การเพิ่มประสิทธิภาพในการกู้คืนเหตุฉุกเฉินสำหรับศูนย์ข้อมูลขนาดเล็กและขนาดกลาง ผ่านโครงสร้างพื้นฐานแบบ Hyper-Converged (HCI)

พันวิทย์ กังแฮ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
บัณฑิตศึกษา สาขาเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น
ปีการศึกษา 2568

ENHANCING BUSINESS CONTINUITY THROUGH HYPER-CONVERGED INFRASTRASTRUCTURE (HCI) DISASTER RECOVERY IN SMALL AND MEDIUM DATA CENTERS

Panvit Kanghae

A Term Paper Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Information Technology
Graduate Studies
Thai-Nichi Institute of Technology
Academic Year 2025

หัวข้อสารนิพนธ์	การเพิ่มประสิทธิภาพในการกู้คืนเหตุฉุกเฉินสำหรับศูนย์ข้อมูลขนาดเล็กและขนาดกลางผ่านโครงสร้างพื้นฐานแบบ Hyper-Converged (HCI)
โดย	พันวิทย์ กังแฮ
สาขาวิชา	เทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษาสารนิพนธ์	ดร.ณปภัช วิชัยดิษฐ์

บัณฑิตศึกษา สถาบันเทคโนโลยีไทย-ญี่ปุ่น อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....รองอธิการบดีฝ่ายวิชาการ
(รองศาสตราจารย์ ดร.วรากร ศรีเชวงทรัพย์)
วันที่.....เดือน.....พ.ศ.....

คณะกรรมการสอบสารนิพนธ์

.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.กันติชา กิตติพีรชล)

.....กรรมการ
(ว่าที่ร้อยตรี ดร.พิชิตชัย คำอินทร์)

.....อาจารย์ที่ปรึกษาสารนิพนธ์
(ดร.ณปภัช วิชัยดิษฐ์)

พันวิทย์ กังแฮ : การเพิ่มประสิทธิภาพในการกู้คืนเหตุฉุกเฉินสำหรับศูนย์ข้อมูลขนาดเล็กและขนาดกลางผ่านโครงสร้างพื้นฐานแบบ Hyper-Converged (HCI). อาจารย์ที่ปรึกษา : ดร.ณปภัช วิชัยดิษฐ์, 36 หน้า.

การกู้คืนระบบจากเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) เป็นกลไกสำคัญในการรักษาความต่อเนื่องทางธุรกิจขององค์กร โดยเฉพาะศูนย์ข้อมูลขนาดเล็กและขนาดกลางที่มักเผชิญข้อจำกัดด้านงบประมาณและทรัพยากร งานวิจัยนี้มุ่งเน้นการศึกษาและพัฒนาแผน DRP บนสถาปัตยกรรม Hyper-Converged Infrastructure (HCI) ของ Nutanix เพื่อนำมาเปรียบเทียบกับแผน DRP แบบดั้งเดิม โดยใช้ตัวชี้วัดหลัก ได้แก่ Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) รวมถึงความถูกต้องของข้อมูลและความต่อเนื่องของบริการ วิธีดำเนินการวิจัยประกอบด้วยการทบทวนวรรณกรรม การออกแบบและจำลองสถานการณ์ฉุกเฉิน (เช่น การปิดระบบเซิร์ฟเวอร์ การล้มเหลวของโหนด และการโจมตีด้วยมัลแวร์) และการเก็บข้อมูลเพื่อวิเคราะห์ผลการกู้คืน กรณีศึกษาในองค์กรขนาดกลางถูกนำมาใช้เพื่อให้การประเมินมีความสมจริง ผลการวิจัยคาดว่าจะชี้ให้เห็นว่า DRP บน HCI สามารถลด RTO และ RPO ได้อย่างมีนัยสำคัญเมื่อเทียบกับ DRP แบบดั้งเดิม และเป็นแนวทางเชิงปฏิบัติสำหรับการประยุกต์ใช้ในองค์กรที่มีทรัพยากรจำกัด

บัณฑิตศึกษา ลายมือชื่อนักศึกษา .....

สาขาวิชา เทคโนโลยีสารสนเทศ ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2568

PANVIT KANGHAE : ENHANCING BUSINESS CONTINUITY THROUGH HYPER-CONVERGED INFRASTRASTRUCTURE (HCI) DISASTER RECOVERY IN SMALL AND MEDIUM DATA CENTERS. ADVISOR : DR.NAPAPHAT VICHAIDIS, 36 PP.

Disaster Recovery Planning (DRP) is a critical mechanism for ensuring business continuity, particularly for small and medium-sized Data Centers that often face budgetary and resource constraints. This study aims to design and develop a DRP based on Nutanix Hyper-Converged Infrastructure (HCI) and compare its performance with traditional DRP approaches. Key evaluation metrics include Recovery Time Objective (RTO), Recovery Point Objective (RPO), data integrity, and service continuity. The research methodology comprises literature review, experimental design, and simulated disaster scenarios (e.g., server shutdown, node failure, and malware attacks), with a case study in a medium-sized organization to ensure realism. The results indicate that DRP implemented on HCI will significantly reduce both RTO and RPO compared to traditional DRP, providing practical insights for organizations with limited resources.

Graduate Studies Student's Signature.....

Field of Study Information Technology Advisor's Signature.....

Academic Year 2025

กิตติกรรมประกาศ

ในการจัดทำสารนิพนธ์ฉบับนี้ได้รับความกรุณาและการสนับสนุนจากหลายภาคส่วน ผู้วิจัยขอขอบพระคุณ ดร.ณปภัช วิชัยดิษฐ์ อาจารย์ที่ปรึกษาสารนิพนธ์ ซึ่งได้ให้คำแนะนำ ตรวจแก้ไข และชี้แนะแนวทางการทำวิจัยอย่างละเอียดตลอดระยะเวลา การสนับสนุนทั้งด้านองค์ความรู้ซึ่งเป็นส่วนสำคัญอย่างยิ่งที่ทำให้งานวิจัยฉบับนี้สำเร็จได้

ผู้วิจัยขอขอบคุณ คุณฐาปน สิทธิเลิศพิศาล เพื่อนร่วมการศึกษา ผู้ให้คำปรึกษาและข้อเสนอแนะด้านรูปเล่ม ตลอดจนเป็นผู้ชักชวนให้เข้ามาศึกษาต่อในหลักสูตรนี้ อีกทั้งยังร่วมแลกเปลี่ยนความรู้และช่วยเหลือกันในการศึกษาอย่างต่อเนื่องจนทำให้การเรียนและการทำสารนิพนธ์สำเร็จลุล่วงไปด้วยดี

สุดท้ายนี้ ผู้วิจัยขอขอบคุณครอบครัว เพื่อนร่วมงาน และผู้เกี่ยวข้องทุกท่านที่ให้การสนับสนุนในทุกด้าน ทำให้ผู้วิจัยสามารถดำเนินงานวิจัยฉบับนี้จนสำเร็จสมบูรณ์

พันวิทย์ กังแฮ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

ปัจจุบัน ข้อมูลและระบบเทคโนโลยีสารสนเทศถือเป็นทรัพยากรที่มีความสำคัญอย่างยิ่งต่อการดำเนินธุรกิจขององค์กร การหยุดชะงักของระบบสารสนเทศอันเนื่องมาจากเหตุฉุกเฉิน เช่น ภัยพิบัติทางธรรมชาติ ภัยคุกคามทางไซเบอร์ หรือความล้มเหลวของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ อาจส่งผลกระทบโดยตรงต่อความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity) ความเชื่อมั่นของลูกค้า และก่อให้เกิดความเสียหายทางการเงินอย่างร้ายแรง [1]

ศูนย์ข้อมูลขนาดเล็กและขนาดกลาง (Small and Medium Data Centers) ซึ่งมักพบในองค์กรขนาดกลางและขนาดเล็ก การจัดทำและบริหารจัดการแผนการกู้คืนจากเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) ยังคงเผชิญกับข้อจำกัดหลายประการ เช่น งบประมาณที่จำกัด ความซับซ้อนของสถาปัตยกรรมแบบดั้งเดิม (Traditional Three-Tier Architecture) และการพึ่งพาบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน ส่งผลให้กระบวนการกู้คืนระบบมีความล่าช้า และไม่สามารถบรรลุเป้าหมายด้านเวลาในการกู้คืน Recovery Time Objective (RTO) และจุดกู้คืนข้อมูล Recovery Point Objective (RPO) ได้ตามที่กำหนดไว้

ในช่วงที่ผ่านมา องค์กรขนาดกลางและขนาดเล็กในประเทศไทยเริ่มนำสถาปัตยกรรมแบบ Hyper-Converged Infrastructure (HCI) มาใช้งานเพิ่มมากขึ้น เนื่องจาก HCI สามารถรวมทรัพยากรด้าน Compute, Storage และ Networking ไว้ในที่เดียว และสนับสนุนการบริหารจัดการและการทำ Disaster Recovery ผ่านซอฟต์แวร์ที่มีการบริหารจัดการอยู่ที่เดียวกัน ซึ่งมีศักยภาพในการลดความซับซ้อน เพิ่มความรวดเร็วในการกู้คืนระบบ และลดต้นทุนในการดำเนินงาน

อย่างไรก็ตาม ศูนย์ข้อมูลขนาดเล็กและขนาดกลาง (Small and Medium Data Centers) ซึ่งพบได้ทั่วไปในองค์กรขนาดเล็กและขนาดกลาง (SMEs) มักประสบข้อจำกัดด้านงบประมาณ บุคลากร และความซับซ้อนของโครงสร้างพื้นฐาน ส่งผลให้การนำ DRP แบบดั้งเดิมที่อาศัยสถาปัตยกรรมแบบแยกส่วน (Traditional Three-Tier Architecture) มาใช้งานมีต้นทุนสูงและมีความซับซ้อนในการบริหารจัดการ อีกทั้งยังอาจไม่สามารถบรรลุค่า RTO และ RPO ได้ตามที่องค์กรต้องการ โดยเฉพาะในกรณีที่เกิดเหตุฉุกเฉินที่ต้องการการตอบสนองอย่างรวดเร็ว

ในช่วงที่ผ่านมา เทคโนโลยี HCI ได้รับความสนใจและถูกนำมาใช้งานในองค์กรขนาดกลางในประเทศไทยเพิ่มมากขึ้น เนื่องจากสามารถรวมทรัพยากรด้านประมวลผล จัดเก็บข้อมูล และเครือข่ายไว้ในสถาปัตยกรรมเดียวกัน พร้อมทั้งสนับสนุนการทำ Snapshot และ Replication ในระดับ Virtual Machine ซึ่ง

มีศักยภาพในการลดระยะเวลาในการกู้คืนระบบและเพิ่มความต่อเนื่องของบริการ อย่างไรก็ตาม แม้องค์กรจำนวนมากเริ่มนำ HCI มาใช้งานจริง แม้จะมีการนำแผน DRP มาใช้อย่างแพร่หลาย แต่ยังไม่มีผลการทดลองที่ชัดเจนยืนยันถึงประสิทธิภาพของแผนดังกล่าวบนสถาปัตยกรรม HCI เมื่อเปรียบเทียบกับแผน DRP แบบดั้งเดิม ทั้งนี้ประสิทธิภาพของแผน DRP ยังขาดการยืนยันจากการทดสอบจริง โดยเฉพาะเมื่อพิจารณาในด้านของศูนย์ข้อมูลและองค์กรขนาดเล็กและขนาดกลาง

นอกจากนี้ เพื่อให้มั่นใจว่าแผนการกู้คืนจากเหตุฉุกเฉิน DRP สามารถนำไปปฏิบัติได้จริง องค์กรจำเป็นอย่างยิ่งที่จะต้องดำเนินการทดสอบแผนอย่างสม่ำเสมอ (Regular Testing) และดำเนินการปรับปรุงแผนให้สอดคล้องกับสถานการณ์และเทคโนโลยีที่เปลี่ยนแปลงอยู่ตลอดเวลา (Continuous Improvement) องค์กรควรจัดทำการฝึกซ้อมหรือจำลองสถานการณ์อย่างน้อยปีละครั้ง เพื่อประเมินประสิทธิภาพของแผนและความพร้อมของบุคลากร [1], [2]

จากผลการศึกษาพบว่า ความล่าช้าในขั้นตอนสำคัญของกระบวนการกู้คืนสามารถส่งผลให้ไม่สามารถบรรลุวัตถุประสงค์ของเวลาในการกู้คืน (Recovery Time Objective: RTO) ได้ ดังนั้น การประยุกต์ใช้เทคโนโลยีและแนวทางที่มีประสิทธิภาพเข้ามาใช้ เช่น การออกแบบแบบจำลองที่ปลอดภัยและมีความยืดหยุ่น (Secure and Resilient Model) จึงมีความสำคัญอย่างยิ่ง เนื่องจากช่วยลดความเสี่ยงที่เกิดจากความล่าช้า เพิ่มประสิทธิภาพในการตอบสนองต่อเหตุการณ์ที่ไม่คาดคิด และส่งเสริมให้องค์กรสามารถตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที และรักษาความต่อเนื่องในการดำเนินธุรกิจได้อย่างมีประสิทธิภาพ

ด้วยเหตุนี้ องค์กรที่มีการเตรียมการ และมีการประเมินพร้อมทั้งบำรุงรักษาแผนการกู้คืนจากเหตุฉุกเฉิน DRP อย่างต่อเนื่อง จะสามารถสร้างความได้เปรียบเชิงกลยุทธ์ สามารถรับมือกับเหตุการณ์ฉุกเฉินที่อาจเกิดขึ้นได้อย่างมั่นใจ ส่งผลให้องค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และลดความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีนัยสำคัญ

1.2 วัตถุประสงค์

1.2.1 เพื่อออกแบบแผนการกู้คืนจากเหตุฉุกเฉิน (DRP) บนสถาปัตยกรรม HCI สำหรับศูนย์ข้อมูลขนาดเล็กและขนาดกลาง และประเมินความสามารถของ HCI ในการลด RTO และ RPO

1.2.2 เพื่อเปรียบเทียบประสิทธิภาพของ DRP แบบดั้งเดิมกับ DRP ที่พัฒนาบนสถาปัตยกรรม HCI โดยใช้เกณฑ์ด้านเวลาในการกู้คืน (RTO) จุดกู้คืนข้อมูล (RPO) ความต่อเนื่องของบริการ และต้นทุนการดำเนินงาน

1.2.3 เพื่อประเมินความเป็นไปได้และประสิทธิผลของการนำ DRP บน HCI ไปประยุกต์ใช้จริงในศูนย์ข้อมูลขนาดเล็กและขนาดกลาง

1.3 คำถามวิจัย

1.3.1 แผนการกู้คืนจากเหตุฉุกเฉิน (DRP) บนสถาปัตยกรรม HCI สามารถลดค่า RTO และ RPO ได้ดีกว่าแผน DRP แบบเดิมหรือไม่

1.3.2 การใช้ HCI ช่วยให้ความต่อเนื่องในการให้บริการ (Service Continuity) ในช่วงเกิดเหตุฉุกเฉินได้อย่างไรในระบบสารสนเทศของศูนย์ข้อมูลขนาดเล็กและขนาดกลาง

1.3.3 HCI มีข้อจำกัดหรือปัจจัยใดบ้างในการนำมาใช้เป็นโครงสร้างพื้นฐานสำหรับ DRP ในองค์กรขนาดเล็กและขนาดกลาง

1.4 ขอบเขตงานวิจัย

1.4.1 ศึกษาและพัฒนาแผนการรองรับเหตุฉุกเฉินสำหรับศูนย์ข้อมูลขนาดเล็กและขนาดกลาง โดยใช้สถาปัตยกรรม HCI ของ Nutanix เป็นกรณีศึกษา

1.4.2 มุ่งเน้นการทดสอบและประเมินผลการกู้คืนในระบบ Virtual Machine (VM) ที่มีความสำคัญต่อการดำเนินงาน ประกอบด้วย Application Server และ Database Server บนระบบปฏิบัติการ Windows Server

1.4.3 จำลองเหตุการณ์ความล้มเหลวที่อาจเกิดขึ้นจริง เช่น การปิดระบบเซิร์ฟเวอร์ (Server Shutdown Simulation)

1.4.4 ศึกษาและทดสอบแผน DRP บนสถาปัตยกรรม HCI โดยใช้กรณีศึกษา บริษัทขนาดกลางเป็นกรณีศึกษา (Case Study) เพื่อประเมินความเหมาะสมในการประยุกต์ใช้ในสภาพแวดล้อมจริง

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ข้อมูลเกี่ยวกับ RTO และ RPO จากการทดลองในสภาพแวดล้อมจริง ซึ่งสามารถใช้เป็นเกณฑ์ประเมินประสิทธิภาพของแผน DRP ในการส่งเสริมความต่อเนื่องทางธุรกิจและลดความเสี่ยงจากเหตุฉุกเฉิน

1.5.2 ได้แนวทางและแผน DRP ที่สามารถปรับใช้ได้จริงในบริบทของสำนักงาน (Office-Based) และสามารถนำไปขยายผลในองค์กรขนาดเล็กและขนาดกลาง (SMEs)

1.5.3 เพิ่มความสามารถในการบริหารความเสี่ยงและการรับมือกับสถานการณ์วิกฤตขององค์กร โดยช่วยลดระยะเวลาหยุดชะงักของระบบงาน (System Downtime) ซึ่งส่งผลให้องค์กรสามารถรักษาความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity) ได้อย่างมีประสิทธิภาพ

บทที่ 2
ทฤษฎีงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับการกู้คืนจากเหตุฉุกเฉิน DRP

การกู้คืนระบบเทคโนโลยีสารสนเทศเป็นกระบวนการที่ครอบคลุมการฟื้นฟูระบบโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ (IT Infrastructure) และข้อมูลขององค์กรที่ได้รับผลกระทบจากภัยพิบัติหรือเหตุการณ์วิกฤต กระบวนการนี้มีเป้าหมายเพื่อให้ระบบ IT กลับมาใช้งานได้ตามปกติหรือมีประสิทธิภาพที่ดียิ่งขึ้น โดยเน้นความรวดเร็ว ความต่อเนื่องของธุรกิจ และการป้องกันความเสียหายในระยะยาว ประเภทของภัยคุกคามและเหตุการณ์ฉุกเฉิน มีหลายรูปแบบได้แก่

1. ภัยธรรมชาติ (Natural Disasters) เป็นสิ่งที่เกิดขึ้นจากธรรมชาติ ซึ่งมีหลากหลายประเภท โดยสามารถแบ่งได้ตามเหตุที่เกิดขึ้นแตกต่างกันและจะส่งผลกระทบต่อโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศแตกต่างกันออกไป [3] สามารถแบ่งได้ดังนี้

(1) แผ่นดินไหว ทำลายโครงสร้างอาคารและอุปกรณ์ฮาร์ดแวร์ เป็นสาเหตุของการหยุดชะงักอย่างกะทันหัน

(2) อุทกภัย ทำให้เกิดน้ำท่วมซึ่งสามารถสร้างความเสียหายต่ออุปกรณ์ไฟฟ้าและเซิร์ฟเวอร์ ส่งผลให้เกิดไฟฟ้าช็อตทำให้ข้อมูลสูญหายถาวร

(3) วาตภัย ก่อให้เกิดพายุและลมแรงทำให้เสาสัญญาณและสายเคเบิลขาด ส่งผลต่อการเชื่อมต่ออุปกรณ์เครือข่าย

(4) อัคคีภัย ทำลายศูนย์ข้อมูลและอุปกรณ์ IT ทั้งหมดในพื้นที่ที่ได้รับผลกระทบ

2. การโจมตีทางไซเบอร์ (Cyber Attacks) มีรูปแบบการโจมตีที่สำคัญในรูปแบบต่างๆ ได้แก่

(1) มัลแวร์และไวรัส เป็นโปรแกรมที่เป็นอันตรายที่ทำลายไฟล์และระบบปฏิบัติการแรนซัมแวร์: การเข้ารหัสข้อมูลและเรียกค่าไถ่เพื่อปลดล็อก

(2) การโจมตี DDoS เป็นการส่งคำขอจำนวนมหาศาลเพื่อทำให้เซิร์ฟเวอร์ล่ม

(3) การขโมยข้อมูล เป็นการเข้าถึงและดาวน์โหลดข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(4) การโจมตีแบบ Advanced Persistent Threat (APT) คือการแทรกซึมระยะยาวเพื่อขโมยข้อมูลหรือทำลายระบบ [4]

3. เหตุขัดข้องของระบบ (System Failures) มีสาเหตุและลักษณะดังนี้

(1) ความเสียหายทางด้านฮาร์ดแวร์เช่น ฮาร์ดดิสก์เสียหาย เซิร์ฟเวอร์ขัดข้อง อุปกรณ์เครือข่ายชำรุด

(2) ปัญหาซอฟต์แวร์ ได้แก่ บั๊กในโปรแกรม การอัปเดตที่ผิดพลาด ความไม่เข้ากันของระบบ

(3) ปัญหาการจ่ายไฟ ไฟดับ ระบบ UPS ล้มเหลว ปัญหาระบบไฟฟ้าสำรอง

(4) ความเสียหายของระบบเครือข่าย เช่น การขาดการเชื่อมต่ออินเทอร์เน็ต [5]

4. ข้อผิดพลาดของมนุษย์ (Human Errors)

(1) การลบข้อมูลโดยไม่ตั้งใจ: การลบไฟล์หรือฐานข้อมูลสำคัญ

(2) การกำหนดค่าระบบผิด: การตั้งค่าเซิร์ฟเวอร์หรือเครือข่ายไม่ถูกต้อง

(3) การใช้รหัสผ่านที่อ่อนแอ: ทำให้เกิดช่องโหว่ด้านความปลอดภัย

(4) การไม่ปฏิบัติตามขั้นตอนความปลอดภัย: การข้ามขั้นตอนสำคัญในการบำรุงรักษาระบบ

2.1.1 เป้าหมายหลักของการกู้คืน

1. การกลับสู่สภาวะปกติอย่างรวดเร็ว (Rapid Recovery) [6]

(1) การจัดลำดับความสำคัญ: กู้คืนระบบที่สำคัญที่สุดก่อน (Critical Systems First)

(2) การใช้เทคโนโลยีอัตโนมัติ: ระบบ Automated Failover และ Recovery Scripts

(3) การเตรียมทีมงานพร้อม: Crisis Response Team ที่ฝึกฝนและพร้อมปฏิบัติงาน 24/7

(4) การทดสอบแผนกู้คืนเป็นประจำ: เพื่อให้แน่ใจว่าสามารถปฏิบัติได้จริงเมื่อเกิดเหตุ

2. การรักษาความต่อเนื่องของธุรกิจ (Business Continuity)

การระบุกระบวนการทางธุรกิจที่สำคัญ วิเคราะห์ว่าระบบ IT ใดบ้างที่สนับสนุนการทำงานหลัก

(1) การจัดเตรียมทางเลือก: มีระบบสำรองและกระบวนการทำงานทางเลือก

(2) การสื่อสารกับผู้มีส่วนได้ส่วนเสีย: แจ้งสถานการณ์และแผนการกู้คืนแก่ลูกค้าและหุ้นส่วน

(3) การบริหารจัดการความเสี่ยงทางการเงิน: ประเมินค่าใช้จ่ายและผลกระทบทางเศรษฐกิจ

2.1.2 การป้องกันความเสียหายในระยะยาว

การสร้างความยืดหยุ่นของระบบ (System Resilience) คือความสามารถของระบบในการทนต่อปัญหา (เช่น ฮาร์ดแวร์เสีย ไฟดับ ถูกโจมตีทางไซเบอร์) และสามารถกลับมาทำงานได้ ภายในระยะเวลาที่เหมาะสม โดยไม่ให้กระทบธุรกิจมากเกินไปสามารถทำได้ดังนี้

(1) การกระจายความเสี่ยง (Risk Distribution): การใช้ Multiple Data Centers และ Geographic Redundancy

(2) การสร้างระบบสำรอง (Redundancy): การมี Backup Systems ที่สามารถทำงานทดแทนได้ทันที

(3) การใช้เทคโนโลยี Fault-Tolerant: ระบบที่สามารถทำงานต่อไปได้แม้มีส่วนประกอบบางส่วนเสียหาย

(4) การเตรียมรับมือภัยคุกคามในอนาคต เช่น Cyber Threats, Physical Threats, เทคโนโลยีใหม่ที่เป็นช่องโหว่

(5) การติดตามแนวโน้มภัยคุกคาม: ศึกษาและวิเคราะห์ภัยใหม่ๆ ที่อาจเกิดขึ้น

(6) การปรับปรุงแผนกู้คืนอย่างสม่ำเสมอ: ทบทวนและปรับปรุงแผนตามการเปลี่ยนแปลงของเทคโนโลยี การลงทุนในเทคโนโลยีใหม่: เช่น AI สำหรับ Threat Detection, Blockchain สำหรับ Data Integrity [7]

การสร้างวัฒนธรรมความปลอดภัย ส่งเสริมให้พนักงานมีจิตสำนึกด้านความปลอดภัยสูง

2.2 ความสำคัญของแผนการกู้คืนจากเหตุฉุกเฉิน

ความสำคัญของแผนการกู้คืนจากเหตุฉุกเฉิน (DRP) ในโลกปัจจุบันที่พึ่งพาเทคโนโลยีและข้อมูลเป็นอย่างมาก องค์กรต่างๆ ไม่ว่าจะขนาดเล็กหรือใหญ่ ต่างต้องเผชิญกับความเสี่ยงจากเหตุการณ์ไม่คาดฝันที่อาจส่งผลกระทบต่อระบบเครือข่ายและโครงสร้างพื้นฐานด้านไอทีอย่างรุนแรง เหตุการณ์เหล่านี้อาจเกิดจากสาเหตุดังต่อไปนี้ [8]

- ภัยธรรมชาติ เช่น น้ำท่วม, แผ่นดินไหว, ไฟไหม้, พายุ
- ความล้มเหลวทางเทคนิค เช่น ระบบล่ม, อุปกรณ์ฮาร์ดแวร์เสียหาย, ซอฟต์แวร์มีข้อผิดพลาด
- การโจมตีจากทางไซเบอร์ เช่น Ransomware, DDoS attacks, การขโมยข้อมูล
- ความผิดพลาดของมนุษย์ เช่น การตั้งค่าผิดพลาด,การลบข้อมูลโดยไม่ตั้งใจ
- การบริการทางด้านสาธารณูปโภคขัดข้อง เช่น ไฟฟ้าดับ, ระบบอินเทอร์เน็ตล่ม

เมื่อเกิดเหตุการณ์เหล่านี้ขึ้น หากองค์กรไม่มีแผนการกู้คืนจากเหตุฉุกเฉิน (DRP) ที่ดีพอ ผลกระทบที่ตามมาอาจรุนแรงและก่อให้เกิดความเสียหายในหลายด้านเช่น

• ความเสียหายทั้งทางด้านการเงิน การสูญเสียรายได้ เมื่อระบบธุรกิจหยุดชะงัก ลูกค้าไม่สามารถเข้าถึงบริการหรือซื้อสินค้าได้ ส่งผลให้รายได้ขององค์กรลดลงอย่างมหาศาล ยิ่งหยุดชะงักนานเท่าไหร่ การสูญเสียก็ยิ่งมากขึ้น ค่าใช้จ่ายในการกู้คืนที่ไม่คาดคิด หากไม่มีแผน DRP ที่ชัดเจน การกู้คืนระบบอาจต้องใช้เวลานานและมีค่าใช้จ่ายสูงในการแก้ไขปัญหาเฉพาะหน้า การจัดซื้ออุปกรณ์ใหม่ การจ้างผู้เชี่ยวชาญเร่งด่วน ซึ่งมักจะมีค่าใช้จ่ายมีมากกว่าปกติมาก ค่าปรับหรือค่าชดเชย ในบางอุตสาหกรรม การหยุดชะงักของบริการอาจนำไปสู่การละเมิดข้อตกลงระดับบริการ (SLA-Service Level Agreement) กับลูกค้า หรือการไม่ปฏิบัติตามกฎระเบียบของภาครัฐ ซึ่งอาจส่งผลให้ต้องจ่ายค่าปรับ ค่าชดเชย หรือถูกฟ้องร้องได้ มูลค่าตลาดลดลง หากเหตุการณ์รุนแรงและส่งผลกระทบต่อการดำเนินธุรกิจอย่างมีนัยสำคัญ นักลงทุนอาจสูญเสียความน่าเชื่อถือหรือความเชื่อมั่น ทำให้มูลค่าหุ้นหรือมูลค่าองค์กรโดยรวมลดลง

• ความเสียหายด้านความเชื่อมั่นขององค์กร ภาพลักษณ์เสียหาย การที่ระบบล่มหรือไม่สามารถให้บริการได้เป็นเวลานาน ส่งผลให้ภาพลักษณ์ขององค์กรเสียหายอย่างรุนแรง ลูกค้าและคู่ค้าอาจมองว่าองค์กรไม่มีความน่าเชื่อถือ ไม่สามารถดูแลระบบพื้นฐานได้ดีพอซึ่งอาจส่งผลต่อการสูญเสียลูกค้า ลูกค้าที่ไม่สามารถเข้าถึงบริการได้ตามปกติ อาจหันไปใช้บริการของคู่แข่ง ทำให้องค์กรสูญเสียฐานลูกค้าในระยะยาว ความไม่พอใจของพนักงาน พนักงานอาจไม่สามารถทำงานได้ตามปกติ ขวัญและกำลังใจลดลง รวมถึงอาจเกิดความเครียดจากการที่ต้องรับมือกับความไม่แน่นอนของระบบ ความเสี่ยงทางกฎหมายและชื่อเสียง : หากข้อมูลลูกค้ารั่วไหลหรือบริการหยุดชะงักอันเนื่องมาจากการขาดการวางแผนที่ดี องค์กรอาจเผชิญกับการฟ้องร้องทางกฎหมายและความเสียหายทางชื่อเสียงที่ไม่สามารถประเมินค่าได้

ดังนั้น การที่องค์กรที่ไม่มีแผน DRP หรือมีแผนที่ไม่มีการทดสอบอย่างต่อเนื่อง มีโอกาสที่จะได้รับความเสียหายจากเหตุการณ์ฉุกเฉินมากกว่าองค์กรที่มีแผน DRP อย่างมีนัยสำคัญ

2.3 กระบวนการจัดทำแผน Disaster Recovery Plan (DRP)

กระบวนการจัดทำ DRP เป็นกระบวนการสำคัญในการเตรียมองค์กรให้สามารถกู้คืนระบบเครือข่ายและโครงสร้างพื้นฐานด้านไอทีให้กลับมาทำงานตามปกติหรือใกล้เคียงปกติให้เร็วที่สุด เมื่อเกิดเหตุการณ์ที่ไม่คาดคิด เช่น ภัยพิบัติ ภัยคุกคามทางไซเบอร์ หรือความผิดพลาดทางระบบต่างๆ โดยประกอบด้วยขั้นตอนหลัก 6 ขั้นตอน ดังนี้

2.3.1 การประเมินความเสี่ยง (Risk Assessment)

เป็นขั้นตอนแรกที่มีความสำคัญในการวางแผน DRP โดยมุ่งเน้นไปที่การวิเคราะห์และระบุปัจจัยเสี่ยงต่างๆ ที่อาจส่งผลกระทบต่อระบบเครือข่ายและโครงสร้างพื้นฐานด้านไอทีขององค์กร เพื่อเตรียมมาตรการป้องกันหรือบรรเทาผลกระทบที่จะเกิดขึ้นอย่างเหมาะสม เพื่อให้องค์กรสามารถระบุจุดอ่อนและช่องโหว่ในระบบ พร้อมทั้งเตรียมมาตรการป้องกันและแผนรับมือที่เหมาะสมเพื่อลดผลกระทบและรักษาความต่อเนื่องในการดำเนินงาน

2.3.2 องค์ประกอบสำคัญของการประเมินความเสี่ยง

การระบุและวิเคราะห์ความเสี่ยง (Risk Identification and Analysis) จากปัจจัยต่างๆ เช่น ความเสี่ยงจากภัยธรรมชาติ (แผ่นดินไหว, น้ำท่วม, พายุ, ฟ้าผ่า) ความเสี่ยงจากอุบัติเหตุ (ไฟไหม้, ระบบไฟฟ้าขัดข้อง, การรั่วไหลของน้ำ) ความเสี่ยงทางเทคนิค (ระบบฮาร์ดแวร์ล้มเหลว, ซอฟต์แวร์ขัดข้อง, การสูญหายของข้อมูล) ความเสี่ยงด้านความปลอดภัยไซเบอร์ (การโจมตีทางไซเบอร์,มัลแวร์, การรั่วไหลของข้อมูล) ความเสี่ยงจากปัจจัยมนุษย์ (ข้อผิดพลาดของพนักงาน,การลาออกของบุคลากรสำคัญ)

การจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization) การประเมินความเสี่ยงตามผลกระทบและโอกาสที่จะเกิดขึ้นการจัดลำดับความเสี่ยง สูง กลาง หรือต่ำ

กำหนดมาตรการลดความเสี่ยง (Risk Mitigation Measures) ให้เหมาะสมกับแต่ละความเสี่ยงที่ระบุไว้ เช่น มาตรการป้องกัน (Preventive Measures)ระบบสำรองไฟฟ้า ระบบดับเพลิง การเข้ารหัสข้อมูล มาตรการตรวจจับ (Detective Measures) ระบบมอนิเตอร์ริง ระบบเตือนภัย มาตรการแก้ไข (Corrective Measures) ขั้นตอนการกู้คืนระบบ แผนการสื่อสาร การถ่ายโอนความเสี่ยง (Risk Transfer) การทำประกันภัย การจ้างบริษัทภายนอก [8]

2.3.3 การวางแผนการสื่อสาร (Communication Plan)

ขั้นตอนนี้เกี่ยวข้องกับการวางแผนในการติดต่อสื่อสารภายในองค์กร และสื่อสารออกไปยังหน่วยงานภายนอกหรือผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในกรณีที่เกิดเหตุฉุกเฉิน เพื่อให้มั่นใจว่าองค์กรสามารถตอบสนองได้อย่างรวดเร็วและเป็นระบบ โดยมีแนวทางดังนี้

กำหนดรายชื่อผู้รับผิดชอบการสื่อสารหลักและรอง (Primary and Secondary Contacts)

ระบุช่องทางการสื่อสาร (Communication Channels) ที่สามารถใช้งานได้ในสถานการณ์ฉุกเฉิน เช่น โทรศัพท์ อีเมล ระบบแจ้งเตือนอัตโนมัติ

จัดทำข้อความแจ้งเตือนและแนวทางในการสื่อสารล่วงหน้า (Pre-defined Messages) เพื่อความชัดเจนและลดความสับสนเมื่อเกิดเหตุการณ์จริง [9]

2.3.4 การวางแผนการสำรองข้อมูล (Data Backup Plan)

การสำรองข้อมูลเป็นส่วนที่สำคัญมากในการวางแผน DRP เนื่องจากข้อมูลเป็นสิ่งสำคัญในการดำเนินธุรกิจขององค์กร หากข้อมูลสูญหายหรือเสียหายจะส่งผลกระทบอย่างมากต่อการดำเนินงานขององค์กร โดยขั้นตอนในการวางแผนการสำรองข้อมูลมีแนวทางในการดำเนินการดังนี้

ระบุความสำคัญของข้อมูลที่จะต้องดำเนินการสำรองข้อมูลและกำหนดระยะเวลาในการดำเนินการสำรองข้อมูล

กำหนดแนวทางและวิธีการในการสำรองข้อมูล (Backup Technologies and Strategies) เช่น Full Backup, Incremental Backup, Snapshot, Cloud Backup หรือ Offsite Backup

กำหนดสถานที่เก็บข้อมูลสำรองและจัดการระบบสำรองข้อมูล (Backup Storage Management) ให้มีความปลอดภัยและพร้อมใช้งานเสมอเมื่อเกิดเหตุการณ์ฉุกเฉินหรือมีความจำเป็นต้องใช้งาน

2.3.5 การพัฒนาแผนกู้คืนระบบ (Recovery Procedures)

เป็นการกำหนดวิธีการในการกู้คืนระบบโครงสร้างพื้นฐานด้านไอที และบริการต่างๆ กลับสู่สภาพที่สามารถใช้งานได้ตามเป้าหมายขององค์กรโดยมีหลักการสำคัญดังต่อไปนี้

กำหนดขั้นตอนการกู้คืนระบบเครือข่ายและอุปกรณ์ที่เกี่ยวข้อง (Network and Infrastructure Restoration Procedures)

จัดหาหรือจัดเตรียมทรัพยากรที่จำเป็นในการกู้คืนระบบ เช่น อุปกรณ์สำรองข้อมูล ซอฟต์แวร์ อุปกรณ์เครือข่าย และบุคลากรที่มีทักษะ

ทำคู่มือหรือเอกสารขั้นตอน (Recovery Procedure Documentation) ที่ชัดเจน เข้าใจง่าย และสามารถนำไปใช้ได้จริงในการดำเนินการเมื่อเกิดเหตุการณ์จริง [9]

2.3.6 การทดสอบและปรับปรุงแผน (Testing and Improvement)

การทดสอบเป็นขั้นตอนสำคัญ เนื่องจากเป็นการสร้างความมั่นใจว่าแผน DRP ที่กำหนดไว้สามารถนำไปใช้งานได้จริง และควรมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อให้สามารถตอบสนองกับเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด ที่เปลี่ยนแปลงอยู่ตลอดเวลาได้อย่างมีประสิทธิภาพ โดยมีแนวทางในการดำเนินการทดสอบดังนี้

- ดำเนินการทดสอบแผน DRP อย่างสม่ำเสมอ (Periodic DRP Testing) เช่น Table-top Exercise, Simulation Test หรือ Full-interruption Test
- วิเคราะห์ผลลัพธ์จากการทดสอบเพื่อระบุช่องโหว่หรือข้อบกพร่อง (Gap Analysis) ที่จำเป็นต้องแก้ไขหรือปรับปรุง
- อัปเดตและปรับปรุงแผน DRP ให้มีความทันสมัยและตอบสนองต่อภัยคุกคามหรือสถานการณ์ที่เปลี่ยนแปลงอยู่ตลอดเวลา (Continuous Improvement)

2.4 RTO และ RPO คืออะไร

2.4.1 RTO คือระยะเวลาสูงสุดที่องค์กรสามารถยอมรับได้

ในการที่ระบบ แอปพลิเคชัน หรือกระบวนการทางธุรกิจสามารถหยุดทำงานได้หลังจากเกิดเหตุการณ์ภัยพิบัติ โดยไม่ก่อให้เกิดความเสียหายที่รุนแรงต่อองค์กรหรือธุรกิจ กล่าวคือ เวลาที่องค์กรตั้งเป้าหมายในการกู้คืนระบบให้กลับมาทำงานได้ตามปกติหลังจากเกิดเหตุขัดข้องนั้นเอง

2.4.2 RPO คือ ระยะเวลาย้อนหลังล่าสุดที่องค์กรสามารถยอมรับได้

ในการสูญเสียข้อมูลความสัมพันธ์ระหว่าง RTO และ RPO ซึ่งมีความสัมพันธ์กันอย่างใกล้ชิดแต่มุ่งเน้นคนละด้านของการกู้คืนระบบ RTO มุ่งเน้นที่ “เวลา” ในการกู้คืนระบบโดยเป้าหมายอยู่ที่การกลับมาให้ บริการ โครงสร้างพื้นฐาน และกระบวนการทำงาน ในส่วนของ RPO มุ่งเน้นที่ “ข้อมูล” ที่ยอมให้สูญเสียโดยเป้าหมายอยู่ที่การสำรองและกู้คืนข้อมูล ทั้งสองค่าต้องพิจารณาร่วมกันในการออกแบบระบบ Disaster Recovery เพราะการมี RTO ที่ต่ำมาก (กู้คืนเร็ว) แต่ RPO สูง (ข้อมูลหายมาก) อาจไม่มีประโยชน์หากข้อมูลที่กู้คืนได้เก่าเกินไปจนไม่สามารถใช้งานได้อย่างมีประสิทธิภาพ

2.4.3 ปัจจัยที่ควรคำนึงถึงการกำหนด RTO และ RPO

1. ความสำคัญทางธุรกิจ (Business Criticality)

ระบบที่มีความสำคัญสูงต่อการดำเนินธุรกิจ เช่น ระบบการทำธุรกรรมการเงิน ระบบ e-commerce หรือระบบที่ให้บริการลูกค้าโดยตรง มักต้องการ RTO และ RPO ที่ต่ำ เพราะการหยุดชะงักส่งผลกระทบโดยตรงต่อรายได้และความพึงพอใจของลูกค้า

2. ผลกระทบทางการเงิน (Financial Impact)

องค์กรต้องคำนึงถึงต้นทุนความเสียหายจากการหยุดให้บริการ (Downtime Cost) เทียบกับต้นทุนในการลงทุนระบบ DR ที่ซับซ้อน ระบบที่มี downtime cost สูงจะคุ้มค่าที่จะลงทุนในโซลูชันที่มี RTO/RPO ต่ำ

3. ข้อกำหนดทางกฎหมายและมาตรฐาน (Regulatory Requirements)

หลายอุตสาหกรรมมีข้อกำหนดทางกฎหมายเกี่ยวกับการเก็บรักษาและกู้คืนข้อมูล เช่น ธนาคารต้องปฏิบัติตามข้อกำหนดของธนาคารแห่งประเทศไทย หรือองค์กรที่เก็บข้อมูลส่วนบุคคลต้องปฏิบัติตาม PDPA

4. ลักษณะของข้อมูลและการทำงาน

ข้อมูลที่มีการเปลี่ยนแปลงบ่อยมีความต้องการ RPO ต่ำเพื่อลดการสูญเสียข้อมูลระบบที่ทำงานแบบ Real-time ต้องการทั้ง RTO และ RPO ที่ต่ำมากระบบ Batch Processing อาจยอมรับ RTO/ RPO ที่สูงกว่าได้

5. งบประมาณและทรัพยากร

เพื่อให้ได้ผลลัพธ์ของ RTO และ RPO ที่ต่ำต้องใช้เทคโนโลยีที่ซับซ้อนและมีราคาสูง เช่น

- RPO ใกล้ศูนย์ ต้องใช้ Synchronous Replication ซึ่งต้องการ Bandwidth สูงและ Latency ต่ำ
- RTO ต่ำ ต้องมี Hot Standby Site พร้อมระบบ Automatic Failover

6. เทคโนโลยีและวิธีการเพื่อให้ได้ RTO และ RPO ที่ต้องการ

2.4.4 Backup Technologies

- Full Backup คือการสำรองข้อมูลทั้งหมด เหมาะกับ RPO 24 ชั่วโมงขึ้นไป
- Incremental Backup เป็นการสำรองเฉพาะข้อมูลที่เปลี่ยนแปลง ช่วยลดเวลาและพื้นที่จัดเก็บ
- Continuous Data Protection (CDP) เป็นการบันทึกการเปลี่ยนแปลงทุกครั้ง สามารถกู้คืนไปยังจุดเวลาใดก็ได้

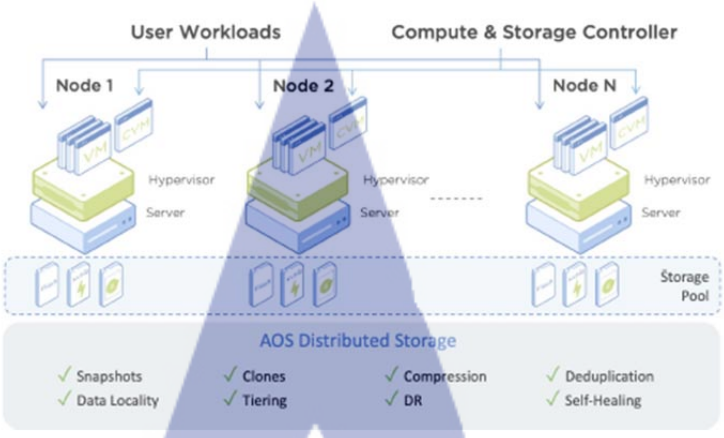
2.4.5 Replication Technologies

- Asynchronous Replication เป็นการส่งข้อมูลไปยัง Site สำรองแบบไม่ Real-time เหมาะกับ RPO หลายนาทีถึงชั่วโมง
- Synchronous Replication เป็นการส่งข้อมูลแบบ Real-time ทำให้ RPO เกือบเป็นศูนย์ แต่ต้องการ network ที่มีประสิทธิภาพสูง
- Semi-Synchronous Replication เป็นการผสมผสานข้อดีของทั้งสองแบบ

2.5 แนวคิดของระบบ Hyper-Converged Infrastructure (HCI)

HCI เป็นโครงสร้างพื้นฐานศูนย์ข้อมูลที่รวมเอา Compute (CPU/RAM) Storage (SDS) Virtualization Management ไว้ใน Cluster เซิร์ฟเวอร์ เดียวกัน แล้วบริหารทุกอย่างด้วยซอฟต์แวร์ (Software-Defined) ผ่านคอนโซลเดียว

สิ่งสำคัญคือ Software-Defined Storage (SDS) ที่กระจายข้อมูลข้ามโหนดในคลัสเตอร์ และ Policy-Based Management ซึ่งจะเป็นสิ่งที่กำหนดนโยบายครั้งเดียว ระบบจัดสรร ป้องกัน ปรับสมดุลให้เองอัตโนมัติ และยังสามารถขยายแบบ Scale-out คือเพิ่มทีละโหนดโดยสามารถเพิ่มขนาดของ CPU RAM Storage ขึ้นเป็นเส้นตรง ทำให้มีความยืดหยุ่น ลดงานดูแลเทียบกับสถาปัตยกรรม 3-Tier เดิม (Server + SAN + Fabric) [10]



รูปที่ 2.1 สถาปัตยกรรมของ Nutanix

ตามรูปที่ 2.1 Nutanix ทำให้แต่ละ Node ทั้ง Server และ Storage รวมกันกลายเป็นหนึ่งเดียวที่ เร็วกว่า SAN, ยืดหยุ่นกว่า และปลอดภัยกว่า

ตารางที่ 2.1 รูปแบบของสถาปัตยกรรม

รูปแบบ	**แนวคิด**	**จุดเด่น**	**ข้อจำกัด**
Traditional 3-Tier (Server + SAN/NAS + Network)	อุปกรณ์เฉพาะแยกกันบริหารจัดการ	ยืดหยุ่นในระดับเอ็นเตอร์ไพรส์	ดูแลหลายระบบซับซ้อน ขยายยาก
Hyper-Converged (HCI)	รวมทุกฟังก์ชันในโหนดเดียวและ Scale-out	จัดการหน้าจอเดียว ขยายทีละโหนด ทำงานอัตโนมัติ	บางกรณี “สเกลไม่พอดี” ระหว่างคอมพิวต์กับสตอเรจ

จากตารางที่ 2.1 เป็นการเปรียบเทียบระหว่าง Traditional 3-Tier Architecture (Server + SAN/NAS + Network) และ Hyper-Converged Infrastructure (HCI)

2.6 องค์ประกอบหลักของ Nutanix

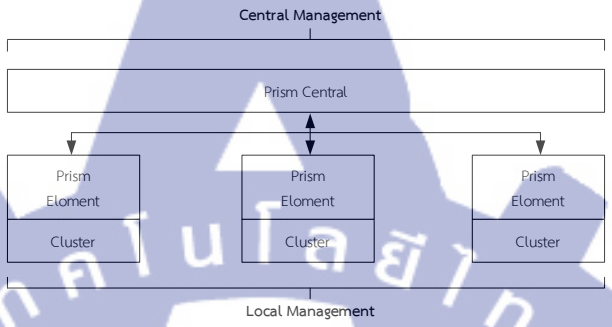
2.6.1 AOS (Acropolis Operating System) เป็นระบบ Software-Defined Storage ที่กระจายข้อมูลข้ามโหนด

2.6.2 AHV (Acropolis Hypervisor) เป็น Hypervisor แบบ KVM-based ของ Nutanix สามารถใช้งานได้แบบ ฟรีลิขสิทธิ์ ใช้ง่าย ทำงานร่วมกับ Prism

2.6.3 Prism คือ Web-based Management Console สำหรับ Nutanix HCI โดยจะแบ่งเป็น

• Prism Element (PE) ทำหน้าที่ บริหารจัดการในแต่ละ Cluster ใช้ดูสถานะ Cluster, Node, VM, Storage, Alert สร้างและแก้ไข Container, Network, VM

• Prism Central (PC) ทำหน้าที่บริหาร หลาย Cluster ในที่เดียวกัน



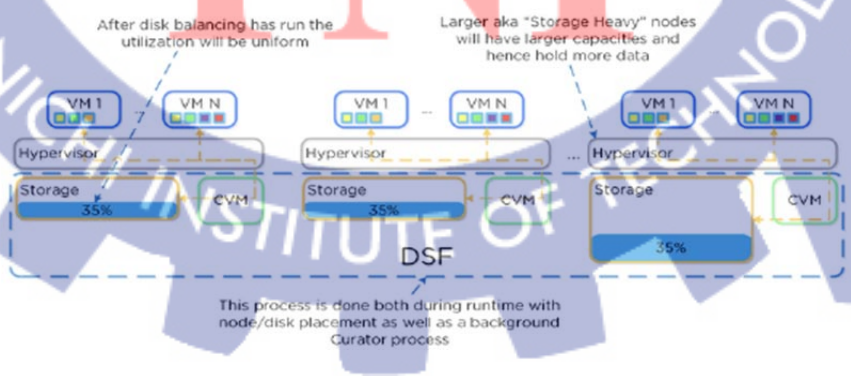
รูปที่ 2.2 รูปแบบการทำงานของ Prism

จากรูปที่ 2.2 เป็นสถาปัตยกรรมการจัดการของ Nutanix ผ่าน Prism ซึ่งแบ่งออกเป็น 2 ระดับหลักๆ คือ Local Management แต่ละ Cluster มี Prism Element เป็นตัวควบคุม แต่ละ Cluster ของตัวเอง และ Central Management Prism Central รวมทุก Cluster บริหารจัดการให้อยู่ที่เดียวกัน

2.6.4 Nutanix DSF (Distributed Storage Fabric) เป็น Layer ของ Storage แบบกระจาย รองรับ VM, Files, Objects, Volumes

2.6.5 LCM (Life-Cycle Manager) เป็นส่วนที่ใช้ อัปเดตซอฟต์แวร์ firmware และ Driver

2.7 Distributed Storage (DSF)



รูปที่ 2.3 Nutanix DSF

จากรูปที่ 2.3 แสดงระบบกระจายไฟล์เพื่อปกป้องข้อมูลเพิ่มประสิทธิภาพทำให้ VM เหมือนมี SAN ที่มีประสิทธิภาพสูงและสามารถขยายได้ง่าย โดยไม่ต้องซื้อ SAN จริง โดยมีความสามารถดังนี้ [11]

2.7.1 vDisk, Extent, Extent Group

vDisk คือ ดิสก์เสมือนของ VM (.vmdk)

Extent คือ ชิ้นข้อมูลขนาดเล็ก (1MB) ของ vDisk

Extent Group คือ การรวม Extent หลายอันเข้าด้วยกัน เพื่อกระจายและทำ Replication ข้ามโหนด [11]

2.7.2 Replication Factor (RF2/RF3) มีจุดประสงค์เพื่อในกรณีที่โหนดหรือดิสก์เสียจะรีบิลด์ Extent ที่ขาดหายไปอัตโนมัติ

RF2 เป็นการทำสำเนา 2 ชุด ข้ามโหนดอย่างน้อย 2 ตัว

RF3 เป็นการทำสำเนา 3 ชุด ซึ่งเหมาะ Cluster ที่มีจำนวนโหนดมากกว่า 4 โหนด และ Workload ที่ Critical [12]

2.7.3 Data Locality เป็นหนึ่งในจุดแข็งที่สุดของ Nutanix DSF และเป็นเหตุผลสำคัญที่ HCI ของ Nutanix ทำงานได้เร็วและเสถียร โดยทำให้ข้อมูลอยู่ใกล้ VM ที่ใช้งานมากที่สุดเมื่อ VM รันอยู่บนโหนดใด Nutanix จะพยายามให้สำเนาหลัก (Primary Copy) ของข้อมูล vDisk อยู่บนโหนดนั้นซึ่งมีผลทำให้ การอ่าน (Read I/O) มี Latency ต่ำลดการใช้ Network ระหว่างโหนด [12]

2.7.4 การเขียนข้อมูล (Write I/O Path) VM เขียนข้อมูล เข้าสู่ Operation Log บน SSD หรือ NVMe ของโหนด ข้อมูลจะ Replicate ตาม RF เมื่อข้อมูลยืนยันเขียนครบทุกชุดแล้ว VM ได้ ACK ว่า Write Complete Operation Log จะ Drain ข้อมูลลง Capacity Tier (SSD/HDD) ทำให้ เขียนเร็ว เพราะ Commit บน SSD และ ปลอดภัย เพราะมีการทำสำเนา

2.7.5 การอ่านข้อมูล (Read I/O Path) ในกรณีที่มีสำเนาอยู่บนโหนดเดียวกันสามารถอ่านจาก local SSD Cacheทำให้สามารถอ่านข้อมูลได้เร็วมาก แต่ในกรณีที่ ถ้าไม่มีสำเนาอยู่สามารถดึงข้อมูลจากโหนดอื่นในคลัสเตอร์ทำให้ Latency สูงขึ้นเล็กน้อย แต่ยังเร็วกว่า SAN [12]

2.7.6 Data Services เป็น ความสามารถที่ซอฟต์แวร์ทำให้กับข้อมูลใน Cluster โดย เน้น 3 เรื่องหลักประสิทธิภาพ (Performance), ประหยัดพื้นที่ (Efficiency), ความปลอดภัย (Protection) โดยมีฟีเจอร์สำคัญๆ [12]

- Compression คือ การบีบอัดข้อมูลเพื่อลดพื้นที่ในการเก็บข้อมูล
- Deduplication คือ การลดการเก็บข้อมูลซ้ำ
- Erasure Coding (EC-X) คือ การแทนที่จะเก็บสำเนาเต็ม 2 ชุด (RF2) โดย ใช้ Parity และ Data Striping ทำงานคล้าย RAID-5/6
- Snapshots & Clones

Snapshots คือการ สร้าง Point-in-Time Copy ของ vDisk, VM, Volume ใช้ Space-Efficient เก็บเฉพาะ Metadata + Changed Blocks Clones คือ การทำสำเนา VM/Disk จาก Snapshot แบบทันที (Zero-Copy) เหมาะสำหรับ Dev/Test, Training Lab

• Data Protection & Replication

Protection Domain คือ การกำหนดชุด VM/Volume ที่ต้อง Snapshot และ Replicate พร้อมกัน

• Async Replication เป็นการ ส่ง Snapshot ไปยัง Remote Cluster ตาม RPO ที่กำหนด

• Metro Availability (Sync) เป็นการ เขียนข้อมูลสองไซต์พร้อมๆ กัน (RPO = 0)

• Cloud Connect คือการส่ง Snapshot ขึ้น Public Cloud (AWS หรือ Azure) เป็น DR tier

• Encryption at Rest คือการปกป้องข้อมูลที่ “ถูกเก็บไว้” บนดิสก์ โดย Native Software Encryption Nutanix จะ เข้ารหัสข้อมูลทุกครั้งที่เขียนและ Commit ลงดิสก์ ซึ่งทำในระดับซอฟต์แวร์ของ DSF โดยที่ VM/แอป ไม่ต้องทำอะไรเพิ่มโดยที่ดิสก์ หากถูกถอดออกไปจะไม่สามารถเข้าถึงข้อมูลดังกล่าวได้เนื่องจากถูกเข้ารหัสไว้

• Data Tiering เป็นฟีเจอร์ของ Nutanix DSF ที่ช่วยให้ใช้ Storage คุ้มค่าและได้ประสิทธิภาพสูงโดยการจัดข้อมูลให้อยู่ “ชั้นที่เหมาะสม” โดยอัตโนมัติโดย Hot Data จะถูกเก็บอยู่บน SSD ทำให้สามารถใช้งานข้อมูลได้เร็ว และ Cold Data จะถูกเก็บอยู่บน HDD ซึ่ง ประหยัด ทำให้ทั้งเร็วและคุ้มค่าในเวลาเดียวกัน

2.8 Virtualization & Networking

Virtualization เป็นการ “จำลอง” ฮาร์ดแวร์ให้รัน หลาย VM หรือContainer บนเครื่องจริงเครื่องเดียว โดยมีองค์ประกอบหลัก คือ Hypervisor (เช่น KVM/ESXi/Hyper-V) ทำหน้าที่ในการจัดสรรทรัพยากร (CPU, RAM, Storage) ให้แต่ละ VM โดยมี Feature ที่สำคัญคือ HA (โหนดล่มแล้ว VM ย้ายอัตโนมัติ), Live Migration, Snapshot/Clone, Resource Scheduling (NUMA/CPU Pinning) [13] Virtual Networking ในโฮสต์จะมี vSwitch ทำหน้าที่เหมือนสวิตช์จริง แต่เป็นซอฟต์แวร์โดยมีแนวทางมาตรฐาน คือ VLAN (802.1Q) แบ่งเครือข่าย (Segmentation) NIC Bonding หรือ LACP เพิ่ม Availability และแบนด์วิดท์ แยกความปลอดภัยระดับ VM [13]

2.8.1 AHV (Acropolis Hypervisor) เป็น Hypervisor ของ Nutanix โดยมีพื้นฐานมาจาก KVM ซึ่งติดมาพร้อมระบบ ไม่ต้องซื้อ licenses เพิ่มโดยมีจุดเด่น ใช้ง่ายผ่าน Prism HA & Live Migration Affinity และ Anti-Affinity และ รักษา Data Locality Resource Scheduling เข้าใจ NUMA, CPU Pinning

2.8.2 Open vSwitch (OVS) เป็น Network ที่ทำงานบน AHV ทำหน้าที่เป็น vSwitch ระดับเคอร์เนลช่วยทำให้ได้ประสิทธิภาพที่ดี รองรับ VLAN, LACP), MTU/Jumbo, QoS, และ IPAM

2.9 Data Protection & DR Nutanix

มีความสามารถในการทำ Snapshot, Replication, และ Orchestration เพื่อให้ได้การปกป้องข้อมูลที่ครอบคลุมทั้งในไซต์เดียว ข้ามไซต์ และการเก็บรักษาข้อมูลในระยะยาว ช่วยลดเวลาที่ระบบไม่สามารถให้บริการได้ (RTO) และระยะเวลาในการสูญเสียข้อมูล (RPO) ให้เป็นไปตามที่กำหนดได้ [13]

2.10 การทดสอบและปรับปรุงแผน DRP

การทดสอบและปรับปรุงแผนการกู้คืนระบบ (DRP Testing & Improvement) เป็นกระบวนการสำคัญที่ทำให้องค์กรมั่นใจได้ว่าแผนการกู้คืนระบบที่จัดทำไว้สามารถปฏิบัติได้จริงภายใต้สถานการณ์วิกฤต กระบวนการนี้ไม่เพียงแต่เป็นการพิสูจน์สมมติฐานในแผน (Plan Validation) แต่ยังเป็นการค้นหาช่องโหว่ ข้อจำกัด และปัจจัยที่ต้องปรับปรุง เพื่อเพิ่มความพร้อมและความยืดหยุ่นของระบบสารสนเทศ (System Resilience) ให้สามารถรองรับกับสถานการณ์ภัยพิบัติได้ โดยมีวัตถุประสงค์ ดังต่อไปนี้

2.10.1 ตรวจสอบว่าสามารถกู้คืนระบบภายในระยะเวลาที่กำหนด (Recovery Time Objective) และระยะเวลาในการสูญเสียข้อมูลให้อยู่ในขอบเขตที่สามารถยอมรับได้ (Recovery Point Objective)

2.10.2 ทดสอบบทบาทและความเข้าใจของทีมปฏิบัติการ (IT Operations, Business Continuity Team)

2.10.3 พิสูจน์การทำงานของระบบสำรอง (Backup), ระบบจำลอง (Replication), เครือข่าย DR ว่าสามารถใช้งานได้จริงเมื่อเกิดเหตุภัยพิบัติ

2.10.4 หาข้อจำกัดเพื่อปรับปรุงแผนและลดความเสี่ยงในอนาคต

ตารางที่ 2.2 ตารางเปรียบเทียบงานวิจัยที่เกี่ยวข้อง

ลำดับ	ผู้วิจัย/ปี	หัวข้องานวิจัย	เทคโนโลยีหรือแนวทางที่ใช้	ตัวชี้วัด (RTO/RPO/Data)	ข้อค้นพบหลัก	ข้อจำกัด/ช่องว่าง (Research Gap)
1	R. Basa [1]	Cloud-Based DR System for SMEs	Cloud DR (AWS Backup, Azure Site Recovery)	RTO, Cost	สามารถลดค่าใช้จ่ายด้าน DR ได้ประมาณ 30% แต่พบว่า Latency สูงในกรณี Failover	ขาดการพิจารณา DR บน HCI สำหรับ Onsite Environment

ตารางที่ 2.2 ตารางเปรียบเทียบงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้วิจัย/ปี	หัวข้องานวิจัย	เทคโนโลยีหรือแนวทางที่ใช้	ตัวชี้วัด (RTO/RPO/Data)	ข้อค้นพบหลัก	ข้อจำกัด/ช่องว่าง (Research Gap)
2	K. Elgdamsi and M. Embarak [14]	Implementing a DR Solution Using VMware SRM	VMware SRM, Virtualization	Downtime, DR Validation	SRM สามารถลด Downtime และทดสอบ DR แบบไม่กระทบ Production	ไม่ได้วิเคราะห์เปรียบเทียบกับ HCI-Based DR และไม่มี Cost Analysis
3	D. M. Kesa [7]	Ensuring Resilience : Integrating IT Disaster Recovery Planning and Business Continuity for Sustainable Information Technology Operations	DR Planning Framework, Replication, Virtualization	RTO, RPO (Conceptual Level)	เสนอกรอบการบูรณาการ IT Disaster Recovery กับ Business Continuity เพื่อเพิ่ม Resilience ขององค์กร	ไม่มีการทดลองเชิงปฏิบัติและไม่มีการวัดค่า RTO/RPO เชิงปริมาณ รวมถึงไม่ได้ประเมิน HCI-based DR
4	P. A. Damayantha [15]	Data Protection for Critical Applications	Distributed Storage + Local Replication	Data Integrity	เพิ่ม Reliability ของ Storage	ไม่เปรียบเทียบกับ DRP เดิม
5	G. S. Atencio and M. U. Ramírez [10]	Evolution and Trends of Hyperconvergence in Telco Sector	HCI, Hypervisor, Bare-metal, SDDC	Performance, CapEx/OpEx	วิเคราะห์แนวโน้ม HCI และเปรียบเทียบ Hypervisor vs Bare-metal ในภาค Telco	ไม่มีการทดลอง DR เชิงปริมาณ และไม่มี RTO/RPO Measurement

จากตารางที่ 2.2 งานวิจัยที่เกี่ยวข้องส่วนใหญ่ให้ความสำคัญกับการพัฒนาและประเมินประสิทธิภาพของแผนการกู้คืนจากเหตุฉุกเฉิน DRP ภายใต้สภาพแวดล้อมการใช้งานของเทคโนโลยีสมัยใหม่ โดยมุ่งเน้นไปที่การลดเวลาในการกู้คืนระบบ RTO และการเพิ่มความสามารถในการปกป้องข้อมูลเป็นหลัก งานวิจัยของ R. Basa [1] ให้ความสำคัญกับการใช้ Cloud-Based Disaster Recovery สำหรับองค์กรขนาดเล็กและขนาดกลาง (SMEs) โดยเน้นประเด็นด้านต้นทุนและความยืดหยุ่นของระบบ Cloud อย่างไรก็ตาม งานวิจัยดังกล่าวยังขาดการพิจารณาความเหมาะสมของการใช้งาน DRP ในสภาพแวดล้อมแบบ On-Site ซึ่งยังคงเป็นรูปแบบที่พบได้ทั่วไปในองค์กรภายในประเทศ

ในขณะที่ K. Elgdamsi and M. Embarak [14] มุ่งเน้นการออกแบบระบบ Hybrid Disaster Recovery สำหรับศูนย์ข้อมูลแบบ Virtualized โดยใช้ VMware Site Recovery Manager (SRM) ร่วมกับ Offsite Backup ซึ่งสามารถทำ Failover ได้แบบอัตโนมัติและลดค่า RTO และ RPO ได้อย่างมี

ประสิทธิภาพ แต่มีข้อจำกัดด้านต้นทุนลิขสิทธิ์และยังไม่มีการทดสอบในสภาพแวดล้อมขององค์กรขนาดเล็กและขนาดกลาง รวมถึงไม่ได้ศึกษาการใช้งานบนแพลตฟอร์ม Hyper-Converged Infrastructure (HCI)

งานวิจัยของ D. M. Kesa [7] เป็นหนึ่งในงานที่เริ่มนำแนวคิด HCI มาใช้ในการสร้างความต่อเนื่องทางธุรกิจ โดยใช้สถาปัตยกรรม Nutanix HCI ร่วมกับ Snapshot และ Replication ซึ่งสามารถลดระยะเวลาหยุดชะงักของระบบได้อย่างมีนัยสำคัญ อย่างไรก็ตาม งานวิจัยดังกล่าวยังขาดการวิเคราะห์ในมิติด้านความคุ้มค่าเชิงต้นทุน (Cost-effectiveness) และไม่ได้ทำการเปรียบเทียบโดยตรงกับแผน DRP แบบดั้งเดิม ทำให้ยังไม่สามารถสรุปความเหมาะสมของ HCI ในบริบทขององค์กรขนาดเล็กและขนาดกลางได้อย่างชัดเจน

นอกจากนี้ P. A. Damayantha [15] มุ่งเน้นการศึกษาเทคโนโลยีด้านการปกป้องข้อมูลและความถูกต้องของข้อมูล (Data Integrity) ผ่านการใช้ Distributed Storage และ Local Replication ซึ่งช่วยเพิ่มความน่าเชื่อถือของระบบจัดเก็บข้อมูล แต่ก็ไม่ได้ให้ความสำคัญกับกระบวนการกู้คืนระบบโดยรวม และไม่มีการเชื่อมโยงผลการศึกษากับการออกแบบแผน DRP หรือการเปรียบเทียบกับแนวทางการกู้คืนแบบเดิม

จากการสรุปงานวิจัยที่เกี่ยวข้อง พบว่ายังไม่มีการศึกษาการเปรียบเทียบระหว่าง DRP แบบดั้งเดิมกับ DRP บนสถาปัตยกรรม HCI (Nutanix) ในองค์กรขนาดกลางของไทย ซึ่งเป็นช่องว่างที่งานวิจัยนี้ต้องการเพิ่มเติม โดยงานวิจัยก่อนหน้านี้ส่วนใหญ่ มุ่งเน้นการพัฒนาเทคโนโลยีหรือโซลูชันเฉพาะด้าน โดยยังขาดการศึกษาเชิงเปรียบเทียบอย่างเป็นระบบระหว่างแผนการกู้คืนจากเหตุฉุกเฉินแบบดั้งเดิมกับแผน DRP ที่พัฒนาบนสถาปัตยกรรม Hyper-Converged Infrastructure โดยเฉพาะในบริบทของศูนย์ข้อมูลขนาดเล็กและขนาดกลาง ดังนั้น งานวิจัยนี้จึงมีความแตกต่างจากงานวิจัยก่อนหน้า โดยมุ่งเน้นการออกแบบ ทดสอบ และประเมินประสิทธิภาพของแผนการกู้คืนจากเหตุฉุกเฉินบนสถาปัตยกรรม HCI (กรณีศึกษา Nutanix) โดยเปรียบเทียบผลลัพธ์กับแผน DRP แบบเดิมในส่วนของค่า RTO, ค่า RPO ความต่อเนื่องในการให้บริการ และการนำไปใช้งานจริงในองค์กรขนาดกลางและขนาดเล็ก

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยทดลองเชิงเปรียบเทียบ (Comparative Experiment) โดยเปรียบเทียบประสิทธิภาพของแผน DRP แบบดั้งเดิมกับแผน DRP บนสถาปัตยกรรม HCI ภายใต้สถานการณ์จำลองที่ควบคุมได้ในศูนย์ข้อมูลขนาดเล็ก-ขนาดกลางโดยจำลองเหตุการณ์ฉุกเฉินที่ใกล้เคียงของจริง เช่น การปิดระบบเซิร์ฟเวอร์, ความล้มเหลวของโหนด, และการถูกโจมตีด้วยมัลแวร์ โดยวัดผลจากตัวชี้วัดหลักคือ

- RTO เวลากู้คืนระบบ
- RPO เวลาการสูญเสียข้อมูล (นาที)
- ความถูกต้องของข้อมูล (Data Integrity)
- ความต่อเนื่องของบริการ (Service Continuity)

3.1 สร้างและทดสอบแผนการกู้คืนหลังเกิดภัยพิบัติ

การสร้างและทดสอบแผนการกู้คืนหลังเกิดเหตุฉุกเฉินเพื่อให้แน่ใจว่าข้อมูลและระบบสารสนเทศสามารถเรียกคืนได้สำเร็จในกรณีที่เกิดเหตุการณ์ไม่คาดคิด ไม่ว่าจะเป็นภัยธรรมชาติ, การโจมตีทางไซเบอร์, หรือความล้มเหลวของระบบ โดยทั่วไป ทฤษฎีและหลักการเหล่านี้อาจรวมถึง การวิเคราะห์ความเสี่ยงและการประเมินผลกระทบต่อธุรกิจ ได้จากการวิเคราะห์เพื่อระบุภัยคุกคามที่อาจเกิดขึ้นและประเมินว่าภัยพิบัติเหล่านั้นจะมีผลกระทบต่อการดำเนินงานขององค์กรอย่างไร ซึ่งช่วยให้สามารถกำหนดระดับความสำคัญของระบบและข้อมูลต่างๆ ได้จาก

ตารางที่ 3.1 โอกาสของสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น [9]

Cause	Organizations
System Upgrades	72%
Power Outage/Failure/Issues	70%
Fire	69%
Configuration Management	64%
Cyber Attacks	63%
Malicious Employees	63%

ตารางที่ 3.1 โอกาสของสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น (ต่อ) [9]

Cause	Organizations
Data Leakage/Loss	63%
Flood	48%
Hurricane	47%
Earthquake	46%
Tornado	46%
Terrorism	45%
Tsunami	44%
Volcano	42%
War	42%
Others	1%

จากตารางที่ 3.1 แสดงถึงข้อมูลโอกาสของสาเหตุ ที่ทำให้องค์กรต้องเผชิญกับปัญหาหรือเหตุที่ทำให้ได้รับผลกระทบทำให้ไม่สามารถใช้งานได้

สภาพแวดล้อมการทดลอง ใช้ Cluster HCI ของ Nutanix อย่างน้อย 3 โหนดและระบบปฏิบัติการ Windows Server สำหรับ Application พร้อมเชื่อมต่อเครือข่าย DR Site เพื่อรองรับการทำ Replication และ Snapshot

3.2 รายละเอียดกรณีศึกษา

จำนวน Virtual Machine (VM)

บริษัทมีการใช้ Nutanix Cluster (Primary Site) จำนวน 5 Node และ DR Site จำนวน 3 Node โดยรวมแล้วมี VM ดังนี้

- Production VM จำนวน 118 เครื่อง
- DR/Backup VM จำนวน 20 เครื่อง (Replicate มาจาก Production)
- รวมทั้งหมด 130 VM

ประเภท Application Server และ Database Server ระบบถูกแบ่งออกตามลักษณะการทำงานของธุรกิจ เช่น

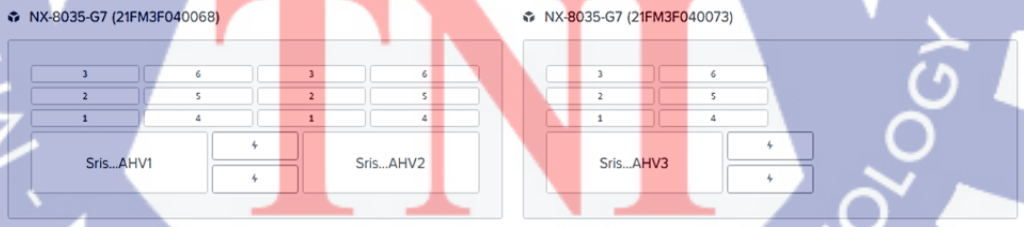
- Application Server
  - Web Server
  - API Server
- Database Server
  - Microsoft SQL Server

Topology ของ DR Site และ Network

- Primary Site: ตั้งอยู่ที่DC ใช้ Nutanix NX-8035-G7 จำนวน 3 เครื่อง และ NX-8035-G8 จำนวน 2 เครื่อง (1 Cluster) ดังรูปที่ 3.1

รูปที่ 3.1 จำนวน Nutanix Server ที่ DC

- DR Site ตั้งอยู่ที่ศูนย์ Data Center ภายนอก (Colocation) ใช้ Nutanix NX-8035-G7 จำนวน 3 เครื่อง (1 Cluster) ดังรูปที่ 3.2



รูปที่ 3.2 จำนวน Nutanix Server ที่ DR

การเชื่อมโยงเครือข่าย (Network Topology)

- Primary และ DR Site เชื่อมต่อผ่าน MPLS
- Bandwidth: 100 Mbps

3.3 ขั้นตอนการทดลอง

3.3.1 ก่อนทดสอบ

• ตรวจสอบสถานะระบบสำรอง

• ตรวจสอบความสมบูรณ์ของ Snapshot และการเชื่อมต่อเครือข่ายระหว่าง Data Center Site และ DR Site

3.3.2 ระหว่างทดสอบ

• จำลองเหตุการณ์ (Shutdown/Failover)

• ดำเนินการกู้คืนตามแผน

• ทดสอบความพร้อมใช้งานของระบบด้วยการทดสอบระบบ (Test/UAT)

• การวัดค่า RTO โดยการตรวจสอบช่วงเวลาตั้งแต่เริ่มเกิดเหตุการณ์จำลองการทดสอบจนถึงเวลาที่ระบบกลับมาอยู่ในสถานะพร้อมใช้งาน เพื่อคำนวณค่า RTO

• การวัดค่า RPO โดยการตรวจสอบช่วงเวลาของ Snapshot และข้อมูลสำรองล่าสุด เพื่อคำนวณค่า RPO

การใช้ Snapshot และข้อมูลสำรองล่าสุดเป็นพื้นฐานในการคำนวณค่า RPO จำเป็นต้องกำหนดช่วงเวลาการทำ Snapshot ให้เหมาะสมกับบริบทของแต่ละองค์กร ในการทดสอบครั้งนี้ได้กำหนดให้ระบบทำ Snapshot ทุก 1 ชั่วโมง ซึ่งเป็นช่วงเวลาที่อยู่ในระดับสมดุลระหว่าง การลดความสูญเสียของข้อมูล และ ภาระที่เกิดขึ้นกับระบบจัดเก็บข้อมูล

การตั้งค่าช่วงเวลา Snapshot ที่ถี่เกินไปอาจทำให้ระบบเกิดภาระการประมวลผลเพิ่มขึ้น ส่งผลต่อประสิทธิภาพของระบบโดยรวม ขณะที่การตั้งช่วงเวลาห่างเกินไปอาจทำให้ปริมาณข้อมูลที่สูญหายจากเหตุฉุกเฉินมากเกินกว่าที่ธุรกิจสามารถยอมรับได้ ดังนั้น การเลือกตั้งค่า Snapshot ทุก 1 ชั่วโมง จึงถือเป็นช่วงเวลาที่เหมาะสมสำหรับการประเมินประสิทธิภาพของแผน DRP ภายใต้ข้อจำกัดด้านทรัพยากรที่ใกล้เคียงกับสภาพแวดล้อมจริงขององค์กรขนาดเล็กและขนาดกลาง

3.3.3 หลังทดสอบ

• บันทึกเวลาและผลลัพธ์

• เก็บหลักฐาน เช่น Log, Screenshot

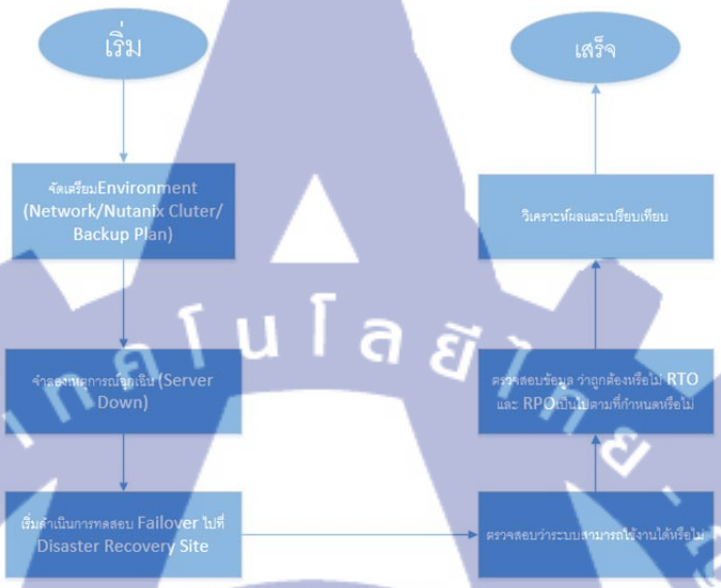
3.4 การเก็บและวิเคราะห์ข้อมูล

3.4.1 บันทึกเวลาการเริ่มเหตุการณ์-เวลาระบบพร้อมใช้งาน เพื่อคำนวณ RTO

3.4.2 ตรวจสอบจุดกู้คืน (Snapshot/Backup) เพื่อคำนวณ RPO

3.4.3 ตรวจสอบความถูกต้องของข้อมูลด้วย Checksum/DBCC

3.4.4 วิเคราะห์เปรียบเทียบค่าเฉลี่ย RTO/RPO ระหว่างสองสถาปัตยกรรม และสรุปผลในตาราง



รูปที่ 3.3 Workflow ในการดำเนินการ

3.5 การกำหนดค่า RTO และ RPO

ในการกำหนดค่า RTO จำเป็นต้องพิจารณาระยะเวลาสูงสุดที่ระบบสามารถหยุดทำงานได้โดยไม่ส่งผลกระทบต่อธุรกิจเกินกว่าระดับที่องค์กรยอมรับได้ ส่วนค่า RPO คือปริมาณข้อมูลย้อนหลังสูงสุดที่สามารถยอมให้สูญหายได้เมื่อเกิดเหตุฉุกเฉิน การกำหนดค่า RTO และ RPO จึงต้องพิจารณาร่วมกับความสามารถของระบบ ทรัพยากรที่ต้องใช้ และต้นทุนที่เกี่ยวข้อง เนื่องจากการตั้งค่าที่เข้มงวดมากขึ้นมักต้องใช้ระบบที่มีประสิทธิภาพสูงขึ้นและมีค่าใช้จ่ายเพิ่มขึ้นตามลำดับ

สำหรับการทดลองในงานวิจัยนี้ ได้กำหนดช่วงเวลา Snapshot ตามลักษณะการทำงานของเซิร์ฟเวอร์แต่ละประเภท ได้แก่

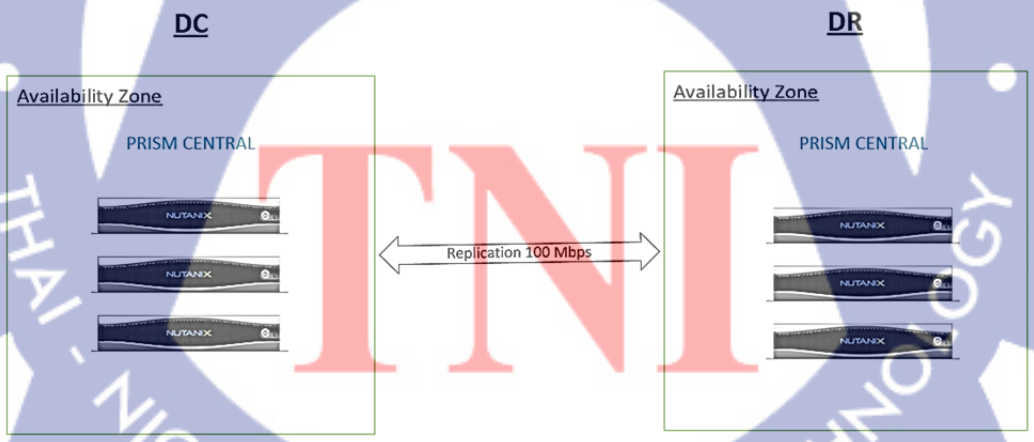
3.5.1 เซิร์ฟเวอร์ประเภท Application กำหนด RPO ไว้ทุก 6 ชั่วโมง เนื่องจากมีการเปลี่ยนแปลงข้อมูลไม่บ่อย และผลกระทบจากข้อมูลสูญหายมีความสำคัญในระดับปานกลาง

3.5.2 เซิร์ฟเวอร์ประเภท Database กำหนด RPO ไว้ทุก 1 ชั่วโมง เนื่องจากมีการอัปเดตข้อมูลบ่อยกว่าและข้อมูลมีความสำคัญต่อธุรกิจสูงกว่า จึงต้องลดความเสี่ยงของข้อมูลสูญหายให้น้อยที่สุด

บทที่ 4
ผลการดำเนินการ

4.1 รายละเอียดที่ใช้ในการทดสอบ (Test Environment Setup)

การทดสอบในงานวิจัยนี้ดำเนินการบนโครงสร้างพื้นฐานแบบไฮเปอร์คอนเวอร์จของ Nutanix โดยใช้ Nutanix Cluster จำนวน 1 คลัสเตอร์ ประกอบด้วย โหนดจำนวน 3 โหนด เชื่อมต่อกันผ่านเครือข่ายความเร็ว 10 Gigabit Ethernet (10GbE) ระบบไฮเปอร์ไวเซอร์ที่ใช้คือ Acropolis Hypervisor (AHV) และใช้ระบบจัดเก็บข้อมูล Acropolis Operating System (AOS) เวอร์ชัน 6.5.5.1 Long Term Support (LTS) สำหรับงานที่ใช้ในการทดสอบ ได้มีการสร้าง Virtual Machines จำนวน 10 เครื่อง โดยใช้ระบบปฏิบัติการ Windows Server 2019 ซึ่งติดตั้งและใช้งานอยู่ในศูนย์ Data Centers นอกจากนี้เพื่อทดสอบความสามารถด้านการกู้คืนความเสียหาย ได้มีการจำลอง ศูนย์ข้อมูลสำรอง (Disaster Recovery Site) จำนวน 1 คลัสเตอร์ ซึ่งประกอบด้วย 3 โหนด เช่นเดียวกัน โดยตั้งอยู่ใน เครือข่ายย่อย (Subnet) ที่แตกต่างจากศูนย์ข้อมูลหลัก การทำ Replication ระหว่างศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองดำเนินการผ่าน เครือข่าย WAN ที่มีแบนด์วิดท์ 100 Mbps การบริหารจัดการและควบคุมการทำงานของคลัสเตอร์ทั้งสองฝั่ง รวมถึงการกำหนดนโยบายการทำ Replication และการติดตามสถานะของระบบ ดำเนินการผ่านเครื่องมือ Nutanix Prism Central



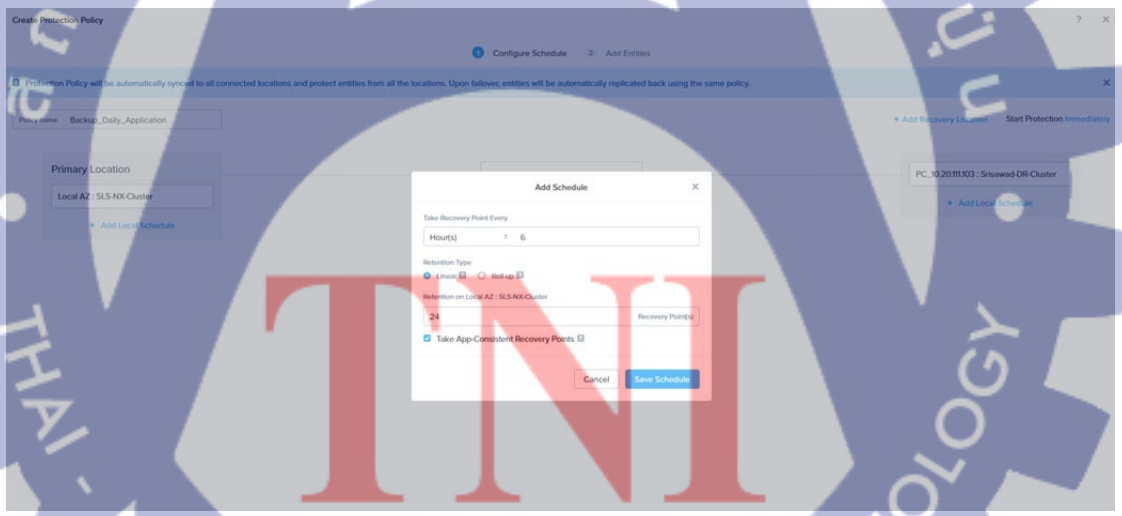
รูปที่ 4.1 Replication ระหว่าง DC/DR

ภาพประกอบแสดงโครงสร้างของระบบทดสอบที่แบ่งออกเป็นสองส่วนหลัก ได้แก่ ศูนย์ข้อมูลหลัก (DC) และ ศูนย์ข้อมูลสำรอง (DR) โดยแต่ละฝั่งถูกกำหนดเป็น Availability Zone แยกจากกัน เพื่อเพิ่มความสามารถของระบบในการรองรับความผิดพลาดและรักษาความต่อเนื่องในการให้บริการ

ทั้งสองศูนย์ข้อมูลใช้ Nutanix Cluster ที่ประกอบด้วย 3 โหนด และมีการบริหารจัดการผ่าน Prism Central แบบรวมศูนย์ การทำ Replication ระหว่าง DC และ DR ดำเนินการผ่านเครือข่าย WAN ที่มีความเร็ว 100 Mbps ซึ่งช่วยให้สามารถประเมินผลกระทบ ข้อจำกัดด้านแบนด์วิดท์ต่อระยะเวลาการกู้คืนระบบ (RTO) และจุดในการกู้คืนข้อมูล (RPO) ได้อย่างชัดเจน โครงสร้างดังกล่าวเป็นการจำลองสภาพแวดล้อมการใช้งานจริงของศูนย์ข้อมูลขนาดเล็กและขนาดกลาง ซึ่งมักมีข้อจำกัดด้านความเร็วของเครือข่ายระหว่างไซต์ แต่ยังจำเป็นต้องมีระบบกู้คืนความเสียหายที่มีประสิทธิภาพและดูแลจัดการได้ง่าย

4.2 การกำหนดค่าการป้องกันข้อมูล

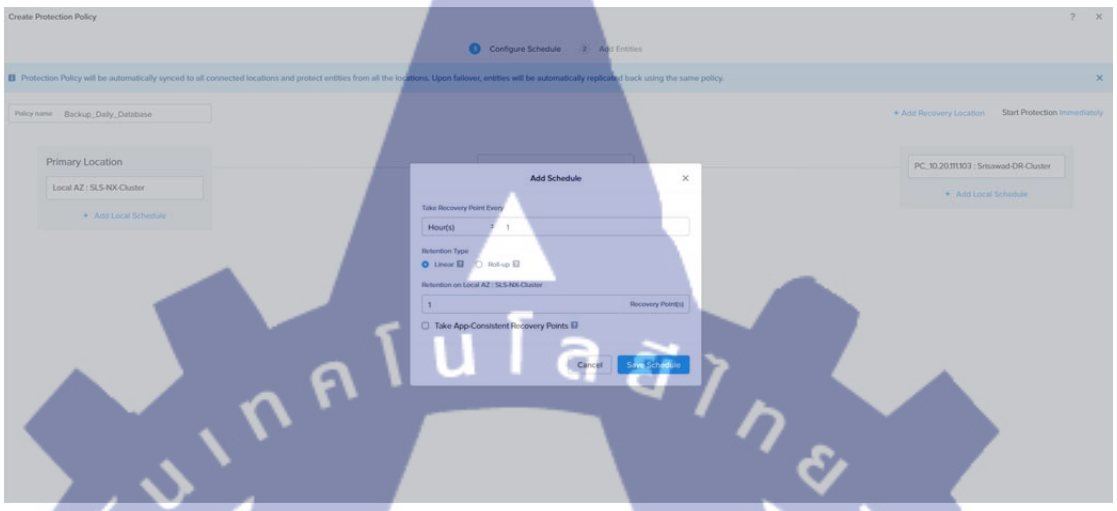
ในการทดสอบระบบกู้คืนความเสียหายในงานวิจัยนี้ ได้มีการกำหนดนโยบายการป้องกันข้อมูล โดยใช้แนวคิด Protection Domain ของ Nutanix เพื่อจัดกลุ่มเครื่อง Virtual Machines ตามลักษณะและความสำคัญของงาน Protection Domain ชื่อ “Backup_Daily_Application” ถูกกำหนดให้ครอบคลุมเครื่อง Virtual Machines ที่ทำหน้าที่เป็น Application Server โดยตั้งค่าการสร้าง Snapshot ทุก 6 ชั่วโมง เพื่อสำรองสถานะของระบบ และกำหนดให้มีการทำ Replication ไปยังศูนย์ข้อมูลสำรอง (DR Site) วันละ 1 ครั้ง เพื่อรองรับการกู้คืนระบบในกรณีที่ศูนย์ข้อมูลหลักไม่สามารถให้บริการได้



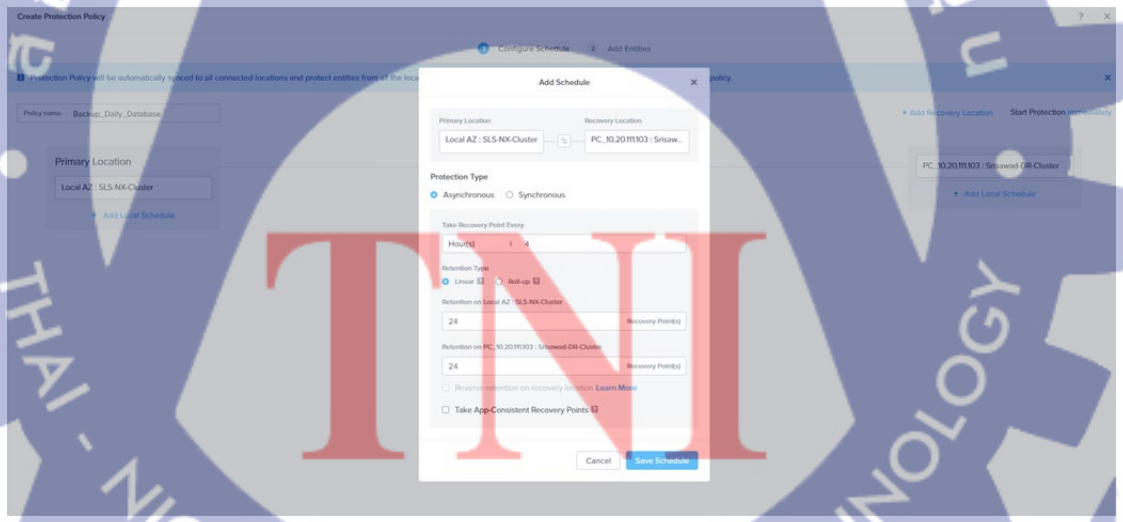
รูปที่ 4.2 กำหนด Replication Policy Database (DB)

ในขณะเดียวกัน ได้มีการกำหนด Protection Domain ชื่อ “Backup_Daily_Database” สำหรับเครื่อง Virtual Machines ที่ทำหน้าที่เป็น Database Server ซึ่งมีความสำคัญต่อความถูกต้องและความต่อเนื่องของข้อมูลมากกว่า โดยตั้งค่าการสร้าง Snapshot ทุก 1 ชั่วโมง และกำหนดให้มีการทำ Replication ไปยังศูนย์ข้อมูลสำรองทุก 4 ชั่วโมง เพื่อจำกัดการสูญหายของข้อมูลให้อยู่ในระดับต่ำ

ที่สุด การกำหนดนโยบายการป้องกันข้อมูลในลักษณะดังกล่าวสะท้อนการจัดการทรัพยากรที่แตกต่างกันตามความสำคัญของระบบงาน และช่วยให้สามารถประเมินประสิทธิภาพของการทำ Replication และผลกระทบต่อค่า RPO ได้อย่างชัดเจน



รูปที่ 4.3 กำหนด Backup Policy



รูปที่ 4.4 กำหนด Replication Policy App

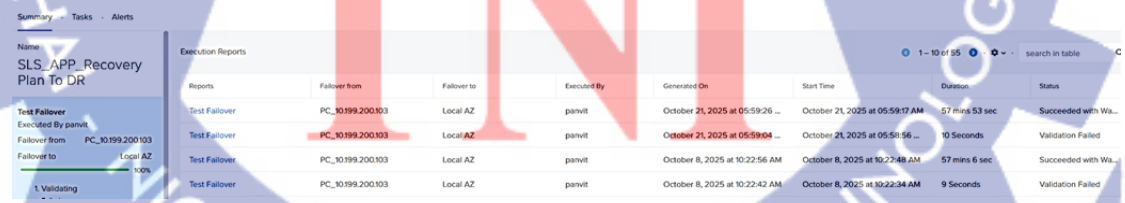
4.3 การทดสอบแผนกู้คืนระบบ

เมื่อทำการจำลองเหตุไฟฟ้าดับใน Production Site (ปิดเครื่อง)

ผลการทดสอบแสดงให้เห็นว่าการกู้คืนระบบสามารถดำเนินการได้ภายในระยะเวลาที่กำหนด (RTO = 1 ชั่วโมง) และข้อมูลที่กู้คืนมีความถูกต้องสอดคล้องกับนโยบายการสำรองข้อมูล โดยไม่พบการสูญเสียข้อมูลเกินกว่าค่า RPO ที่กำหนด (4 ชั่วโมง)” โดย

1. เครื่อง Active Directory Domain Services Server สามารถใช้งานได้ Servers อื่นๆ ภายใต้ Domain สามารถ Login ด้วย User Domain ได้
2. ระบบงานที่ได้ทำการกู้คืนสามารถ Login เข้าระบบผ่าน Network ที่อยู่ที่ DR Site ได้
3. วันที่ในระบบเป็นวันที่ตรงกับ Servers Production ตามที่ได้กำหนดไว้โดยวันที่ของ Servers เป็นวันที่ 21 ตุลาคม 2025 และ Business Date ในระบบงานเป็นวันที่ 20 ตุลาคม 2025 แสดงว่าเป็นไปตาม Data Protection Policies และระบบ Data Protection ทำงานได้ตามปกติ
4. ตั้งแต่เริ่มดำเนินการ Restore Servers จนถึงทดสอบความพร้อมใช้ของระบบสามารถทำได้ภายในวัน เป็นไปตามกำหนด RTO (Recovery Time Objective) 1 ชม.
5. ข้อมูลที่เรียกคืนได้ เป็นไปตามกำหนด RPO (Recovery Point Objective) 4 ชั่วโมง

รูปที่ 4.5 ผลการทดสอบกู้คืนข้อมูล Database



รูปที่ 4.6 ผลการทดสอบกู้คืน Application

4.4 ผลการวิเคราะห์

ตารางที่ 4.1 สรุปผลการทดสอบ

รายการทดสอบ	ค่าเป้าหมายผลการทดสอบ	ผลที่ได้	สรุปผล
RPO	≤ 4 ชั่วโมง	ย้อนหลัง ประมาณ 2 ชั่วโมง	ผ่าน
RTO	≤ 1 ชั่วโมง	55 นาที	ผ่าน
Data Consistency	ได้ข้อมูลตามที่กำหนดไว้	ถูกต้อง	ผ่าน

จากรูปที่ 4.5 แสดงผลการทดสอบการกู้คืนฐานข้อมูล (Database) ภายหลังการจำลองเหตุการณ์ที่ระบบ Production Site หยุดทำงาน โดยระบบ Disaster Recovery ได้ทำการกู้คืนข้อมูลจาก Snapshot ล่าสุดตามที่กำหนดไว้ ผลการทดสอบพบว่าฐานข้อมูลสามารถเปิดใช้งานได้ตามปกติ ไม่มีความเสียหายของข้อมูล และยังคงรักษาความสอดคล้องของข้อมูลได้อย่างครบถ้วน

โดยการวัดค่า RPO ดำเนินการโดยตรวจสอบเวลาของ Snapshot ล่าสุดที่ถูกนำมาใช้กู้คืน เปรียบเทียบกับเวลาที่เกิดเหตุการณ์จำลอง เพื่อคำนวณช่วงเวลาของข้อมูลที่อาจสูญหาย โดยสามารถแสดงในรูปแบบสมการได้ดังนี้

RPO = เวลาเกิดเหตุการณ์ – เวลา Snapshot ล่าสุด

นอกจากนี้ มีการตรวจสอบความถูกต้องของข้อมูล (Data Integrity) ด้วยการตรวจสอบโครงสร้างฐานข้อมูล การอ่าน/เขียนข้อมูล และการเปรียบเทียบข้อมูลกับระบบต้นทาง เพื่อยืนยันว่ากระบวนการกู้คืนสามารถรักษาคุณภาพของข้อมูลได้โดยไม่มีความคลาดเคลื่อน

ผลการวัดแสดงให้เห็นว่าการสูญเสียข้อมูลอยู่ภายในช่วง RPO ที่กำหนด และฐานข้อมูลยังคงมีความสมบูรณ์ ซึ่งสะท้อนถึงประสิทธิภาพของกลไก Snapshot และ Replication บนสถาปัตยกรรม HCI

จากรูปที่ 4.6 แสดงผลการทดสอบการกู้คืนระบบ Application ภายหลังการดำเนินการ Failover ไปยัง Disaster Recovery Site โดยระบบสามารถเริ่มให้บริการได้ตามปกติ ผู้ใช้งานสามารถเข้าสู่ระบบ เชื่อมต่อฐานข้อมูล และใช้งาน Application ได้อย่างต่อเนื่อง

หลังจากนั้น มีการทดสอบความพร้อมใช้งานของระบบ (Service Validation) ทดสอบเชื่อมต่อเครือข่าย และทดสอบการทำงานของ Application เพื่อยืนยันว่าระบบสามารถให้บริการได้ตามปกติ

จากผลการวัดและคำนวณทั้ง RPO และ RTO พบว่าระบบสามารถกู้คืนข้อมูลและบริการได้ภายในเกณฑ์ที่กำหนด โดยยังคงรักษาความถูกต้องของข้อมูลและความต่อเนื่องของระบบได้อย่างมีประสิทธิภาพ กระบวนการ Disaster Recovery บนสถาปัตยกรรม HCI จึงเหมาะสมสำหรับการนำไปใช้ในศูนย์ข้อมูลขนาดเล็กและขนาดกลาง เพื่อสนับสนุนความต่อเนื่องทางธุรกิจในสถานการณ์ฉุกเฉิน

4.5 การเปรียบเทียบกับระบบเดิม

ตารางที่ 4.2 ผลการเปรียบเทียบกับระบบเดิม

หัวข้อเปรียบเทียบ	ระบบเดิม (Traditional)	ระบบใหม่ (HCI)
วิธีการสำรองข้อมูล	การสำรองข้อมูลแบบกำหนดเวลา (Scheduled Backup) โดยใช้เครื่องมือของ SQL Server และการดำเนินการด้วยตนเอง	การสำรองข้อมูลด้วย Snapshot และการทำ Replication อัตโนมัติ
ระยะเวลาการหยุดให้บริการ (Downtime)	ประมาณ 2–3 ชั่วโมง	น้อยกว่า 1 ชั่วโมง
กระบวนการกู้คืนระบบ	ต้องอาศัยเจ้าหน้าที่ไอทีและมีหลายขั้นตอนในการดำเนินการ	ดำเนินการแบบอัตโนมัติ ขั้นตอนการกู้คืนมีความซับซ้อนต่ำ
การบริหารจัดการ	ใช้เครื่องมือหลายระบบแยกจากกัน	บริหารจัดการผ่าน Nutanix Prism Central เพียงเครื่องมือเดียว

บทที่ 5
สรุปและอภิปราย

5.1 ผลสรุปตามวัตถุประสงค์

จากการดำเนินการทดสอบระบบกู้คืนความเสียหายบนโครงสร้างพื้นฐานแบบไฮเปอร์คอนเวอร์จ (Hyper-Converged Infrastructure : HCI)

5.1.1 ตามวัตถุประสงค์ข้อที่ 1 เพื่อออกแบบแผนการกู้คืนจากเหตุฉุกเฉิน (DRP) บนสถาปัตยกรรม HCI และประเมินความสามารถในการลด RTO และ RPO พบว่าสถาปัตยกรรมแบบ HCI ที่ใช้ Snapshot และ Replication สามารถตอบสนองต่อเหตุฉุกเฉินได้อย่างมีประสิทธิภาพ โดยระบบสามารถกู้คืนระบบได้ภายใน 1 ชั่วโมง (RTO) และสามารถจำกัดการสูญเสียข้อมูลให้อยู่ภายใต้ระยะเวลา 4 ชั่วโมง (RPO) ตามที่ได้กำหนดไว้ และยังสามารถรักษาความถูกต้องของข้อมูลได้อย่างครบถ้วน ตามผลลัพธ์ ได้แสดงให้เห็นว่า การออกแบบ DRP บน HCI สามารถลดระยะเวลาการกู้คืนและช่วยจำกัดการสูญเสียข้อมูลได้ตามความต้องการขององค์กรขนาดเล็กและขนาดกลาง

5.1.2 ตามวัตถุประสงค์ ข้อที่ 2 เพื่อเปรียบเทียบประสิทธิภาพของ DRP แบบดั้งเดิมกับ DRP ที่พัฒนาบนสถาปัตยกรรม HCI จากผลการทดสอบ พบว่าระบบแบบดั้งเดิมมีขั้นตอนการกู้คืนซับซ้อนหลายขั้นตอน ต้องพึ่งพาการดำเนินการของบุคลากรที่มีความชำนาญในหลายระบบ และใช้เวลาประมาณ 2-3 ชั่วโมง ในขณะที่ HCI สามารถดำเนินการกู้คืนแบบกึ่งอัตโนมัติ มีขั้นตอนที่ง่ายกว่า ใช้เครื่องมือบริหารจัดการเพียงอย่างเดียวโดยผ่าน Prism Central และสามารถลด Downtime ให้ต่ำกว่า 1 ชั่วโมง ผลการเปรียบเทียบทำให้เห็นว่า HCI สามารถลดขั้นตอน เพิ่มความเร็ว และลดความเสี่ยงจาก Human Error ได้

5.1.3 ตามวัตถุประสงค์ ข้อที่ 3 เพื่อประเมินความเป็นไปได้และประสิทธิผลของการนำ DRP บน HCI ไปประยุกต์ใช้งานได้จริง จากผลการทดสอบในสภาพแวดล้อมจำลองแสดงให้เห็นว่า HCI สามารถใช้งานได้ง่าย ลดภาระของบุคลากรไอที รองรับ Resource ที่จำกัดได้ สามารถทำงานกับ WAN Link ขนาด 100 Mbps ได้ มีความเป็นไปได้สูงในการนำไปใช้จริงใน SMEs และองค์กรขนาดกลางที่ต้องการระบบ DR ที่เชื่อถือได้โดยไม่เพิ่มความซับซ้อนของโครงสร้างพื้นฐาน

5.2 ข้อจำกัด

การทดลองสามารถแสดงให้เห็นถึงประสิทธิภาพของระบบกู้คืนความเสียหายบนสถาปัตยกรรม HCI ได้อย่างชัดเจน แต่ยังมีข้อจำกัดบางประการที่ควรพิจารณา ได้แก่

5.2.1 การทดสอบดำเนินการในสภาพแวดล้อมจำลองที่ควบคุมได้ ซึ่งอาจแตกต่างจากสถานการณ์จริงที่มีปัจจัยภายนอกอื่นๆ เช่น ข้อจำกัดทางด้านเครือข่าย หรือเหตุการณ์ฉุกเฉินหลายรูปแบบเกิดขึ้นพร้อมกัน

5.2.2 การทดสอบนี้มุ่งเน้นการใช้เทคโนโลยีของผู้ให้บริการรายเดียว (Nutanix) จึงอาจไม่สามารถสรุปผลไปยังแพลตฟอร์ม HCI อื่น ๆ ได้โดยตรง

5.2.3 จำนวน Virtual Machines ที่ใช้ทดสอบมีข้อจำกัด (เพียง 10 เครื่อง) หากมี VM จำนวนมากหรือมี Workload มากขึ้นอาจทำให้ค่า RTO และ RPO เปลี่ยนแปลงไปจากผลที่ได้

งานวิจัยนี้เป็นการวิจัยเชิงประยุกต์ (Applied Research) ที่มุ่งเน้นการออกแบบและประเมินประสิทธิภาพของแผนการกู้คืนจากเหตุฉุกเฉินบนสถาปัตยกรรม Hyper-Converged Infrastructure ในบริบทขององค์กรขนาดเล็กและขนาดกลางในประเทศไทย โดยใช้สภาพแวดล้อมการทดลองที่ใกล้เคียงกับการใช้งานจริง ผลการศึกษาสามารถนำไปประยุกต์ใช้เป็นแนวทางเชิงปฏิบัติสำหรับองค์กรที่มีข้อจำกัดด้านงบประมาณ บุคลากร และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม

5.3 ข้อเสนอแนะ

จากการทดสอบ สามารถเสนอแนะแนวทางเชิงปฏิบัติสำหรับองค์กรที่ต้องการนำ HCI ไปใช้ในการจัดทำระบบกู้คืนความเสียหาย ดังนี้

5.3.1 องค์กรควรกำหนดค่า RTO และ RPO ให้สอดคล้องกับความสำคัญของระบบงานทางธุรกิจ และข้อจำกัดด้านงบประมาณและทรัพยากรที่มีอยู่

5.3.2 ควรจัดกลุ่มระบบงานตามระดับความสำคัญ และกำหนดนโยบาย Snapshot และ Replication ที่แตกต่างกัน เพื่อใช้ทรัพยากรอย่างมีประสิทธิภาพ

5.3.3 ควรทดสอบแผนกู้คืนความเสียหายอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนสามารถนำไปใช้งานได้จริงเมื่อเกิดเหตุฉุกเฉิน

5.3.4 ควรพิจารณาประสิทธิภาพของเครือข่าย WAN ระหว่างศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง เนื่องจากมีผลโดยตรงต่อค่า RPO และระยะเวลาการกู้คืนระบบ

จากผลการทดสอบ สามารถเสนอแนวทางต่อยอดสำหรับงานวิจัยในอนาคต ได้โดยขยายจำนวน Virtual Machines และ Workload ให้ใกล้เคียงสภาพจริงมากขึ้น หรือ ศึกษาเปรียบเทียบ HCI หลายแพลตฟอร์ม เช่น Nutanix, VMware vSAN, HPE SimpliVity เพื่อประเมินประสิทธิภาพและความคุ้มค่าในภาพรวม

5.4 อภิปรายผล (Discussion)

จากผลการทดสอบพบว่า สถาปัตยกรรมแบบ Hyper-Converged (HCI) สามารถลดค่า RTO และ RPO ได้ และสามารถรองรับความต่อเนื่องทางธุรกิจได้ ภายใต้ข้อจำกัดทางด้านทรัพยากร ซึ่งสอดคล้องกับทฤษฎีพื้นฐานและแนวโน้มที่กล่าวไว้ในบทที่ 2 โดยเฉพาะอย่างยิ่งงานที่ชี้ให้เห็นว่า HCI ช่วยลด Downtime ได้มากกว่า 45% โดยจากการรวม Compute, Storage, Virtualization และ Replication ไว้ในแพลตฟอร์มเดียว ทำให้การกู้คืนระบบมีความรวดเร็วและลดความซับซ้อนของกระบวนการ DR ผลในการทดสอบ พบแนวโน้มเดียวกัน คือสามารถลด Downtime ให้ต่ำกว่า 1 ชั่วโมง ซึ่งถือว่าอยู่ในระดับที่ดีกว่า DR แบบดั้งเดิมที่ใช้เวลาประมาณ 2-3 ชั่วโมง

นอกจากนี้ ผลการทดสอบยังสอดคล้องกับข้อค้นพบของงานวิจัยที่เกี่ยวข้องในด้านประสิทธิภาพของการทำ Snapshot และ Replication ได้แก่งานที่ระบุว่าเทคนิคการทำ Snapshot & Local Replication สามารถเพิ่ม Reliability ของข้อมูลได้ โดยผลการทดสอบพบว่า การทำ Snapshot และ Replication ตามรอบเวลา (1 ชั่วโมงสำหรับ Database และ 6 ชั่วโมงสำหรับ Application) ช่วยรักษาความถูกต้องของข้อมูล และสามารถกู้คืนข้อมูลได้ตรงตามค่า RPO ที่ตั้งไว้

โดยสรุป ผลการทดสอบมีแนวโน้มสนับสนุนงานวิจัยเดิมในแง่ของประสิทธิภาพด้าน DR แต่ยังมีความแตกต่างเมื่อเปรียบเทียบกับโซลูชัน DR ประเภท Cloud และ Hybrid โดยเฉพาะด้าน Latency, ความเสถียรในการทำ Failover และง่ายในการบริหารจัดการ ซึ่งเป็นสิ่งที่ที่องค์กรขนาดเล็กและขนาดกลางควรนำมาพิจารณาในการเลือกใช้เทคโนโลยี DR ที่เหมาะสม


สถาบันเทคโนโลยีไทย-ญี่ปุ่น
THAI - NICHI INSTITUTE OF TECHNOLOGY
TNI

บรรณานุกรม

บรรณานุกรม

[1] R. Basa, “Cloud disaster recovery : Best practices for business continuity in the cloud,” *International Journal for Multidisciplinary Research (IJFMR),* vol. 6, no. 5, pp. 1-2, October 2024.

[2] S. Khatoon et al., “Enhancing institutional resilience : A strategic study of disaster preparedness practices in university libraries of khyber pakhtunkhwa (KPK) peshawar,” *Strategic Research & Analysis,* vol. 3, no. 3, pp. 409-425, July 2025.

[3] K. Alexis, “Effects of notable natural disasters of 2017 on information and communication networks infrastructure,” *IEEE International Telecommunications Energy Conference, INTELEC 2018,* Torino, Italy, October 7-11, 2018, pp. 1-8.

[4] M. Gajić, *“Quantifying the Impact of 5G Network Slicing on Quality of Experience and Survivability,”* B.S. Thesis (Information and Communication Technology), Norwegian University of Science and Technology (NTNU), Trondheim, Norway, 2025.

[5] A. Babin et al., “Perspectives of sustainable development of cluster organizations through internationalization and dual use,” *Smart Cities and Regional Development Journal,* vol. 9, no. 3, pp. 99-120, September 2025.

[6] G. Kambala, “Designing resilient enterprise applications in the cloud : Strategies and best practices,” *World Journal of Advanced Research and Review,* vol. 17, no. 3, pp. 1,078-1,094, March 2023.

[7] D. M. Kesa, “Ensuring resilience : Integrating IT disaster recovery planning and business continuity for sustainable information technology operations,” *World Journal of Advanced Research and Review,* vol. 18, no. 3, pp. 970-992, June 2023.

[8] European Union Agency for Cybersecurity (ENISA), *“Technical Implementation Guidance on Commission Implementing Regulation (EU),”* [Online]. Available : https:// www.enisa.europa.eu/publications/nis2-technical-implementation-guidance. [Accessed : February 15, 2026].

[9] J. S. Patel et al., “Disaster recovery in business continuity management,” *International Journal of Trend in Scientific Research and Development,* vol. 3, no. 4, pp. 319-322, June 2019.

[10] G. S. Atencio and M. U. Ramírez, "The evolution and trends of hyperconvergence in the telecommunications sector : A competitive intelligence review," *KKU Engineering Journal,* vol. 90, no. 227, pp. 126-132, August 2023.

[11] S. Sinclair, *"Modernize IT Infrastructure for Modern Applications with Nutanix, HPE, and Intel,"* [Online]. Available : https://www.esg-global.com. [Accessed : February 15, 2026].

[12] S. Nutanix, *"The Definitive Guide to Hyperconverged Infrastructure : How Nutanix Works,"* [Online]. Available : https://www.nutanix.com. [Accessed : February 15, 2026].

[13] A. P. Veiga, *"Hyper Converged Infrastructures: Beyond Virtualization,"* B.Eng. Thesis (Automation Engineering), University of Maryland University College, Adelphi, USA. 2017.

[14] K. Elgdamsi and M. Embarak, "Implementing a disaster recovery solution for datacenters using VMware site recovery manager," *Tobruk University Journal of Engineering Sciences,* vol. 4, no. 1, pp. 25-47, May 2023.

[15] P. A. Damayantha, *"Cisco Intersight for Karelia ICT Laboratory : Integration of Cisco Intersight and Nutanix in Karelia ICT Laboratory Data Centre,"* B.Eng. Thesis (Information and Communication Technology), Karelia University of Applied Sciences, Joensuu, Finland. 2025.