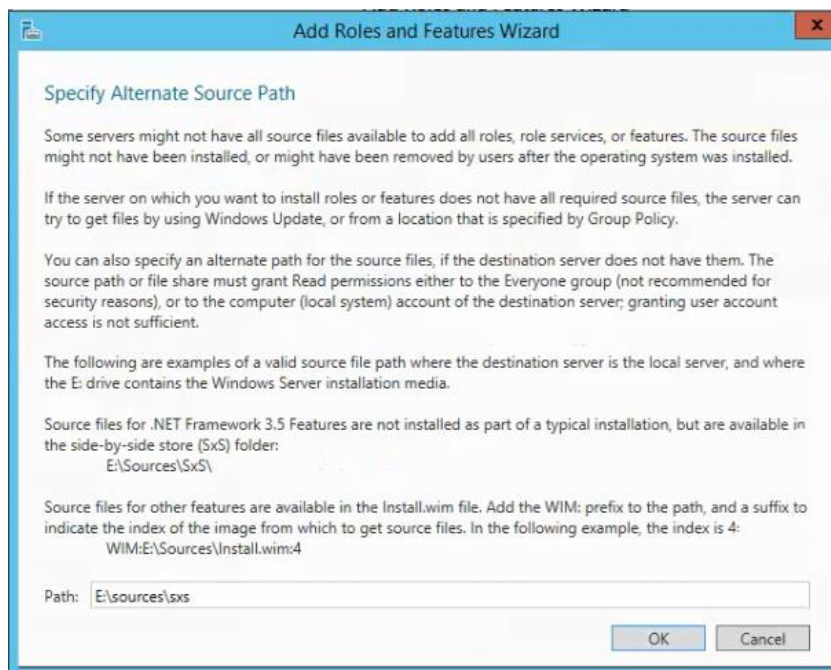




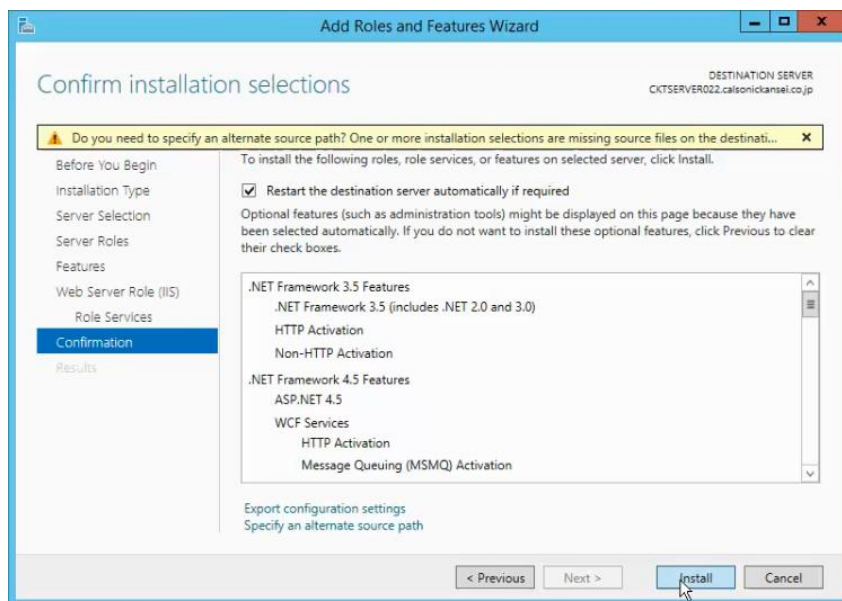
8. คลิก Specify an alternate source path.



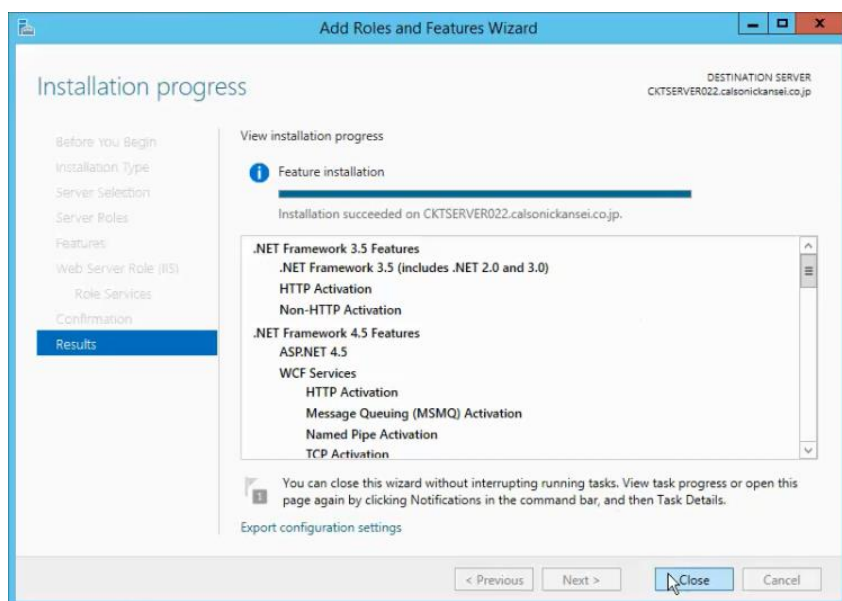
9. เลือก Path ในแผ่นติดตั้งวินโดวส์



10. คลิกเลือก Restart the destination Server automatically require แล้วกด Install



11. คลิก Close เป็นการติดตั้งเสร็จสิ้นแล้ว



ภาคผนวก ง

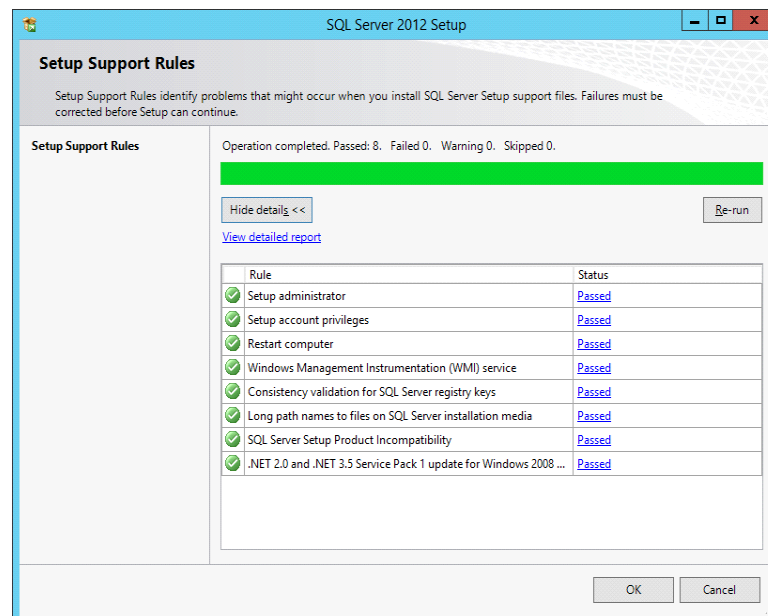
ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์ฐานข้อมูล (Database site)

## การติดตั้ง SQL Server 2012 Standard SP2 (SQL Cluster)

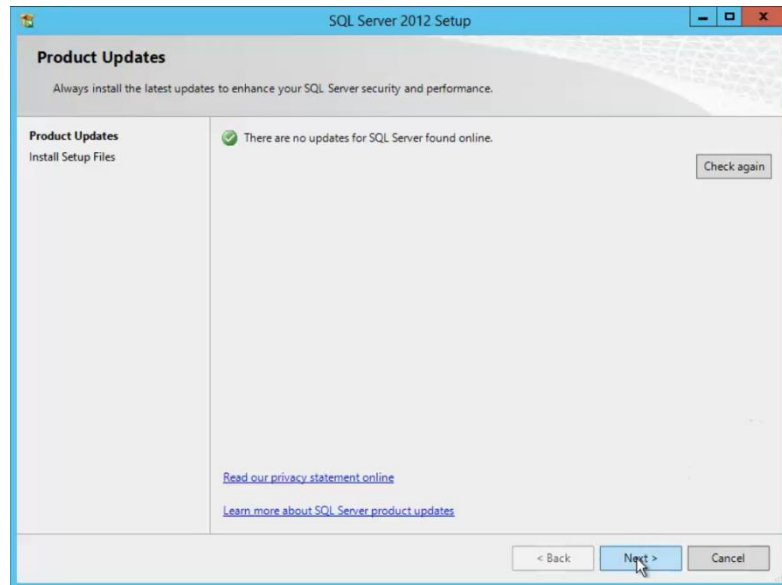
1. เปิดแผ่นติดตั้ง SQL 2012 Sp2 Standard คลิก New SQL Server failover cluster



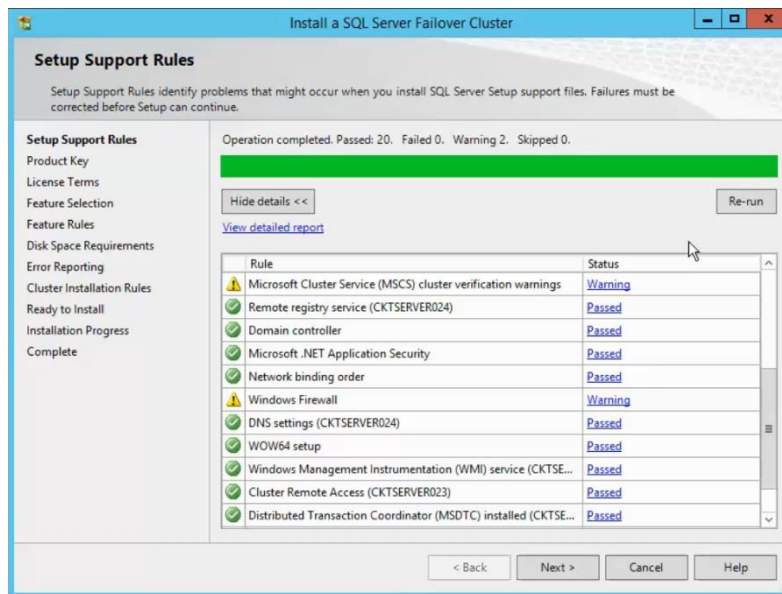
2. คลิก OK



## 3. คลิก Next



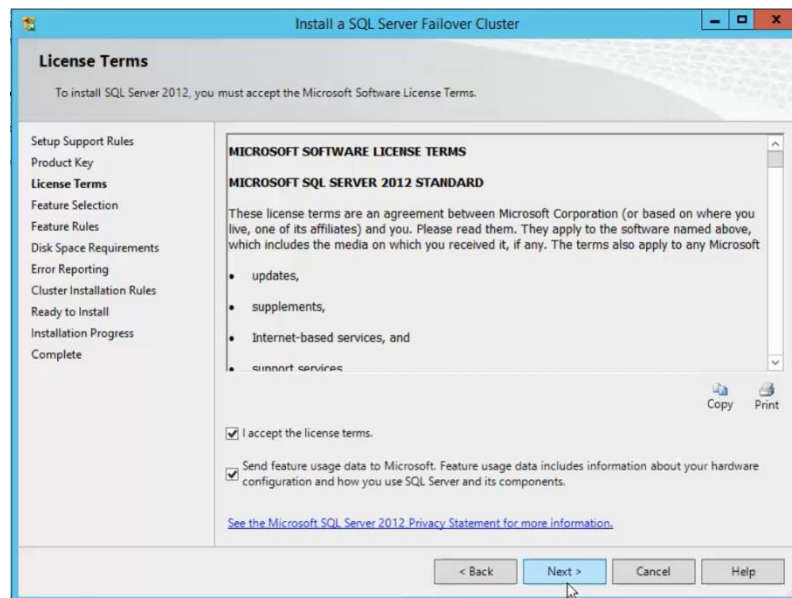
## 4. คลิก Next



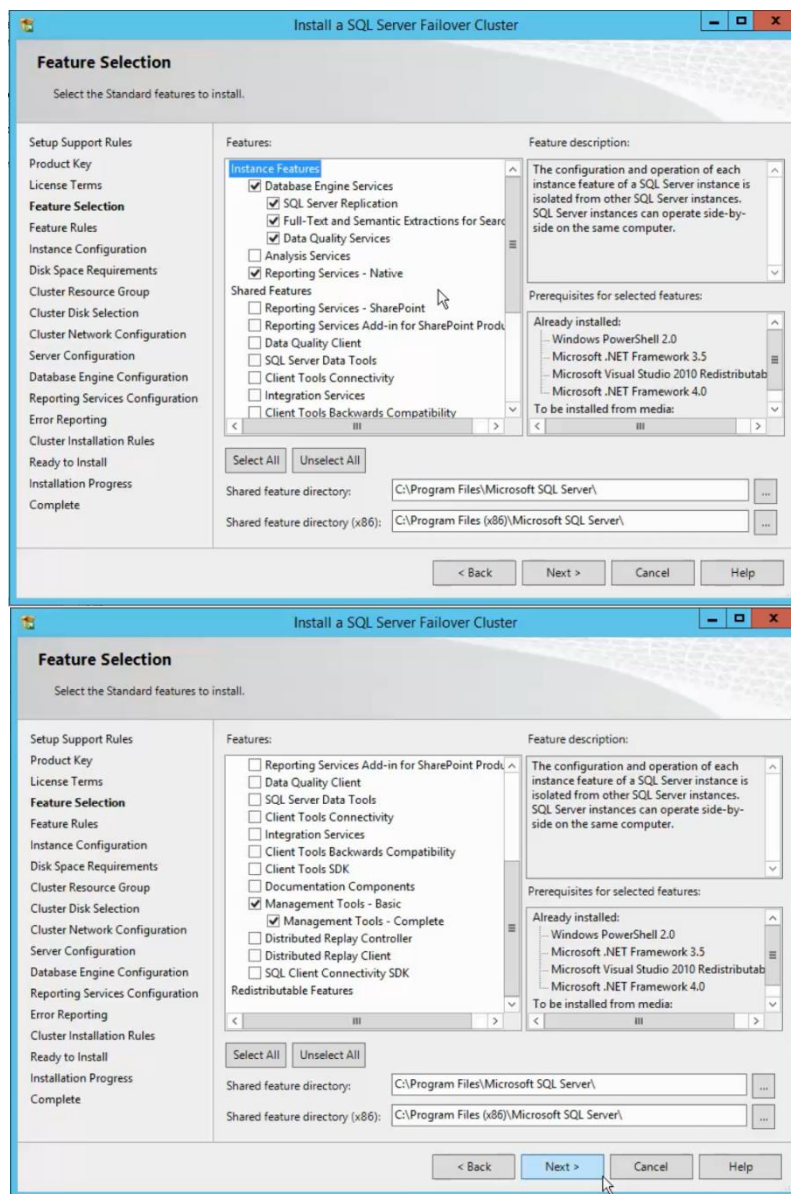
## 5. ป้อนคีย์ Product key License



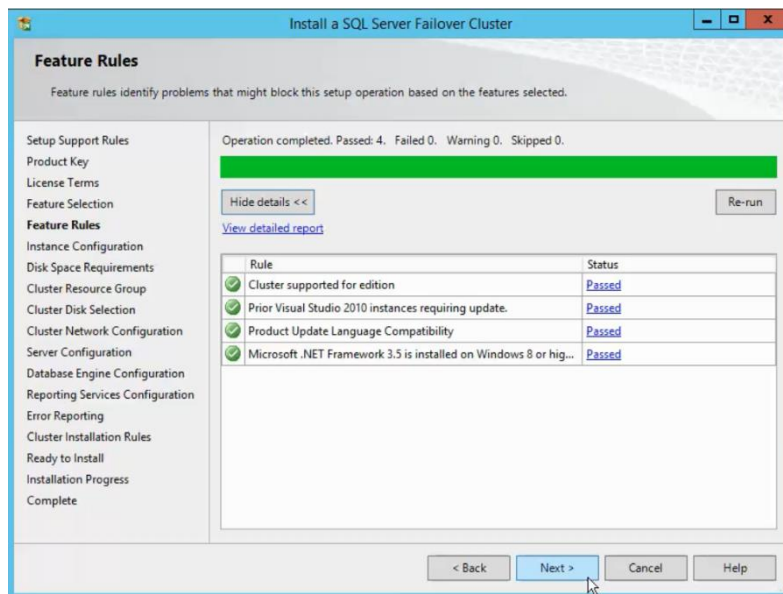
## 6. คลิกเลือก *accept the license*. แล้วคลิก Next.



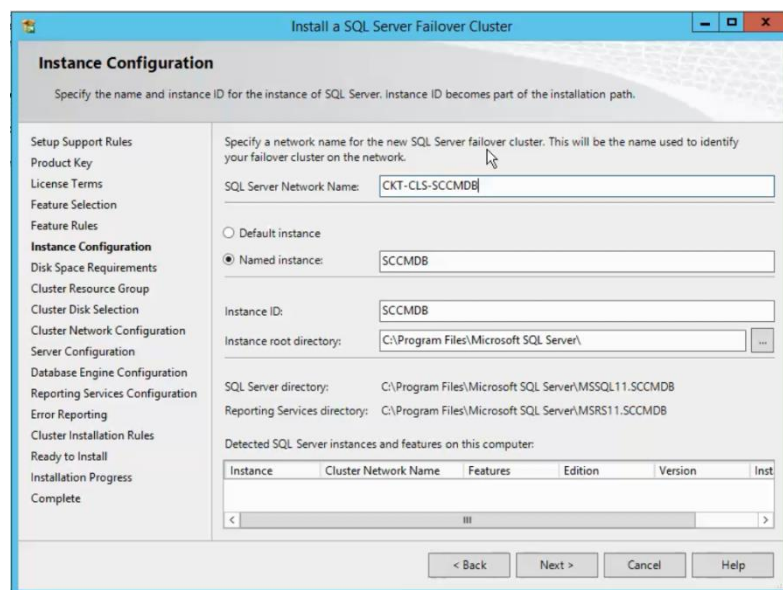
7. เลือก SQL features Database Engine Services และ Reporting Service – Native. และ Management Tools – Basic. ดังภาพด้านล่างนี้



8. คลิก Next

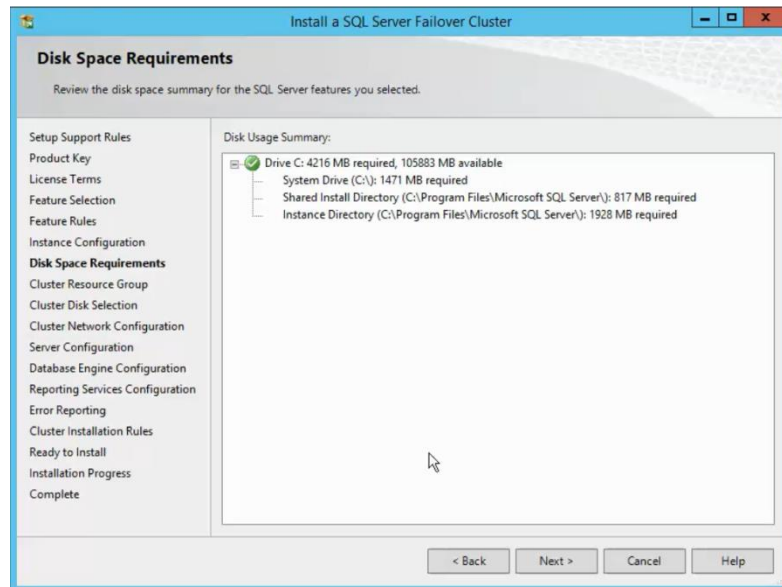


9. ตั้งค่า SQL Server Network name เป็น *CKT-CLS-SCCMDB* และ Named instance เป็น *SCCMDB*.

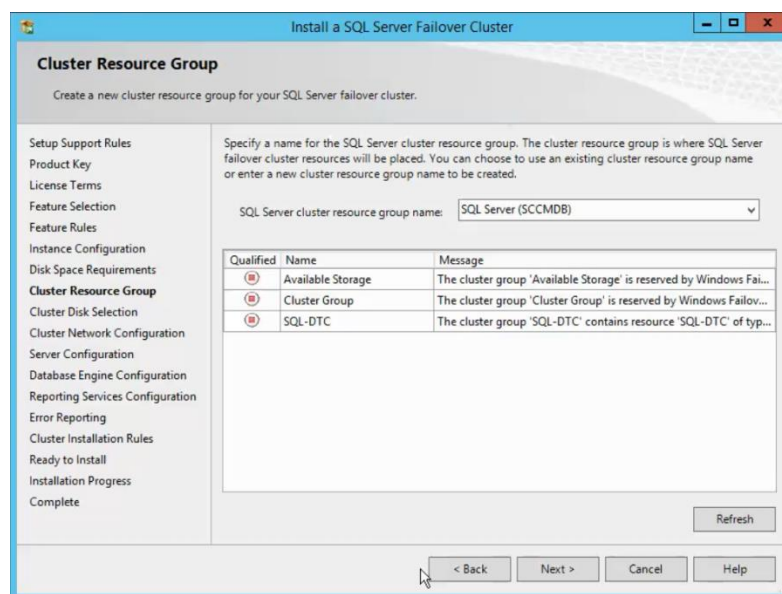




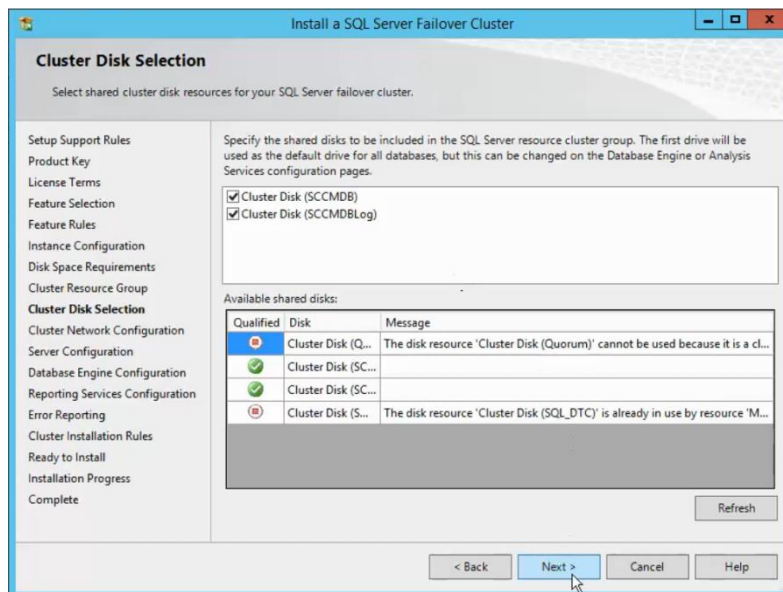
## 10.คลิก Next



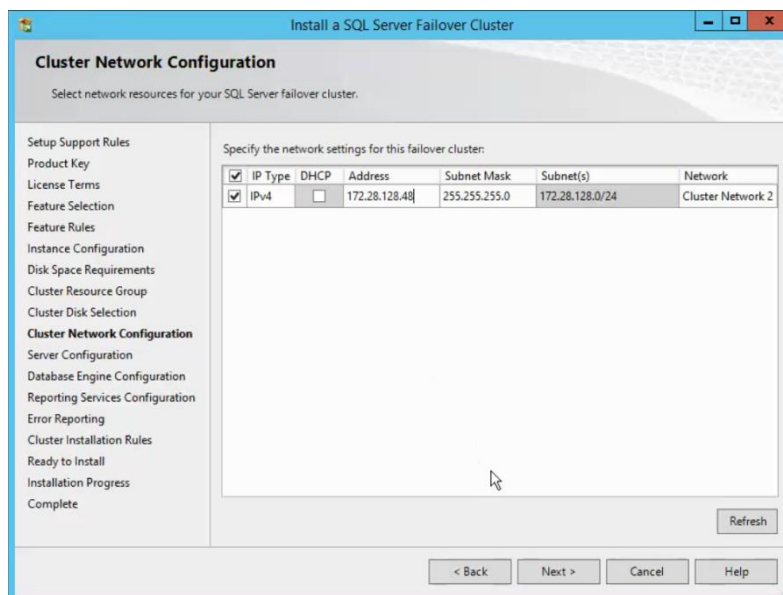
## 11.คลิก Next



12. เลือก *Cluster Disk (SCCMDB)* และ *Cluster Disk (SCCMDBLog)* แล้วคลิก Next.



13. เลือก IPv4 และพิมพ์ IP address 172.28.128.48 และ Subnet mask 255.255.255.0 จากนั้นคลิก Next.

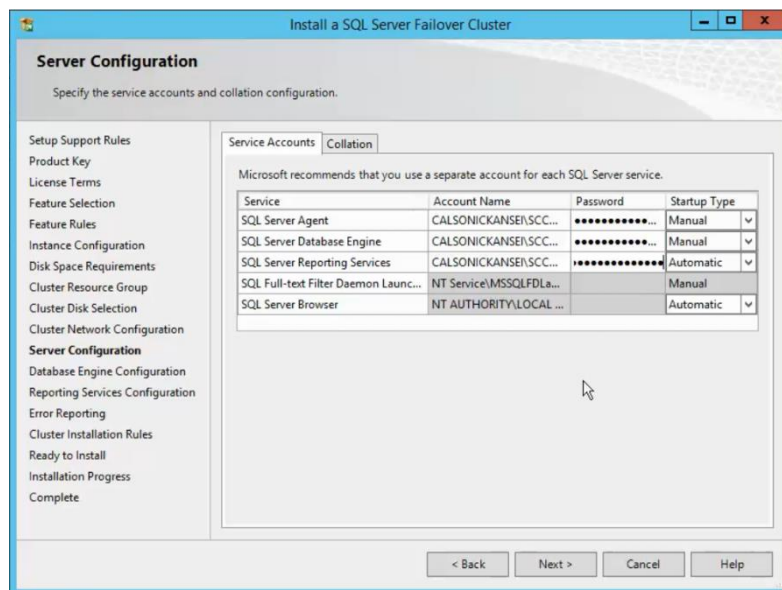


14. ใส่ข้อมูล service account ที่ได้เตรียมไว้แล้ว ดังนี้.

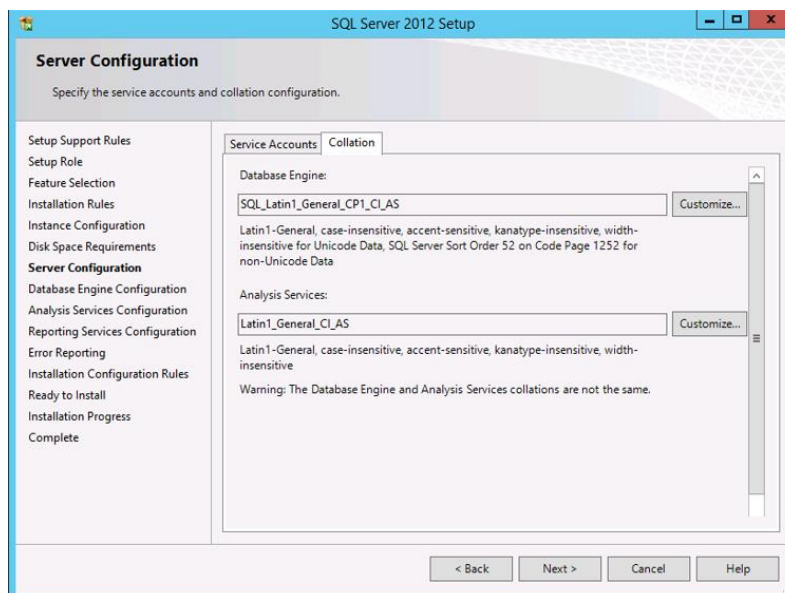
SQL Server Agent : SCCM\_CKT\_SQLAgent

SQL Server Database Engine : SCCM\_CKT\_SQLDatabase

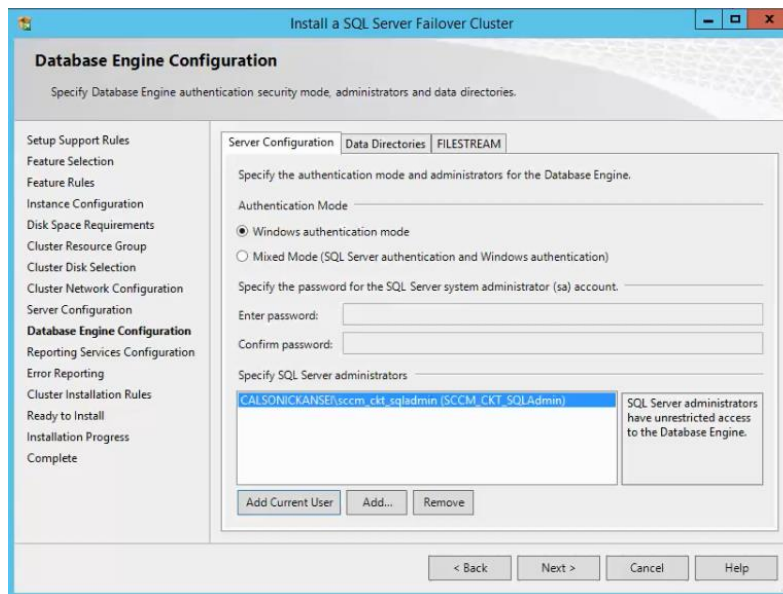
SQL Server Reporting Services : SCCM\_CKT\_REPORTING



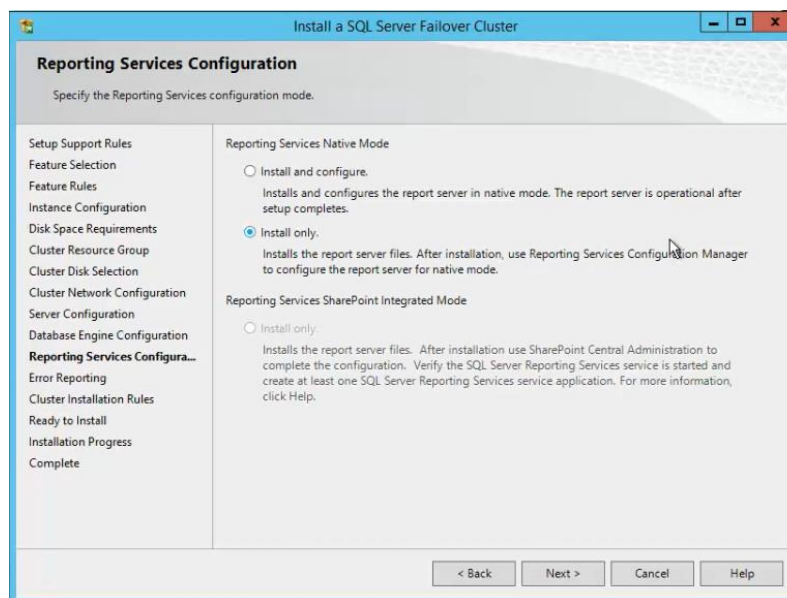
15. เลือก Tab Collation แล้วปรับตั้งค่าตามภาพ คลิก Next



## 16. คลิก Add Current User.



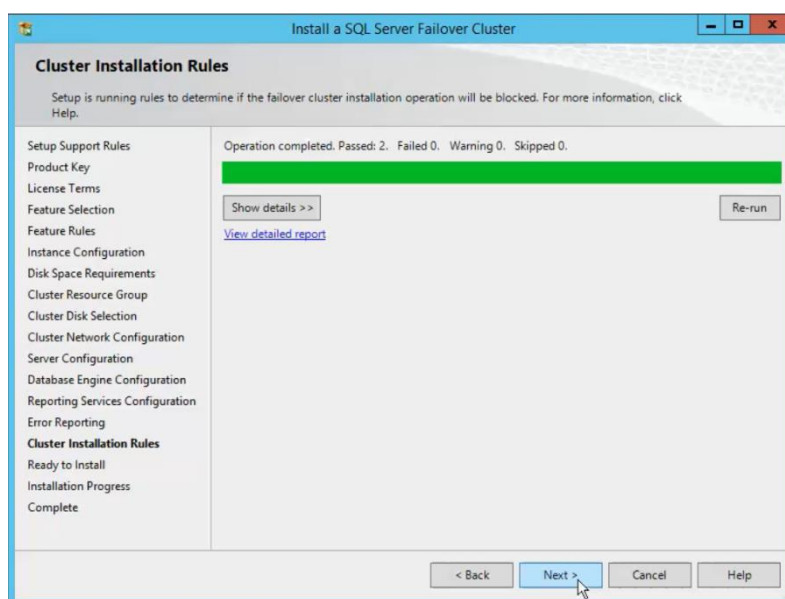
## 17. เลือก Install Only แล้วคลิก Next



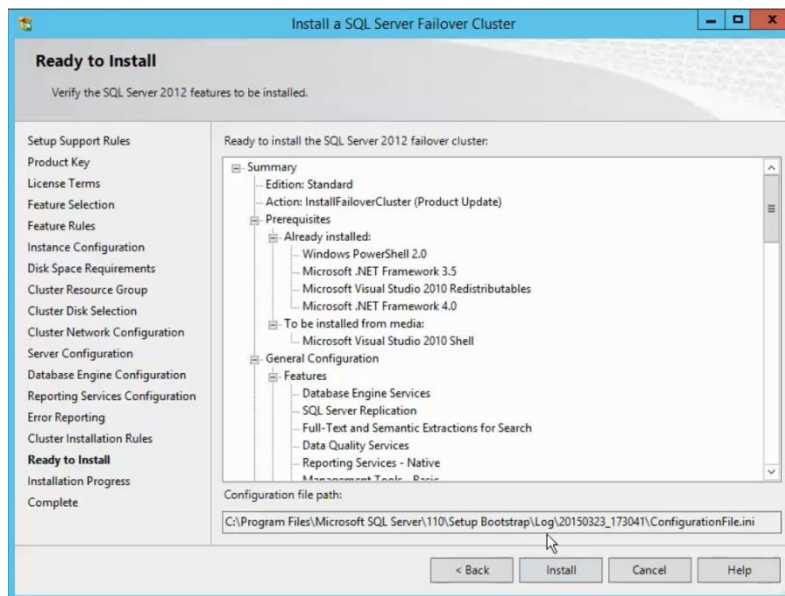
## 18. คลิก Next



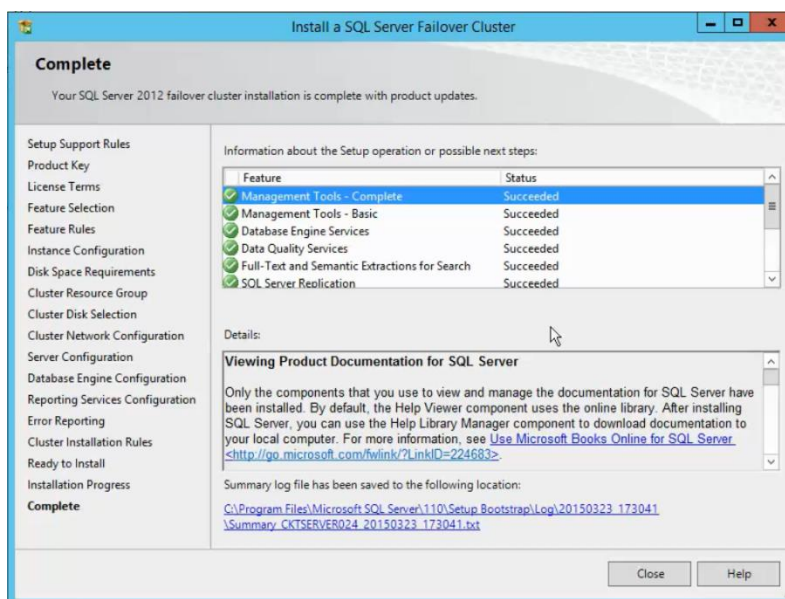
## 19. คลิก Next



## 20. คลิก Install



## 21. คลิก Close เสร็จสิ้นการติดตั้ง SQL Database

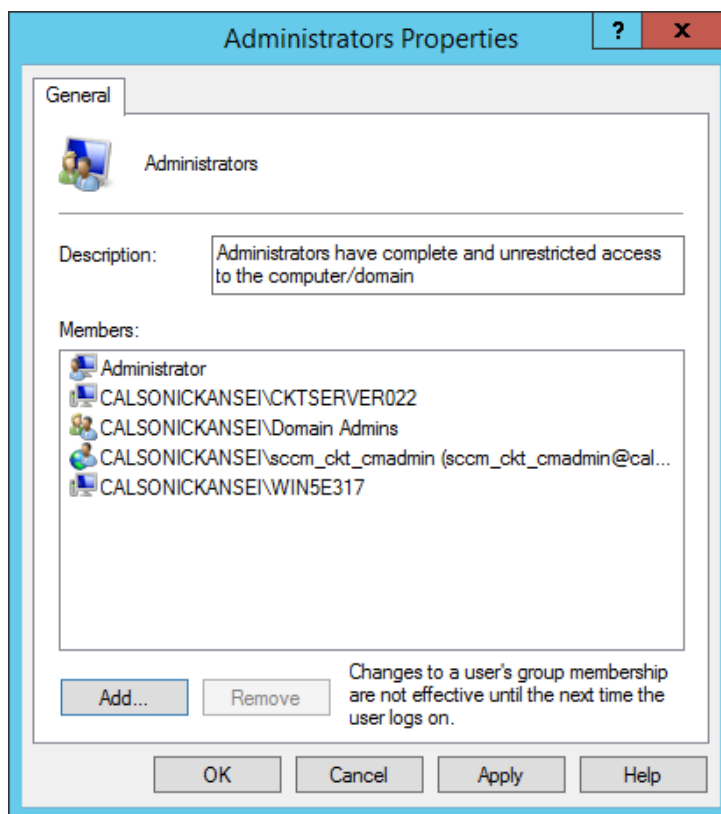


ภาคผนวก จ

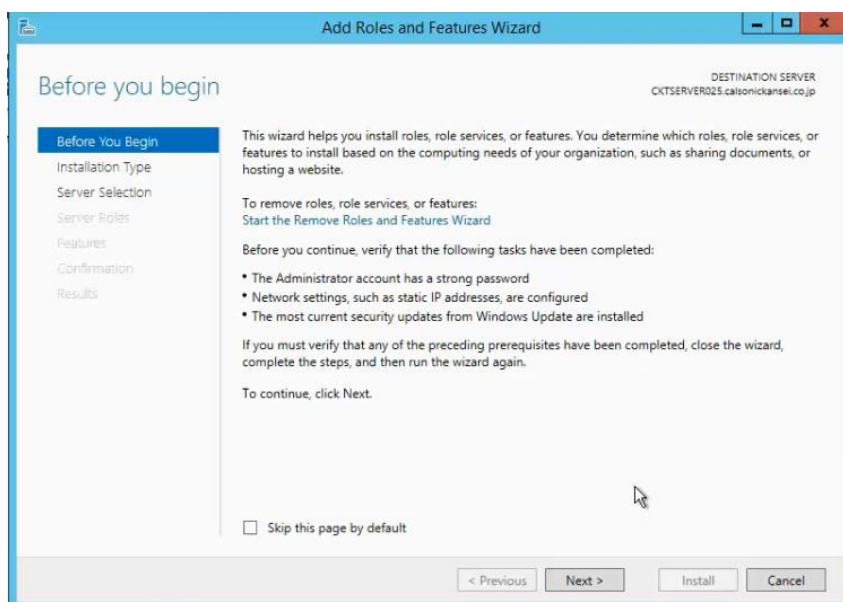
ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์สาขาบางนา  
(Distribution point server)

ติดตั้งระบบ SCCM 2012 R2 เซิร์ฟเวอร์สาขาบางนา (Distribution point server)

1. เพิ่มผู้ดูแลระบบ SCCM\_CKT\_cmadmin และ WIN5e317 ต้องเพิ่มให้อยู่ในกลุ่ม local admin group บนเครื่อง CKTSERVER025.calsonickansei.co.jp.

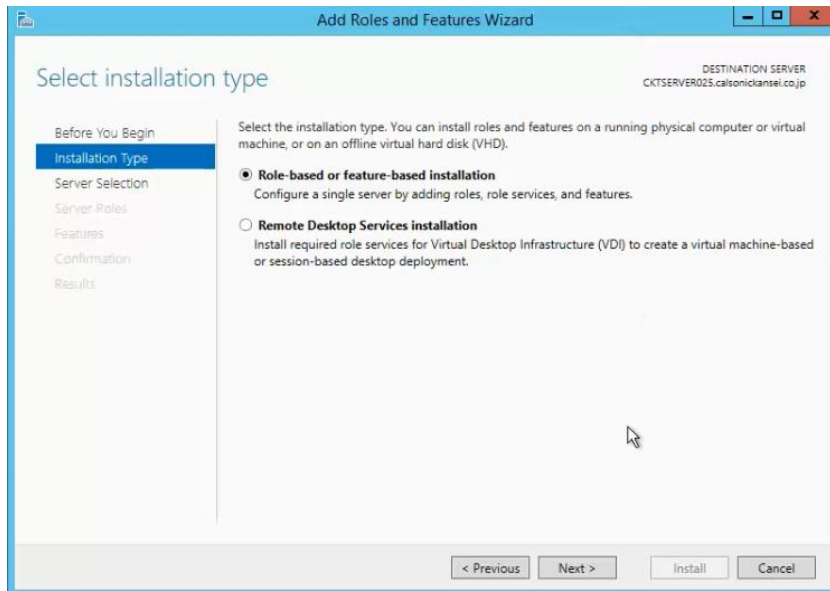


2. เปิด Server Manager แล้วคลิก *Add role and features*, คลิก *Next*.

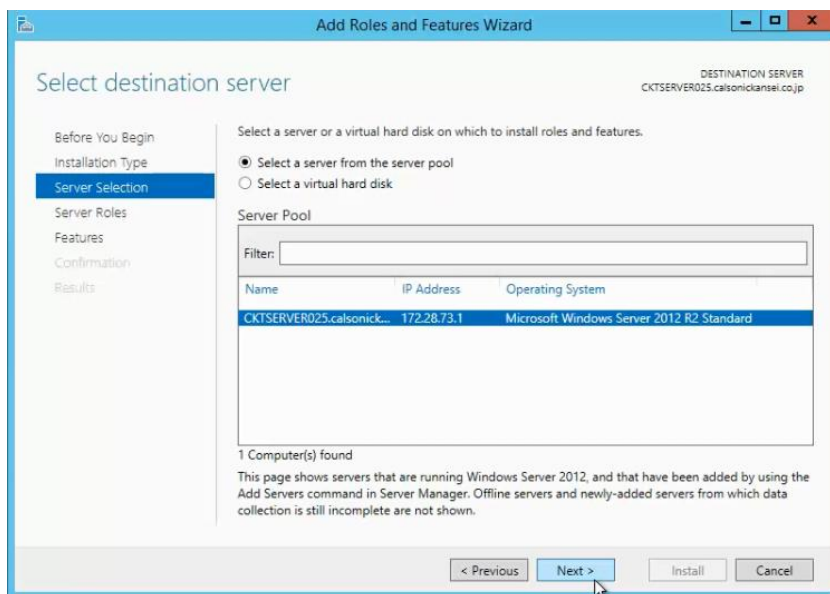




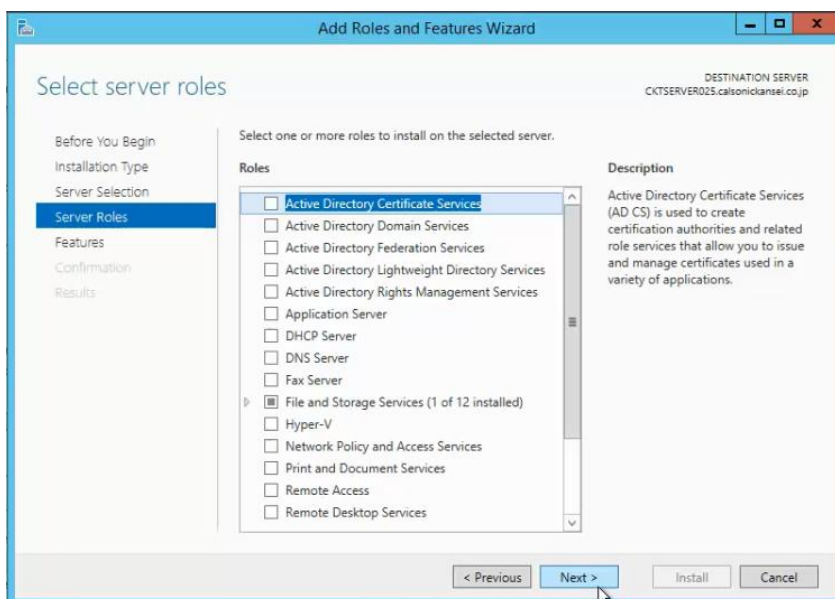
## 3.คลิก Next



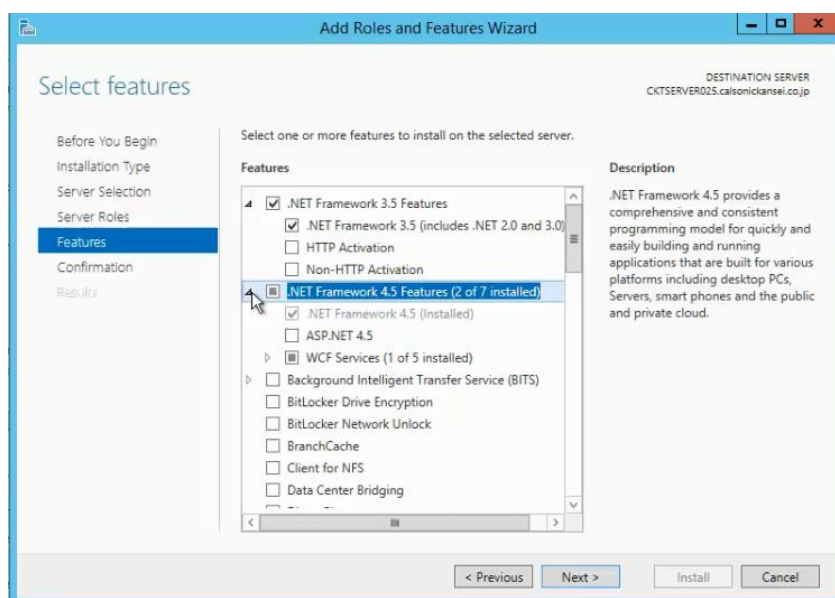
## 4.คลิก Next



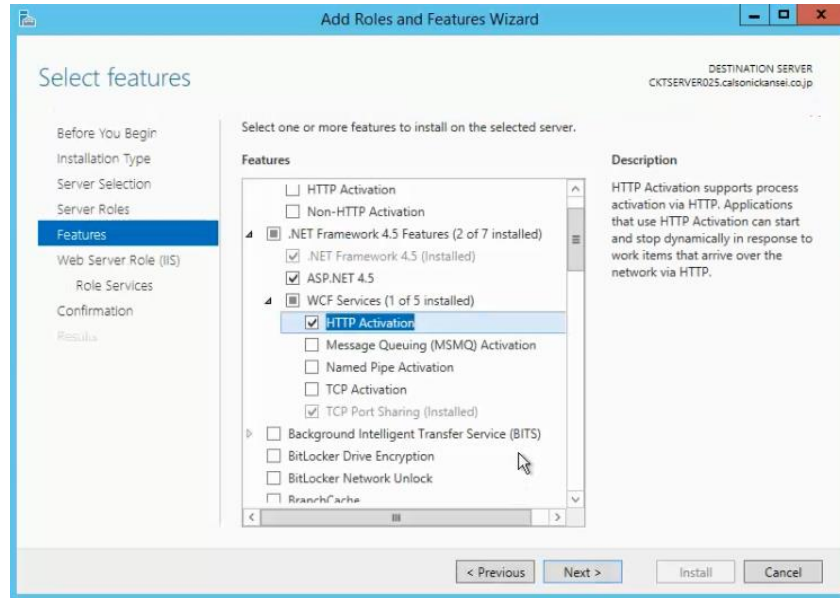
## 5. คลิก Next



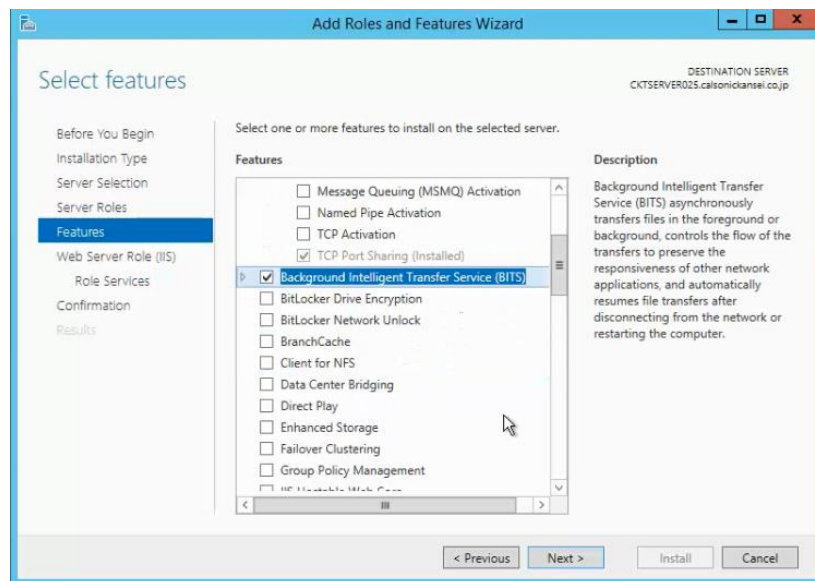
## 6. เปิดใช้งาน Feature ตามภาพด้านล่างนี้



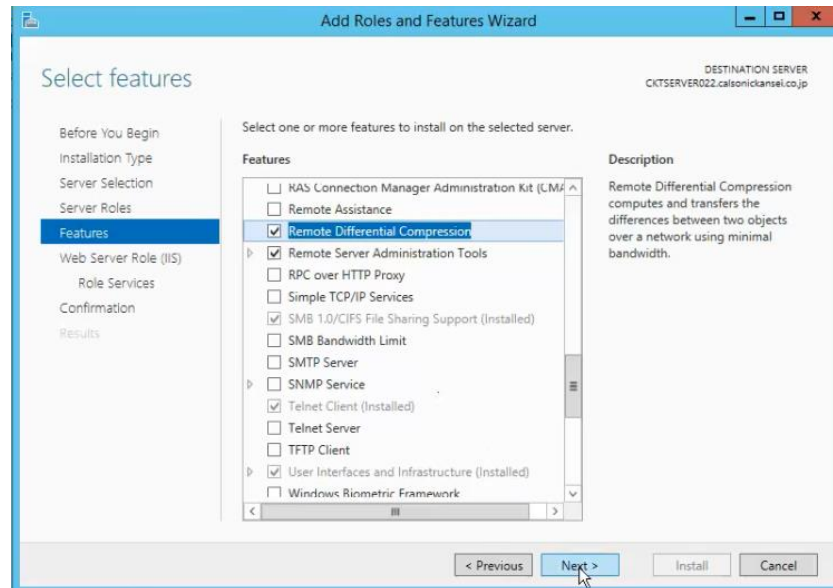
## 7. เลือก WCF service และ HTTP Activation



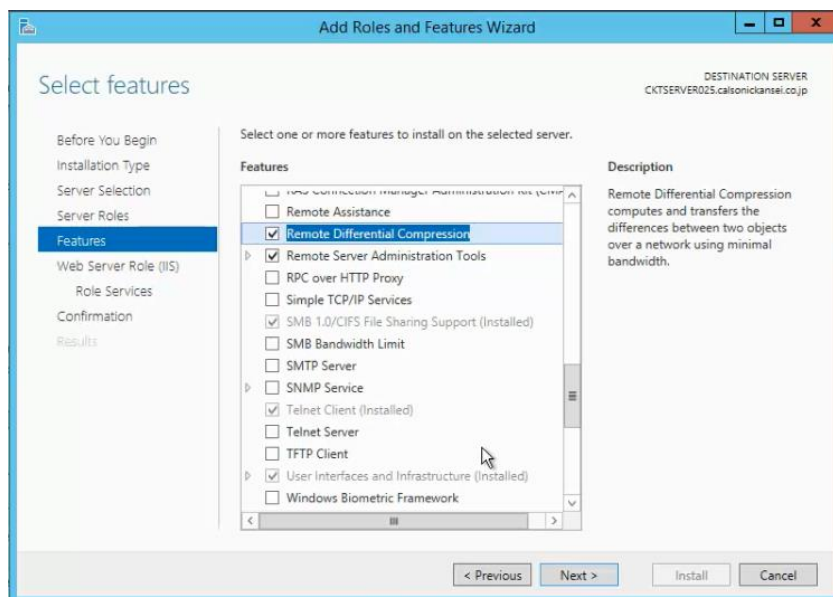
## 8. เลือก Background Intelligent Transfer Service (BITS)



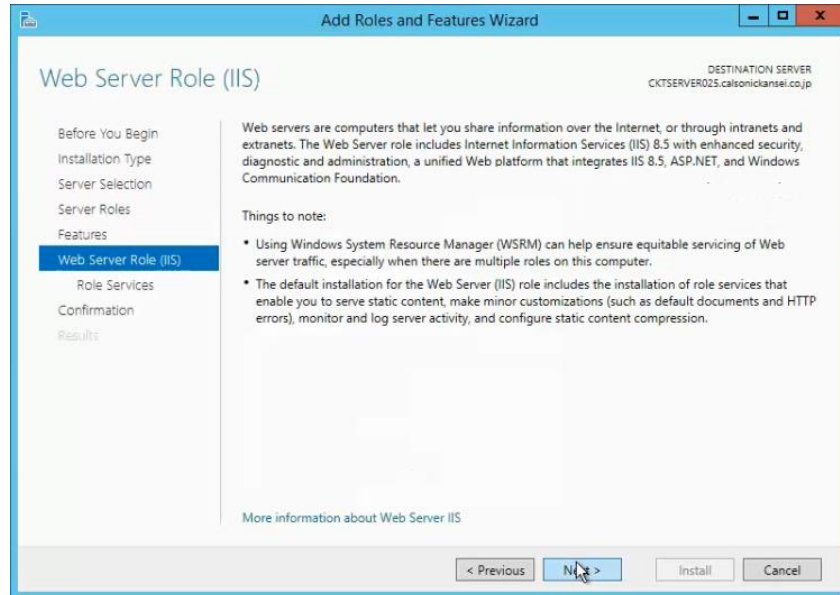
## 9. เลือก Remote Differential Compression



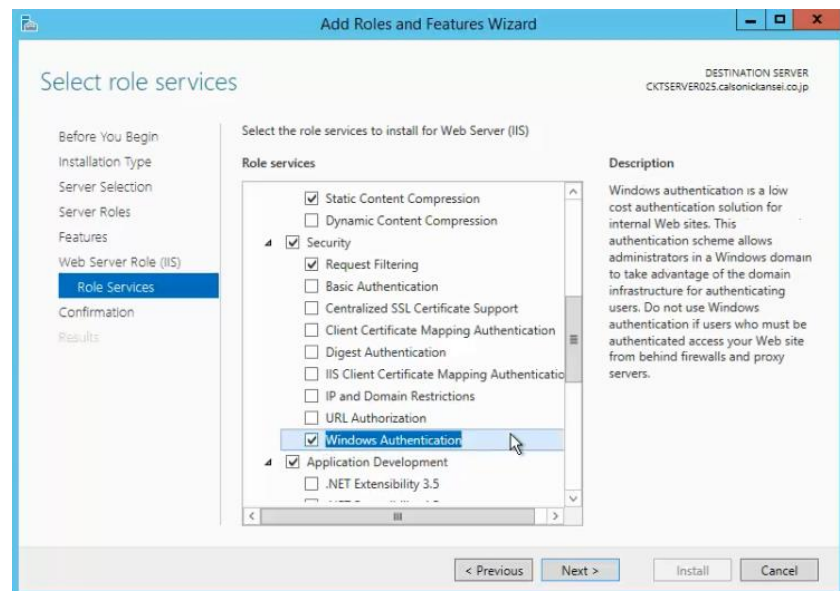
## 10.คลิก Next



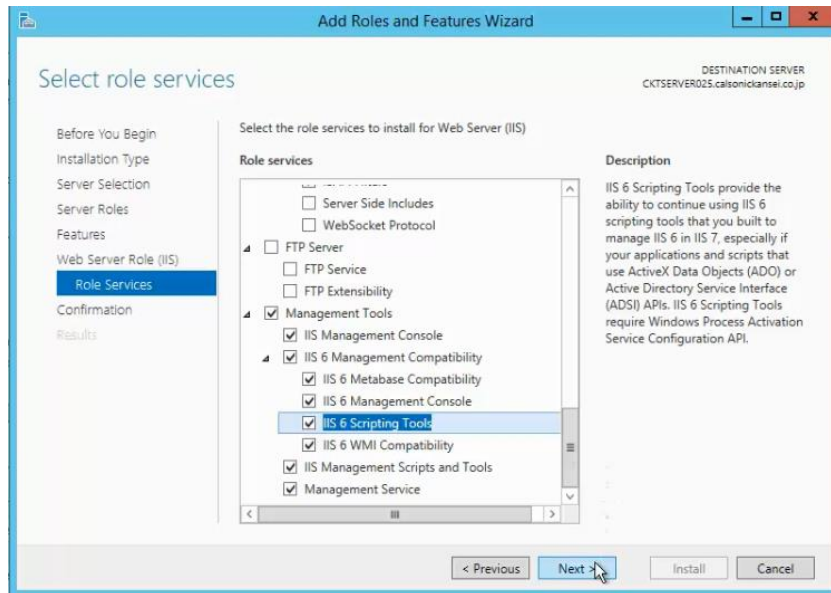
## 11. คลิก Next



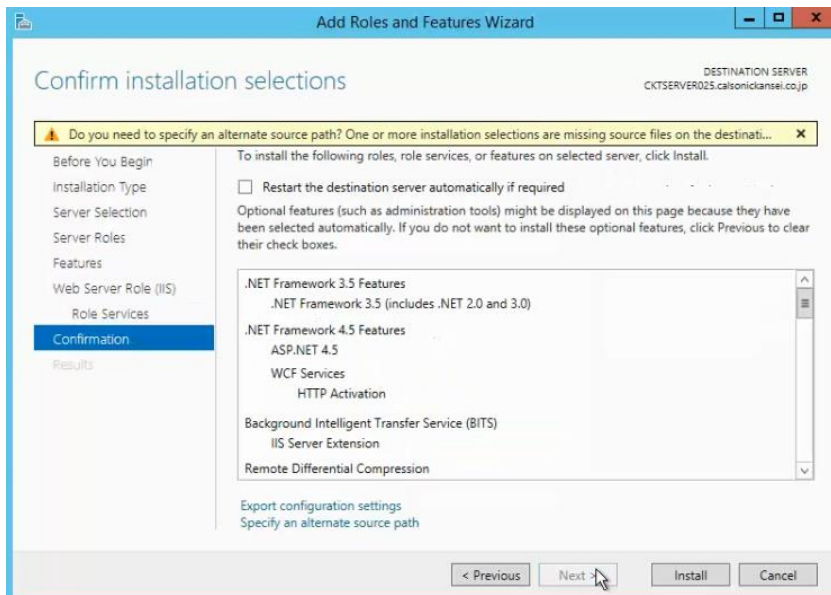
## 12. เปิดใช้งาน role services ตามภาพด้านล่างนี้



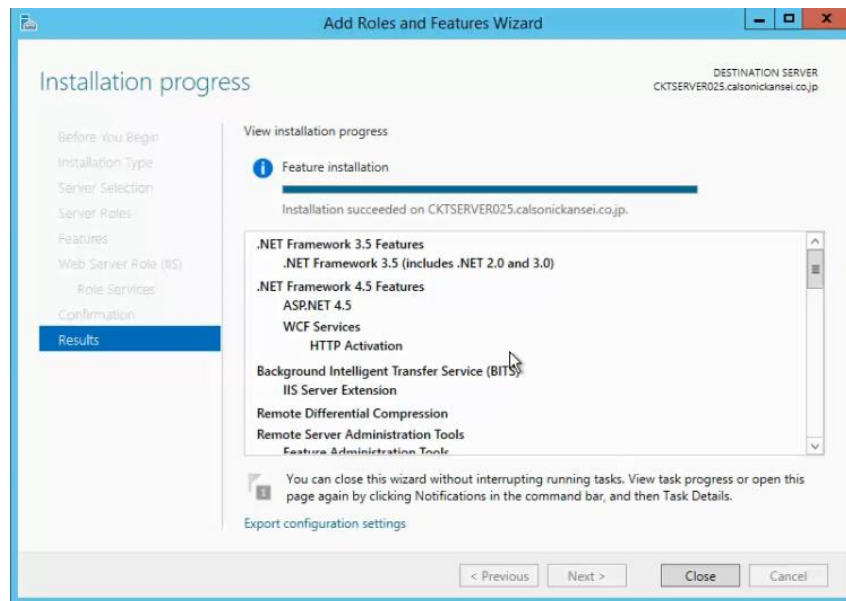
## 13. คลิก Next



## 14. คลิก Install



## 15. คลิก Close



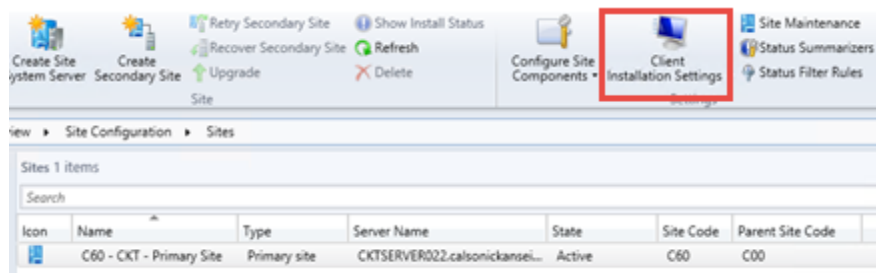
ติดตั้งเสร็จเรียบร้อยแล้ว

ภาคผนวก ฉ  
ติดตั้ง Agent ที่เครื่องผู้ใช้ (Client setting)

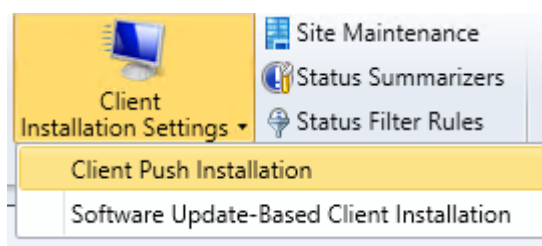


## ติดตั้ง Agent ที่เครื่องผู้ใช้ (Client setting)

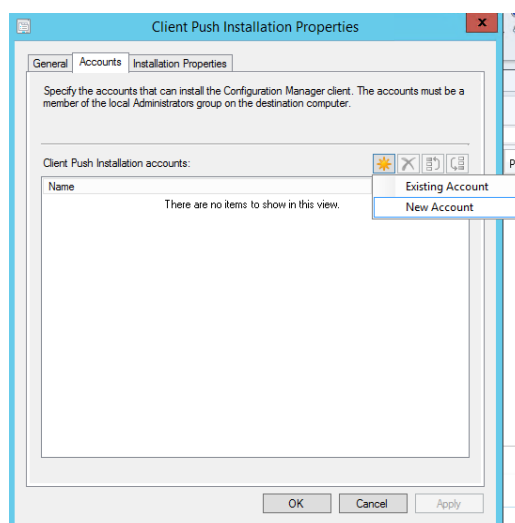
1. เปิดหน้า SCCM console, เข้าไปที่ Administration Workspace เลือก Site node คลิก *Site*. จากนั้นคลิก *Client Installation Setting*. ดังภาพด้านล่างนี้



2. คลิกเลือก Client Push Installation



3. คลิก Tab Accounts แล้วเลือก New Account

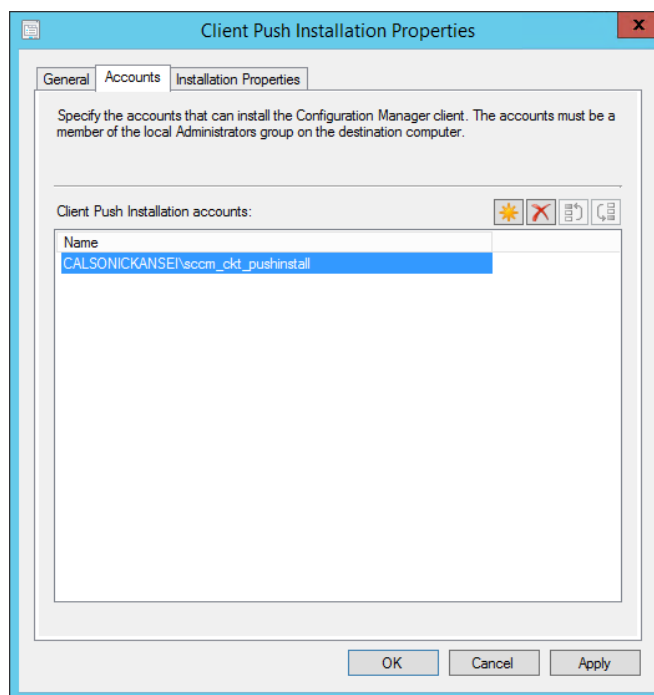


## 4. คลิก Browse

5. *Browse* แล้วเลือก sccm\_ckt\_pushinstall account. แล้วคลิก *OK*.

6. ใส่ Password ของ Account sccm\_ckt\_pushinstall ให้ถูกต้องจากนั้นคลิก *OK*

7.คลิก OK

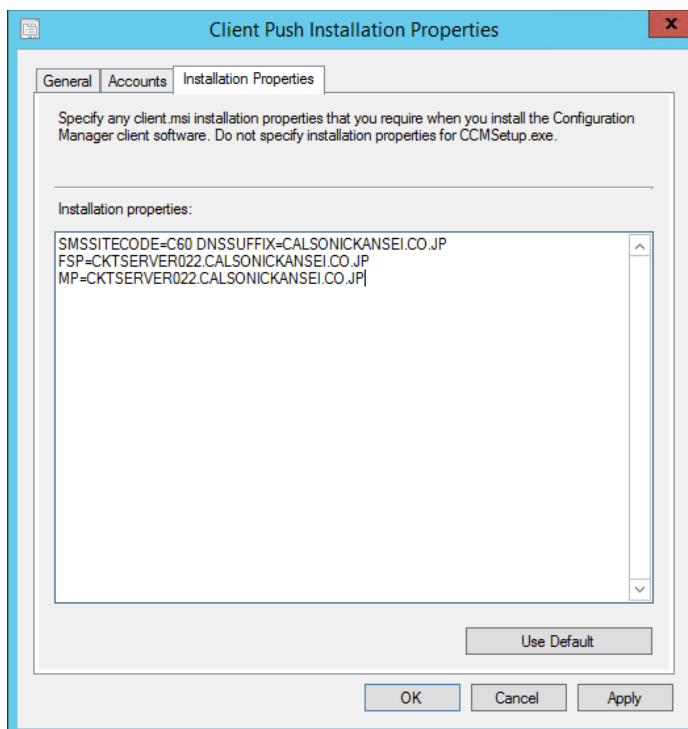


8. ใน Tab installation Properties

DNSSUFFIX=CALSONICKANSEI.CO.JP FSP=CKTSERVER022.CALSONICKANSEI.CO.JP

MP=CKTSERVER022.CALSONICKANSEI.CO.JP.

จากนั้น กด OK เป็นอันเสร็จสิ้น



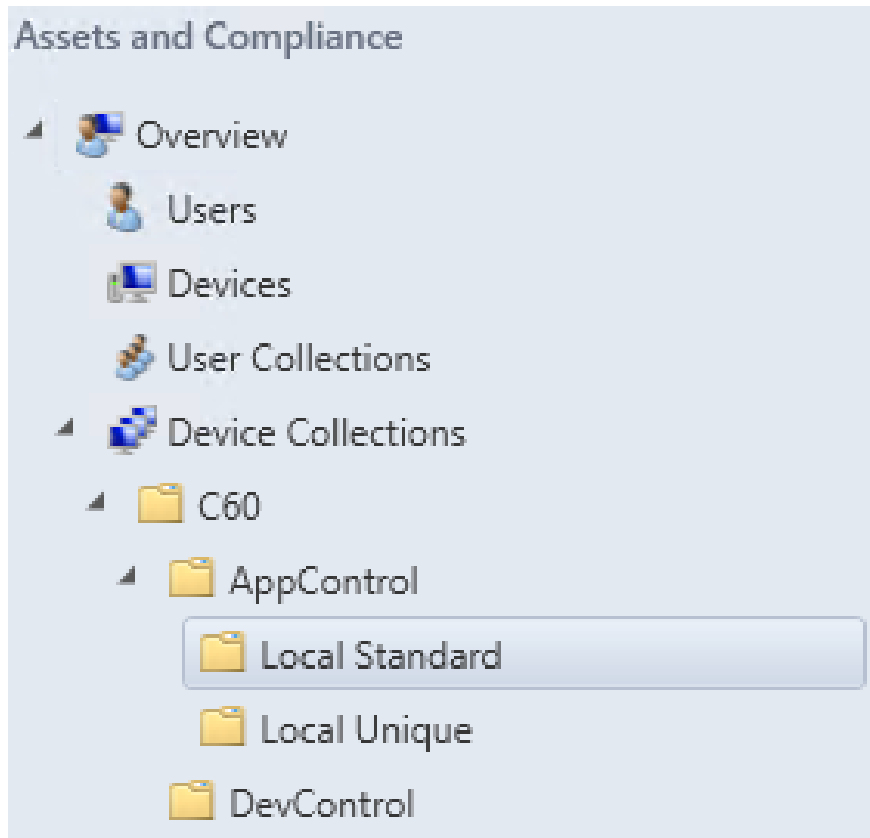
### ภาคผนวก ข

สร้างกลุ่มคอมพิวเตอร์ของผู้ใช้ใน SCCM (Device collections)

## สร้างกลุ่มคอมพิวเตอร์ของผู้ใช้ใน SCCM (Device collections)

การสร้างกลุ่ม Device Collections ชื่อ C60-LS-V Up

1. เปิด SCCM แล้วเข้าไปที่ Assets and Compliance คลิก Device Collections เลือกโฟลเดอร์ C60> AppControl>Local Standard ดังรูป



2. คลิก Create Device Collection บน Ribbon



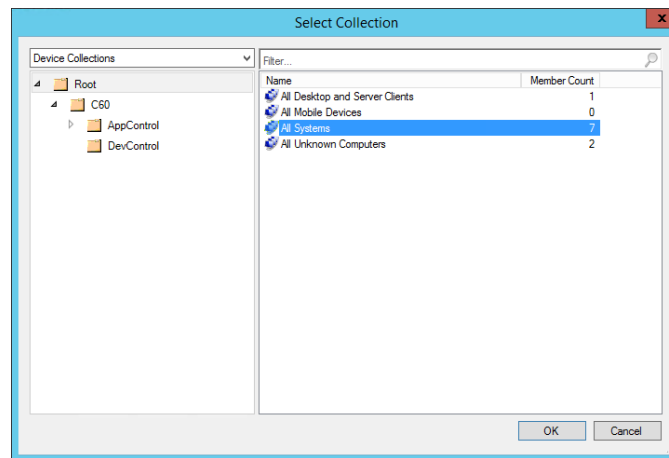
3. ตั้งชื่อ และเลือก Limiting Collection

The screenshot shows the "Create Device Collection Wizard" dialog box. The title bar reads "Create Device Collection Wizard". The "General" tab is selected in the left-hand navigation pane. The main area is titled "Specify details for this collection". It contains the following fields and controls:

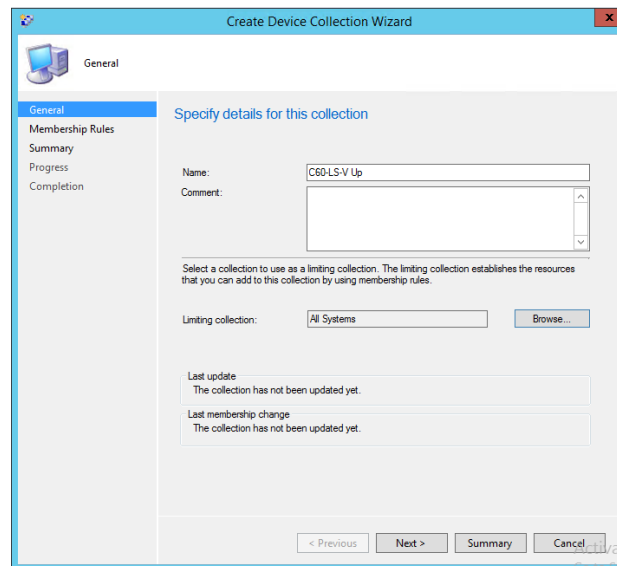
- Name:** A text input field with a red warning icon to its right.
- Comment:** A multi-line text area with up and down arrow buttons on the right side.
- Limiting collection:** A text input field with a red warning icon to its right, followed by a "Browse..." button.
- Last update:** A text box containing the message "The collection has not been updated yet."
- Last membership change:** A text box containing the message "The collection has not been updated yet."

At the bottom of the dialog, there are four buttons: "< Previous", "Next >", "Summary", and "Cancel".

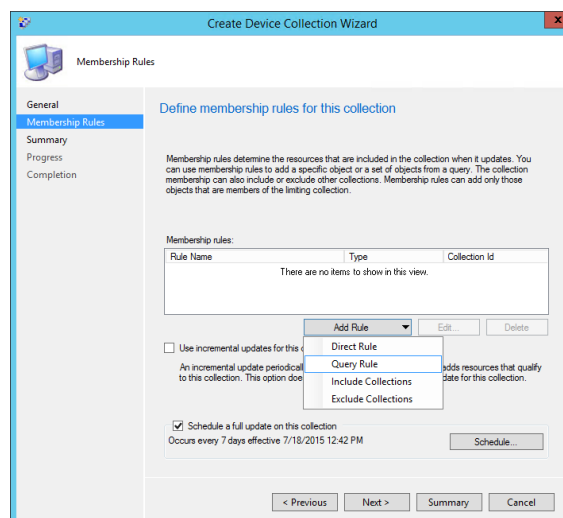
4. คลิก **Browse** ตรง Limiting collection แล้วเลือก **All systems**.



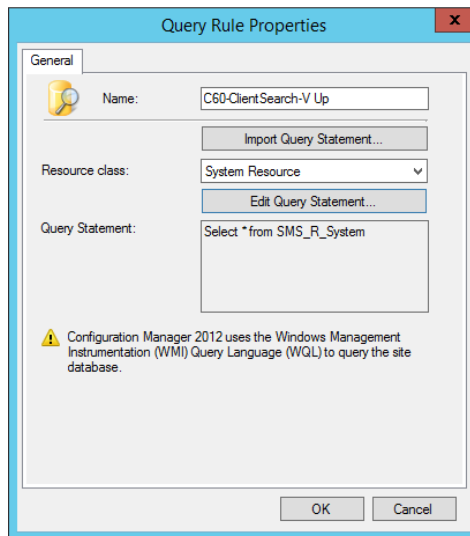
5. คลิก Next



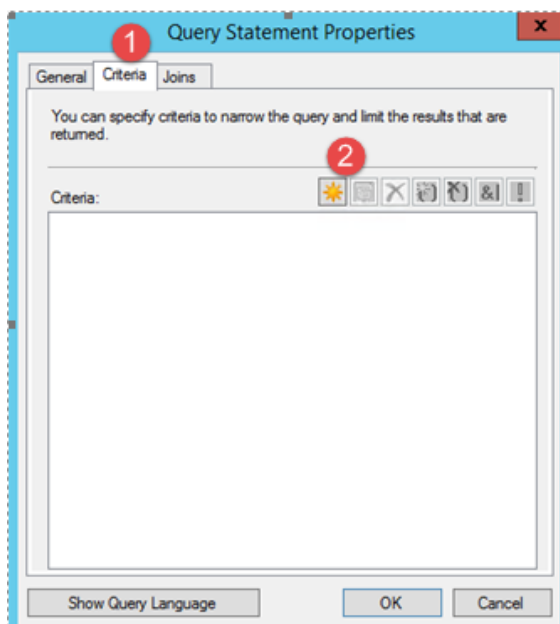
6. ใน Membership Rules.เลือก Drop down แล้วเลือก Add Rule>> Query Rule.



7. หน้า Query Rule Properties, ใส่ค่าในช่อง Name เป็นชื่อ C60-ClientSearch-V Up จากนั้นคลิก Edit Query Statement



8. แล้วเลือก Criteria tab กดที่ปุ่มหมายเลข 2





9. ใน General คลิก *Select*

The screenshot shows the 'Criterion Properties' dialog box with the 'General' tab selected. The 'Criterion Type' is set to 'Simple value'. The 'Where' field is empty, and the 'Select...' button is highlighted. The 'Operator' and 'Value' fields are also empty, with 'Value...' buttons next to them. The 'Type' is set to 'String'. The 'OK' and 'Cancel' buttons are at the bottom.

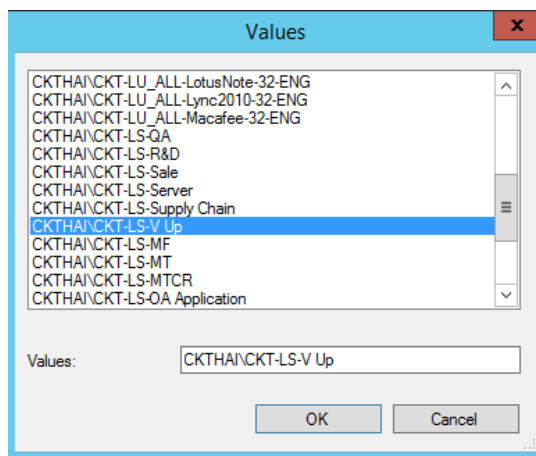
10. Attribute class: เลือก *System Resource* และ Attribute: เลือก *Security Group Name*  
จากนั้นคลิก OK

The screenshot shows the 'Select Attribute' dialog box. The 'Attribute class' is set to 'System Resource', 'Alias as' is set to '<No Alias>', and 'Attribute' is set to 'Security Group Name'. The 'OK' and 'Cancel' buttons are at the bottom.

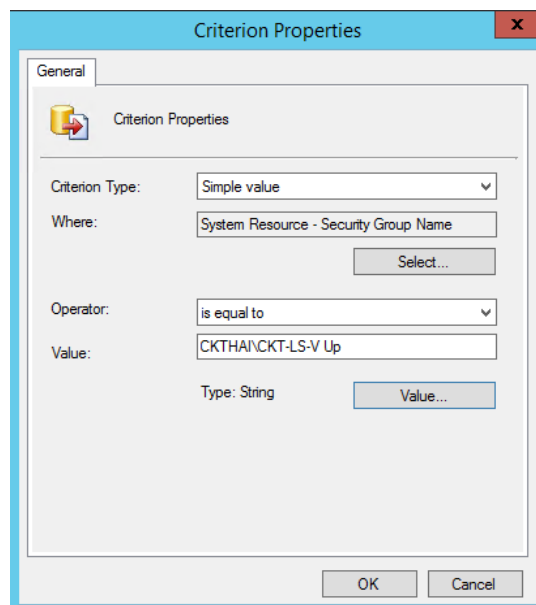
11.คลิก Value

The screenshot shows the 'Criterion Properties' dialog box with the 'General' tab selected. The 'Criterion Type' is 'Simple value'. The 'Where' field is now populated with 'System Resource - Security Group Name'. The 'Operator' is set to 'is equal to'. The 'Value' field is empty, and the 'Value...' button is highlighted. The 'Type' is 'String'. The 'OK' and 'Cancel' buttons are at the bottom.

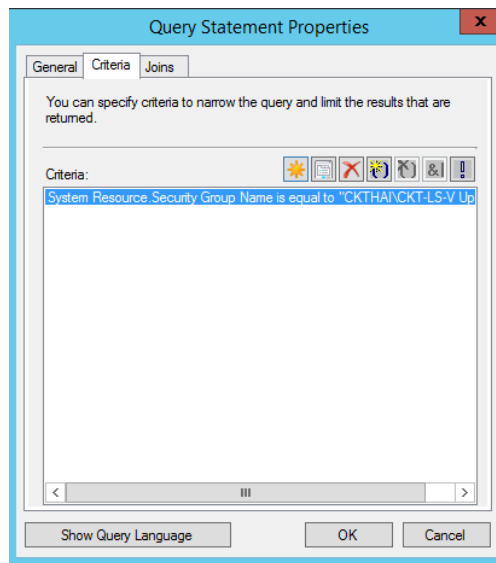
12. เลือก *CKTHA\CKT-LS-V-Up*



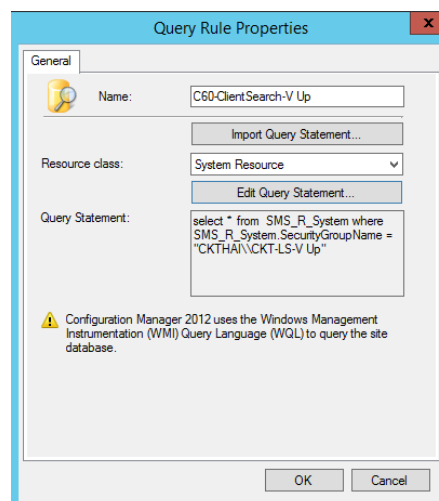
13. คลิก OK



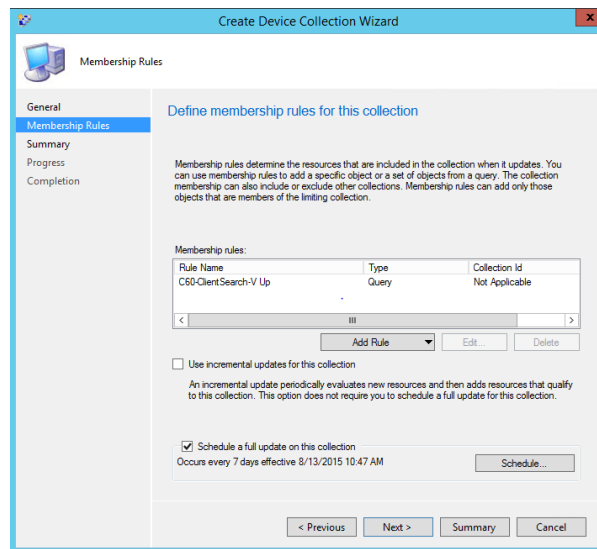
14. คลิก OK



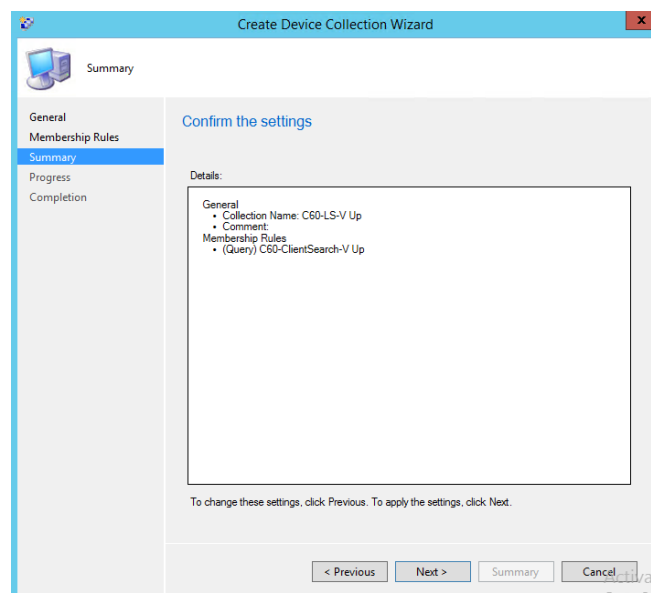
15. คลิก OK



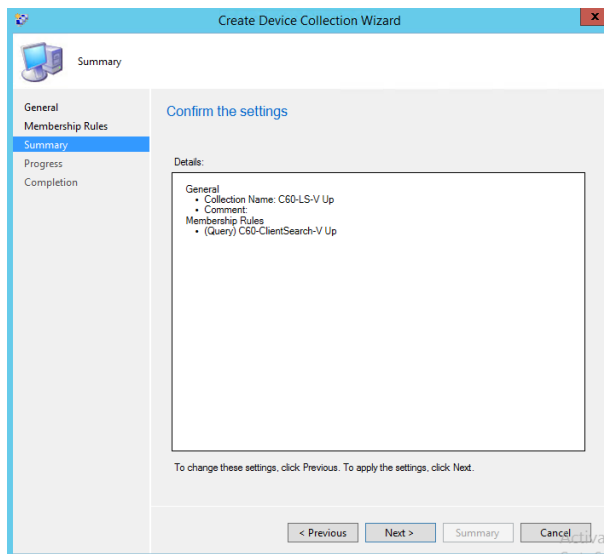
16. คลิก Next



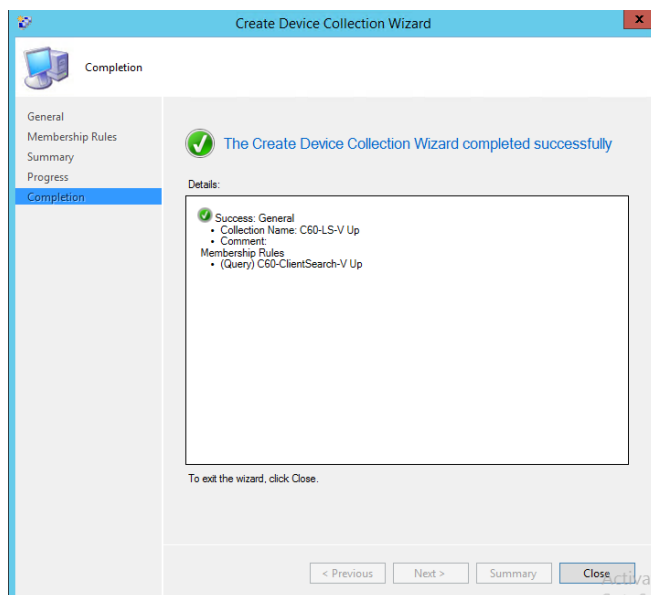
17. คลิก Next



18. คลิก Next



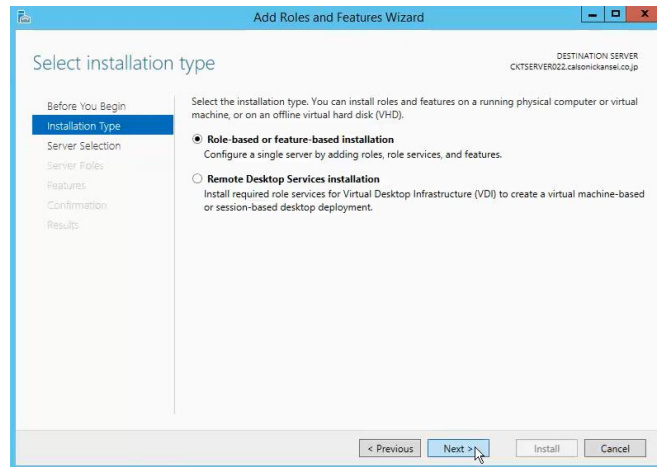
19. คลิก Close



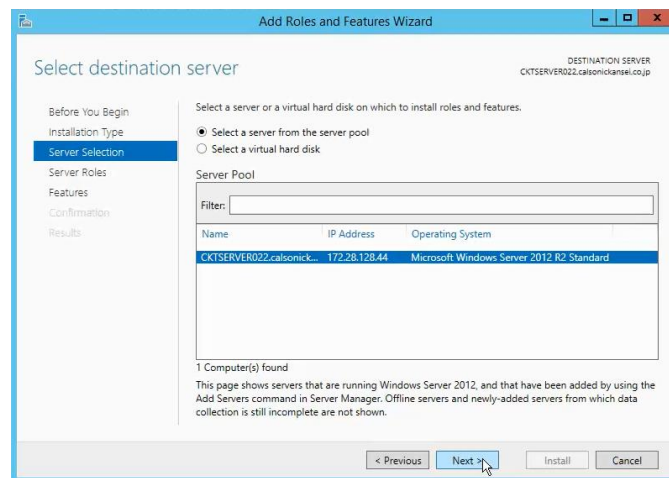
ภาคผนวก ซ  
ตั้งค่าส่วนการ deploy ระบบปฏิบัติการ  
(Operating system deployment)

ตั้งค่าส่วนการ deploy ระบบปฏิบัติการ (Operating system deployment)  
เปิดใช้งาน roles & Features Windows Deployment Service (WDS)

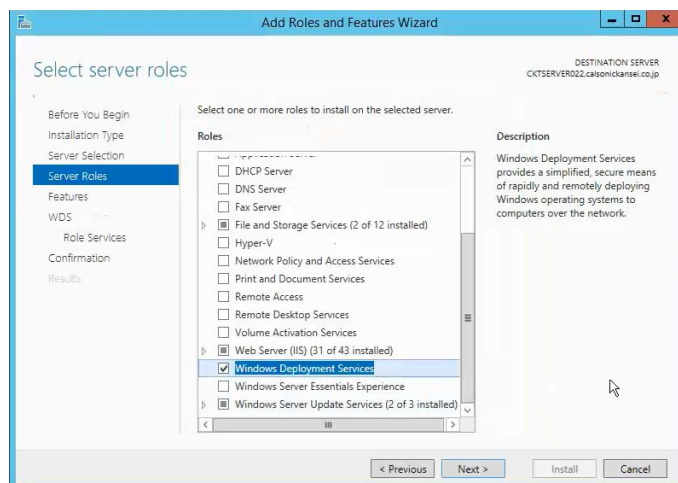
1. เปิด Server Manager เลือกร **Add Roles and Feature**, คลิก **Next**.



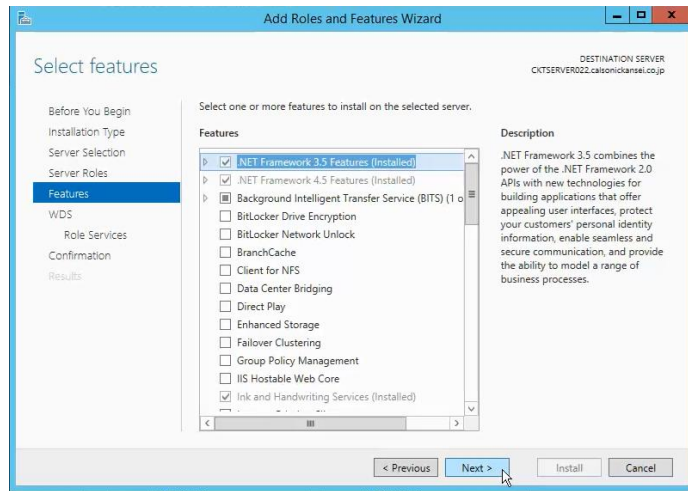
2. คลิก **Next**



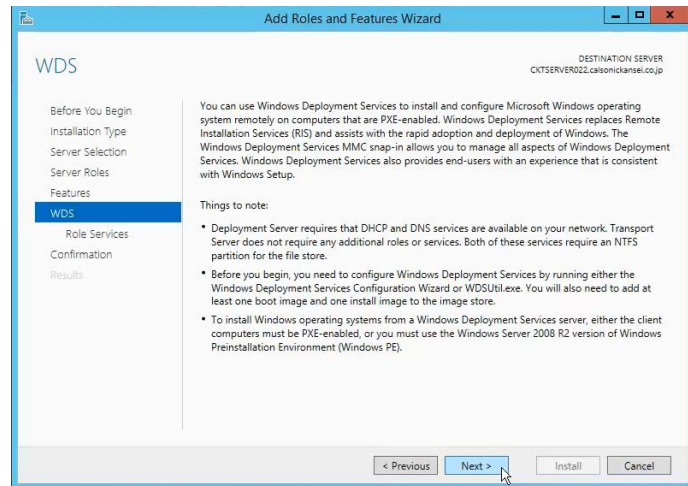
3. เลือก **Windows Deployment Services** จากนั้นคลิก **Next**.



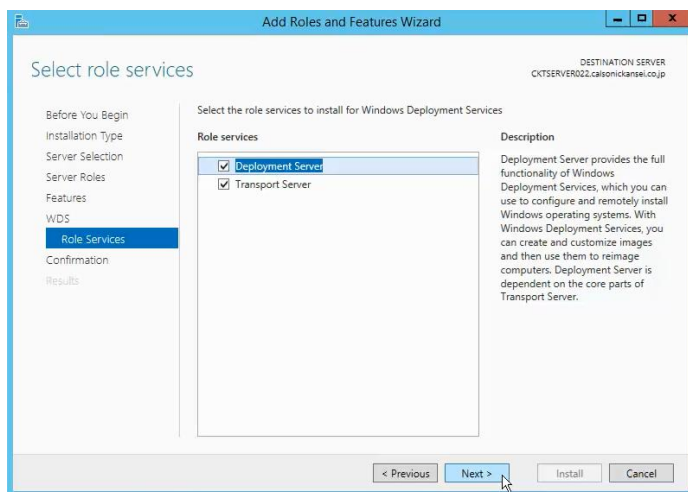
## 4. คลิก Next



## 5. คลิก Next

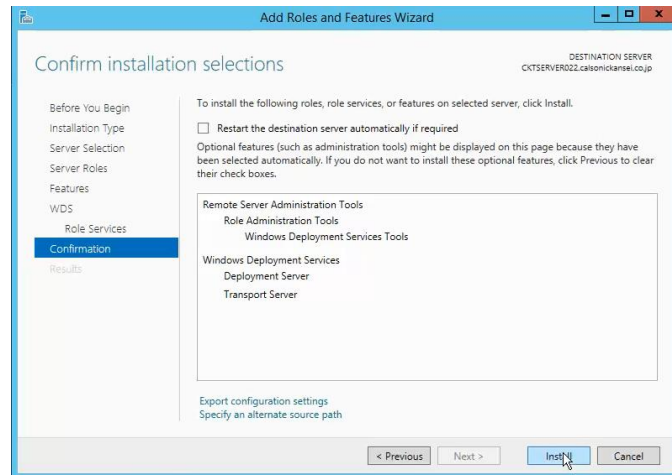


## 6. เลือก Role Services ทั้งสองแล้วคลิก Next.

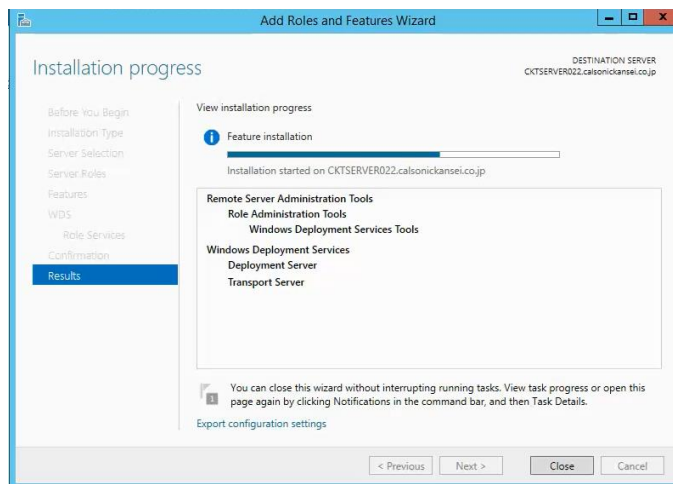




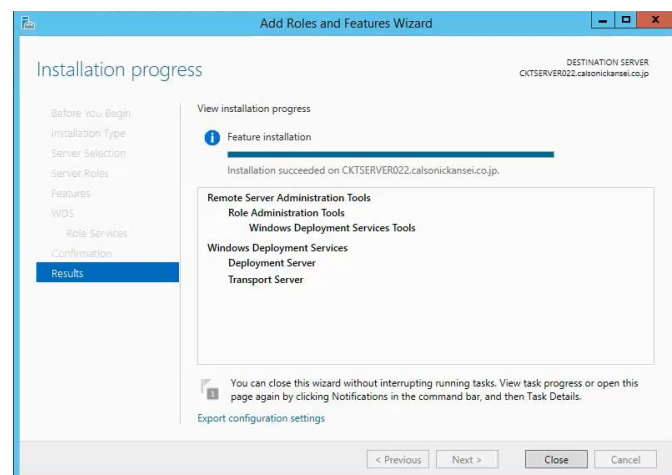
## 7. คลิก Install



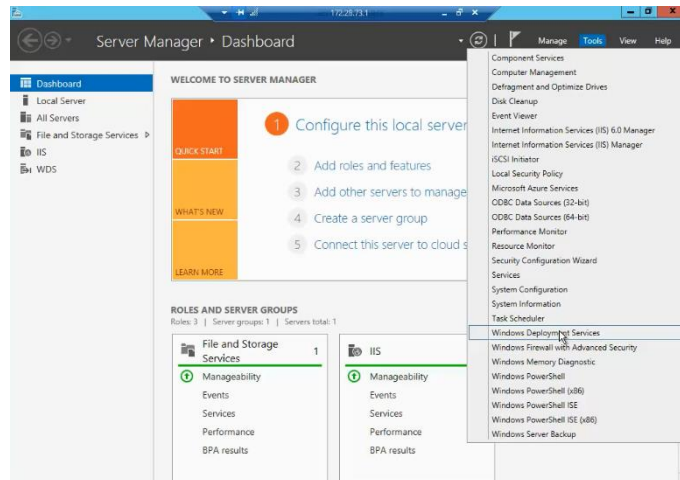
## 8. รอการติดตั้ง installation process.



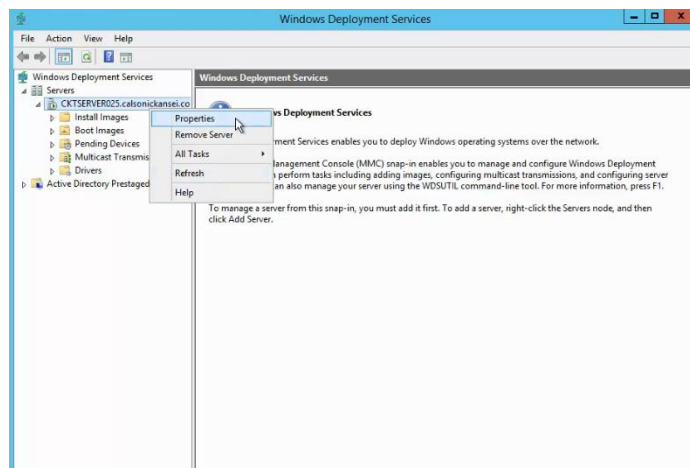
## 9. คลิก Close



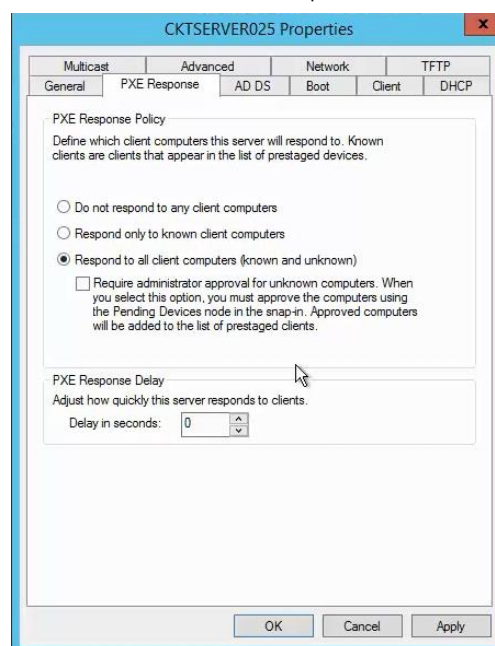
10. เปิด Service Manager Dashboard แล้วเลือก Tools>Windows Deployment Service



11. ในหน้า Windows Deployment Services คลิกขวาที่ CKTSERVER025 เลือก Properties



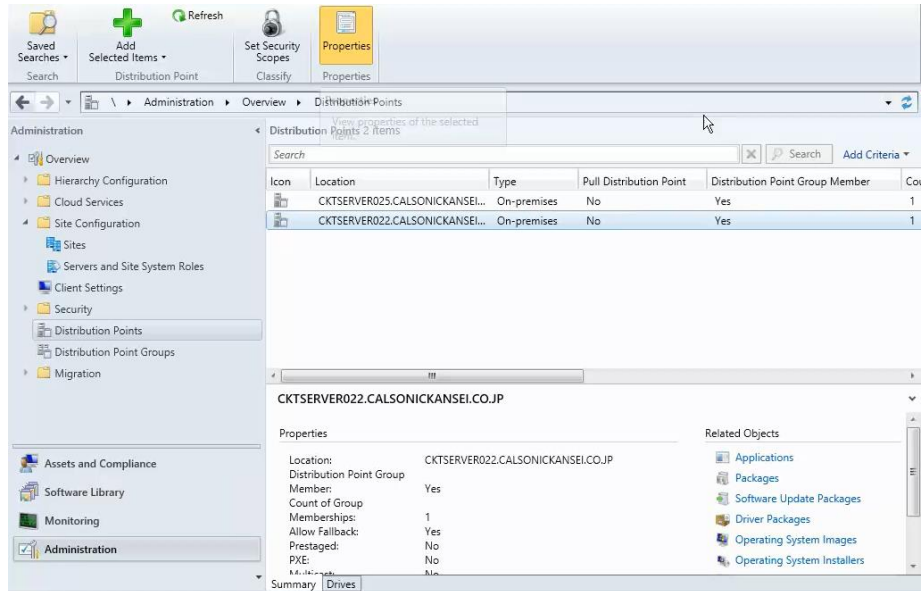
12. เข้าไปที่ PXE Response tab, เลือก enable Respond to all client computers, คลิก OK.



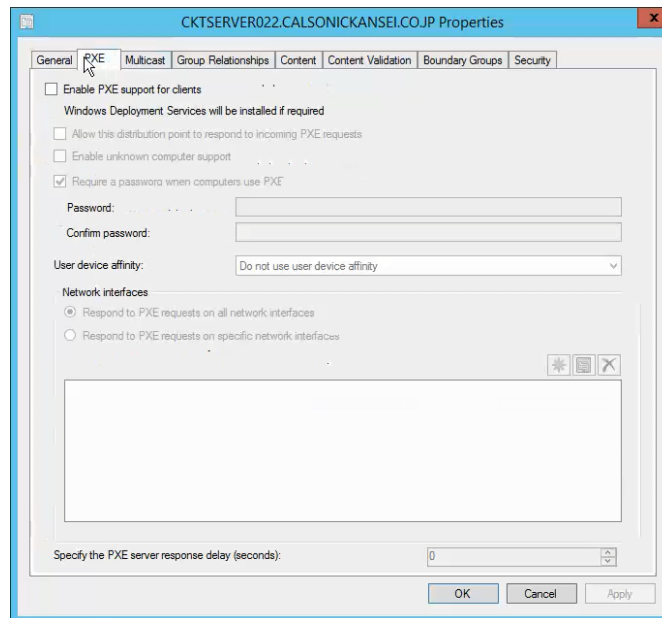
ภาคผนวก ฅ  
เปิดใช้ PXE on Distribution Point role

## เปิดใช้ PXE on Distribution Point role

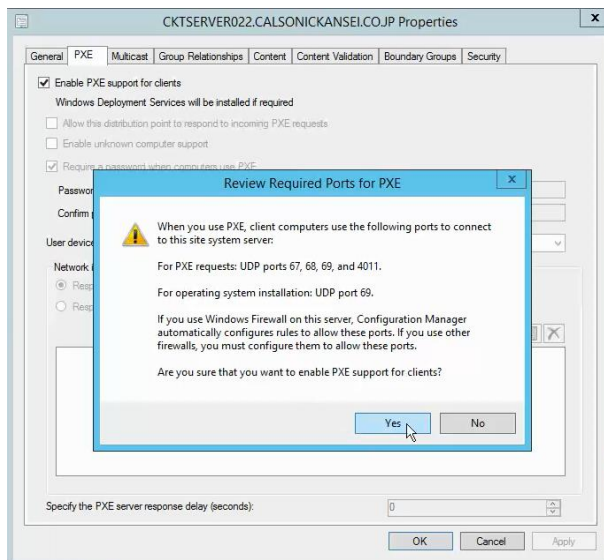
1. เปิด SCCM แล้วเข้าไปที่ Distribution Points, คลิก CKTSERVER022 แล้วเลือก *Properties*.



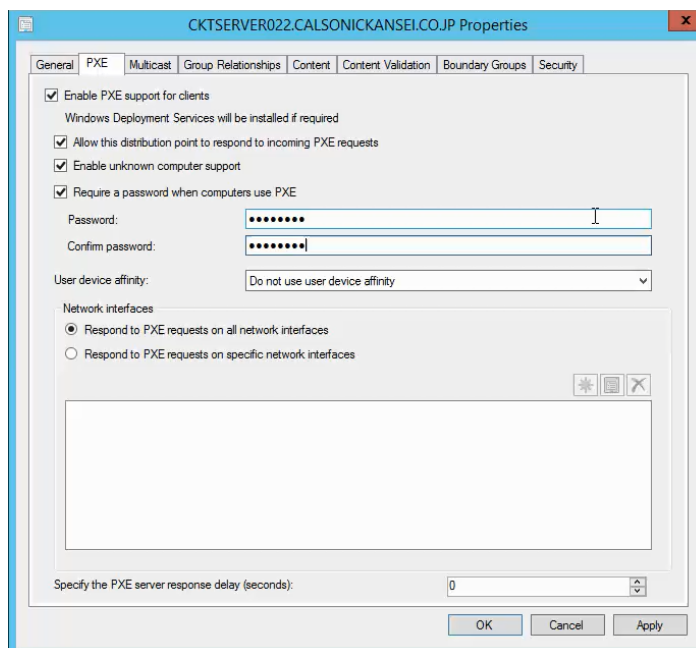
2. เข้าไปที่ PXE tab



3. เลือกเปิดใช้งาน Enable PXE support for clients แล้วคลิก Yes.



4. คลิกเปิดใช้งานตามรูป แล้วใส่ Password สำหรับ Administrator เครื่องที่ deploy ด้วย



ภาคผนวก ญ

สร้างโปรแกรมประยุกต์สำหรับ deploy (Application Management)

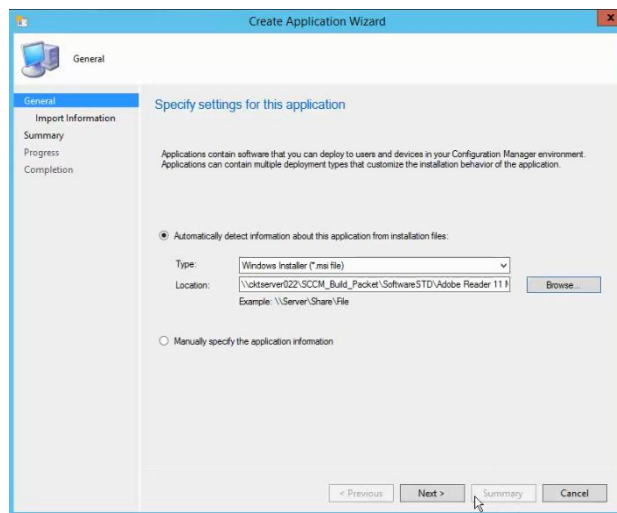
## สร้างโปรแกรมประยุกต์สำหรับ deploy (Application Management)

การสร้าง Application Adobe Reader XI

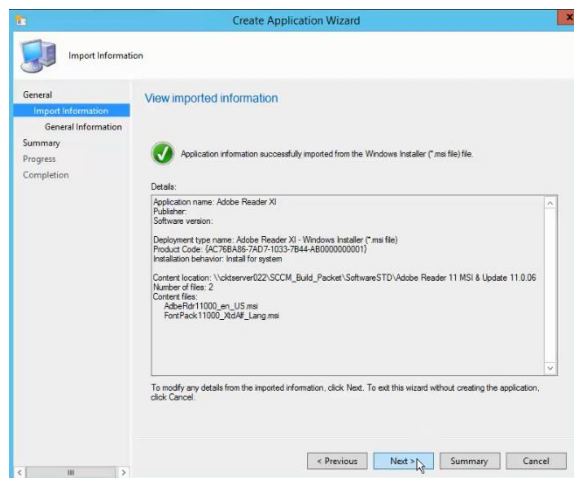
1. เปิด Software Library แล้วไปที่ Application Management>>Application จากนั้นคลิก Create Application.



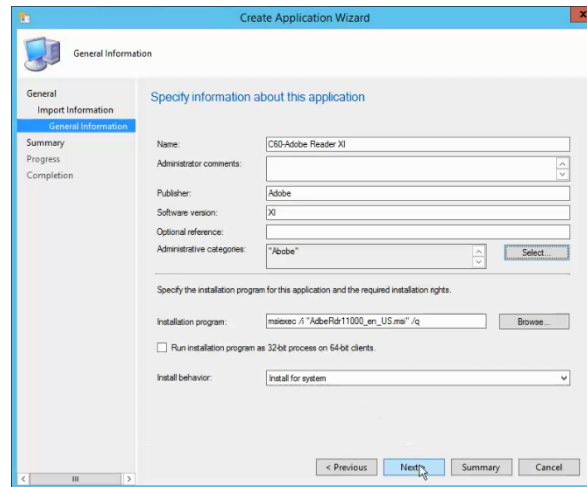
2. ในหน้า Create Application Wizard เลือก Source path ตามข้างล่างนี้  
[\\vktserver022\SCCM\\_Build\\_Packet\SoftwareSTD](#) ดังภาพด้านล่าง



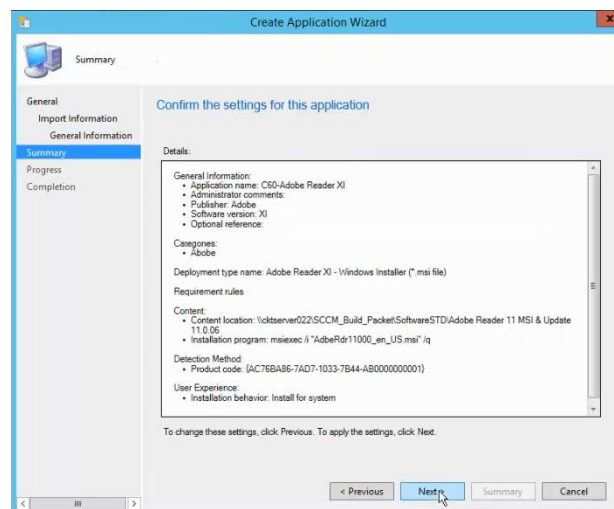
3. คลิก Next



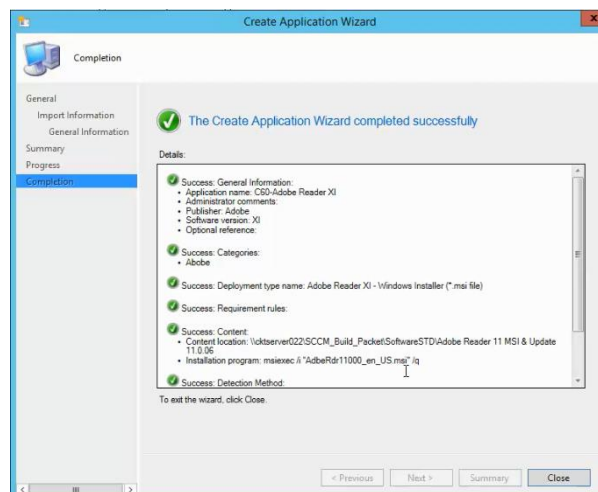
## 4. คลิก Next



## 5. คลิก Next

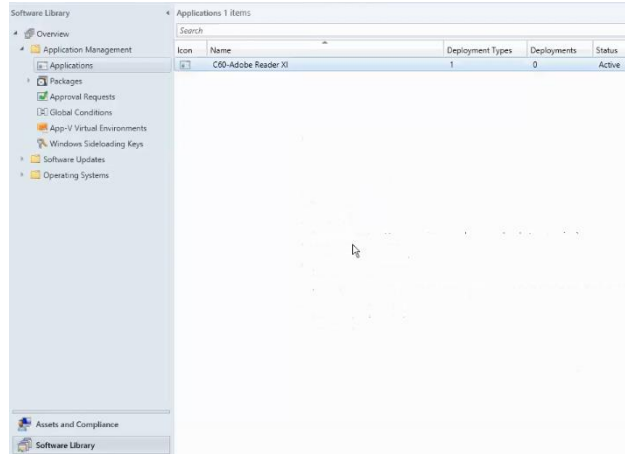


## 6. คลิก Close





7. C60-Adobe Reader XI ถูกสร้างแล้ว สามารถตรวจสอบดูได้ที่หน้า Applications item.

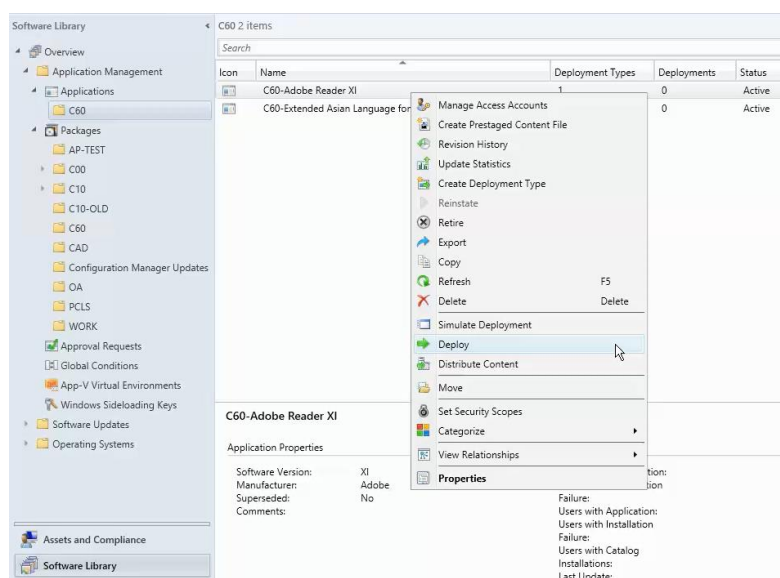


ภาคผนวก ก  
การ deploy โปรแกรมประยุกต์ไปที่ Collection เครื่องผู้ใช้

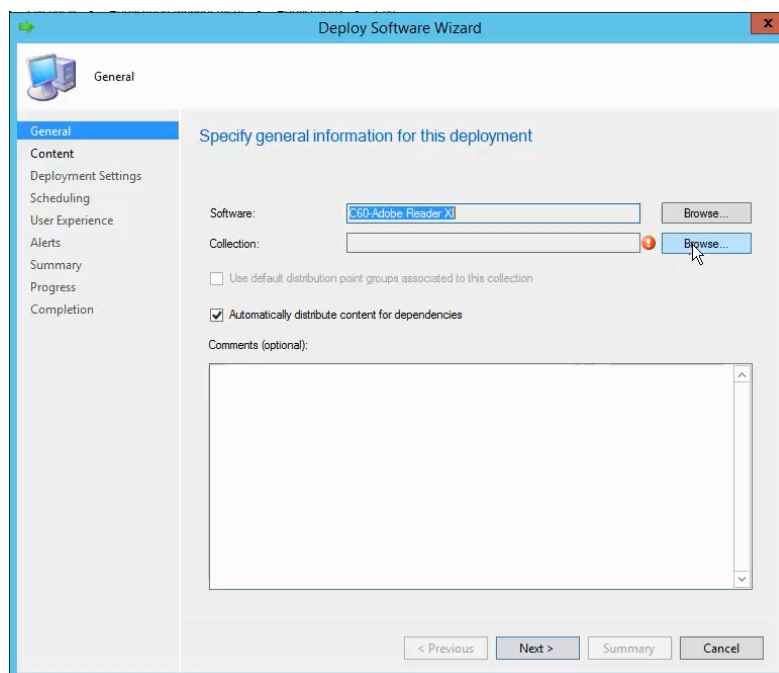
## การ deploy โปรแกรมประยุกต์ไปที่ Collection เครื่องผู้ใช้

Deploy โปรแกรมประยุกต์ที่ได้สร้างไว้แล้วชื่อ C60-Adobe Reader XI ไปที่ Collection ชื่อ **C60-CKT Test Department**

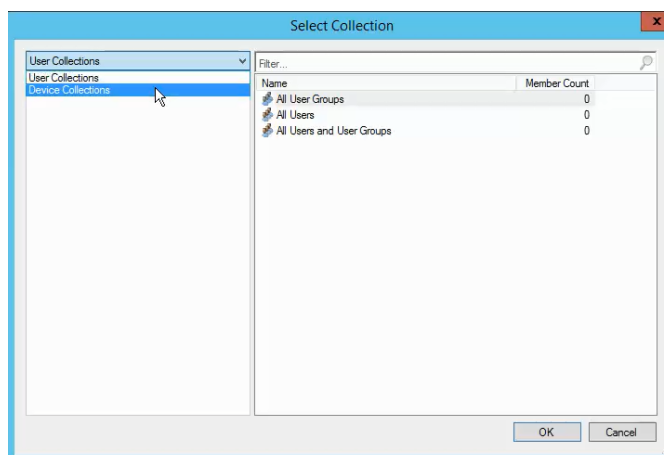
1. เข้าไปที่ Applications แล้วเลือกโปรแกรมประยุกต์ที่ต้องการ deploy โดยในที่นี้จะทดสอบ deploy C60-Adobe Reader XI โดยคลิกขวาที่ C60-Adobe Reader XI แล้วเลือก Deploy



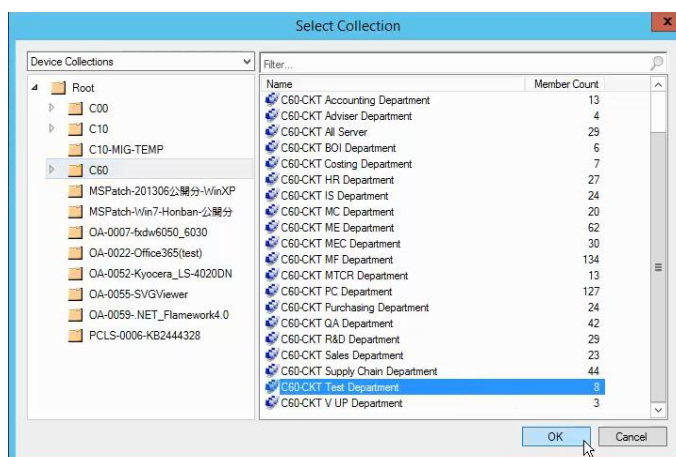
2. คลิก Browse เพื่อเลือก Collection



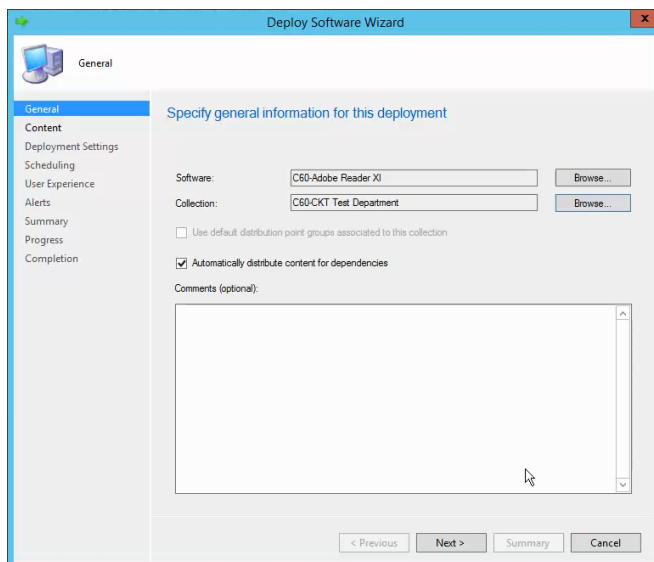
3. เลือก Device Collections ดังภาพด้านล่าง



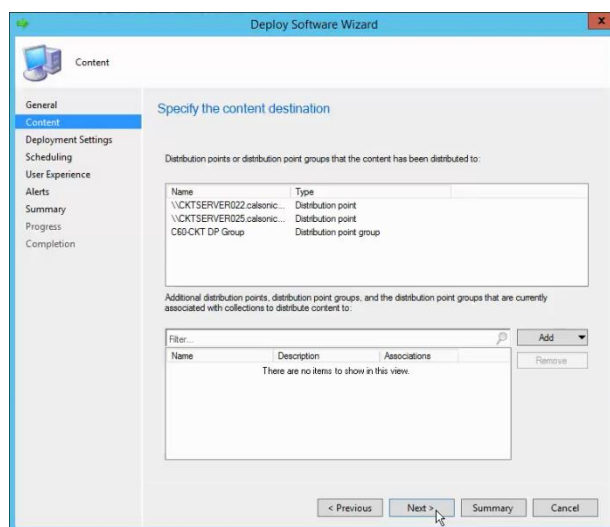
4. เลือก Collection ชื่อ *C60-CKT Test Department* and then click OK



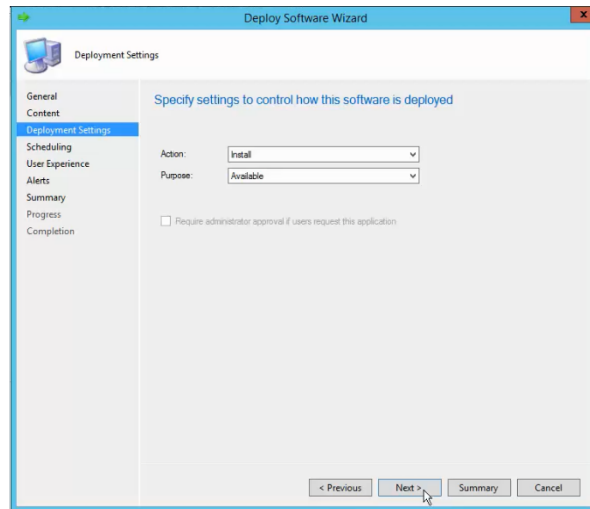
5. คลิก Next



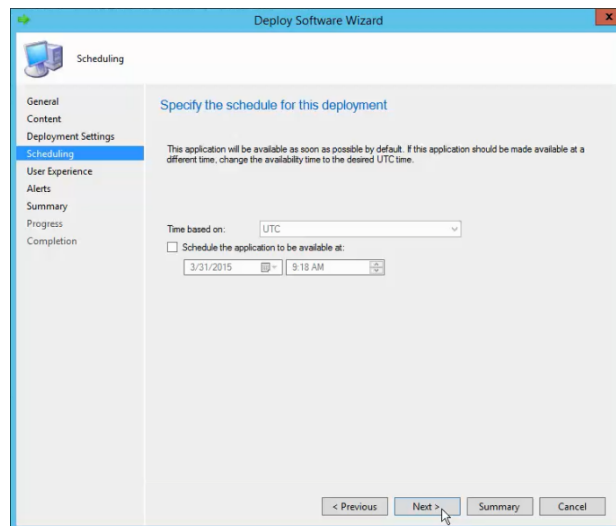
6. คลิก Next



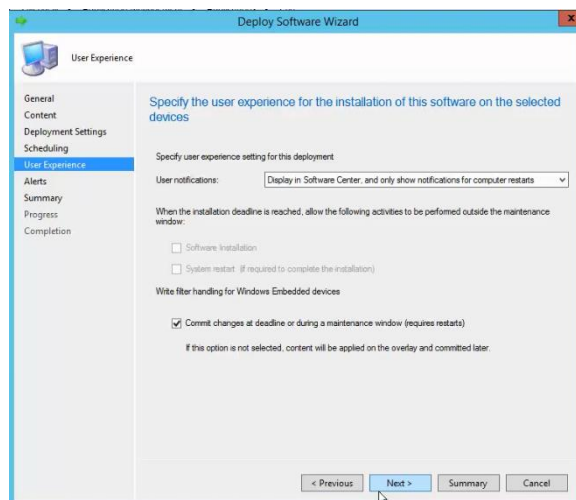
7. Action filed ให้เลือก Install และ purpose ให้เลือก Available แล้วคลิก Next



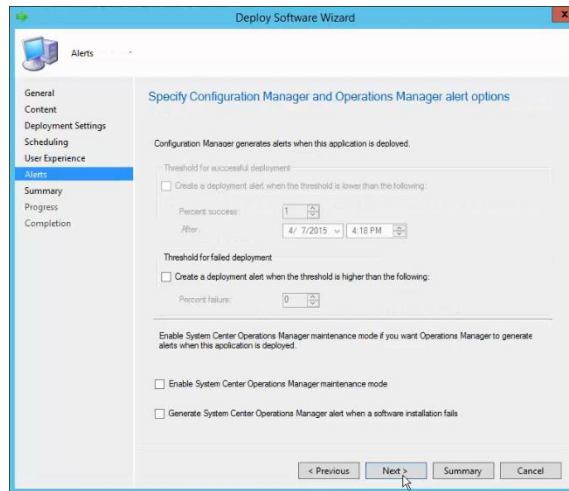
8. คลิก Next



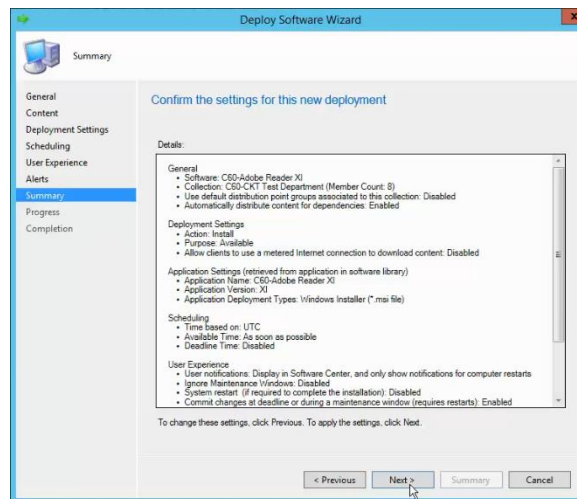
9. คลิก Next



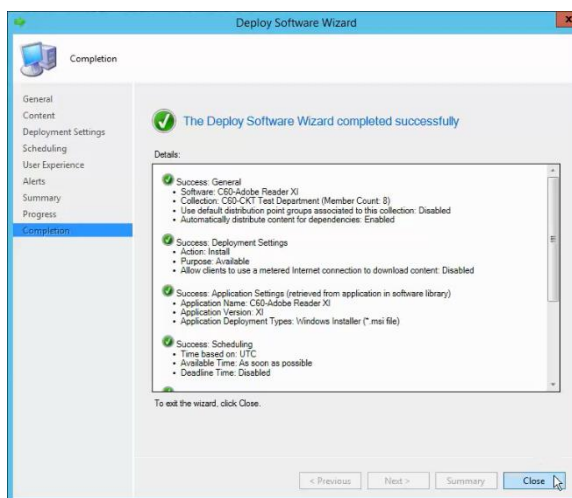
10. คลิก Next



11. คลิก Next



12. คลิก close

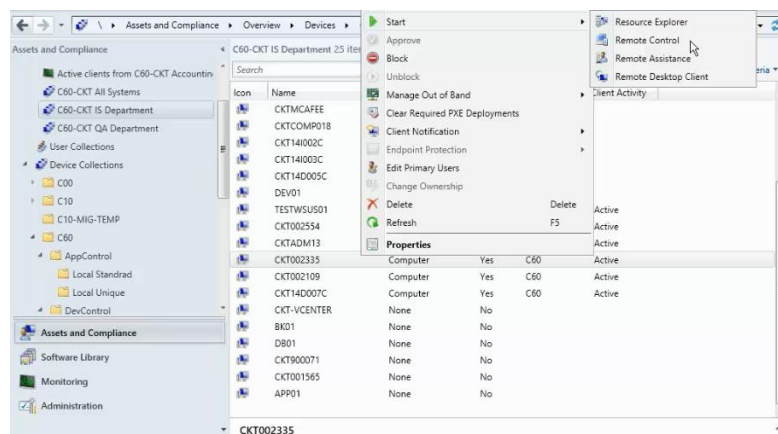


ภาคผนวก ฏ  
การควบคุมจากทางระยะไกล (Helpdesk remote assistance)

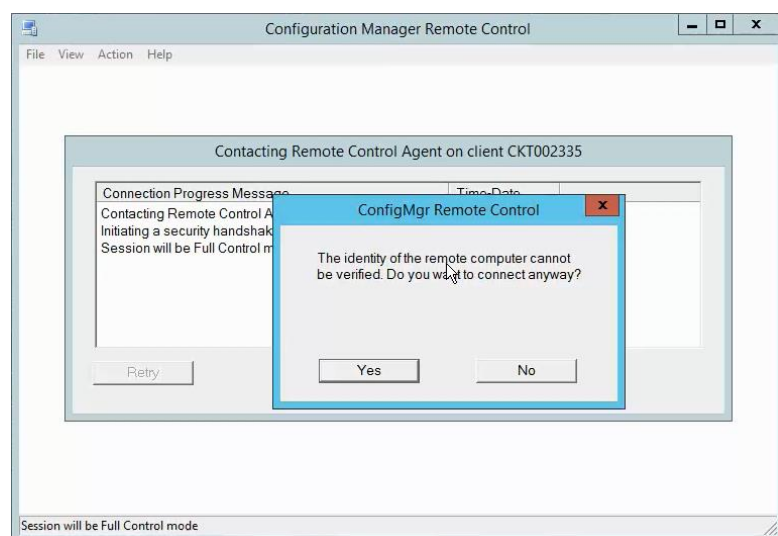


## การควบคุมจากทางระยะไกล (Helpdesk remote assistance)

1. ค้นหา Device ที่ต้องการ remote จากนั้นคลิกขวาที่ Start > Remote Control



2. จะมีหน้าต่าง pop up ขึ้นมา ให้คลิก Yes



3. กำลังทำการเชื่อมต่อไปเครื่องปลายทาง

