

หลักสูตรรายวิชา

หลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567 ประเภทวิชา กลุ่มอาชีพซอฟต์แวร์และการประยุกต์
 ประเภทวิชาอุตสาหกรรมดิจิทัลและเทคโนโลยีสารสนเทศ
 สาขาวิชา เทคโนโลยีสารสนเทศ
 รหัส 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย
 ทฤษฎี 1 ชั่วโมง/สัปดาห์ ปฏิบัติ 4 ชั่วโมง/สัปดาห์ จำนวน 1-4-3 หน่วยกิต

อ้างอิงมาตรฐาน

มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

ผลลัพธ์การเรียนรู้ระดับรายวิชา

ติดตั้งและสนับสนุนด้านเทคนิค เพื่อการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศและระบบเครือข่ายตามหลักการ ด้วยความละเอียดรอบคอบ รับผิดชอบ การสื่อสาร การคิดเชิงนวัตกรรมและการทำงานเป็นทีม

จุดประสงค์รายวิชา เพื่อให้

1. เข้าใจเกี่ยวกับการติดตั้ง การใช้งานระบบปฏิบัติการเครื่องแม่ข่ายและแพ็กเก็ต (Packet) ที่สนับสนุนการให้บริการในระบบเครือข่าย
2. มีทักษะในการติดตั้ง การใช้งานระบบปฏิบัติการเครื่องแม่ข่ายและแพ็กเก็ต (Packet) ที่สนับสนุนการให้บริการในระบบเครือข่าย
3. มีเจตคติและกิจนิสัยที่ดีในการปฏิบัติงานด้วยความละเอียดรอบคอบ รับผิดชอบ การสื่อสาร การคิดเชิงนวัตกรรมและการทำงานเป็นทีม
4. มีความสามารถประยุกต์ใช้ระบบปฏิบัติการเครื่องแม่ข่ายและแพ็กเก็ต (Packet) เพื่อให้บริการในระบบเครือข่าย

สมรรถนะรายวิชา

1. ประมวลความรู้เกี่ยวกับการติดตั้ง การใช้งานระบบปฏิบัติการเครื่องแม่ข่ายและแพ็กเก็ต (Packet) ที่สนับสนุนการให้บริการในระบบเครือข่ายตามหลักการ
2. ติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายและแพ็กเก็ต (Packet) ที่สนับสนุนการให้บริการในระบบเครือข่ายตามขั้นตอน
3. ใช้งานระบบปฏิบัติการเครื่องแม่ข่ายตรงตามวัตถุประสงค์
4. ประยุกต์ใช้ระบบปฏิบัติการเครื่องแม่ข่ายและเลือกใช้แพ็กเก็ต (Packet) เพื่อให้บริการในระบบเครือข่าย

คำอธิบายรายวิชา

ศึกษาและปฏิบัติเกี่ยวกับ ระบบปฏิบัติการบนเครื่องแม่ข่าย (Network Operating System) การติดตั้งโปรแกรมระบบปฏิบัติการบนเครื่องแม่ข่าย การตั้งค่าพื้นฐานบนระบบปฏิบัติการเครื่องแม่ข่าย การจัดการเกี่ยวกับ รายละเอียดของผู้ใช้งานการกำหนดสิทธิ์ใช้งาน การกำหนดการทำงานของ Firewall เบื้องต้น การควบคุมเครื่องแม่ข่ายระยะไกลผ่านเครือข่าย การติดตั้งและบริหารจัดการโปรแกรมในการให้บริการในรูปแบบต่าง ๆ ในระบบเครือข่ายได้แก่ บริการด้านโดเมนเนม (DNS Server) บริการด้านเว็บ (Web Server) บริการ

ด้านฐานข้อมูล (Database Server) บริการด้านการจัดสรรหมายเลขไอพี (DHCP Server) บริการด้านการแบ่งปันข้อมูลและทรัพยากร (File and Resource Sharing Server) บริการด้านการเป็นตัวกลาง (Proxy Server) การบริการตรวจสอบยืนยันตัวตน (AAA Server) บริการด้าน Container Platform บริการด้าน IoT Platform การเขียนคำสั่งสคริปต์ การสร้างการเชื่อมต่อ ที่ปลอดภัย (SSL Certificate) และโปรแกรมให้บริการในด้านอื่น ๆ ที่จำเป็น ติดตั้งและสนับสนุนด้านเทคนิคการใช้งานคอมพิวเตอร์แม่ข่าย ด้านเครือข่าย และด้านระบบสารสนเทศ ให้ใช้งานตามความต้องการของผู้ใช้

ตารางวิเคราะห์หน่วยการเรียนรู้
ผลลัพธ์การเรียนรู้ระดับรายวิชา (Job)

งานหลัก (Duty)	งานย่อย (Task)	สมรรถนะย่อย (มาตรฐานอาชีพ)	ความรู้ (Knowledge)	ทักษะ (Skill)
งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย	1.1 งานวางแผนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย 1.2 งานเตรียมความพร้อมฮาร์ดแวร์และสื่อบันทึก 1.3 งานติดตั้งโปรแกรมระบบปฏิบัติการเครื่องแม่ข่าย 1.4 งานตรวจสอบการทำงานและการอัปเดตระบบ 1.5 งานจัดทำรายงานผลการติดตั้ง 1.6 งานจัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์	40106. 01	1. เข้าใจประเภทและสถาปัตยกรรมของระบบปฏิบัติการเครื่องแม่ข่าย 2. เข้าใจข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์สำหรับการติดตั้ง 3. ติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายแต่ละชนิด 4. แบ่งพาร์ติชันและรูปแบบระบบไฟล์ 5. ตรวจสอบและแก้ไขปัญหาเบื้องต้นในการติดตั้ง 6. อัปเดตและแพตช์ระบบปฏิบัติการ	1. วางแผนและกำหนดค่าระบบ 2. เตรียมสื่อและอุปกรณ์ติดตั้ง 3. ติดตั้งและกำหนดค่าเริ่มต้นระบบปฏิบัติการ 4. ทดสอบและตรวจสอบความเข้ากันได้ของระบบ 5. ประยุกต์ใช้เครื่องมือช่วยเหลือการติดตั้ง 6. สื่อสารเพื่อขอข้อมูลและแจ้งความคืบ
งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	2.1 งานวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง 2.2 งานกำหนดค่าพื้นฐานของระบบและเครือข่าย 2.3 งานจัดการผู้ใช้งานและกลุ่มผู้ใช้งาน 2.4 งานกำหนดสิทธิ์การเข้าถึงทรัพยากรบนเครื่องแม่ข่าย 2.5 งานตั้งค่าการควบคุมเครื่องแม่ข่ายระยะไกล 2.6 งานตรวจสอบและบันทึกการตั้งค่าระบบ 2.7 งานจัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์	40106. 01	1. เข้าใจแนวคิดและหลักการจัดการผู้ใช้งานและกลุ่ม 2. เข้าใจการจัดการสิทธิ์การเข้าถึงไฟล์และโฟลเดอร์ 3. เข้าใจหลักการกำหนดค่าเครือข่ายพื้นฐาน (IP Address, Subnet Mask, Gateway, DNS) 4. เข้าใจหลักการเครื่องมือและวิธีการควบคุมเครื่องแม่ข่ายระยะไกล 5. เข้าใจหลักการความปลอดภัยในการจัดการสิทธิ์และควบคุมระยะไกล 6. เข้าใจการจัดทำเอกสารและบันทึกการตั้งค่า	1. บริหารจัดการบัญชีผู้ใช้และกลุ่ม 2. กำหนดสิทธิ์การเข้าถึงทรัพยากร 3. ตั้งค่าการเชื่อมต่อเครือข่าย 4. ใช้คำสั่งและเครื่องมือสำหรับการควบคุมระยะไกล 5. ประยุกต์ใช้แนวคิดความรับผิดชอบในการจัดการระบบ 6. สื่อสารและขอความร่วมมือจากผู้ใช้งาน
งานจัดตั้งและบริหารจัดการบริการเครือข่าย	3.1 งานวิเคราะห์ความต้องการและออกแบบบริการเครือข่าย 3.2 งานวางแผนการติดตั้งและตั้งค่าบริการเครือข่าย 3.3 งานติดตั้งและตั้งค่าโปรแกรมให้บริการเครือข่าย (เช่น DNS, DHCP,	40106. 01, 40106. 02	1. เข้าใจหลักการทำงานของบริการเครือข่ายแต่ละประเภท (DNS, DHCP, Web, File, DB, Proxy, AAA, Container, IoT) 2. ติดตั้งและตั้งค่าบริการเครือข่าย 3. เข้าใจโปรโตคอลและพอร์ตที่เกี่ยวข้องกับแต่ละ	1. ออกแบบและวางแผนโครงสร้างบริการ 2. ติดตั้งและกำหนดค่าซอฟต์แวร์บริการ 3. ใช้คำสั่งและเครื่องมือบริหารจัดการบริการ 4. ทดสอบการเชื่อมต่อและการทำงานของบริการ 5. วิเคราะห์ Log และข้อมูล

	Web, File, DB, Proxy, AAA, Container, IoT) 3.4 งานทดสอบการทำงานของบริษัทเครือข่าย 3.5 งานตรวจสอบและบำรุงรักษาบริการเครือข่ายอย่างสม่ำเสมอ 3.6 งานจัดทำรายงานผลการให้บริการ 3.7 งานจัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์		บริการ 4. ปรับแต่งและเพิ่มประสิทธิภาพบริการ 5. ตรวจสอบสถานะและแก้ไขปัญหาบริการ 6. จัดการทรัพยากรที่ใช้โดยบริการ (เช่น พื้นที่จัดเก็บ, แรม)	การทำงาน 6. สามารถทำงานเป็นทีมในการประสานงานบริการ
งานรักษาความปลอดภัยระบบเครือข่ายและบริการ	4.1 งานประเมินความเสี่ยงและภัยคุกคามต่อระบบ 4.2 งานวางแผนการตั้งค่าและมาตรการความปลอดภัย 4.3 งานกำหนดการทำงานของ Firewall เบื้องต้น 4.4 งานสร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัย 4.5 งานตั้งค่าการตรวจสอบยืนยันตัวตนและการอนุญาต (AAA Server) 4.6 งานตรวจสอบและทดสอบมาตรการความปลอดภัย	40106. 01,40106. 02	4.1 ประเมินความเสี่ยงและภัยคุกคามต่อระบบเครือข่ายและบริการได้อย่างรอบคอบ 4.2 วางแผนมาตรการและตั้งค่าความปลอดภัยได้อย่างเหมาะสม 4.3 กำหนดค่า Firewall เบื้องต้นเพื่อป้องกันภัยคุกคามได้ 4.4 สร้างและติดตั้ง SSL Certificate เพื่อสร้างการเชื่อมต่อที่ปลอดภัยได้อย่างถูกต้อง 4.5 ตั้งค่า AAA Server เพื่อการตรวจสอบยืนยันตัวตนได้ 4.6 ตรวจสอบและทดสอบมาตรการความปลอดภัยได้อย่างมีประสิทธิภาพ 4.7 จัดทำรายงานการประเมินความปลอดภัยได้อย่างครบถ้วนและเป็นประโยชน์ 4.8 บำรุงรักษาและจัดเก็บเครื่องมือได้อย่างเป็นระเบียบและปลอดภัย	1. สามารถใช้แนวคิดและหลักการความปลอดภัยของระบบเครือข่ายและเครื่องมือช่วยในการจัดการ 2. แบ่งประเภทของภัยคุกคามและช่องโหว่ทางความปลอดภัย 3. การกำหนดค่า Firewall 4. สามารถใช้หลักการของ SSL/TLS และ Certificate Authority 5. สามารถใช้แนวคิดของ AAA (Authentication, Authorization, Accounting) และการตั้งค่า 6. สามารถใช้เครื่องมือและวิธีการทดสอบความปลอดภัยเบื้องต้น 7. กำหนดนโยบายและมาตรฐานความปลอดภัยข้อมูล
งานปรับแต่งและเพิ่มประสิทธิภาพระบบเครือข่ายด้วยสคริปต์	5.1 งานวิเคราะห์ความต้องการในการปรับแต่งหรือทำงานอัตโนมัติ 5.2 งานวางแผนการเขียนคำสั่งสคริปต์ 5.3 งานเขียนคำสั่งสคริปต์เพื่อจัดการและปรับแต่งระบบ 5.4 งานทดสอบและแก้ไขคำสั่งสคริปต์ 5.5 งานนำคำสั่งสคริปต์	40106. 01,40106. 02	1. เข้าใจหลักการเขียนโปรแกรมเชิงสคริปต์ (เช่น Bash, PowerShell, Python) 2. คำสั่งและไวยากรณ์พื้นฐานในการเขียนสคริปต์ 3. จัดการกับข้อผิดพลาดและ Log ในสคริปต์ 4. เข้าใจประโยชน์ของการทำงานอัตโนมัติและการเพิ่ม	1. สามารถวิเคราะห์ปัญหาและการออกแบบอัลกอริทึม 2. สามารถ เขียนและการดีบั๊กสคริปต์ 3. สามารถประยุกต์ใช้สคริปต์ในการจัดการระบบ 4. ทดสอบและปรับปรุงประสิทธิภาพสคริปต์

	ไปใช้งานและติดตามผล 5.6 งานจัดทำคู่มือการใช้ และบำรุงรักษาสคริปต์ 5.7 งานจัดเก็บและดูแล รักษาเครื่องมืออุปกรณ์		ประสิทธิภาพด้วยสคริปต์	
งานสนับสนุนและ แก้ไขปัญหาการใช้ งานระบบเครื่องแม่ ข่าย	6.1 รับแจ้งปัญหาและ รวบรวมข้อมูลเบื้องต้น 6.2 วิเคราะห์และวินิจฉัย สาเหตุของปัญหา 6.3 วางแผนการแก้ไข ปัญหาและกำหนด แนวทาง 6.4 ดำเนินการแก้ไข ปัญหาตามขั้นตอน 6.5 ทดสอบและยืนยัน ผลการแก้ไขปัญหา 6.6 ให้คำแนะนำและ สนับสนุนแก่ผู้ใช้งาน 6.7 จัดทำรายงานการ แก้ไขปัญหาและสรุปผล 6.8 จัดเก็บและดูแล รักษาเครื่องมืออุปกรณ์	40106. 01,40106. 02	1. การรวบรวมข้อมูลและ สอบถามปัญหา 2. การวิเคราะห์และ แยกแยะปัญหา 3. การใช้เครื่องมือวิเคราะห์ และแก้ไขปัญหา (เช่น ping, netstat, tcpdump, top) 4. การแก้ไขปัญหาเฉพาะ หน้าและถาวร 5. การสื่อสารอย่างมี ประสิทธิภาพกับผู้ใช้งาน 6. การทำงานเป็นทีมในการ แก้ไขปัญหาร่วมกัน 7. ความรับผิดชอบในการ ติดตามผลและแก้ปัญหา	1. สามารถรวบรวมข้อมูล และสอบถามปัญหา 2. สามารถวิเคราะห์และ แยกแยะปัญหา 3. สามารถใช้เครื่องมือ วิเคราะห์และแก้ไขปัญหา (เช่น ping, netstat, tcpdump, top) 4. สามารถแก้ไขปัญหา เฉพาะหน้าและถาวร 5. สามารถสื่อสารอย่าง มีประสิทธิภาพกับผู้ใช้งาน 6. สามารถทำงานเป็นทีมใน การแก้ไขปัญหาร่วมกัน 7. ความรับผิดชอบในการ ติดตามผลและแก้ปัญหา



มาตรฐานอาชีพและคุณวุฒิวิชาชีพ
Occupational Standard and Professional Qualifications

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย

จัดทำโดย สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
ร่วมกับ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

1. ชื่อมาตรฐานอาชีพ

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย

2. ประวัติการปรับปรุงมาตรฐาน

ไม่มี

3. ทะเบียนอ้างอิง (Imprint)

ไม่มี

4. ข้อมูลเบื้องต้น

มาตรฐานสาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network & Security)

มีวัตถุประสงค์สำคัญเพื่อพัฒนาศักยภาพของบุคลากรในสาขาอาชีพ ICT ให้สามารถแข่งขันและเป็นที่ยอมรับในระดับสากล สนับสนุนบุคลากรในกลุ่มอาชีพให้มีสมรรถนะตรงตามความต้องการของผู้ว่าจ้าง มีทักษะทางเทคนิคในการปฏิบัติงาน

5. ประวัติการปรับปรุงมาตรฐานในแต่ละครั้ง

การทบทวนมาตรฐานอาชีพและคุณวุฒิวิชาชีพตามกรอบคุณวุฒิวิชาชีพ 8 ระดับ ครั้งที่ 1

6. ครั้งที่

1 (ปี พุทธศักราช 2563)

การเปลี่ยนแปลงที่สำคัญ

การทบทวนมาตรฐานอาชีพและคุณวุฒิวิชาชีพตามกรอบคุณวุฒิวิชาชีพ 8 ระดับ มีรายละเอียด ดังนี้

- ทบทวนคุณลักษณะผลการเรียนรู้ให้มีความสอดคล้องกับสมรรถนะของคุณวุฒิวิชาชีพ
- ทบทวนการเลื่อนระดับคุณวุฒิวิชาชีพสาขาวิชาชีพ
- ทบทวนสมรรถนะอาชีพ (หน่วยสมรรถนะ หน่วยสมรรถนะย่อย เกณฑ์การปฏิบัติงาน และรายละเอียดหน่วยสมรรถนะ)
- ทบทวนเครื่องมือประเมิน กระบวนการประเมิน คู่มือการประเมิน สัดส่วนคะแนน เกณฑ์การผ่านการประเมิน

กรอบคุณวุฒิ 7 ชั้น จำนวน 5 อาชีพ 16 ชั้นคุณวุฒิ 37 หน่วยสมรรถนะ	กรอบคุณวุฒิ 8 ระดับ จำนวน 5 อาชีพ 16 ระดับคุณวุฒิ 36 หน่วยสมรรถนะ
1. ช่างสนับสนุนด้านเทคนิค ชั้น 3 - 6	1. ช่างสนับสนุนด้านเทคนิค ระดับ 3 - 6
2. นักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ชั้น 4 - 6	2. นักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ระดับ 4 - 6
3. นักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ชั้น 4 - 6	3. นักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ระดับ 4 - 6
4. นักจัดการความมั่นคงระบบสารสนเทศ ชั้น 4 - 6	4. นักจัดการความมั่นคงระบบสารสนเทศ ระดับ 4 - 6
5. นักจัดการอุปกรณ์พิกพาและเครือข่ายไร้สาย ชั้น 4 - 6	5. นักจัดการอุปกรณ์พิกพาและเครือข่ายไร้สาย ระดับ 4 - 6

7. คุณวุฒิวิชาชีพที่ครอบคลุม (Professional Qualifications included)

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล

อาชีพช่างสนับสนุนด้านเทคนิค ระดับ 5

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

ไม่มี

9. หน่วยสมรรถนะทั้งหมดในมาตรฐานอาชีพ (List of All Units of Competence within this Occupational Standards)

รหัสหน่วยสมรรถนะ	เนื้อหา
40104	ตั้งค่าพร้อมทั้งทดสอบอุปกรณ์เครือข่าย
40106	ติดตั้งและสนับสนุนการใช้งานระบบปฏิบัติการ การและซอฟต์แวร์ที่ให้บริการในระบบเครือข่าย

10. ระดับคุณวุฒิ

10.1 สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล อาชีพช่างสนับสนุนด้านเทคนิค ระดับ 5

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

เป็นผู้มีสมรรถนะทางเทคนิคในการจัดการงานสนับสนุนทางเทคนิคระบบเครือข่าย สามารถแก้ไขปัญหาในบริบทที่มีการเปลี่ยนแปลงทั่วไป สามารถคิดวิเคราะห์และประเมินสถานการณ์ได้ด้วยตนเอง มีความเป็นผู้นำจัดการผลิตภาพการทำงาน ถ่ายทอดงาน สอนงาน และกำกับดูแลผู้ร่วมงานให้บรรลุงานตามแผนได้ โดยมีสมรรถนะในการตั้งค่าพร้อมทั้งทดสอบอุปกรณ์เครือข่าย ติดตั้งและสนับสนุนการใช้งานระบบปฏิบัติการและซอฟต์แวร์ที่ให้บริการในระบบเครือข่ายและฝึกอบรมเพื่อให้ความรู้และทักษะกับผู้อื่น

การเลือกระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

- คุณสมบัติของผู้ที่สามารถเข้ารับการประเมินคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพช่างสนับสนุนด้านเทคนิค ระดับ 5
 - มีประสบการณ์ทำงานด้านงานสนับสนุนระบบเครือข่ายและคอมพิวเตอร์ หรือที่เกี่ยวข้องไม่น้อยกว่า 5 ปี หรือ
 - ผู้ที่สำเร็จการศึกษาระดับปริญญาตรี ในด้านงานสนับสนุนระบบเครือข่ายและคอมพิวเตอร์ หรือที่เกี่ยวข้อง หรือ
 - ได้รับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร และดิจิทัลคอนเทนต์ สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพช่างสนับสนุนด้านเทคนิค ระดับ 4 แล้วเป็นระยะเวลาไม่น้อยกว่า 1 ปี
- ผู้ที่ผ่านการประเมินและได้รับการรับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพช่างสนับสนุนด้านเทคนิค ระดับ 5
 - ผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะของอาชีพช่างสนับสนุนด้านเทคนิค ระดับ 5 จำนวน 3 หน่วย
- ในกรณีต่ออายุหนังสือรับรองมาตรฐานอาชีพให้เข้าไปตามคู่มือสำหรับผู้เข้ารับการประเมินหรือคู่มือเจ้าหน้าที่สอบ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

N/A

กลุ่มบุคคลในอาชีพ (Target Group)

N/A

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

40104 ตั้งค่าพร้อมทั้งทดสอบอุปกรณ์เครือข่าย

40106 ติดตั้งและสนับสนุนการใช้งานระบบปฏิบัติการ การและซอฟต์แวร์ที่ให้บริการในระบบเครือข่าย

ตารางแผนผังแสดงหน้าที่

1. ตารางแสดงหน้าที่ 1

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

ประกาศใช้ ณ 03/03/2563

ตาราง 1 : FUNCTIONAL MAP แสดง KEY PURPOSE , KEY ROLES , KEY FUNCTION

ความมุ่งหมายหลัก Key Purpose	บทบาทหลัก Key Roles		หน้าที่หลัก Key Function	
คำอธิบาย	รหัส	คำอธิบาย	รหัส	คำอธิบาย
พัฒนาศักยภาพของบุคลากรในสาขาอาชีพ ICT ให้สามารถแข่งขันและเป็นที่ยอมรับในระดับสากล	40	ปฏิบัติงานด้าน เครือข่ายและความปลอดภัย ให้ได้ตามมาตรฐานอาชีพ	401	งานสนับสนุนระบบเครือข่ายและคอมพิวเตอร์

คำอธิบาย ตารางแนบผังแสดงหน้าที่เป็นแผนผังที่ผู้ใช้วิเคราะห์หน้าที่งานเพื่อให้ได้หน้าที่หลัก (Key Function)

2. ตารางแสดงหน้าที่ 1 (ต่อ)

ประกาศใช้ ณ 03/03/2563

ตาราง 2 : FUNCTIONAL MAP แสดง KEY FUNCTION , UNIT OF COMPETENCE , ELEMENT OF COMPETENCE

หน้าที่หลัก Key Function		หน่วยสมรรถนะ Unit of Competence		หน่วยสมรรถนะย่อย Element of Competence	
รหัส	คำอธิบาย	รหัส	คำอธิบาย	รหัส	คำอธิบาย
401	งานสนับสนุนระบบเครือข่ายและคอมพิวเตอร์	40104	ตั้งค่าพารามิเตอร์ทดสอบอุปกรณ์เครือข่าย	40104.01	ตั้งค่าการทำงาน ให้ทำงานได้ตามแผนผังเครือข่าย
				40104.02	ทดสอบการทำงานของอุปกรณ์เครือข่าย
		40106	ติดตั้งและสนับสนุนการใช้งานระบบปฏิบัติการและซอฟต์แวร์ที่ให้บริการในระบบเครือข่าย	40106.01	ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่าย
				40106.02	ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศ

คำอธิบาย

ตารางแผนผังแสดงหน้าที่ (ต่อ) เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานหลังจากได้หน้าที่หลัก (Key Function) เพื่อให้ได้ หน่วยสมรรถนะ (Unit of Competence) และหน่วยสมรรถนะย่อย (Element of Competence)

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

1. รหัสหน่วยสมรรถนะ 40104
2. ชื่อหน่วยสมรรถนะ ตั้งค่าพร้อมทั้งทดสอบอุปกรณ์เครือข่าย
3. ทบทวนครั้งที่ 1 / -
4. สร้างใหม่ ☐ ปรับปรุง ☒

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถตั้งค่าการทำงาน ให้ทำงานได้ตามแผนผังเครือข่าย และทดสอบการใช้งานอุปกรณ์เครือข่าย

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☒	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้ประกอบการวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2523 ผู้ประกอบวิชาชีพด้านเครือข่ายคอมพิวเตอร์

3513 ช่างเทคนิคด้านเครือข่ายและระบบคอมพิวเตอร์

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
40104.01 ตั้งค่าการทำงาน ให้ทำงานได้ตามแผนผังเครือข่าย	1.1 ตั้งค่าอุปกรณ์เครือข่ายในระดับพอร์ตเชื่อมต่อ โปรโตคอล และ ตามแผนผังเครือข่าย 1.2 บันทึกสำรองข้อมูลการตั้งค่า	ข้อสอบข้อเขียน การสาธิตการปฏิบัติงาน
40104.02 ทดสอบการใช้งานอุปกรณ์เครือข่าย	2.1 ทดสอบการทำงาน ของเครือข่ายตามแผนผังเครือข่าย 2.2 ทดสอบประสิทธิภาพการทำงาน ของเครือข่ายตามแผนผังเครือข่าย	ข้อสอบข้อเขียน การสาธิตการปฏิบัติงาน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. ความสามารถในการทดสอบการทำงานของ เครือข่ายตามแผนผังเครือข่าย
2. ความสามารถในการทดสอบประสิทธิภาพการทำงานของ เครือข่ายตามแผนผังเครือข่าย

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับ มาตรฐานอีเทอร์เน็ต
2. ความรู้เกี่ยวกับ มาตรฐาน Wi-Fi
3. ความรู้เกี่ยวกับ ฮาร์ดแวร์อุปกรณ์เครือข่ายที่ระดับระดับที่ 1-4 ได้แก่ Hub, Repeater, Bridge, Switch, Router, Layer 3 Switch, Gateway
4. ความรู้เกี่ยวกับ พื้นฐาน TCP/IP
5. ความรู้เกี่ยวกับ ไอพีแอดเดรสแบบ Static
6. ความรู้เกี่ยวกับ ไอพีแอดเดรสแบบ Dynamic
7. ความรู้เกี่ยวกับ การแบ่งไอพีแอดเดรส
8. ความรู้เกี่ยวกับ มาตรฐานอีเทอร์เน็ต
9. ความรู้เกี่ยวกับ การตั้งค่าการทำงานของ อุปกรณ์เครือข่ายที่ระดับระดับที่ 1-4 ได้แก่ Hub, Repeater, Bridge, Switch, Router, Layer 3 Switch และ Gateway
10. ความรู้เกี่ยวกับ การตั้งค่าการกำหนดเส้นทางเครือข่ายแบบ Static
11. ความรู้เกี่ยวกับ การตั้งค่าการกำหนดเส้นทางเครือข่ายแบบ Dynamic
12. ความรู้เกี่ยวกับ การแบ่งกลุ่มของอุปกรณ์สวิตช์ ได้แก่ การทำ Spanning Tree Protocol, Virtual Local Area Network
13. ความรู้เกี่ยวกับ การแบ่งกลุ่มของอุปกรณ์สวิตช์ ได้แก่ VLAN Trunking Protocol, InterVLAN Routing และ Load Balancing

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมินและควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน
2. ผลจากการทดสอบภาคปฏิบัติ

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่มีการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์
3. ทดสอบโดยใช้แบบปฏิบัติ

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ไม่มี

(ข) คำอธิบายรายละเอียด

1. ตั้งค่าอุปกรณ์เครือข่ายที่ Repeater, Bridge, Switch, Router, Layer 3 Switch
2. ตั้งค่าอุปกรณ์เครือข่ายที่ Gateway ในระดับพอร์ทเชื่อมต่อ และโปรโตคอล ตามแผนผังเครือข่าย
3. ทดสอบฟังก์ชันการทำงานของเครือข่ายตามแผนผังเครือข่าย

4. บันทึกสำรองข้อมูลการตั้งค่า
5. กำหนดกระบวนการในการทดสอบการทำงานของ เครือข่ายตามแผนผังเครือข่าย
6. ทดสอบประสิทธิภาพการทำงาน
7. ทำรายงานสรุปผลการทดสอบของทุกอุปกรณ์ในระบบเครือข่าย

16. หน่วยสมรรถนะรวม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 40104.01 ตั้งค่าการทำงาน ให้ทำงานได้ตามแผนผังเครือข่ายให้ทำการทดสอบโดยใช้แบบข้อเขียน แบบสัมภาษณ์และแบบปฏิบัติ
2. สมรรถนะย่อย 40104. 02 ทดสอบการใช้งานอุปกรณ์เครือข่ายให้ทำงานได้ตามแผนผังเครือข่ายให้ทำการทดสอบโดยใช้แบบข้อเขียน แบบสัมภาษณ์และแบบปฏิบัติ

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

1. รหัสหน่วยสมรรถนะ 40106
2. ชื่อหน่วยสมรรถนะ ติดตั้งและสนับสนุนการใช้งานระบบปฏิบัติการ การและซอฟต์แวร์ที่ให้บริการในระบบเครือข่าย
3. ทบทวนครั้งที่ 1 / -
4. สร้างใหม่ ☐ ปรับปรุง ☒
5. สำหรับอาชีพและรหัสอาชีพ (Occupational Classification)
6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)
- เป็นผู้ที่สามารถติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่าย ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศ

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☒	☐	☐	☐

8. กลุ่มอาชีพ (Sector)

ผู้ประกอบการวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2523 ผู้ประกอบวิชาชีพด้านเครือข่ายคอมพิวเตอร์

3513 ช่างเทคนิคด้านเครือข่ายและระบบคอมพิวเตอร์

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
40106.01 ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่าย	1.1 ติดตั้งการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่ายให้ใช้งาน 1.2 สนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่ายให้ใช้งาน	ข้อสอบข้อเขียน การสัมภาษณ์
40106.02 ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศ	2.1 ติดตั้งการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศให้ใช้งาน 2.2 สนับสนุนด้านเทคนิคการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศให้ใช้งาน	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

- 1.ความสามารถในการติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่ายให้ใช้งานได้
- 2.ความสามารถในการด้านเอกสารเอกสารแสดงการติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศได้
- 3.ความสามารถทักษะการให้คำปรึกษาด้านเทคนิคการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศได้

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับ แบบจำลอง OSI 7 เลเยอร์
 - 1.1 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 1 The Physical Layer เช่น อุปกรณ์ที่ใช้ในการเชื่อมต่อ เช่น สายเคเบิล Lanสายไฟฟ้า หรือ Connector ต่าง ๆ
 - 1.2 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 2 The Data Link Layer สื่อกลางของการส่งข้อมูล เช่น ระบุหมายเลข addressของอุปกรณ์ต่างๆ ที่เรียกว่า MAC Address
 - 1.3 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 3 The Network Layer โปรโตคอล ต่าง ๆ เช่น IP, Novell's IPX, IBM's APPN, Apple talk
 - 1.4 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 4 The Transport Layer การแบ่งข้อมูลใน Layer ต่าง ๆ ให้เหมาะสม กับการใช้งาน ซึ่งเรียกว่า Segmentation protocol ในชั้นนี้คือ TCP, UDP, SPX
 - 1.5 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 5 The Session Layer ซึ่งเป็นตัวควบคุมการส่งผ่านข้อมูลการสื่อสาร จากต้นทางไปยังปลายทาง โดยไม่เกิดผลกระทบต่ออินเตอร์เฟสต่าง ๆ
 - 1.6 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 6 The Presentation Layer ซึ่งแสดงผลออกมาในรูปของ ภาพต่าง ๆ ที่สามารถมองเห็นได้ เช่น รูปภาพ ที่ปรากฏบนจอคอมพิวเตอร์ และอาจจะรวมไปถึง การส่งผ่านข้อมูลต่าง ๆ ในรูปแบบของตัวโปรแกรม ที่มีการเข้ารหัส เป็นต้น
- 1.7 ความรู้เกี่ยวกับ แบบจำลอง เลเยอร์ 7 The Application Layer เป็นส่วนของการแสดงผล จากตัวโปรแกรมต่างๆ ที่มีการส่งผ่านข้อมูล ทางอินเตอร์เน็ต หรือเป็นโปรแกรมที่ใช้ในการโอนถ่ายข้อมูล ระหว่างเครือข่ายของ protocol
2. ความรู้เกี่ยวกับ ชุดโปรโตคอล TCP/IP
3. ความรู้เกี่ยวกับ ระบบปฏิบัติการ Windows, Windows Server, Unix, Mac OS และ Linux
4. ความรู้เกี่ยวกับ โปรแกรมประยุกต์ที่ให้บริการระบบสารสนเทศ

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และ ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ได้รับการประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งทนายสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ไม่มี

(ข) คำอธิบายรายละเอียด

1. ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่ายให้ใช้งานได้มีประสิทธิภาพได้แก่

- Domain Name Service (DNS)

- Network Time Protocol (NTP)
- Windows Internet Name Service (WINS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- World Wide Web
- Mail Server
- Web Proxy/Cache
- Active Directory/LDAP
- RADIUS Server
- คอมพิวเตอร์แม่ข่ายฐานข้อมูล
- คอมพิวเตอร์แม่ข่ายโปรแกรมประยุกต์

2. ให้คำปรึกษาด้านเทคนิคการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่ายให้ใช้งานได้มีประสิทธิภาพ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 40106.01 ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านเครือข่ายให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 40106.02 ติดตั้งและสนับสนุนการใช้งานคอมพิวเตอร์แม่ข่ายด้านระบบสารสนเทศให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

ตารางวิเคราะห์พฤติกรรมการเรียนรู้

รหัส 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย

ทฤษฎี 1 ชั่วโมง/สัปดาห์ ปฏิบัติ 4 ชั่วโมง/สัปดาห์ จำนวน 3 หน่วยกิต

[illegible]

หน่วยการเรียนรู้
รหัส 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย
ทฤษฎี 1 ชั่วโมง/สัปดาห์ ปฏิบัติ 4 ชั่วโมง/สัปดาห์ จำนวน 3 หน่วยกิต

หน่วย ที่	หน่วยการเรียนรู้	เวลาเรียน (ชม.)		
		ทฤษฎี	ปฏิบัติ	รวม
หน่วยที่ 1	งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย 1.1 วางแผนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย 1.2 เตรียมความพร้อมฮาร์ดแวร์และสื่อบันทึก 1.3 ติดตั้งโปรแกรมระบบปฏิบัติการเครื่องแม่ข่าย 1.4 ตรวจสอบการทำงานและการอัปเดตระบบ 1.5 จัดทำรายงานผลการติดตั้ง (ชิ้นงาน: รายงานผลการติดตั้งระบบ) 1.6 จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (ชิ้นงาน: ระบบปฏิบัติการเครื่องแม่ข่ายที่ติดตั้งสำเร็จ)	4	16	20
หน่วยที่ 2	งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น 2.1 วางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง 2.2 กำหนดค่าพื้นฐานของระบบและเครือข่าย 2.3 จัดการผู้ใช้งานและกลุ่มผู้ใช้งาน 2.4 กำหนดสิทธิ์การเข้าถึงทรัพยากรบนเครื่องแม่ข่าย 2.5 ตั้งค่าการควบคุมเครื่องแม่ข่ายระยะไกล 2.6 ตรวจสอบและบันทึกการตั้งค่าระบบ (ชิ้นงาน: แผนการจัดการผู้ใช้และสิทธิ์, รายงานการตั้งค่าระบบ) 2.7 จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (ชิ้นงาน: ระบบปฏิบัติการเครื่องแม่ข่ายที่ได้รับการบริหารจัดการเบื้องต้น)	4	16	20
หน่วยที่ 3	งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย 3.1 วิเคราะห์ความต้องการและออกแบบบริการเครือข่ายพื้นฐาน (DNS, DHCP, File/Resource Sharing) 3.2 วางแผน ติดตั้งและตั้งค่าบริการ DNS Server 3.3 วางแผน ติดตั้งและตั้งค่าบริการ DHCP Server 3.4 วางแผน ติดตั้งและตั้งค่าบริการ File and Resource Sharing Server 3.5 ทดสอบการทำงานของบริการโครงสร้างพื้นฐานเครือข่าย 3.6 จัดทำรายงานผลการให้บริการ (ชิ้นงาน: รายงานผลการให้บริการเครือข่ายพื้นฐาน) 3.7 จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (ชิ้นงาน: บริการเครือข่ายพื้นฐานที่ติดตั้งและทำงานได้)	4	16	20
หน่วยที่ 4	งานรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ 4.1 ประเมินความเสี่ยงและภัยคุกคามต่อระบบ	3	12	15

หน่วย ที่	หน่วยการเรียนรู้	เวลาเรียน (ชม.)		
		ทฤษฎี	ปฏิบัติ	รวม
	4.2 วางแผนการตั้งค่าและมาตรการความปลอดภัย 4.3 กำหนดการทำงานของ Firewall เบื้องต้น 4.4 สร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัย 4.5 ตั้งค่าการตรวจสอบยืนยันตัวตนและการอนุญาต (AAA Server) 4.6 ตรวจสอบและทดสอบมาตรการความปลอดภัย 4.7 จัดทำรายงานการประเมินความปลอดภัย (ชิ้นงาน: รายงานการประเมินความปลอดภัย, ระบบที่ได้รับการรักษาความปลอดภัย) 4.8 จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์			
	ประเมินผลสัมฤทธิ์การเรียนรู้ระดับรายวิชา ติดตั้งโปรแกรมระบบปฏิบัติการบนเครื่องแม่ข่าย การตั้งค่าพื้นฐานบน ระบบปฏิบัติการเครื่องแม่ข่าย จัดการรายละเอียดของผู้ใช้งานการกำหนดสิทธิ์ใช้ งาน การกำหนดการทำงานของ Firewall เบื้องต้น การควบคุมเครื่องแม่ข่าย ระยะไกลผ่านเครือข่าย	0	0	0
รวม		15	60	75

กิจกรรมการเรียนรู้การสอน

1. บทนำก่อนเข้าสู่บทเรียน อธิบายเนื้อหาหารายวิชา คำอธิบายรายวิชาและจุดประสงค์รายวิชา
2. สรุปและการประยุกต์บทเรียนตามเนื้อหาของแต่ละหน่วย
3. แบบฝึกหัด/ปฏิบัติ ประจำหน่วยการสอน
4. แบบประเมินผลการเรียนรู้

การวัดผลประเมินผล/ระดับคะแนน

รายละเอียดการวัดผล

การระหว่างหน่วยการเรียนรู้	20.....คะแนน
การสอบกลางภาค	คะแนน
การสอบปลายภาค	30.....คะแนน
บูรณาการคุณธรรม จริยธรรม และคุณลักษณะอันพึงประสงค์	20.....คะแนน
งานมอบหมาย/ รายงาน/กิจกรรม	30.....คะแนน
อื่น ๆ	คะแนน
รวม	100.....คะแนน

ระดับคะแนน

คะแนน 80 - 100	ระดับผลการเรียนระดับ	4
คะแนน 75 - 79	ระดับผลการเรียนระดับ	3
คะแนน 65 - 69	ระดับผลการเรียนระดับ	2.5
คะแนน 60 - 64	ระดับผลการเรียนระดับ	2
คะแนน 55 - 59	ระดับผลการเรียนระดับ	1.5
คะแนน 50 - 54	ระดับผลการเรียนระดับ	1
คะแนน 0 - 49	ระดับผลการเรียนระดับ	0

สื่อการเรียนการสอน/หนังสือเรียน/หนังสือประกอบ/แหล่งเรียนรู้เพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube Group Policy
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	แผนการจัดการเรียนรู้	หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 1-4
	ชื่อหน่วยการเรียนรู้ งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย	ทฤษฎี 4 ชม. ปฏิบัติ 16 ชม.
ชื่อเรื่อง/งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

จัดเตรียมติดตั้งและตรวจสอบระบบปฏิบัติการเครื่องแม่ข่ายให้พร้อมใช้งานพร้อมจัดทำรายงานผลการติดตั้งได้อย่างถูกต้อง

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
2. จัดเตรียม ติดตั้ง ตรวจสอบระบบปฏิบัติการเครื่องแม่ข่ายให้พร้อมใช้งาน และจัดทำรายงานผลการติดตั้ง

4. จุดประสงค์เชิงพฤติกรรม (เขียนให้ครบด้าน พุทธิพิสัย ทักษะพิสัย จิตพิสัย และ ประยุกต์ใช้)

4.1 พุทธิพิสัย

- 1) บอกส่วนประกอบและหลักการทำงานของระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
- 2) อธิบายขั้นตอนการเตรียมการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
- 3) เลือกใช้วิธีการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายให้เหมาะสมกับสถานการณ์ได้ถูกต้อง
- 4) ประเมินความเหมาะสมของการเลือกใช้ระบบปฏิบัติการเครื่องแม่ข่ายสำหรับงานเฉพาะได้ถูกต้อง

4.2 ทักษะพิสัย

- 1) จัดเตรียมเครื่องแม่ข่ายและอุปกรณ์ที่จำเป็นสำหรับการติดตั้งระบบปฏิบัติการได้ถูกต้อง
- 2) ติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายตามคู่มือได้ถูกต้อง
- 3) ตรวจสอบความพร้อมใช้งานของระบบปฏิบัติการเครื่องแม่ข่ายหลังการติดตั้งได้ถูกต้อง
- 4) จัดทำรายงานผลการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง

4.3 จิตพิสัย

- 1) มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

- 1) ประยุกต์ใช้ความรู้และทักษะในการจัดเตรียม ติดตั้ง และตรวจสอบระบบปฏิบัติการเครื่องแม่ข่ายเพื่อรองรับการให้บริการในระบบเครือข่ายได้อย่างมีประสิทธิภาพ

5. สารการเรียนรู้

- 5.1 บทบาท องค์ประกอบ รุ่น และรูปแบบการติดตั้ง Windows Server 2019
- 5.2 การวิเคราะห์ความต้องการและการจัดทำแผนติดตั้ง
- 5.3 การเตรียมฮาร์ดแวร์ เครื่องเสมือน ไฟล์ ISO และข้อมูลเครือข่าย
- 5.4 ขั้นตอนติดตั้ง Windows Server 2019
- 5.5 การกำหนดค่าหลังติดตั้งและการอัปเดตระบบ
- 5.6 การตรวจสอบความพร้อม การบันทึกหลักฐาน การรายงาน และการดูแลเครื่องมือ

6. กิจกรรมการเรียนรู้

1. ขั้นเตรียมความพร้อม

- 1.ครูตรวจสอบความพร้อมของห้องปฏิบัติการ เครื่องคอมพิวเตอร์ เครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการเรียน
- 2.ครูเตรียมสื่อการสอน ได้แก่ เอกสารประกอบการเรียน ใบงาน โปรแกรม VMware หรือ VirtualBox และไฟล์ติดตั้ง Windows Server 2019
- 3.ครูชี้แจงผลลัพธ์การเรียนรู้ สมรรถนะประจำหน่วย จุดประสงค์เชิงพฤติกรรม และเกณฑ์การวัดและประเมินผล
- 4.ครูเน้นย้ำเรื่องความปลอดภัยในการใช้งานอุปกรณ์คอมพิวเตอร์และการดูแลรักษาทรัพยากรส่วนรวม

2. ชี้นำเข้าสู่บทเรียน

- 1.ครูตั้งคำถามกระตุ้นความคิดเกี่ยวกับประสบการณ์ในการติดตั้งระบบปฏิบัติการที่ผู้เรียนเคยพบหรือเคยปฏิบัติ
- 2.ครูนำเสนอสถานการณ์ปัญหา เช่น การติดตั้งระบบปฏิบัติการผิดเวอร์ชัน หรือการเตรียมอุปกรณ์ไม่พร้อมจนส่งผลให้ระบบไม่สามารถใช้งานได้
- 3.ผู้เรียนร่วมอภิปรายถึงผลกระทบที่อาจเกิดขึ้นจากการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายที่ไม่ถูกต้อง

3. ขั้นให้เนื้อหา

- 1.ครูอธิบายความหมาย ความสำคัญ และหน้าที่ของระบบปฏิบัติการเครื่องแม่ข่าย
- 2.ครูอธิบายองค์ประกอบและหลักการทำงานของระบบปฏิบัติการเครื่องแม่ข่าย
- 3.ครูอธิบายขั้นตอนการวางแผนและการเตรียมความพร้อมก่อนการติดตั้ง
- 4.ครูสาธิตการตรวจสอบความต้องการของระบบ (System Requirements)
- 5.ครูอธิบายวิธีการสร้างสื่อบันทึกสำหรับติดตั้งและการตั้งค่า BIOS/UEFI
- 6.ครูสาธิตขั้นตอนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
- 7.ครูอธิบายวิธีตรวจสอบการทำงานหลังการติดตั้ง การอัปเดตระบบ และการจัดทำรายงานผลการติดตั้ง

4. ขั้นฝึกปฏิบัติ

1. ผู้เรียนสำรวจและตรวจสอบความพร้อมของเครื่องคอมพิวเตอร์หรือเครื่องเสมือน
2. ผู้เรียนจัดเตรียมสื่อบันทึกและตั้งค่าการบูตเครื่องสำหรับการติดตั้ง
3. ผู้เรียนดำเนินการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายตามคู่มือที่กำหนด
4. ผู้เรียนกำหนดค่าพื้นฐานของระบบ เช่น ชื่อเครื่อง รหัสผ่านผู้ดูแลระบบ และการตั้งค่าที่จำเป็น
5. ผู้เรียนตรวจสอบความพร้อมใช้งานของระบบหลังการติดตั้ง และดำเนินการอัปเดตระบบ
6. ผู้เรียนบันทึกภาพหน้าจอและจัดทำรายงานผลการติดตั้ง โดยระบุขั้นตอน ปัญหาที่พบ และแนวทางการแก้ไข
7. ครูให้คำแนะนำ ติดตาม และประเมินผลการปฏิบัติงานของผู้เรียนเป็นรายบุคคล

5. ขั้นสรุปและประเมินผล

1. ผู้เรียนร่วมกันสรุปองค์ความรู้เกี่ยวกับการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
2. ผู้เรียนสะท้อนผลการเรียนรู้ ปัญหาที่พบ และแนวทางพัฒนาการปฏิบัติงานของตนเอง
3. ผู้เรียนนำเสนอรายงานผลการติดตั้งและแลกเปลี่ยนความคิดเห็นภายในชั้นเรียน
4. ครูประเมินผลด้านความรู้ ทักษะปฏิบัติ และคุณลักษณะอันพึงประสงค์ตามเกณฑ์ที่กำหนด

7. สื่อและแหล่งเรียนรู้

- 7.1. ใบความรู้หน่วยที่ 1 และคู่มือใบงาน 1-4 ในเอกสารฉบับนี้
- 7.2. คอมพิวเตอร์ที่รองรับเทคโนโลยีเสมือน โปรแกรม VMware Workstation หรือ VirtualBox
- 7.3. ไฟล์ ISO Windows Server 2019 ที่ได้จากแหล่งถูกต้องตามลิขสิทธิ์ใช้งาน
- 7.4. เว็บไซต์ Microsoft Learn และ Microsoft Evaluation Center ที่ระบุในเอกสารอ้างอิง

8. หลักฐานการเรียนรู้

1. หลักฐานความรู้
คะแนนจากการทำแบบฝึกหัด และแบบทดสอบในหนังสือประกอบการเรียน
2. หลักฐานการปฏิบัติงาน
คะแนนการทำการกิจกรรมการเรียนรู้ และภาพถ่ายการทำการกิจกรรมของผู้เรียน

9. การวัดและประเมินผล

1. เกณฑ์การปฏิบัติงาน
ตอบคำถามหรือแบบทดสอบได้อย่างถูกต้อง ไม่น้อยกว่า 60%
ปฏิบัติตามขั้นตอนกิจกรรม และใช้เทคโนโลยีได้อย่างเหมาะสมถูกต้อง
เข้าร่วม สื่อสาร และร่วมมือกับสมาชิกในกลุ่มได้ดี มีความรับผิดชอบ
2. วิธีการประเมิน
แบบฝึกหัดหลังเรียน ตรวจสอบความเข้าใจในเนื้อหา
แบบทดสอบหลังเรียนถูกต้อง ไม่น้อยกว่า 60%
3. เครื่องมือประเมิน

แบบทดสอบหลังเรียน

10. บันทึกผลหลังจัดการเรียนรู้

1. ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

2. ปัญหา อุปสรรคที่พบ

3. การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

11. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบความรู้ ที่ 1	หน่วยที่ 1
	รหัสวิชา 20001-1005 ชื่อวิชาการใช้เทคโนโลยีดิจิทัลเพื่ออาชีพ	สอนครั้งที่ 1
	ชื่อหน่วยการเรียนรู้ งานใช้งานคอมพิวเตอร์	ทฤษฎี 2 ชม. ปฏิบัติ 2 ชม.
ชื่อเรื่อง/งานใช้งานคอมพิวเตอร์		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

จัดเตรียมติดตั้งและตรวจสอบระบบปฏิบัติการเครื่องแม่ข่ายให้พร้อมใช้งานพร้อมจัดทำรายงานผลการติดตั้งได้อย่างถูกต้อง

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
2. จัดเตรียม ติดตั้ง ตรวจสอบระบบปฏิบัติการเครื่องแม่ข่ายให้พร้อมใช้งาน และจัดทำรายงานผลการติดตั้ง

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

- 1) บอกส่วนประกอบและหลักการทำงานของระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
- 2) อธิบายขั้นตอนการเตรียมการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
- 3) เลือกใช้วิธีการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายให้เหมาะสมกับสถานการณ์ได้ถูกต้อง
- 4) ประเมินความเหมาะสมของการเลือกใช้ระบบปฏิบัติการเครื่องแม่ข่ายสำหรับงานเฉพาะได้ถูกต้อง

4.2 ทักษะพิสัย

- 1) จัดเตรียมเครื่องแม่ข่ายและอุปกรณ์ที่จำเป็นสำหรับการติดตั้งระบบปฏิบัติการได้ถูกต้อง
- 2) ติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายตามคู่มือได้ถูกต้อง
- 3) ตรวจสอบความพร้อมใช้งานของระบบปฏิบัติการเครื่องแม่ข่ายหลังการติดตั้งได้ถูกต้อง
- 4) จัดทำรายงานผลการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง

4.3 จิตพิสัย

- 1) มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ประยุกต์ใช้และรับผิดชอบ

- 1) ประยุกต์ใช้ความรู้และทักษะในการจัดเตรียม ติดตั้ง และตรวจสอบระบบปฏิบัติการเครื่องแม่ข่าย เพื่อรองรับการให้บริการในระบบเครือข่ายได้อย่างมีประสิทธิภาพ

5. เนื้อหาสาระ

- 5.1 บทบาท องค์ประกอบ รุ่น และรูปแบบการติดตั้ง Windows Server 2019
- 5.2 การวิเคราะห์ความต้องการและการจัดทำแผนติดตั้ง
- 5.3 การเตรียมฮาร์ดแวร์ เครื่องเสมือน ไฟล์ ISO และข้อมูลเครือข่าย
- 5.4 ขั้นตอนติดตั้ง Windows Server 2019
- 5.5 การกำหนดค่าหลังติดตั้งและการอัปเดตระบบ
- 5.6 การตรวจสอบความพร้อม การบันทึกหลักฐาน การรายงาน และการดูแลเครื่องมือ

1. ความหมายและบทบาทของระบบปฏิบัติการเครื่องแม่ข่าย

ระบบปฏิบัติการเครื่องแม่ข่าย (Server Operating System) เป็นซอฟต์แวร์หลักที่ควบคุม ฮาร์ดแวร์ จัดสรรหน่วยประมวลผล หน่วยความจำ พื้นที่จัดเก็บและการสื่อสารเครือข่ายพร้อมเป็นฐานให้บริการแก่ผู้ใช้ หรือเครื่องไคลเอนต์หลายเครื่อง เช่น การพิสูจน์ตัวตน การแจกที่อยู่ IP การแปลงชื่อโดเมน การจัดเก็บไฟล์ การพิมพ์ และเว็บเซิร์ฟเวอร์ความแตกต่างสำคัญจากระบบปฏิบัติการไคลเอนต์ไม่ได้อยู่เพียงหน้าต่างโปรแกรม แต่เป็นความสามารถในการให้บริการพร้อมกัน การควบคุมสิทธิ์แบบรวมศูนย์ การตรวจสอบเหตุการณ์ ความต่อเนื่องของบริการ และการบริหารจากระยะไกล ดังนั้นก่อนติดตั้งต้องกำหนดหน้าที่ของเครื่องให้ชัดเจน ไม่ควรเริ่มจากการกดติดตั้งโดยไม่มีแผน

1.1 องค์ประกอบที่เกี่ยวข้องกับการติดตั้ง

- ฮาร์ดแวร์หรือเครื่องเสมือน: CPU, RAM, Storage, Network Interface และเฟิร์มแวร์ BIOS/UEFI
- สื่อการติดตั้ง: ไฟล์ ISO, DVD หรือ USB Boot ที่ตรวจสอบแหล่งที่มาและความสมบูรณ์แล้ว
- ตัวติดตั้ง Windows Setup: ใช้เลือกภาษา รุ่น รูปแบบติดตั้ง ดิสก์ และสร้างระบบไฟล์
- ระบบหลังติดตั้ง: Server Manager, Windows Update, Device Manager, Event Viewer และเครื่องมือคำสั่ง
- ข้อมูลกำหนดค่า: ชื่อเครื่อง รหัสผ่านผู้ดูแล เขตเวลา ที่อยู่ IP, Subnet/Prefix, Gateway และ DNS

2. รุ่นและรูปแบบการติดตั้ง Windows Server 2019

2.1 Standard และ Datacenter

Windows Server 2019 Standard เหมาะกับสภาพแวดล้อมจริงที่มีการทำ Virtualization ไม่มาก และต้องการบทบาทบริการพื้นฐาน ส่วน Datacenter เหมาะกับศูนย์ข้อมูลที่มีเครื่องเสมือนจำนวนมาก และต้องการความสามารถระดับศูนย์ข้อมูลเพิ่มขึ้น การเลือกต้องพิจารณาหน้าที่ สิทธิ์ใช้งาน จำนวนเครื่องเสมือน และงบประมาณ ไม่ใช่เลือก Datacenter เพียงเพราะมีความสามารถมากกว่า

2.2 Server Core และ Server with Desktop Experience

ประเด็น	Server Core	Desktop Experience
ส่วนติดต่อ	ไม่มีเดสก์ท็อปแบบเต็ม จัดการด้วย SConfig, PowerShell หรือระยะไกล	มี GUI, Server Manager และเครื่องมือกราฟิก
ทรัพยากร/พื้นที่ผิวโจมตี	ติดตั้งองค์ประกอบน้อยกว่า จึงใช้พื้นที่และมีพื้นผิวโจมตีน้อยกว่า	มีองค์ประกอบมากกว่า ใช้งานง่ายสำหรับผู้เริ่มต้น
การใช้งานในชั้นเรียน	ใช้ศึกษาการบริหารด้วยคำสั่งหรือระยะไกล	เหมาะสำหรับฝึกครั้งแรกและสังเกตขั้นตอนได้ชัดเจน
ข้อควรจำ	ต้องวางแผนวิธีบริหารก่อนติดตั้ง	ไม่ควรติดตั้ง GUI หากไม่มีความจำเป็นในงานจริง

ข้อกำหนดของหน่วยนี้: ใช้ Windows Server 2019 Standard Evaluation (Desktop Experience) บนเครื่องเสมือน เพื่อให้ผู้เรียนเห็นขั้นตอนและเครื่องมือชัดเจน การใช้รุ่นประเมินต้องเป็นไปตามเงื่อนไขของ Microsoft

3. การวิเคราะห์ความต้องการและวางแผนติดตั้ง

แผนติดตั้งที่ดีต้องตอบคำถามว่า “ติดตั้งเพื่ออะไร ติดตั้งที่ใด ใช้ทรัพยากรเท่าใด ใช้เครือข่ายอย่างไร และจะพิสูจน์อย่างไรว่าพร้อมใช้งาน” ข้อมูลเหล่านี้ต้องบันทึกก่อนเริ่มงาน

3.1 ข้อมูลที่ต้องรวบรวม

หัวข้อ	รายละเอียดที่ต้องบันทึก
วัตถุประสงค์	บทบาทบริการที่คาดว่าจะติดตั้ง จำนวนผู้ใช้ ระดับความสำคัญ และช่วงเวลาให้บริการ
แพลตฟอร์ม	เครื่องจริงหรือเครื่องเสมือน โปรแกรม Virtualization และความเข้ากันได้ของ CPU
ทรัพยากร	จำนวน vCPU, RAM, ขนาดดิสก์ ชนิดดิสก์ และพื้นที่สำรอง
เครือข่าย	ชนิด Network Adapter, VLAN/วงเครือข่าย, IPv4, Prefix, Gateway และ DNS
ซอฟต์แวร์	รุ่น Windows Server รูปแบบ Core/Desktop Experience และไฟล์ ISO
ความปลอดภัย	รหัสผ่านผู้ดูแล การจำกัดการเข้าถึง แหล่ง ISO และแผนสำรอง/ย้อนกลับ
การทดสอบ	เงื่อนไขผ่าน เช่น บูตได้ ชื่อเครื่องถูก IP ถูก อัปเดตได้ และไม่มี Critical error

3.2 ความต้องการฮาร์ดแวร์และค่าฝึกปฏิบัติ

เอกสาร Microsoft ระบุค่าขั้นต่ำของ Windows Server ซึ่งเป็นเพียงจุดเริ่มต้น การใช้งานจริงต้องเพิ่มทรัพยากรตามบทบาทและภาระงาน สำหรับห้องเรียนนี้กำหนดค่าฝึกปฏิบัติที่สูงกว่าขั้นต่ำเพื่อให้ติดตั้งและใช้งาน GUI ได้เหมาะสม

รายการ	หลักพิจารณา	ค่าฝึกปฏิบัติที่แนะนำ
CPU	สถาปัตยกรรม x64 และเปิด Virtualization Technology	2 vCPU
RAM	ต้องเพียงพอกับ Desktop Experience และโปรแกรมบน Host	4 GB ต่อ VM
Storage	ระบบต้องมีพื้นที่ติดตั้ง อัปเดต และเก็บหลักฐาน	60 GB แบบ Dynamically allocated
Network	เลือกโหมดให้ตรงวัตถุประสงค์และไม่รบกวนเครือข่ายจริง	NAT หรือ Host-only ตามครูกำหนด
Display/อื่น ๆ	ใช้ค่ามาตรฐานของโปรแกรมเครื่องเสมือน	ค่าเริ่มต้นที่โปรแกรมรองรับ

ข้อควรระวัง: อย่านำค่าที่อยู่ IP ตัวอย่างไปใช้ในเครือข่ายจริงโดยไม่ตรวจสอบ เพราะอาจเกิด IP Address Conflict และกระทบผู้ใช้งาน ให้ใช้วงทดลองที่ครูกำหนดหรือเครือข่าย Host-only

4. การเตรียมเครื่องเสมือนและสื่อการติดตั้ง

4.1 ตรวจสอบเครื่อง Host

1. ตรวจสอบพื้นที่ว่างให้เพียงพอสำหรับไฟล์ VM และ Snapshot
2. ตรวจสอบว่าเปิด Intel VT-x/AMD-V หรือ Virtualization Technology ใน BIOS/UEFI แล้ว
3. ปิดโปรแกรมที่ใช้ RAM สูงและหลีกเลี่ยงการรัน VM เกินกำลังเครื่อง
4. กำหนดพอลเดอร์จัดเก็บงานตามชื่อผู้เรียนและสำรองไฟล์สำคัญก่อนเริ่ม

4.2 ตรวจสอบไฟล์ ISO

ไฟล์ ISO ควรมาจาก Microsoft หรือแหล่งที่สถานศึกษามีสิทธิ์ใช้งาน ระบุชื่อไฟล์ รุ่น ภาษา สถาปัตยกรรม และขนาดไฟล์ให้ชัดเจน หากผู้สอนให้ค่าแฮช ให้เปรียบเทียบค่าแฮชก่อนใช้งาน เพื่อยืนยันว่าไฟล์ไม่เสียหายหรือถูกเปลี่ยนแปลง

4.3 สร้างเครื่องเสมือน

1. เลือก Create a New Virtual Machine และกำหนดชนิดระบบเป็น Microsoft Windows Server 2019 (64-bit)
2. ตั้งชื่อ VM ตามรูปแบบ เช่น WS19-ชื่อผู้เรียน และเลือกตำแหน่งจัดเก็บที่มีพื้นที่เพียงพอ
3. กำหนด 2 vCPU, RAM 4 GB และดิสก์เสมือน 60 GB แบบขยายตามการใช้งาน
4. เลือก Network Adapter เป็น NAT หรือ Host-only ตามแผนของห้องปฏิบัติการ
5. เชื่อมต่อไฟล์ ISO กับอุปกรณ์ CD/DVD ของ VM และตั้งให้ Connect at power on
6. ตรวจสอบสรุปค่าก่อนเปิด VM แล้วบันทึกภาพหน้าจอเป็นหลักฐาน

5. ขั้นตอนการติดตั้ง Windows Server 2019

ขั้นตอนต่อไปนี้จะใช้กับการติดตั้งใหม่บนดิสก์เสมือนว่าง หากเป็นเครื่องจริงหรือมีข้อมูลเดิม ต้องสำรองข้อมูลและตรวจพาร์ทิชันอย่างรอบคอบ เพราะการลบหรือฟอร์แมตพาร์ทิชันอาจทำให้ข้อมูลสูญหาย

ขั้น	การปฏิบัติ
เริ่มต้นจาก ISO	เปิด VM และกดปุ่มเพื่อบูตจาก CD/DVD หากระบบร้องขอ ตรวจสอบว่าหน้าต่าง Windows Setup ปรากฏ
เลือกภาษาและแป้นพิมพ์	เลือกภาษาติดตั้ง รูปแบบเวลา และ Keyboard ให้เหมาะสม แล้วเลือก Install now
เลือกรุ่น	เลือก Windows Server 2019 Standard Evaluation (Desktop Experience) ให้ตรงกับแผน ห้ามเลือก Core โดยไม่ตั้งใจ
ยอมรับเงื่อนไข	อ่านเงื่อนไขสิทธิ์ใช้งานและเลือกยอมรับเมื่อได้รับอนุญาต

ขั้น	การปฏิบัติ
เลือกวิธีติดตั้ง	เลือก Custom: Install Windows only (advanced) สำหรับการติดตั้งใหม่
เลือกดิสก์	เลือกดิสก์เสมือนที่เตรียมไว้ ตรวจสอบขนาดให้ถูกต้อง แล้วให้ตัวติดตั้งสร้างพาร์ติชันที่จำเป็น
รอกัดลอกและรีสตาร์ท	ระบบจะคัดลอกไฟล์ ติดตั้งคุณลักษณะ และรีสตาร์ทหลายครั้ง ห้ามปิด VM หรือถอด ISO ระหว่างเขียนไฟล์
ตั้งรหัสผ่าน Administrator	กำหนดรหัสผ่านที่เป็นไปตามนโยบาย จดบันทึกในช่องทางปลอดภัย ไม่ใช่รหัสผ่านจริงลงในรายงาน
เข้าสู่ระบบครั้งแรก	ส่ง Ctrl+Alt+Delete ผ่านเมนูของโปรแกรม VM แล้วเข้าสู่ระบบด้วย Administrator

จุดตรวจหลังติดตั้ง: เข้าสู่ระบบได้, Server Manager เปิดได้, ไม่ค้างที่หน้าติดตั้ง, ดิสก์ระบบมองเห็นได้ และไม่ปรากฏอุปกรณ์สำคัญที่ไม่มีไดรเวอร์

6. การกำหนดค่าพื้นฐานหลังติดตั้ง

6.1 เปลี่ยนชื่อเครื่อง

ชื่อเครื่องควรสั้น อ่านความหมายได้ ไม่ซ้ำ และสอดคล้องมาตรฐานองค์กร เช่น BKT-WS19-01
หลีกเลี่ยงชื่อบุคคลที่เปลี่ยนผู้รับผิดชอบได้ง่าย หลังเปลี่ยนชื่อให้รีสตาร์ท และตรวจด้วยคำสั่ง hostname

6.2 กำหนดเขตเวลาและเวลา

ตั้ง Time zone เป็น (UTC+07:00) Bangkok, Hanoi, Jakarta และตรวจวันที่เวลาให้ถูกต้อง
เวลาไม่ตรงอาจทำให้บันทึกเหตุการณ์ การพิสูจน์ตัวตน ใบบรรอง และการวิเคราะห์ปัญหาคลาดเคลื่อน

6.3 กำหนด IPv4 แบบคงที่

เครื่องแม่ข่ายมักต้องมีที่อยู่คงที่เพื่อให้ไคลเอนต์และบริการอ้างอิงได้แน่นอน ค่าที่ต้องได้รับจากผู้ดูแลเครือข่าย ได้แก่ IP Address, Prefix length/Subnet mask, Default gateway และ DNS server ห้ามคาดเดาค่าเอง

รายการ	ตัวอย่างวงทลง	ความหมาย
IP Address	192.168.56.10	หมายเลขประจำเครื่องในวงทลง ต้องไม่ซ้ำ
Prefix/Subnet	/24 หรือ 255.255.255.0	กำหนดขอบเขตเครือข่ายเดียวกัน
Default Gateway	192.168.56.1	ทางออกไปยังเครือข่ายอื่น หากวงทลงมี Router
DNS Server	ตามที่ครูกำหนด	แปลงชื่อเป็น IP; ต้องสอดคล้องแผนบริการ

คำสั่งตรวจสอบที่ใช้ในหน่วยนี้

hostname — แสดงชื่อเครื่อง

ipconfig /all — แสดงการกำหนดค่าเครือข่ายโดยละเอียด

ping <IP เป้าหมาย> — ทดสอบการเข้าถึงปลายทาง (ต้องพิจารณา Firewall ประกอบ)

systeminfo — แสดงรุ่นระบบปฏิบัติการ ชนิดระบบ วันติดตั้ง และข้อมูลเครื่อง
Get-ComputerInfo — แสดงข้อมูลระบบด้วย PowerShell

7. การอัปเดตและตรวจสอบความพร้อมใช้งาน

7.1 Windows Update

เชื่อมต่อเครือข่ายตามที่ได้รับอนุญาต เปิด Windows Update ตรวจสอบรายการอัปเดต ติดตั้งและรีสตาร์ทเมื่อจำเป็น จากนั้นตรวจสอบว่างานไม่มีรายการสำคัญค้างอยู่ ต้องบันทึกวันเวลาและผลการอัปเดต เพราะการอัปเดตอาจเปลี่ยนสถานะระบบและต้องวางแผนช่วงหยุดบริการ

7.2 รายการตรวจสอบหลังติดตั้ง

ลำดับ	จุดตรวจ	หลักฐาน
1	เข้าสู่ระบบด้วยบัญชี Administrator ได้	ภาพหน้าจอเดสก์ท็อป/Server Manager
2	ชื่อเครื่องตรงแผน	ผล hostname
3	รุ่นและชนิดระบบตรงแผน	ผล systeminfo
4	IPv4, Prefix, Gateway และ DNS ถูกต้อง	ผล ipconfig /all
5	ติดต่อปลายทางที่กำหนดได้	ผล ping พร้อมคำอธิบาย
6	วันที่ เวลา และ Time zone ถูกต้อง	หน้าต่าง Date and Time
7	ตรวจสอบและติดตั้ง Update แล้ว	หน้า Windows Update และวันเวลา
8	Event Viewer ไม่มี Critical error ที่เกี่ยวกับการติดตั้ง	ภาพ/บันทึกเหตุการณ์ที่ตรวจ

7.3 การวิเคราะห์เมื่อทดสอบไม่ผ่าน

อาการ	สาเหตุที่เป็นไปได้	แนวทางตรวจสอบ
VM ไม่บูตจาก ISO	ISO ไม่ได้เชื่อมต่อ ลำดับบูตไม่ถูก หรือไฟล์เสีย	ตรวจ CD/DVD, Connect at power on, แหล่ง ISO และ Boot menu
เลือก Desktop Experience ไม่ได้	เลือก ISO/รุ่นไม่ตรง หรือเลือกรายการ Core	ย้อนตรวจชื่อ ISO และรายการ Edition ก่อนเริ่มติดตั้งใหม่
ติดตั้งค้าง/ช้ามาก	RAM/CPU/พื้นที่ Host ไม่พอ หรือดิสก์ช้า	ปิดโปรแกรมอื่น ตรวจพื้นที่ เพิ่มทรัพยากรอย่างเหมาะสม
ไม่มีเครือข่าย	Network Adapter ปิด โหมดเครือข่ายผิด หรือค่า IPv4 ผิด	ตรวจสอบสถานะ Adapter, NAT/Host-only และ ipconfig /all
Ping ไม่ผ่าน	ปลายทางไม่พร้อม คนละวง Gateway ผิด หรือ Firewall ปิดกั้น	แยกทดสอบ 127.0.0.1, IP ตนเอง, Gateway และปลายทางตามลำดับ

8. การจัดทำรายงานผลการติดตั้ง

รายงานไม่ใช่เพียงรวมภาพหน้าจอ แต่ต้องทำให้ผู้ตรวจสอบสามารถย้อนรอยได้ว่า ติดตั้งอะไร ด้วยค่าใด พบปัญหาใด แก้อย่างไร และระบบผ่านเงื่อนไขใด

1. ข้อมูลผู้ปฏิบัติ วันเวลา สถานที่ และเลขที่เครื่อง/ชื่อ VM
2. วัตถุประสงค์ ขอบเขต รุ่นระบบ และรูปแบบ Desktop Experience
3. ค่าทรัพยากรก่อนติดตั้ง: vCPU, RAM, Disk, Network และชื่อ ISO
4. ลำดับดำเนินงานพร้อมภาพหลักฐานที่มีคำบรรยายและหมายเลขภาพ
5. ตารางค่าหลังติดตั้ง: ชื่อเครื่อง รุ่นระบบ เวลา และเครือข่าย (ไม่เปิดเผยรหัสผ่าน)
6. ผลการทดสอบ จุดที่ผ่าน/ไม่ผ่าน ปัญหา สาเหตุ วิธีแก้ และผลหลังแก้
7. ข้อเสนอแนะสำหรับการนำไปใช้งานจริง และลายมือชื่อผู้ปฏิบัติ/ผู้ตรวจ

การรักษาความลับ: ห้ามบันทึกรหัสผ่านจริง Product Key ข้อมูลบัญชี หรือข้อมูลเครือข่ายที่เป็นความลับลงในภาพและรายงาน ให้ปิดบังข้อมูลที่ไม่จำเป็นก่อนส่งงาน

9. การจัดเก็บและดูแลรักษาเครื่องมือ

1. Shutdown ระบบปฏิบัติการก่อนปิด VM ไม่ใช้การปิดโปรแกรมแบบบังคับโดยไม่จำเป็น
2. ถอด/ยกเลิกการเชื่อมต่อ ISO หลังติดตั้งเพื่อป้องกันบูตเข้าตัวติดตั้งซ้ำ
3. ตั้งชื่อไฟล์ VM, Snapshot และรายงานให้เป็นมาตรฐาน ไม่ย้ายไฟล์ระหว่างที่ VM ทำงาน
4. ลบ Snapshot ที่ไม่จำเป็นตามนโยบาย เพราะใช้พื้นที่มากและไม่ใช้ระบบสำรองข้อมูลระยะยาว
5. คำนวณค่าการตั้งค่าห้องปฏิบัติการและจัดเก็บอุปกรณ์ตามจุดที่กำหนด

10. เอกสารอ้างอิง

Microsoft Learn. Hardware requirements for Windows Server.

<https://learn.microsoft.com/windows-server/get-started/hardware-requirements>

Microsoft Learn. Install Windows Server from installation media.

<https://learn.microsoft.com/windows-server/get-started/install-windows-server>

Microsoft Learn. Server Core vs Server with Desktop Experience install options.

<https://learn.microsoft.com/windows-server/get-started/install-options-server-core-desktop-experience>

Microsoft Learn. Configure a Server Core installation with SConfig.

<https://learn.microsoft.com/windows-server/administration/server-core/server-core-sconfig>

Microsoft Evaluation Center. Windows Server 2019.

<https://www.microsoft.com/evalcenter/evaluate-windows-server-2019>

สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน). อาชีพช่างสนับสนุนด้านเทคนิค ระดับ 5. <https://tpqi-net.tpqi.go.th/qualifications/2869>



1.1 วางแผนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย Windows Server



1. ความหมาย

การวางแผนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย (Windows Server) คือ การกำหนดขั้นตอนและทรัพยากรที่จำเป็น เพื่อให้การติดตั้งระบบเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และรองรับการให้บริการในระบบเครือข่ายได้อย่างเหมาะสม

2. วัตถุประสงค์

- ✓ เพื่อกำหนดความต้องการของระบบและทรัพยากรที่เหมาะสม
- ✓ เพื่อเลือกเวอร์ชันและรูปแบบการติดตั้งที่เหมาะสมกับงาน
- ✓ เพื่อวางแผนการจัดเก็บข้อมูลและความปลอดภัย
- ✓ เพื่อให้การติดตั้งเป็นไปอย่างราบรื่นและตรวจสอบได้
- ✓ เพื่อรองรับการให้บริการและการขยายระบบในอนาคต

3. ปัจจัยที่ต้องพิจารณาในการวางแผน

- 1 **วัตถุประสงค์การใช้งาน**
ระบุบทบาทและบริการที่เครื่องแม่ข่ายต้องให้บริการ เช่น Active Directory, File Server, Web Server, DHCP ฯลฯ
- 2 **เลือกเวอร์ชันของ Windows Server**
เลือกเวอร์ชันให้เหมาะสมกับความต้องการและงบประมาณ เช่น Windows Server 2019, 2022
- 3 **ความต้องการของระบบ (System Requirements)**
ตรวจสอบข้อกำหนดขั้นต่ำของฮาร์ดแวร์และซอฟต์แวร์
- 4 **ฮาร์ดแวร์และอุปกรณ์**
ตรวจสอบสเปกเครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล การ์ดเครือข่าย และอุปกรณ์สำรองไฟ (UPS)
- 5 **การจัดเก็บข้อมูล (Storage Plan)**
วางแผนการแบ่งพาร์ติชัน ระบบไฟล์ และพื้นที่สำหรับระบบ ข้อมูล และไฟล์สำรอง
- 6 **เครือข่าย (Network Plan)**
กำหนดชื่อเครื่องแม่ข่าย (Hostname), IP Address, Gateway, DNS และการเชื่อมต่อเครือข่าย
- 7 **ความปลอดภัยและการสำรองข้อมูล**
วางแผนการกำหนดสิทธิ์ การอัปเดตระบบ และการสำรอง/กู้คืนข้อมูล

4. ข้อกำหนดของระบบ (แนะนำขั้นต่ำ)

รายการ	Windows Server 2019/2022 (แนะนำขั้นต่ำ)
CPU	1.4 GHz 64-bit processor (แนะนำ 2 CPU ขึ้นไป)
RAM	2 GB (Server Core) 4 GB (Desktop Experience) แนะนำ 8 GB ขึ้นไป
พื้นที่ว่างบนดิสก์	32 GB ขึ้นไป (ควรมีพื้นที่ว่างเพิ่มเติมสำหรับอัปเดตและข้อมูล)
เครือข่าย	Ethernet Adapter 1 Gbps ขึ้นไป
อื่น ๆ	DVD Drive หรือ USB สำหรับติดตั้ง จอภาพ, คีย์บอร์ด, เมาส์



หมายเหตุ : ข้อกำหนดอาจเปลี่ยนแปลงตามรุ่นและบทบาทของเซิร์ฟเวอร์ ควรตรวจสอบข้อมูลล่าสุดจากเว็บไซต์ของ Microsoft

5. ขั้นตอนการวางแผนการติดตั้ง (โดยสังเขป)



6. ผลลัพธ์ที่ได้จากการวางแผนที่ดี

- ✓ ติดตั้งระบบได้รวดเร็ว ไม่เกิดข้อผิดพลาด
- ✓ ระบบทำงานได้เสถียรและปลอดภัย
- ✓ รองรับการให้บริการและการขยายระบบในอนาคต
- ✓ ลดค่าใช้จ่ายและเวลาในการแก้ไขปัญหา



7. แบบฟอร์มสรุปการวางแผน (ตัวอย่าง)

วัตถุประสงค์การใช้งาน	
เวอร์ชัน Windows Server	
บทบาทและบริการ	
ชื่อเครื่อง (Hostname)	
IP Address / Gateway / DNS	
พื้นที่จัดเก็บข้อมูล	
หน่วยงานที่รับผิดชอบ	
วันที่ติดตั้ง	



ข้อควรจำ

"การวางแผนที่ดี คือ จุดเริ่มต้นของระบบที่มีคุณภาพ"
ตรวจสอบความต้องการให้ครบถ้วน วางแผนรอบคอบ และบันทึกข้อมูลทุกขั้นตอน

สแกนเพื่อศึกษาข้อมูลเพิ่มเติม





ใบความรู้

1.2 เตรียมความพร้อมฮาร์ดแวร์และสื่อบันทึก สำหรับการติดตั้ง Windows Server



1. ความสำคัญ

การเตรียมความพร้อมของฮาร์ดแวร์และสื่อบันทึกที่ถูกต้อง จะช่วยให้การติดตั้ง Windows Server เป็นไปอย่างราบรื่น ลดปัญหาระหว่างการติดตั้ง และทำให้ระบบสามารถใช้งานได้ อย่างมีประสิทธิภาพและปลอดภัย

2. เตรียมความพร้อมฮาร์ดแวร์

2.1 ตรวจสอบสเปกและความต้องการของระบบ

รายการ	ขั้นต่ำ (แนะนำสำหรับ Windows Server 2019/2022)
CPU	1.4 GHz 64-bit processor (แนะนำ 2 CPU ขึ้นไป)
RAM	2 GB (Server Core) / 4 GB (Desktop Experience) แนะนำ 8 GB ขึ้นไป
พื้นที่ว่างบนดิสก์	32 GB ขึ้นไป (แนะนำแบบ SSD) ควรมีพื้นที่ว่างเพิ่มสำหรับอัปเดตและเก็บข้อมูล
เครือข่าย	Ethernet Adapter 1 Gbps ขึ้นไป
อื่น ๆ	DVD Drive หรือ USB Port (สำหรับติดตั้ง) จอภาพ, คีย์บอร์ด, เมาส์

2.2 ตรวจสอบอุปกรณ์

- ตรวจสอบการเชื่อมต่อสายไฟและระบบระบายความร้อน
- ตรวจสอบฮาร์ดดิสก์และสถานะ SMART (ถ้ามี)
- ตรวจสอบการทำงานของหน่วยความจำ (RAM)
- ตรวจสอบการ์ดเครือข่ายและพอร์ตเชื่อมต่อ
- ตรวจสอบอุปกรณ์สำรองไฟ (UPS) ให้พร้อมใช้งาน

3. เตรียมความพร้อมสื่อบันทึกสำหรับติดตั้ง

3.1 ดาวนโหลดไฟล์ติดตั้ง (ISO)

ดาวน์โหลดไฟล์ ISO ของ Windows Server จากเว็บไซต์ของ Microsoft (<https://www.microsoft.com/evalcenter>)



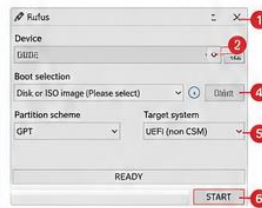
ตัวอย่างไฟล์ ISO

Windows_Server_2022.iso

3.2 สร้างสื่อบันทึกสำหรับติดตั้ง (แนะนำใช้ USB)

วิธีที่ 1 : ใช้โปรแกรม Rufus

1. เสียบ USB Flash Drive ขนาด 8 GB ขึ้นไป
2. เปิดโปรแกรม Rufus
3. เลือก Device : แฟลชไดรฟ์ที่เสียบอยู่
4. เลือก Boot selection : DISK or ISO image และเลือกไฟล์ .iso ที่ดาวน์โหลด
5. Partition scheme : GPT
Target system : UEFI (ไม่ใช่ CSM)
6. คลิก START เพื่อสร้างสื่อบันทึก



วิธีที่ 2 : ใช้โปรแกรม Media Creation Tool

1. ดาวน์โหลด Media Creation Tool จาก Microsoft
2. เลือก Create installation media for another PC
3. เลือกภาษา รุ่น และสถาปัตยกรรม
4. เลือก USB flash drive
5. รอให้โปรแกรมสร้างสื่อบันทึกเสร็จสิ้น



ข้อควรระวัง

- ควรใช้ USB แท้ คุณภาพดี และมีพื้นที่ว่างเพียงพอ
- สำรองข้อมูลใน USB ก่อนใช้งาน เพราะข้อมูลจะถูกลบ
- ตรวจสอบไฟล์ ISO ให้ถูกต้องและครบถ้วน

4. การตั้งค่า BIOS/UEFI สำหรับการติดตั้ง

1. เปิดเครื่องและกดปุ่มเข้าสู่ BIOS/UEFI (เช่น Del, F2, F10, Esc แล้วแต่รุ่น)
2. ตั้งค่าโหมดการทำงานเป็น UEFI
3. ปิดการทำงานของ Secure Boot ชั่วคราว (ถ้ามีปัญหาในการบูต)
4. ตั้งค่าลำดับการบูต (Boot Priority) ให้ USB/DVD เป็นอันดับแรก
5. บันทึกการตั้งค่า (Save & Exit)
6. บูตจากสื่อบันทึกเพื่อเริ่มการติดตั้ง

Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.		
Main	Advanced	Boot
Boot Configuration		Set the system boot order
UEFI Boot		[Enabled]
Secure Boot		[Disabled]
Boot Option Priorities		
Boot Option #1		[UEFI: USB Flash Drive]
Boot Option #2		[Hard Disk]
Boot Option #3		[UEFI: DVD/CDROM]
		T1 : Select Item
		Enter : Select
		+/- : Change Opt.
		F9 : Optimized Defaults
		F10 : Save & Exit
		ESC : Exit

5. ตรวจสอบความพร้อมก่อนติดตั้ง



- ✓ ตรวจสอบสื่อบันทึกว่าใช้งานได้ (ลองบูตเครื่องจาก USB)
- ✓ ตรวจสอบฮาร์ดแวร์ทั้งหมดพร้อมใช้งาน
- ✓ สำรองข้อมูลสำคัญก่อนเริ่มติดตั้ง
- ✓ เตรียมหาข้อมูลเครือข่าย เช่น IP Address, Gateway, DNS
- ✓ จด License Key (ถ้ามี) ให้พร้อมใช้งาน

6. สรุป

การเตรียมความพร้อมฮาร์ดแวร์และสื่อบันทึกที่ถูกต้อง จะช่วยให้การติดตั้ง Windows Server เป็นไปอย่างรวดเร็ว ปลอดภัย และลดปัญหาที่อาจเกิดขึ้นระหว่างการติดตั้ง



เคล็ดลับ ควรเตรียมแผนการสำรองข้อมูลและการกู้คืนระบบไว้ล่วงหน้า เพื่อความปลอดภัยของข้อมูลและระบบในระยะยาว

สแกนเพื่อดูขั้นตอนการสร้าง USB ติดตั้ง Windows Server เพิ่มเติม





1.3 ติดตั้งโปรแกรมระบบปฏิบัติการเครื่องแม่ข่าย (Windows Server)



การติดตั้ง Windows Server คือการติดตั้งระบบปฏิบัติการลงบนเครื่องแม่ข่าย เพื่อให้สามารถทำงานและให้บริการต่าง ๆ บนระบบเครือข่ายได้



1. เริ่มติดตั้ง (Boot from Install Media)

1. ใส่ USB/DVD ที่สร้างสื่อบันทึกสำหรับติดตั้ง Windows Server
2. เปิดเครื่อง และเข้า BIOS/UEFI ตั้งค่า Boot จาก USB/DVD
3. เมื่อบูตขึ้นมา จะปรากฏหน้าต่าง "Windows Setup"



2. เลือกภาษาและตั้งค่าเริ่มต้น

1. เลือก Language to install
2. เลือก Time and currency format
3. เลือก Keyboard or input method
4. คลิก Next



3. คลิก Install Now

คลิกปุ่ม Install Now เพื่อเริ่มการติดตั้ง



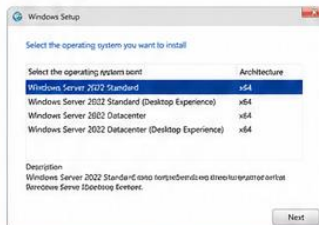
4. ใส่ Product Key

1. ใส่ Product Key ของ Windows Server
2. หากยังไม่มี โคลลิค "I don't have a product key"



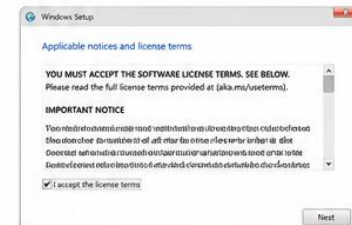
5. เลือก Edition ของ Windows Server

1. เลือก Edition ที่ต้องการติดตั้ง
2. คลิก Next



6. ยอมรับข้อตกลงการใช้งาน

1. ตี๊กที่ช่อง "I accept the license terms"
2. คลิก Next



7. เลือกประเภทการติดตั้ง (Installation Type)

- Upgrade: อัปเดตจากระบบเดิม

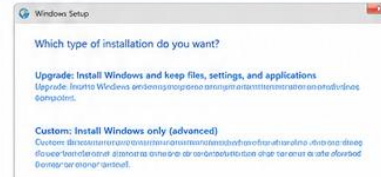
ใช้สำหรับอัปเดตจาก Windows Server เวอร์ชันเก่า (ข้อมูลและการตั้งค่าจะถูกเก็บไว้)

Upgrade: ติดตั้งทับของเดิม

- Custom: ติดตั้งใหม่ทั้งหมด (แนะนำ)

ใช้สำหรับติดตั้งใหม่ทั้งหมด (ข้อมูลเดิมจะถูกลบ)

Custom: ติดตั้งใหม่ทั้งหมด



8. เลือกพาร์ติชันสำหรับติดตั้ง

1. เลือกไดรฟ์หรือพื้นที่ว่าง (Unallocated Space)
2. คลิก New เพื่อตั้งพาร์ติชัน หรือเลือกไดรฟ์ที่ต้องการ
3. คลิก Next เพื่อเริ่มการติดตั้ง

Name	Total size	Free space	Type
Drive 0 Partition 1: System Reserved	100.0 MB	69.0 MB	System
Drive 0 Partition 2	59.4 GB	59.4 GB	Primary
Drive 0 Unallocated Space	40.0 GB	40.0 GB	

Refresh Delete Format New Load driver Extend Next

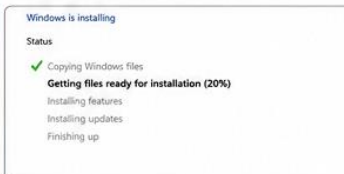
คำแนะนำการแบ่งพาร์ติชัน

พาร์ติชัน	ขนาดแนะนำ	ประเภท	ใช้สำหรับ
System Reserved	100-500 MB	System	สำหรับบูตระบบ
C: (OS)	50-100 GB ขึ้นไป	Primary	ติดตั้งระบบปฏิบัติการ
D: (Data)	ตามความต้องการ	Primary	เก็บข้อมูล
อื่น ๆ (ถ้ามี)	ตามความต้องการ	Primary/Logical	งานเฉพาะเพิ่มเติม

หมายเหตุ : ขนาดขึ้นอยู่กับความต้องการและพื้นที่ของดิสก์

9. เริ่มการติดตั้ง

- ระบบจะทำการคัดลอกไฟล์ ติดตั้งฟิเจอร์ และติดตั้งอุปกรณ์อัตโนมัติ
- อาจใช้เวลามากขึ้นหากเครื่องหรือฮาร์ดแวร์หลายตัว
- ห้ามปิดเครื่องหรือถอดสื่อบันทึกในระหว่างการติดตั้ง



10. ตั้งค่าหลังติดตั้ง

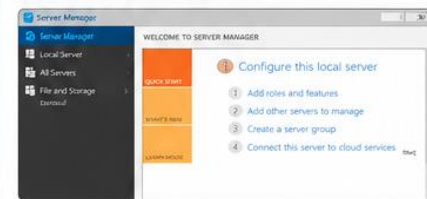
หลังจากติดตั้งเสร็จ ระบบจะให้ตั้งค่าพื้นฐานดังนี้

- ตั้งรหัสผ่าน Administrator
- ตั้งชื่อคอมพิวเตอร์ (Computer name)
- ตั้งค่าเครือข่าย (Network)
- ตั้งค่า Time zone
- ตั้งค่าความเป็นส่วนตัวและการอัปเดต



11. เสร็จสิ้นการติดตั้ง

เมื่อเข้าสู่หน้าจอ Desktop หรือ Server Manager แสดงว่าติดตั้ง Windows Server สำเร็จแล้ว



ข้อควรระวัง

- ตรวจสอบความเข้ากันได้ของฮาร์ดแวร์กับ Windows Server ก่อนติดตั้ง
- สำรองข้อมูลสำคัญก่อนติดตั้ง
- ควรใช้สื่อบันทึกที่ถูกต้องและเป็นเวอร์ชันลิขสิทธิ์

สรุป



ใบความรู้ (INFORMATION SHEET) | รหัสวิชา: 31901-2002 | ชื่อวิชา: ระบบปฏิบัติการเครื่องแม่ข่าย
หน่วยที่ 1: งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย | หัวข้อเรื่อง: 1.4 ตรวจสอบการทำงานและอัปเดตระบบ



1.4 การตรวจสอบการทำงานและการอัปเดตระบบ (OPERATIONAL CHECKING & SYSTEM UPDATES)

1. การตรวจสอบสถานะการทำงานของฮาร์ดแวร์และระบบ (Operational Status of Hardware & System)



1.1 ตรวจสอบไดรเวอร์ (Device Drivers)

ยืนยันความถูกต้องของไดรเวอร์อุปกรณ์ทั้งหมด
(Device Manager, lspci, lsusb)



1.2 ตรวจสอบการตั้งค่าเครือข่าย (Network Settings)

ตั้งค่า Static IP, Subnet Mask, Gateway, DNS
(ipconfig /ip a) - ทดสอบการเชื่อมต่อ (ping)



1.3 ตรวจสอบการทำงานของบริการพื้นฐาน (Resource Usage) (Basic Services) เบื้องต้น

ตรวจสอบบริการที่เปิดทำงาน
(System Services, systemctl status)



ดูการใช้ CPU, RAM, Disk Space
(Task Manager, htop, df -h)

2. การอัปเดตระบบปฏิบัติการ (System Update & Patching)

ข้อควรระวัง
สำรองข้อมูล (Backup)
ก่อนทำ เสมอ!



2.1 ตรวจสอบรายการอัปเดต (Check for Updates)



สแกนหา Patch และอัปเดตใหม่ๆ
(Windows Update, sudo apt update)

2.2 ติดตั้งการอัปเดต (Install Updates)



ดาวน์โหลดและติดตั้งการอัปเดต
(Install Patches, sudo apt upgrade)

2.3 รีสตาร์ทและยืนยันการทำงาน (Restart & Verify)



รีสตาร์ทระบบหลังติดตั้ง
และตรวจสอบการทำงาน
(System Status, No Errors)



ตารางสรุปขั้นตอน: 1. เข้าสู่ระบบผู้ดูแลระบบ 2. ตรวจสอบไดรเวอร์ 3. ตั้งค่า Static IP 4. อัปเดตระบบ 5. บันทึกผล

จัดทำโดย: กลุ่มสาระการเรียนรู้เทคโนโลยีสารสนเทศและการสื่อสาร

ใบความรู้ (INFORMATION SHEET) | รหัสวิชา: 31901-2002 | ชื่อวิชา: ระบบปฏิบัติการเครื่องแม่ข่าย
หน่วยที่ 1: งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย | หัวข้อเรื่อง: 1.4 ตรวจสอบการทำงานและอัปเดตระบบ



1.5 จัดทำรายงานผลการติดตั้ง

1. การตรวจสอบสถานะการทำงานของฮาร์ดแวร์และระบบ (Operational Status of Hardware & System)



1.1 ตรวจสอบไดรเวอร์ (Device Drivers)

ยืนยันความถูกต้องของไดรเวอร์อุปกรณ์ทั้งหมด (Device Manager, lspci, lsusb)



1.2 ตรวจสอบการตั้งค่าเครือข่าย (Network Settings)

ตั้งค่า Static IP, Subnet Mask, Gateway, DNS (ipconfig /ip a) - ทดสอบการเชื่อมต่อ (ping)



1.3 ตรวจสอบการทำงานของบริการพื้นฐาน (Resource Usage) (Basic Services) เบื้องต้น

ตรวจสอบบริการที่เปิดทำงาน (System Services, systemctl status)



ดูการใช้ CPU, RAM, Disk Space (Task Manager, htop, df -h)

2. การอัปเดตระบบปฏิบัติการ (System Update & Patching)

ข้อควรระวัง
สำรองข้อมูล (Backup) ก่อนทำ เสมอ!



2.1 ตรวจสอบรายการอัปเดต (Check for Updates)

2.2 ติดตั้งการอัปเดต (Install Updates)

2.3 รีสตาร์ทและยืนยันการทำงาน (Restart & Verify)

ปัญหาที่พบและการแก้ไข : อีเมลรายงานผลการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย, การตรวจสอบการกดปุ่มเปิดของปัญหาและการแก้ไข และทำการตรวจสอบและการทดสอบ

Kennelly

Technical Support Specialist
Technical Support Specialist

วิมลจิต

Department Supervisor
Department Supervisor

วันที่ 24 ก.พ. 2022



ตารางสรุปขั้นตอน: 1. เข้าสู่ระบบผู้ดูแลระบบ 2. ตรวจสอบไดรเวอร์ 3. ตั้งค่า Static IP 4. อัปเดตระบบ 5. บันทึกผล

จัดทำโดย: กลุ่มสาระการเรียนรู้เทคโนโลยีสารสนเทศและการสื่อสาร

ใบความรู้ (INFORMATION SHEET) | รหัสวิชา: 31901-2002 | ชื่อวิชา: ระบบปฏิบัติการเครื่องแม่ข่าย
หน่วยที่ 1: งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย | หัวข้อเรื่อง: 1.4 ตรวจสอบการทำงานและอัปเดตระบบ



1.6 การจัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (Storage and Maintenance of Tools & Equipment)

1. การตรวจสอบสถานะการทำงานของฮาร์ดแวร์และระบบ (Operational Status of Hardware & System)



1.6.1 การจัดเก็บเซิร์ฟเวอร์ (Server Storage)
จัดเก็บเซิร์ฟเวอร์ในที่ที่ปลอดภัย ปราศจากฝุ่น
(Device Manager, lspci, lsusb)

1.6.2 ตรวจสอบการตั้งค่าเครือข่าย (Network Settings)
ตั้งค่า Static IP, Subnet Mask, Gateway, DNS
(ipconfig /ip a) - ทดสอบการเชื่อมต่อ (ping)

1.3 ตรวจสอบการทำงานของบริการพื้นฐาน (Resource Usage)
(Basic Services)
เบื้องต้น



ตรวจสอบบริการที่เปิดทำงาน
(System Services, systemctl status)



ดูการใช้ CPU, RAM, Disk Space
(Task Manager, htop, df -h)

2. การอัปเดตระบบปฏิบัติการ (System Update & Patching)

ข้อควรระวัง
สำรองข้อมูล (Backup)
ก่อนทำ เสมอ!



2.1 ตรวจสอบรายการอัปเดต
(Check for Updates)



สแกนหา Patch และอัปเดตใหม่ๆ
(Windows Update, sudo apt update)

2.2 ติดตั้งการอัปเดต
(Install Updates)



ดาวน์โหลดและติดตั้งการอัปเดต
(Install Patches, sudo apt upgrade)

2.3 รีสตาร์ทและยืนยันการทำงาน
(Restart & Verify)



รีสตาร์ทระบบหลังติดตั้ง
และตรวจสอบการทำงาน
(System Status, No Errors)



ตารางสรุปขั้นตอน: 1. เข้าสู่ระบบผู้ดูแลระบบ 2. ตรวจสอบไดเรกทอรี 3. ตั้งค่า Static IP 4. อัปเดตระบบ 5. บันทึกผล

จัดทำโดย: กลุ่มสาระการเรียนรู้เทคโนโลยีสารสนเทศและการสื่อสาร

6. แบบฝึกหัด

แบบฝึกหัดหน่วยที่ 1

1. ข้อใดอธิบายบทบาทของระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้องที่สุด
 - ก. ใช้สร้างเอกสารของผู้ใช้คนเดียวเท่านั้น
 - ข. จัดการทรัพยากรและให้บริการแก่ไคลเอนต์หลายเครื่อง
 - ค. ใช้แทนสวิตช์เครือข่ายทุกกรณี
 - ง. ทำหน้าที่เป็นสื่อบันทึกข้อมูล
2. หากผู้เรียนต้องการเห็น GUI และ Server Manager ระหว่างฝึก ควรเลือกรูปแบบใด
 - ก. Server Core
 - ข. Nano Server
 - ค. Server with Desktop Experience
 - ง. Recovery Console
3. สิ่งใดควรกำหนดก่อนเริ่มติดตั้งมากที่สุด
 - ก. สีพื้นหลังเดสก์ท็อป
 - ข. วัตถุประสงค์ บทบาท ทรัพยากร และเครือข่าย
 - ค. โปรแกรมเกมที่จะติดตั้ง
 - ง. ชื่อภาพหน้าจอหลังทำงานเสร็จ
4. ค่าฝึกปฏิบัติใดสอดคล้องกับใบความรู้นี้
 - ก. 1 vCPU, RAM 512 MB, Disk 10 GB
 - ข. 2 vCPU, RAM 4 GB, Disk 60 GB
 - ค. 8 vCPU, RAM 64 GB, Disk 2 TB เท่านั้น
 - ง. ไม่ต้องกำหนดทรัพยากร
5. เหตุใดต้องตรวจสอบแหล่งที่มาของไฟล์ ISO
 - ก. เพื่อให้ชื่อไฟล์สั้นลง
 - ข. เพื่อยืนยันสิทธิ์ ความสมบูรณ์ และลดความเสี่ยงไฟล์ถูกเปลี่ยนแปลง
 - ค. เพื่อเพิ่ม RAM ให้ VM
 - ง. เพื่อเปลี่ยน IP อัตโนมัติ
6. ในการติดตั้งใหม่บนดิสก์เสมือนว่างควรเลือกวิธีใด
 - ก. Upgrade โดยไม่ตรวจระบบเดิม
 - ข. Custom: Install Windows only (advanced)
 - ค. Repair your computer เท่านั้น
 - ง. Exit Setup
7. หลังเปลี่ยนชื่อเครื่อง คำสั่งใดใช้ตรวจสอบชื่อได้
 - ก. format
 - ข. hostname
 - ค. del
 - ง. diskpart clean

8. ข้อมูลใดจำเป็นสำหรับ IPv4 แบบคงที่
 - ก. IP, Prefix/Subnet, Gateway และ DNS
 - ข. ชื่อผู้เรียนและเลขที่
 - ค. Product Key และรหัสผ่านเท่านั้น
 - ง. สีของสาย LAN
9. คำสั่งใดแสดงรายละเอียดการกำหนดค่าเครือข่าย
 - ก. ipconfig /all
 - ข. shutdown /s
 - ค. notepad
 - ง. calc
10. ข้อใดเป็นหลักฐานที่ดีในรายงานผลการติดตั้ง
 - ก. ภาพจำนวนมากโดยไม่มีคำบรรยาย
 - ข. รหัสผ่าน Administrator จริง
 - ค. ผลทดสอบพร้อมวันเวลา ค่าที่ตรวจ และคำอธิบาย
 - ง. คัดลอกข้อความจากผู้อื่น

ตอนที่ 2 คำถามอัตนัย (5 ข้อ)

1. เปรียบเทียบ Server Core กับ Server with Desktop Experience และระบุเหตุผลที่หน่วยนี้เลือก Desktop Experience

.....

.....

.....

2. จากสถานการณ์ “สำนักงาน 30 ผู้ใช้ ต้องการเครื่องแม่ข่ายสำหรับทดลองบริการไฟล์” จงระบุข้อมูลอย่างน้อย 6 รายการที่ต้องเก็บก่อนวางแผนติดตั้ง

.....

.....

.....

3. อธิบายขั้นตอนติดตั้ง Windows Server 2019 ตั้งแต่เปิด VM จนเข้าสู่ระบบครั้งแรกอย่างเป็นลำดับ

.....

.....

.....

4. อธิบายวิธีตั้งค่าและตรวจสอบชื่อเครื่อง เวลา และ IPv4 หลังติดตั้ง พร้อมระบุคำสั่งตรวจสอบ

.....

.....

.....

5. ออกแบบรายการหลักฐานอย่างน้อย 6 รายการสำหรับรายงานผลการติดตั้ง โดยคำนึงถึงการรักษาความลับ

.....

.....

.....

7. เอกสารอ้างอิง

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

8. ภาคผนวก

8.1 เฉลย แบบฝึกหัดบทเรียนที่ 1

เฉลยแบบฝึกหัด ตอนที่ 1

ข้อ	1	2	3	4	5	6	7	8	9	10
คำตอบ	ข	ค	ข	ข	ข	ข	ข	ก	ก	ค

แนวคำตอบแบบฝึกหัด ตอนที่ 2

ข้อ	แนวคำตอบสำคัญ
1	Server Core ไม่มี GUI แบบเต็ม จัดการด้วย SConfig/PowerShell/ระยะไกล ใช้องค์ประกอบน้อยกว่า; Desktop Experience มี GUI และ Server Manager หน่วยนี้เลือกแบบหลังเพื่อให้ผู้เริ่มต้นเห็นขั้นตอนและเครื่องมือชัดเจน
2	วัตถุประสงค์/บทบาท, จำนวนผู้ใช้, แพลตฟอร์มจริงหรือ VM, CPU/RAM/Disk, รุ่นและรูปแบบติดตั้ง, ข้อมูล IP/Prefix/Gateway/DNS, ความปลอดภัย, ช่วงเวลา และเกณฑ์ทดสอบ
3	เชื่อมต่อ ISO และบูต → เลือกภาษา → Install now → เลือก Standard Evaluation (Desktop Experience) → ยอมรับเงื่อนไข → Custom → ตรวจสอบและเลือกดิสก์ → รอคัดลอก/รีสตาร์ท → ตั้งรหัสผ่าน Administrator → เข้าสู่ระบบ
4	เปลี่ยนชื่อและรีสตาร์ท ตรวจสอบด้วย hostname; ตั้ง UTC+07:00; กำหนด IPv4/Prefix/Gateway/DNS ตามแผน ตรวจสอบด้วย ipconfig /all และทดสอบ ping ตามลำดับ
5	ควรมีข้อมูลผู้ปฏิบัติ/วันเวลา, แผนและค่าทรัพยากร, รุ่น/รูปแบบติดตั้ง, ภาพลำดับขั้น, ค่าหลังติดตั้ง, ผลทดสอบ, ปัญหา-สาเหตุ-วิธีแก้-ผลหลังแก้ และปิดบังรหัสผ่าน/Product Key/ข้อมูลลับ

	ใบงานที่ 1		หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย		สอนครั้งที่ 1
	ชื่อหน่วยการเรียนรู้ งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย		ทฤษฎี 1 ชม.
	ชื่อเรื่อง/งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย		ปฏิบัติ 4 ชม.

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

ผู้เรียนสามารถวางแผน จัดเตรียม ติดตั้ง กำหนดค่าพื้นฐาน ตรวจสอบ และอัปเดต Windows Server 2019 ให้พร้อมใช้งานบนเครื่องเสมือน พร้อมจัดทำรายงานผลการติดตั้ง ที่มีหลักฐานครบถ้วนได้อย่างถูกต้องและปลอดภัย

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. วิเคราะห์ความต้องการและวางแผนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
2. จัดเตรียมฮาร์ดแวร์ เครื่องเสมือน ไฟล์ ISO และข้อมูลเครือข่ายสำหรับการติดตั้ง
3. Windows Server 2019 ตามแผนและข้อกำหนดที่ได้รับ
4. พื้นฐาน อัปเดต และตรวจสอบความพร้อมใช้งานของระบบ
5. บันทึกหลักฐาน วิเคราะห์ปัญหา และจัดทำรายงานผลการติดตั้ง

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. วิเคราะห์ข้อกำหนดด้านฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และความปลอดภัยก่อนติดตั้งได้
2. อธิบายลำดับการติดตั้ง การตั้งค่าพื้นฐาน การอัปเดต และการตรวจสอบระบบได้

4.2 ทักษะพิสัย

1. สร้างและกำหนดทรัพยากรเครื่องเสมือนสำหรับ Windows Server 2019 ได้เหมาะสม
2. ติดตั้ง Windows Server 2019 แบบ Desktop Experience บนเครื่องเสมือนได้สำเร็จ
3. กำหนดชื่อเครื่อง เขตเวลา ที่อยู่ IPv4 และการอัปเดตระบบได้
4. ตรวจสอบสถานะระบบและจัดทำรายงานพร้อมภาพหลักฐานได้ครบถ้วน

4.3 จิตพิสัย

1. ปฏิบัติงานด้วยความรอบคอบ รับผิดชอบ ซื่อสัตย์ต่อหลักฐาน ใช้ทรัพยากรอย่างคุ้มค่า และปฏิบัติตามข้อกำหนดความปลอดภัยของห้องปฏิบัติการ

4.4 ประยุกต์ใช้และรับผิดชอบ

1. เลือกใช้งานอุปกรณ์ได้อย่างเหมาะสม ปฏิบัติงานด้วยความรับผิดชอบ รอบคอบ และรักษาความปลอดภัยในการทำงาน

5. เครื่องมือ วัสดุ และอุปกรณ์

- 1.คอมพิวเตอร์ Host ที่รองรับ Virtualization
- 2.VMware Workstation หรือ VirtualBox
- 3.ไฟล์ ISO Windows Server 2019 จากแหล่งที่ได้รับอนุญาต
- 4.ข้อมูลวงเครือข่ายทดลองและใบความรู้

6. คำแนะนำ/ข้อควรระวัง

- 1.สำรองข้อมูลสำคัญและตรวจพื้นที่ว่างก่อนสร้างดิสก์เสมือน
- 2.ใช้ไฟล์ ISO จากแหล่งที่สถานศึกษาอนุญาต และตรวจสอบชื่อรุ่น ภาษา สถาปัตยกรรม
- 3.และค่าแฮชเมื่อผู้สอนกำหนด
- 4.ห้ามคัดลอกหรือใช้ IP ของเครือข่ายจริงเอง และห้ามเปิดเผย Product Key หรือข้อมูลบัญชีในภาพหลักฐาน
- 5.ห้ามเปิด VM ก่อนผู้สอนตรวจแผนและค่าทรัพยากร เพราะอาจทำให้เครื่อง Host ทำงานเกินกำลัง

7. ขั้นตอนการปฏิบัติงาน

- 1.อ่านสถานการณ์งาน ระบุวัตถุประสงค์ ผู้ใช้ บทบาทบริการ และเกณฑ์ที่ใช้ตัดสินว่าการติดตั้งสำเร็จ
- 2.บันทึกข้อกำหนด CPU, RAM, Disk, ชื่อเครื่อง รูปแบบเครือข่าย และข้อมูล IPv4 ที่ได้รับ
- 3.ตรวจว่าเครื่อง Host เปิดใช้ Virtualization มี RAM และพื้นที่ว่างเพียงพอ พร้อมบันทึกผล
- 4.ตรวจไฟล์ ISO โดยระบุชื่อไฟล์ รุ่น ภาษา สถาปัตยกรรม แหล่งที่มา และค่าแฮชเมื่อมีข้อมูลอ้างอิง
- 5.สร้าง VM ตั้งชื่อให้สื่อความหมาย กำหนด 2 vCPU, RAM 4 GB และ Disk 60 GB
แบบขยายตามการใช้งาน
- 6.กำหนด Network Adapter เป็น NAT หรือ Host-only ตามแผน เชื่อม ISO และเลือก Connect at power on
- 7.เปรียบเทียบหน้าสรุป Hardware ของ VM กับแผน แก่ค่าที่ไม่ตรง แล้วบันทึกภาพหลักฐาน
- 8.เสนอแผนและหลักฐานให้ผู้สอนตรวจอนุมัติก่อนเปิด VM

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

1. ความถูกต้องของขั้นตอน การประกอบ

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows 10”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยแต่ไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ลำดับและความถูกต้อง	ปฏิบัติครบ ถูกลำดับ อีสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกจุดตรวจ มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ อ่านง่าย ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ/อธิบายน้อย	ไม่มีหลักฐานที่ใช้ตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ เป็นระเบียบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด/ไม่รับผิดชอบ

	ใบงานที่ 2	หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 2
	ชื่อหน่วยการเรียนรู้ งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/การวิเคราะห์อุปกรณ์เคลื่อนที่ และการแยกแยะข้อมูลกับสารสนเทศ		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

ผู้เรียนสามารถติดตั้ง Windows Server 2019 Standard Evaluation (Desktop Experience) บนเครื่องเสมือนและเข้าสู่ระบบครั้งแรกได้สำเร็จโดยไม่ทำลายข้อมูลนอกขอบเขตงาน

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ติดตั้ง Windows Server 2019 แบบ Desktop Experience บนดิสก์เสมือนว่างตามแผน
2. ควบคุมความเสี่ยงในการเลือกรุ่น ดิสก์ และพาร์ทิชัน พร้อมบันทึกจุดตรวจสอบสำคัญ
3. ตรวจสอบการเข้าสู่ระบบครั้งแรกและความพร้อมเบื้องต้นของ Server Manager
4. อย่างถูกต้อง

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายความแตกต่างระหว่าง Server Core กับ Desktop Experience และระบุเหตุผลที่เลือกใช้ได้
2. อธิบายผลกระทบของการเลือก Custom และการเลือกดิสก์เป้าหมายผิดได้

4.2 ทักษะพิสัย (Psychomotor Domain)

1. บูต VM จาก ISO เลือก Edition และดำเนินการติดตั้งตามลำดับได้
2. กำหนดรหัสผ่าน Administrator เข้าสู่ระบบ และตรวจ Server Manager ได้

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ความรู้และทักษะในการจัดเตรียม ติดตั้ง และตรวจสอบระบบปฏิบัติการเครื่องแม่ข่าย เพื่อรองรับการให้บริการในระบบเครือข่ายได้อย่างมีประสิทธิภาพ

5. เครื่องมือ วัสดุ และอุปกรณ์

1. สมุดจด
2. คอมพิวเตอร์ / สมาร์ทโฟน
3. อินเทอร์เน็ต
4. USB Boot windows 10

6. คำแนะนำ/ข้อควรระวัง

1. ยืนยันว่าเป็นดิสก์เสมือนของงานก่อนลบ สร้าง หรือฟอร์แมตพาร์ติชัน เพราะการเลือกผิดทำให้ข้อมูลสูญหาย
2. เลือกรุ่นที่มีคำว่า Desktop Experience ให้ตรงกับโจทย์ ห้ามเลือก Edition ตามความคุ้นเคยโดยไม่ตรวจสอบ
3. ห้ามปิดเครื่อง Host ปิด VM หรือถอด ISO ระหว่างคัดลอกและติดตั้งไฟล์
4. กำหนดรหัสผ่านตามนโยบาย ห้ามเขียนรหัสผ่านจริงในใบงาน รายงาน หรือภาพหน้าจอ

7. ขั้นตอนการปฏิบัติงาน

1. เปิด VM และยืนยันว่าบูตจาก ISO จนปรากฏหน้า Windows Setup
2. เลือกภาษา รูปแบบเวลา และแป้นพิมพ์ตามที่ผู้สอนกำหนด แล้วเลือก Install now
3. เลือก Windows Server 2019 Standard Evaluation (Desktop Experience) และตรวจสอบชื่อ Edition ซ้ำก่อนดำเนินการ
4. ยอมรับข้อตกลงสิทธิ์ใช้งาน แล้วเลือก Custom: Install Windows only (advanced)
5. ตรวจสอบชื่อและขนาดดิสก์เสมือนให้ตรงกับแผน เลือกพื้นที่ว่างเป้าหมาย และเริ่มติดตั้ง
6. รอการคัดลอกไฟล์และการรีสตาร์ทโดยไม่รบกวนระบบ หากวนกลับมาที่ Setup ให้ตรวจสอบลำดับบูตหรือถอด ISO ตามคำแนะนำผู้สอน
7. กำหนดรหัสผ่าน Administrator ตามนโยบายและเข้าสู่ระบบครั้งแรก
8. ตรวจสอบว่า Server Manager เปิดได้ ตรวจสอบ Edition เบื้องต้นและบันทึกภาพหลักฐานโดย

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

1. ความถูกต้องของขั้นตอน การประกอบ
2. ความถูกต้องของขั้นตอน การติดตั้งระบบปฏิบัติการ
3. ความถูกต้องของขั้นตอน การตั้งค่าระบบปฏิบัติการพื้นฐาน

4. ความถูกต้องของขั้นตอน การติดตั้งโปรแกรมใช้งานพื้นฐาน

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows 10”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยแต่ไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ลำดับและความถูกต้อง	ปฏิบัติครบ ถูกลำดับ อีสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกจุดตรวจ มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ อ่านง่าย ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ/อธิบายน้อย	ไม่มีหลักฐานที่ใช้ตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ เป็นระเบียบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด/ไม่รับผิดชอบ

	ใบงานที่ 3	หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 3
	ชื่อหน่วยการเรียนรู้ งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

ผู้เรียนสามารถเปลี่ยนชื่อเครื่อง ตั้งเขตเวลา กำหนด IPv4 แบบคงที่ ตรวจสอบการสื่อสาร และอัปเดต Windows Server 2019 ได้ถูกต้องตามข้อมูลที่ได้รับ

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. กำหนดชื่อเครื่อง เขตเวลา และ IPv4 แบบคงที่ตามมาตรฐานและแผนเครือข่าย
2. ใช้คำสั่งตรวจสอบและทดสอบเครือข่ายอย่างเป็นลำดับเพื่อยืนยันค่าที่กำหนด
3. ตรวจสอบและติดตั้งรายการอัปเดต พร้อมตรวจค่าซ้ำหลังรีสตาร์ท

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายเหตุผลของการใช้ชื่อเครื่องที่ไม่ซ้ำ เวลา UTC+07:00 และ IPv4 แบบคงที่สำหรับเครื่องแม่ข่ายได้
2. วิเคราะห์ผล hostname, ipconfig /all และ ping เพื่อระบุจุดผิดปกติเบื้องต้นได้

4.2 ทักษะพิสัย

1. เปลี่ยนชื่อเครื่อง ตั้งเขตเวลา และกำหนด IP, Prefix/Subnet, Gateway และ DNS ได้
2. ตรวจสอบค่า ทดสอบการสื่อสาร และดำเนินการ Windows Update ได้

4.3 จิตพิสัย

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1. ประยุกต์ใช้ความรู้และทักษะในการจัดเตรียม ติดตั้ง และตรวจสอบระบบปฏิบัติการเครื่องแม่ข่าย เพื่อรองรับการให้บริการในระบบเครือข่ายได้อย่างมีประสิทธิภาพ

5. เครื่องมือ วัสดุ และอุปกรณ์

1. VM ที่ติดตั้งสำเร็จจากใบงานที่ 2
2. ข้อมูลชื่อเครื่องและเครือข่ายจากผู้สอน
3. ใบความรู้
4. สิทธิ์เข้าถึงเครือข่ายทดลองหรืออินเทอร์เน็ตตามที่กำหนด

6. คำแนะนำ/ข้อควรระวัง

1. บันทึกค่าปัจจุบันก่อนเปลี่ยนทุกครั้ง และตรวจว่า IP ที่ได้รับไม่ซ้ำกับอุปกรณ์อื่น
2. ห้ามคาดเดา Gateway หรือ DNS และห้ามทดลองใช้ IP ในเครือข่ายจริงโดยไม่ได้รับอนุญาต
3. อย่าปิด Windows Firewall หรือระบบป้องกันเพื่อให้ ping ผ่านโดยไม่มีเหตุผลและการอนุมัติ
4. รีสตาร์ทเมื่อระบบร้องขอ และตรวจค่าซ้ำหลังรีสตาร์ทเพื่อป้องกันการสรุปผลจากค่าชั่วคราว

7. ขั้นตอนการปฏิบัติงาน

1. บันทึกชื่อเครื่อง เขตเวลา และค่าการเชื่อมต่อเครือข่ายเดิมก่อนแก้ไข
2. เปลี่ยนชื่อเครื่องตามรูปแบบที่กำหนด ตรวจสอบตัวสะกดและความไม่ซ้ำ แล้วรีสตาร์ท
3. ตั้ง Time zone เป็น (UTC+07:00) Bangkok, Hanoi, Jakarta และตรวจวันที่เวลา
4. กำหนด IPv4, Prefix/Subnet, Default gateway และ DNS ตามโจทย์ โดยตรวจทุกช่องก่อนบันทึก
5. ใช้ hostname และ ipconfig /all ตรวจชื่อเครื่องและค่าการ์ดเครือข่ายเทียบกับแผน
6. ทดสอบตามลำดับที่ผู้สอนกำหนด เช่น loopback, IP ของตนเอง, Gateway และปลายทาง พร้อมบันทึกผลและเงื่อนไข
7. เปิด Windows Update ตรวจหาและติดตั้งรายการอัปเดต รีสตาร์ทเมื่อจำเป็น และตรวจซ้ำจนได้สถานะตามเกณฑ์
8. ตรวจชื่อเครื่อง เวลา เครือข่าย และการสื่อสารซ้ำหลังรีสตาร์ท พร้อมบันทึกภาพหลักฐาน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

1. ความถูกต้องของขั้นตอน การประกอบ
2. ความถูกต้องของขั้นตอน การติดตั้งระบบปฏิบัติการ

3. ความถูกต้องของขั้นตอน การตั้งค่าระบบปฏิบัติการ windows server พื้นฐาน
4. ความถูกต้องของขั้นตอน การติดตั้งโปรแกรมใช้งาน windows server พื้นฐาน

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยแต่ไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ลำดับและความถูกต้อง	ปฏิบัติครบ ถูกลำดับ อีสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกจุดตรวจ มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ อ่านง่าย ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ/อธิบายน้อย	ไม่มีหลักฐานที่ใช้ตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ เป็นระเบียบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด/ไม่รับผิดชอบ

	ใบงานที่ 4	หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 3
	ชื่อหน่วยการเรียนรู้ งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

ผู้เรียนสามารถตรวจสอบความพร้อมของระบบ วิเคราะห์และแก้ปัญหาจากหลักฐาน และจัดทำรายงานส่งมอบการติดตั้งที่ครบถ้วน ตรวจสอบย้อนกลับได้ และไม่เปิดเผยข้อมูลลับ

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ตรวจสอบระบบปฏิบัติการ ฮาร์ดแวร์ ชื่อเครื่อง เวลา เครือข่าย เหตุการณ์ และสถานะอัปเดตตาม Checklist
2. วิเคราะห์สาเหตุ แก้ไข และทดสอบซ้ำเมื่อผลไม่ผ่านเกณฑ์
3. จัดทำรายงานผลการติดตั้งพร้อมหลักฐานและข้อเสนอแนะสำหรับการส่งมอบ

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายเกณฑ์ตรวจสอบความพร้อมและความสำคัญของหลักฐานที่มีวันเวลาและคำบรรยายได้
2. วิเคราะห์ความสัมพันธ์ระหว่างอาการ สาเหตุ วิธีแก้ และผลทดสอบซ้ำได้

4.2 ทักษะพิสัย

1. ใช้ hostname, systeminfo, ipconfig /all, ping, Event Viewer และ Windows Update ตรวจสอบระบบได้
2. จัดทำรายงานและตารางผลทดสอบพร้อมภาพหลักฐานได้ครบถ้วน

4.3 จิตพิสัย

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

- 1.ประยุกต์ใช้ความรู้และทักษะในการจัดเตรียม ติดตั้ง และตรวจสอบระบบปฏิบัติการเครื่องแม่ข่าย เพื่อรองรับการให้บริการในระบบเครือข่ายได้อย่างมีประสิทธิภาพ

5. เครื่องมือ วัสดุ และอุปกรณ์

- 1.VM ที่ผ่านใบงานที่ 3
- 2.รายการตรวจสอบหลังติดตั้ง
- 3.โปรแกรมจับภาพหน้าจอ

6. คำแนะนำ/ข้อควรระวัง

- 1.ปิดบังรหัสผ่าน Product Key หมายเลขบัญชี และข้อมูลเครือข่ายที่ผู้สอนกำหนดเป็นความลับ
- 2.ภาพทุกภาพต้องอ่านได้ มีคำบรรยาย และสัมพันธ์กับรายการตรวจห้ามตกแต่งจนผลทดสอบคลาดเคลื่อน
- 3.อย่าสรุปว่าระบบพร้อมจากการทดสอบเพียงรายการเดียว และห้ามละเว้นผลที่ไม่ผ่าน
- 4.ปิดระบบด้วยคำสั่ง Shutdown อย่างถูกต้อง ถอด ISO และจัดเก็บไฟล์ก่อนสิ้นสุดงาน

7. ขั้นตอนการปฏิบัติงาน

- 1.เปิด Checklist และระบุเกณฑ์ผ่านของชื่อเครื่อง รุ่นระบบ เวลา เครือข่าย การอัปเดต และสถานะอุปกรณ์
- 2.รัน hostname, systeminfo และ ipconfig /all บันทึกผลพร้อมวันเวลา และเทียบกับแผนติดตั้ง
- 3.ทดสอบการสื่อสารเครือข่ายตามลำดับ พร้อมระบุปลายทาง เงื่อนไข และผลผ่าน/ไม่ผ่าน
- 4.เปิด Event Viewer ตรวจสอบเหตุการณ์ Critical หรือ Error ที่เกี่ยวข้องกับช่วงติดตั้งและการเริ่มระบบ
- 5.ตรวจสอบ Windows Update และ Device Manager หรือสถานะอุปกรณ์ตามเครื่องมือที่มี
- 6.เมื่อพบผลไม่ผ่าน ให้บันทึกอาการ ตั้งสมมติฐาน ตรวจสอบหลักฐาน แก้ไขทีละประเด็น และทดสอบซ้ำ
- 7.จัดทำรายงานประกอบด้วยวัตถุประสงค์ แผน/ค่าติดตั้ง ขั้นตอน ผลตรวจ ปัญหาและวิธีแก้ สรุปความพร้อม และข้อเสนอแนะ
- 8.ตรวจจายงานว่าหลักฐานครบ มีคำบรรยาย ไม่เปิดเผยข้อมูลลับ และผลสรุปสอดคล้องกับตารางทดสอบ
- 9.Shutdown VM อย่างถูกต้อง ถอด ISO จัดเก็บไฟล์ตามชื่อที่กำหนด และส่งมอบงาน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

1. รายงานผลการติดตั้งฉบับสมบูรณ์
2. ภาพหลักฐานอย่างน้อย 6 ภาพพร้อมคำบรรยาย
3. ตารางผลทดสอบผ่าน/ไม่ผ่าน
4. บันทึกปัญหา สาเหตุ วิธีแก้ และผลหลังแก้

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยแต่ไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ลำดับและความถูกต้อง	ปฏิบัติครบ ถูกลำดับ อีสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกจุดตรวจ มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ อ่านง่าย ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ/อธิบายน้อย	ไม่มีหลักฐานที่ใช้ตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ เป็นระเบียบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด/ไม่รับผิดชอบ

	แผนการจัดการเรียนรู้	หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 5-8
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	ทฤษฎี 4 ชม. ปฏิบัติ 16 ชม.
ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

ผู้เรียนสามารถวางแผนและบริหารบัญชีผู้ใช้ กลุ่ม และสิทธิ์การเข้าถึง กำหนดค่าพื้นฐานของ Windows Server 2019 ควบคุมเครื่องแม่ข่ายจากระยะไกลอย่างปลอดภัย พร้อมตรวจสอบและจัดทำรายงานการตั้งค่าที่ใช้ตรวจสอบย้อนหลังได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น
2. วางแผน บริหารจัดการผู้ใช้งาน สิทธิ์การเข้าถึง กำหนดค่าพื้นฐาน และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกล

4. จุดประสงค์เชิงพฤติกรรม (เขียนให้ครบด้าน พุทธิพิสัย ทักษะพิสัย จิตพิสัย และ ประยุกต์ใช้)

4.1 พุทธิพิสัย (Cognitive Domain)

1. อธิบายความแตกต่างระหว่างบัญชีผู้ใช้ กลุ่ม และสิทธิ์ได้ถูกต้อง
2. อธิบายหลัก Least Privilege และวงจรชีวิตบัญชีผู้ใช้ได้ถูกต้อง
3. จำแนก Share Permissions และ NTFS Permissions ได้ถูกต้อง
4. วิเคราะห์สิทธิ์ที่มีผลเมื่อเข้าถึงทรัพยากรผ่านเครือข่ายได้

4.2 ทักษะพิสัย (Psychomotor Domain)

1. ออกแบบแผนบัญชีผู้ใช้ กลุ่ม และสิทธิ์จากสถานการณ์ที่กำหนดได้
2. สร้างและจัดการบัญชีผู้ใช้และกลุ่มได้ตามแผน
3. แชรโฟลเดอร์ กำหนด Share/NTFS Permissions และทดสอบ Effective Access ได้
4. กำหนดชื่อเครื่อง IPv4 เวลา และตรวจสอบการเชื่อมต่อได้
5. เปิดใช้ Remote Desktop จำกัดผู้ใช้ และทดสอบการเชื่อมต่อได้
6. จัดทำรายงานการตั้งค่าพร้อมภาพหลักฐานที่ย้อนตรวจได้

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการวางแผน บริหารจัดการผู้ใช้งาน สิทธิ์การเข้าถึง และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลด้วยความละเอียดรอบคอบและรับผิดชอบ

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ความรู้และทักษะในการบริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง กำหนดค่าพื้นฐาน และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลเพื่อรักษาความปลอดภัยของระบบ

5. การเรียนรู้

1. การวิเคราะห์บทบาทงานและวางแผนบัญชีผู้ใช้ กลุ่ม และสิทธิ์
2. การบริหาร Local Users and Groups และคำสั่งตรวจสอบ
3. การแชร์ทรัพยากร Share Permissions, NTFS Permissions และ Effective Access
4. การกำหนดชื่อเครื่อง IPv4 เวลา Windows Update และ Firewall
5. การเปิดใช้ Remote Desktop, Network Level Authentication และการจำกัดผู้ใช้
6. การตรวจสอบ บันทึกหลักฐาน จัดทำรายงาน และดูแลสภาพแวดล้อมปฏิบัติการ

6. กิจกรรมการเรียนรู้

1. ขั้นเตรียมความพร้อม

1. ครูตรวจสอบรายชื่อผู้เรียน การแต่งกาย และความพร้อมของอุปกรณ์ที่ใช้ในการเรียน
2. ครูแจ้งจุดประสงค์การเรียนรู้ สมรรถนะประจำหน่วย และผลลัพธ์การเรียนรู้ที่คาดหวัง
3. ครูทบทวนความรู้เดิมเกี่ยวกับระบบปฏิบัติการเครื่องแม่ข่ายและการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
4. ครูตั้งคำถามกระตุ้นความคิดเกี่ยวกับการจัดการผู้ใช้งาน สิทธิการเข้าถึง และการควบคุมเครื่องแม่ข่ายจากระยะไกล
5. ครูชี้แจงกิจกรรมการเรียนรู้ วิธีการประเมินผล และชิ้นงานที่ผู้เรียนต้องจัดทำ

2. ขั้นนำเข้าสู่บทเรียน

1. ครูนำเสนอกรณีศึกษาปัญหาที่เกิดจากการกำหนดสิทธิ์ผู้ใช้งานไม่เหมาะสมในองค์กร
2. ครูและผู้เรียนร่วมกันอภิปรายถึงผลกระทบที่อาจเกิดขึ้นต่อระบบและข้อมูล
3. ครูเชื่อมโยงเข้าสู่เนื้อหาเรื่องการบริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง และการควบคุมเครื่องแม่ข่าย

3. ขั้นให้เนื้อหา

1. ครูบรรยายและสาธิตการวางแผนการจัดการผู้ใช้งานและสิทธิการเข้าถึง
2. ผู้เรียนศึกษาและปฏิบัติการสร้างบัญชีผู้ใช้งานและกลุ่มผู้ใช้งาน
3. ผู้เรียนฝึกกำหนดสิทธิการเข้าถึงทรัพยากรบนเครื่องแม่ข่าย
4. ผู้เรียนปฏิบัติการกำหนดค่าพื้นฐานของระบบและเครือข่าย
5. ผู้เรียนฝึกใช้งานเครื่องมือควบคุมเครื่องแม่ข่ายจากระยะไกล
6. ผู้เรียนตรวจสอบ บันทึก และจัดทำรายงานผลการตั้งค่าระบบ
7. ครูให้คำแนะนำและติดตามการปฏิบัติงานของผู้เรียนเป็นรายบุคคลและรายกลุ่ม

4. ขั้นฝึกปฏิบัติ

1. ผู้เรียนศึกษาและปฏิบัติการสร้างบัญชีผู้ใช้งานและกลุ่มผู้ใช้งาน
2. ผู้เรียนฝึกกำหนดสิทธิการเข้าถึงทรัพยากรบนเครื่องแม่ข่าย

3. ผู้เรียนปฏิบัติการกำหนดค่าพื้นฐานของระบบและเครือข่าย
4. ผู้เรียนฝึกใช้งานเครื่องมือควบคุมเครื่องแม่ข่ายจากระยะไกล
5. ผู้เรียนตรวจสอบ บันทึก และจัดทำรายงานผลการตั้งค่าระบบ
6. ครูให้คำแนะนำและติดตามการปฏิบัติงานของผู้เรียนเป็นรายบุคคลและรายกลุ่ม

5. ขั้นสรุปและประเมินผล

1. ผู้เรียนร่วมกันสรุปองค์ความรู้เกี่ยวกับการติดตั้งระบบปฏิบัติการเครื่องแม่ข่าย
2. ผู้เรียนสะท้อนผลการเรียนรู้ ปัญหาที่พบ และแนวทางการพัฒนาการปฏิบัติงานของตนเอง
3. ผู้เรียนนำเสนอรายงานผลการติดตั้งและแลกเปลี่ยนความคิดเห็นภายในชั้นเรียน
4. ครูประเมินผลด้านความรู้ ทักษะปฏิบัติ และคุณลักษณะอันพึงประสงค์ตามเกณฑ์ที่กำหนด

6. คำแนะนำ/ข้อควรระวัง

1. ศึกษาใบความรู้และคู่มือปฏิบัติงานก่อนเริ่มปฏิบัติการทุกครั้ง
2. ปฏิบัติตามขั้นตอนการใช้งานระบบปฏิบัติการเครื่องแม่ข่ายอย่างเคร่งครัด
3. ตรวจสอบความถูกต้องของคำสั่งก่อนดำเนินการทุกครั้ง โดยเฉพาะคำสั่งที่เกี่ยวข้องกับการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง
4. บันทึกข้อมูลการตั้งค่าระบบและผลการปฏิบัติงานอย่างเป็นระบบเพื่อใช้ในการตรวจสอบและแก้ไขปัญหา
5. ใช้บัญชีผู้ดูแลระบบ (Administrator/Root) เท่าที่จำเป็น และออกจากระบบเมื่อใช้งานเสร็จ
6. รักษาความลับของรหัสผ่านและข้อมูลสำคัญของระบบ
7. ปฏิบัติงานด้วยความรอบคอบ รับผิดชอบ และคำนึงถึงความปลอดภัยของข้อมูลและระบบเครือข่าย
8. ดูแลรักษาเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และสื่อบันทึกข้อมูลให้อยู่ในสภาพพร้อมใช้งาน

7. สื่อและแหล่งเรียนรู้

1. ห้องปฏิบัติการคอมพิวเตอร์และเครือข่าย
2. คู่มือการใช้งานระบบปฏิบัติการเครื่องแม่ข่าย
3. เว็บไซต์ผู้พัฒนาระบบปฏิบัติการเครื่องแม่ข่าย เช่น Microsoft Learn และ Ubuntu Documentation
5. สถานประกอบการหรือหน่วยงานที่ใช้ระบบเครื่องแม่ข่ายในการดำเนินงานจริง

8. หลักฐานการเรียนรู้

1. หลักฐานความรู้
 - คะแนนจากการทำแบบฝึกหัด และแบบทดสอบในหนังสือประกอบการเรียน
2. หลักฐานการปฏิบัติงาน
 - คะแนนการทํากิจกรรมการเรียนรู้ และภาพถ่ายการทํากิจกรรมของผู้เรียน

9. การวัดและประเมินผล

1. เกณฑ์การปฏิบัติงาน

ตอบคำถามหรือแบบทดสอบได้อย่างถูกต้อง ไม่น้อยกว่า 80%

ปฏิบัติตามขั้นตอนกิจกรรม และใช้เทคโนโลยีได้อย่างเหมาะสมถูกต้อง
เข้าร่วม สื่อสาร และร่วมมือกับสมาชิกในกลุ่มได้ดี มีความรับผิดชอบ

2. วิธีการประเมิน

แบบฝึกหัดหลังเรียน ตรวจสอบความเข้าใจในเนื้อหา

แบบทดสอบหลังเรียนถูกต้อง ไม่น้อยกว่า 80%

3. เครื่องมือประเมิน

แบบทดสอบหลังเรียน

10. บันทึกผลหลังจัดการเรียนรู้

1. ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

2. ปัญหา อุปสรรคที่พบ

3. การแก้ไขปัญหา

3) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

4) แนวทางแก้ปัญหาในครั้งต่อไป

11. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”

2. เว็บไซต์: classroom <https://learn.microsoft.com/>

3. YouTube

4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบความรู้ ที่ 1	หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 5-8
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 4 ชม. ปฏิบัติ 16 ชม.
ชื่อเรื่อง/งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

สามารถวางแผนและบริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง รวมถึงกำหนดค่าพื้นฐานและควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลได้อย่างปลอดภัย

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น
2. วางแผน บริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง กำหนดค่าพื้นฐาน และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกล

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. บอกคำสั่งและเครื่องมือที่ใช้ในการบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้นได้ถูกต้อง
2. อธิบายหลักการจัดการผู้ใช้งานและสิทธิการเข้าถึงบนระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
3. ประยุกต์ใช้คำสั่งหรือเครื่องมือในการกำหนดค่าพื้นฐานของระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
4. วิเคราะห์ผลกระทบจากการกำหนดสิทธิการเข้าถึงของผู้ใช้งานได้ถูกต้อง
5. ประเมินความเหมาะสมของวิธีการควบคุมเครื่องแม่ข่ายจากระยะไกลได้ถูกต้อง
6. กำหนดนโยบายการจัดการผู้ใช้งานและสิทธิการเข้าถึงสำหรับหน่วยงานขนาดเล็กได้ถูกต้อง

4.2 ทักษะพิสัย

1. วางแผนการบริหารจัดการผู้ใช้งานและสิทธิการเข้าถึงบนระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
2. บริหารจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานบนระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
3. กำหนดสิทธิการเข้าถึงทรัพยากรสำหรับผู้ใช้งานแต่ละรายได้ถูกต้อง
4. ตั้งค่าพื้นฐานที่จำเป็นบนระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
5. ควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลด้วยเครื่องมือที่เหมาะสมได้ถูกต้อง

4.3 จิตพิสัย

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการวางแผน บริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลด้วยความละเอียดรอบคอบและรับผิดชอบ

4.4 ประยุกต์ใช้และรับผิดชอบ

1. ประยุกต์ใช้ความรู้และทักษะในการบริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง กำหนดค่าพื้นฐาน และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลเพื่อรักษาความปลอดภัยของระบบ

5. เนื้อหาสาระ

1. วางแผนการจัดการผู้ใช้งานและสิทธิการเข้าถึง
2. กำหนดค่าพื้นฐานของระบบและเครือข่าย
3. จัดการผู้ใช้งานและกลุ่มผู้ใช้งาน
4. กำหนดสิทธิการเข้าถึงทรัพยากรบนเครื่องแม่ข่าย
5. ตั้งค่าการควบคุมเครื่องแม่ข่ายระยะไกล
6. ตรวจสอบและบันทึกการตั้งค่าระบบ (ชิ้นงาน: แผนการจัดการผู้ใช้และสิทธิ, รายงานการตั้งค่าระบบ)
7. จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (ชิ้นงาน: ระบบปฏิบัติการเครื่องแม่ข่ายที่ได้รับการบริหารจัดการเบื้องต้น)

1. ภาพรวมการบริหารเครื่องแม่ข่ายหลังติดตั้ง

หลังติดตั้ง Windows Server แล้ว เครื่องยังไม่พร้อมให้บริการทันที ผู้ดูแลต้องกำหนดตัวตนของเครื่อง สร้างตัวตนของผู้ใช้ จัดกลุ่มผู้ใช้ กำหนดสิทธิ์ทรัพยากร ตั้งค่าเครือข่ายและเวลา เปิดเฉพาะช่องทางบริหารที่จำเป็น และบันทึกค่าทุกส่วน การตั้งค่าทั้งหมดต้องสอดคล้องกับงานจริง ไม่ใช่ให้ทุกคนเป็นผู้ดูแลเพื่อความสะดวก

คำสำคัญ	ความหมายในการปฏิบัติงาน
Authentication	การพิสูจน์ว่าผู้ที่เข้าสู่ระบบเป็นใคร เช่น ชื่อผู้ใช้และรหัสผ่าน
Authorization	การตัดสินใจว่าตัวต้นนั้นทำอะไรกับทรัพยากรใดได้บ้าง
Account	ข้อมูลประจำตัวที่ระบบใช้พิสูจน์ตัวตนและติดตามกิจกรรม
Group	หน่วยรวมบัญชีหลายบัญชีเพื่อกำหนดสิทธิ์ร่วมกัน
Permission	สิทธิ์ต่อวัตถุ เช่น อ่าน แก้ไข หรือลบไฟล์
Privilege/Right	สิทธิ์ระดับระบบ เช่น เข้าสู่ระบบจากระยะไกลหรือปิดเครื่อง

2. การวางแผนบัญชีผู้ใช้ กลุ่ม และสิทธิ์

2.1 หลักให้สิทธิ์เท่าที่จำเป็น (Least Privilege)

ให้ผู้ใช้เฉพาะสิทธิ์ขั้นต่ำที่จำเป็นต่อหน้าที่ และให้เฉพาะช่วงเวลาที่ต้องใช้

หลักนี้ลดผลกระทบจากความผิดพลาด มัลแวร์ และการใช้บัญชีผิดพลาดประสงค์ การให้ Full Control หรือสมาชิก Administrators โดยไม่มีเหตุผลจึงไม่ใช่วิธีแก้ปัญหาปกติ

2.2 ลำดับการวางแผน

- รวบรวมรายชื่อบุคลากร บทบาท หน่วยงาน ทรัพยากรที่ใช้ และช่วงเวลาที่ต้องใช้
- ออกแบบรูปแบบบัญชีที่ไม่ซ้ำและสื่อถึงเจ้าของโดยไม่เปิดเผยข้อมูลเกินจำเป็น
- สร้างกลุ่มตามบทบาท เช่น Teachers_RW, Staff_R และ Server_Remote_Operators
- กำหนดสิทธิ์ให้กลุ่ม แล้วเพิ่มบัญชีเป็นสมาชิก แทนการกำหนดสิทธิ์ทีละคน
- กำหนดผู้อนุมัติ วันทบทวนสิทธิ์ และวิธีปิดใช้บัญชีเมื่อย้ายงานหรือพ้นสภาพ
- ทดสอบทั้งกรณีที่ควรอนุญาตและควรปฏิเสธ พร้อมเก็บหลักฐาน

บทบาท	กลุ่มตัวอย่าง	ทรัพยากร	สิทธิ์ที่เหมาะสม
ครูผู้สอน	Teachers_RW	โพลเดอร์ Teachers	Read/Write/Modify ตามงาน
เจ้าหน้าที่	Staff_R	โพลเดอร์ Staff	Read เท่านั้น
ผู้ดูแลระบบ	Server_Admins	ทรัพยากรที่รับผิดชอบ	Full Control เฉพาะผู้ได้รับมอบหมาย
ผู้ควบคุมระยะไกล	Server_Remote_Operators	Remote Desktop	เข้าสู่ระบบระยะไกล ไม่มีสิทธิ์ผู้ดูแลโดยอัตโนมัติ

3. การบริหาร Local Users and Groups

Local account ถูกเก็บและตรวจสอบโดยเครื่องนั้น จึงใช้สิทธิ์กับทรัพยากรของเครื่องนั้นเป็นหลัก เหมาะกับเครื่อง Standalone หรือห้องทดลอง ส่วนระบบโดเมนใช้ Active Directory เพื่อจัดการบัญชีและกลุ่มแบบรวมศูนย์ ใบงานหน่วยนี้ใช้ Local Users and Groups เพื่อให้เห็นหลักการก่อน

3.1 การจัดการผ่านส่วนติดต่อกราฟิก

- 13.เปิด Server Manager > Tools > Computer Management
- 14.ไปที่ System Tools > Local Users and Groups > Users หรือ Groups
- 15.สร้างบัญชีโดยกำหนดชื่อ คำอธิบาย รหัสผ่าน และตัวเลือกการใช้งานตามนโยบาย
- 16.สร้างกลุ่ม Security ตามบทบาท แล้วเพิ่มบัญชีที่เกี่ยวข้องเป็นสมาชิก
- 17.บัญชีที่เลิกใช้ควร Disable ก่อนลบ เพื่อหยุดการเข้าสู่ระบบและคงข้อมูลตรวจสอบไว้

3.2 คำสั่งสำหรับตรวจสอบและบันทึกผล

วัตถุประสงค์	Command Prompt	PowerShell
ดูบัญชีผู้ใช้	net user	Get-LocalUser
ดูรายละเอียดบัญชี	net user username	Get-LocalUser -Name username
ดูกลุ่ม	net localgroup	Get-LocalGroup
ดูสมาชิกกลุ่ม	net localgroup groupname	Get-LocalGroupMember -Group groupname
ดูตัวตนปัจจุบัน	whoami	whoami /all

ข้อควรระวัง: อย่าใส่รหัสผ่านจริงลงในรายงานหรือภาพหน้าจอ ถ้าต้องสาธิตคำสั่งสร้างบัญชี ให้ใช้รหัสผ่านทดลองตามที่ครูกำหนดและเปลี่ยน/ลบบัญชีหลังจาก

4. การกำหนดสิทธิ์โฟลเดอร์และการแชร์

4.1 NTFS Permissions

NTFS Permissions อยู่ที่แท็บ Security และควบคุมการเข้าถึงไฟล์หรือโฟลเดอร์ทั้งจากหน้าเครื่องและผ่านเครือข่าย สิทธิ์สำคัญ ได้แก่ Read, Read & Execute, List Folder Contents, Write, Modify และ Full Control Modify อนุญาตอ่าน เขียน เปลี่ยนแปลง และลบ ส่วน Full Control เพิ่มความสามารถเปลี่ยนสิทธิ์และความเป็นเจ้าของ

4.2 Share Permissions

Share Permissions ทำงานเมื่อเข้าถึงผ่านเส้นทางเครือข่ายแบบ UNC เช่น \\SERVER-01\SchoolData ระดับหลักคือ Read, Change และ Full Control ถ้าเปิดโฟลเดอร์จากหน้าเครื่องโดยตรง Share Permissions จะไม่ถูกใช้

4.3 สิทธิ์ที่มีผลจริง

- ระบบรวมสิทธิ์ Allow จากบัญชีและกลุ่มที่ใช้เป็นสมาชิก
- Explicit Deny มีผลยับยั้ง Allow ที่ขัดกัน จึงควรใช้เท่าที่จำเป็น
- เมื่อเข้าถึงผ่านเครือข่าย ต้องผ่านทั้ง Share และ NTFS; สิทธิ์ที่มีผลจึงถูกจำกัดด้วยชั้นที่เข้มงวดกว่า
- Inheritance ทำให้โฟลเดอร์/ไฟล์รับสิทธิ์จากโฟลเดอร์แม่ ควรตรวจแหล่งที่มาของสิทธิ์ก่อนแก้ไข
- ใช้ Advanced Security Settings > Effective Access เพื่อตรวจสอบสิทธิ์ของผู้ใช้หรือกลุ่มเป้าหมาย

การเข้าถึง	Share	NTFS	ผลที่คาดหวัง
ผ่านเครือข่าย	Read	Modify	อ่านได้ แต่แก้ไขไม่ได้เพราะ Share จำกัดกว่า
ผ่านเครือข่าย	Change	Read	อ่านได้ แต่แก้ไขไม่ได้เพราะ NTFS จำกัดกว่า
ผ่านเครือข่าย	Change	Modify	อ่าน เขียน แก้ไข และลบได้ตามขอบเขต
หน้าเครื่อง	ไม่เกี่ยวข้อง	Read	อ่านได้ตาม NTFS

5. การกำหนดค่าพื้นฐานของระบบและเครือข่าย

5.1 ชื่อเครื่องและเวลา

ชื่อเครื่องควรสั้น ไม่ซ้ำ และเป็นไปตามมาตรฐานหน่วยงาน เช่น SERVER-01 หลังเปลี่ยนชื่อมักต้อง Restart เวลาและ Time zone ต้องถูกต้อง เพราะเกี่ยวข้องกับบันทึกเหตุการณ์ การตรวจสอบย้อนหลัง ไปรับรอง และการพิสูจน์ตัวตน

5.2 IPv4 แบบคงที่

เครื่องแม่ข่ายควรมีที่อยู่ที่ใช้และบริการค้นหาได้สม่ำเสมอ จึงมักกำหนด Static IPv4 หรือ DHCP Reservation ตามแบบเครือข่าย ก่อนตั้งค่าต้องทราบ IP address, Prefix/Subnet mask, Default gateway และ DNS server ที่ถูกต้อง ห้ามคาดเดาค่าในเครือข่ายจริง

ค่า	หน้าที่	จุดตรวจ
IP address	ระบุตำแหน่งของเครื่องในเครือข่าย	อยู่ในวงที่กำหนดและไม่ซ้ำ
Subnet mask/Prefix	ระบุส่วนเครือข่ายและส่วนเครื่อง	สอดคล้องกับแผน IP
Default gateway	ทางออกไปยังเครือข่ายอื่น	อยู่ในเครือข่ายเดียวกับเครื่อง
DNS server	แปลงชื่อเป็น IP และสนับสนุนบริการระบบ	ใช้ DNS ตามแบบระบบ ไม่เลือกสุ่ม

5.3 ลำดับการตรวจสอบเมื่อเชื่อมต่อไม่ได้

18. ใช้ ipconfig /all ตรวจสอบค่า Adapter, IP, Prefix, Gateway และ DNS
19. ใช้ ping 127.0.0.1 ตรวจสอบ TCP/IP ภายในเครื่อง
20. ใช้ ping IP ของตนเองและ Gateway เพื่อตรวจสอบเส้นทางในวงเดียวกัน
21. ใช้ ping IP ปลายทาง แล้วจึงทดสอบชื่อ เพื่อแยกปัญหาเครือข่ายออกจาก DNS
22. ตรวจสอบ Network profile, Windows Defender Firewall และเส้นทาง/พอร์ตที่บริการใช้

6. การควบคุมเครื่องแม่ข่ายด้วย Remote Desktop

Remote Desktop Protocol (RDP) ช่วยให้ผู้ดูแลเห็นหน้าจอและสั่งงานเครื่องแม่ข่ายจาก Client การเปิดใช้ RDP เพิ่มช่องทางเข้าสู่ระบบ จึงต้องอนุญาตเฉพาะผู้ที่จำเป็น ใช้รหัสผ่านแข็งแรง เปิด Network Level Authentication (NLA) และจำกัดขอบเขตเครือข่าย/Firewall

6.1 ขั้นตอนเปิดใช้และทดสอบ

23. ตรวจสอบชื่อเครื่อง IP เวลา และการติดต่อเครือข่ายให้ถูกต้องก่อน
24. เปิด Server Manager > Local Server > Remote Desktop หรือ System Properties > Remote
25. เลือก Allow remote connections และคก NLA ไว้เมื่อ Client รองรับ
26. เพิ่มเฉพาะบัญชีหรือกลุ่มที่ได้รับอนุญาตใน Select Users/Remote Desktop Users
27. ตรวจสอบว่า Windows Defender Firewall อนุญาตกฎ Remote Desktop เฉพาะ Profile/Scope ที่ต้องใช้
28. จาก Client เปิด Remote Desktop Connection (mstsc) ใส่ชื่อหรือ IP แล้วเข้าสู่ระบบ
29. ตรวจสอบด้วย whoami ทดสอบงานที่อนุญาต จากนั้น Sign out และบันทึกผล

ความปลอดภัย: ไม่ควรเปิดพอร์ต RDP จากอินเทอร์เน็ตตรงถึงเครื่องแม่ข่าย

การเข้าถึงจากภายนอกควรใช้ช่องทางที่องค์กรออกแบบ เช่น VPN หรือ RD Gateway พร้อม MFA และนโยบายบันทึกเหตุการณ์ตามความเหมาะสม

7. การตรวจสอบและบันทึกการตั้งค่าระบบ

เอกสารการตั้งค่าทำหน้าที่เป็น Baseline สำหรับตรวจเปรียบเทียบเมื่อเกิดปัญหา ส่งมอบงาน หรือทบทวนสิทธิ์ รายงานที่ระบุค่าที่คาดหวัง ค่าที่พบ วิธีตรวจ วันเวลา ผู้ตรวจ และผลผ่าน/ไม่ผ่าน

หัวข้อตรวจ	ตัวอย่างหลักฐาน	ข้อมูลสำคัญ
ข้อมูลเครื่อง	hostname, systeminfo	ชื่อเครื่อง รุ่น OS วันเวลา
เครือข่าย	ipconfig /all, ping	IP/Prefix/Gateway/DNS และผลติดต่อ
ผู้ใช้/กลุ่ม	net user, net localgroup	สถานะบัญชี สมาชิกกลุ่ม
Share/NTFS	Get-SmbShare, Get-SmbShareAccess, ภาพ Security	เส้นทาง กลุ่ม สิทธิ์
Remote Desktop	ภาพสถานะ RDP/NLA/Firewall และผล mstsc	ผู้ได้รับอนุญาตและผลเชื่อมต่อ
เหตุการณ์/อัปเดต	Event Viewer, Windows Update	Critical/Error ที่เกี่ยวข้องและสถานะอัปเดต

7.1 โครงสร้างรายงาน

30. ข้อมูลผู้ปฏิบัติ เครื่อง และวันเวลา
31. วัตถุประสงค์และขอบเขต
32. แผนผู้ใช้ กลุ่ม และสิทธิ์
33. ตารางค่าระบบและเครือข่ายก่อน/หลัง

- 34.ผลทดสอบแต่ละกรณีพร้อมหลักฐาน
- 35.ปัญหา สาเหตุ การแก้ไข และผลทดสอบซ้ำ
- 36.ข้อเสนอแนะและรายการส่งมอบ

การรักษาความลับ: ปิดบังรหัสผ่าน Product Key, Token และข้อมูลลับ ภาพหน้าจอต้องพอใช้ยืนยันผล แต่ไม่เปิดเผยข้อมูลเกินความจำเป็น

8. แนวทางวิเคราะห์ปัญหาที่พบบ่อย

อาการ	จุดตรวจตามลำดับ	แนวทางแก้ไขที่ปลอดภัย
เข้าสู่ระบบไม่ได้	ชื่อบัญชี สถานะ Disabled รหัสผ่าน กลุ่ม และนโยบาย	ยืนยันตัวตน/ขอขงเขตบัญชีก่อน Reset หรือ Enable
เปิด Share ไม่ได้	ชื่อเครื่อง/IP การเชื่อมต่อ ชื่อ Share Firewall และสิทธิ์	แยกปัญหา Network, Share และ NTFS ทีละชั้น
อ่านได้แต่แก้ไขไม่ได้	Share Change และ NTFS Modify รวมถึง Deny/Inheritance	ตรวจสอบ Effective Access ก่อนเปลี่ยนสิทธิ์
RDP ไม่เชื่อมต่อ	Ping, RDP enabled, ผู้ได้รับอนุญาต, NLA และ Firewall	แก้ไขเฉพาะจุดที่ไม่ผ่าน ไม่ปิด Firewall ทั้งระบบ
เชื่อมด้วย IP ได้แต่ชื่อไม่ได้	DNS server, DNS record และการค้นชื่อ	แก้ DNS/ชื่อ ไม่เปลี่ยนสิทธิ์หรือปิด Firewall

ใบความรู้ที่ 1

การวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง



จุดประสงค์

เพื่อให้ผู้เรียนสามารถวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึงบนระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างเหมาะสม ปลอดภัย และสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร

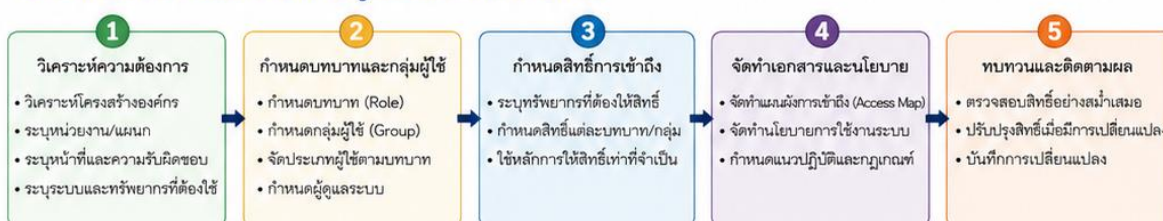
1. ความสำคัญของการวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง

การวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง เป็นขั้นตอนสำคัญในการรักษาความปลอดภัยของระบบ ป้องกันการเข้าถึงทรัพยากรโดยไม่ได้รับอนุญาต ลดความเสี่ยงของการรั่วไหลหรือการสูญหายของข้อมูล และช่วยให้การบริหารจัดการระบบเป็นไปอย่างมีประสิทธิภาพ

2. หลักการสำคัญในการวางแผน

หลักการให้สิทธิ์เท่าที่จำเป็น (Principle of Least Privilege)	การแบ่งแยกหน้าที่ (Separation of Duties)	การตรวจสอบได้ (Accountability)	ความปลอดภัยเป็นหลัก (Security First)	การทบทวนและปรับปรุง (Review & Update)
ให้ผู้ใช้งานมีสิทธิ์เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น ไม่ให้สิทธิ์เกินความจำเป็น	แยกหน้าที่ความรับผิดชอบที่สำคัญออกจากกัน เพื่อลดความเสี่ยงจากการทุจริตหรือความผิดพลาด	สามารถตรวจสอบได้ว่าใครทำอะไร เมื่อใด เพื่อการติดตามและรับผิดชอบ	คำนึงถึงความปลอดภัยของข้อมูลระบบ และเครือข่ายเป็นลำดับแรกในการกำหนดสิทธิ์	ทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ และปรับปรุงเมื่อมีการเปลี่ยนแปลง

3. ขั้นตอนการวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึง



4. ตัวอย่างการกำหนดบทบาท (Role) และกลุ่มผู้ใช้ (Group)

บทบาท (Role)	กลุ่มผู้ใช้ (Group)	หน้าที่โดยย่อ	ตัวอย่างสิทธิ์ที่กำหนด
ผู้ดูแลระบบ (Administrator)	IT_Admins	ดูแลระบบทั้งหมด	- เข้าถึงทุกระบบและข้อมูล - ติดตั้ง/ปรับแต่งระบบ - จัดการผู้ใช้และสิทธิ์
ผู้ดูแลเครือข่าย (Network Admin)	IT_Network	ดูแลระบบเครือข่าย	- จัดการอุปกรณ์เครือข่าย - ดูแลบริการเครือข่าย
ผู้ใช้งานทั่วไป (General User)	Users	ใช้งานระบบตามหน้าที่	- เข้าถึงไฟล์/โฟลเดอร์ที่ได้รับอนุญาต - ใช้งานโปรแกรมที่จำเป็น
ผู้ใช้งานแขก (Guest User)	Guests	ใช้งานจำกัด	- ใช้อินเทอร์เน็ตเท่านั้น - ไม่สามารถเข้าถึงข้อมูลภายใน

5. ตัวอย่างการกำหนดสิทธิ์การเข้าถึงทรัพยากร

ทรัพยากร	บทบาท/กลุ่มผู้ใช้			
	Admin	IT_Network	Users	Guests
ไฟล์เครื่องแม่ข่ายภายใน	✓	✓	✓	✗
การตั้งค่าระบบ	✓	✗	✗	✗
เครื่องพิมพ์เครือข่าย	✓	✓	✓	✗
อินเทอร์เน็ต	✓	✓	✓	✓
ฐานข้อมูลลูกค้า	✓	✓	✗	✗

✓ = อนุญาตให้เข้าถึง ✗ = ไม่อนุญาตให้เข้าถึง

6. สิ่งที่ต้องพิจารณาในการวางแผน

- ✓ ขนาดและโครงสร้างขององค์กร
- ✓ ความสำคัญของข้อมูลและทรัพยากร
- ✓ กฎหมายและข้อกำหนดที่เกี่ยวข้อง (เช่น PDPA)
- ✓ ความสามารถของระบบปฏิบัติการหรือเครื่องมือที่ใช้
- ✓ การรองรับการขยายตัวในอนาคต
- ✓ การฝึกอบรมและสร้างความตระหนักให้กับผู้ใช้งาน

7. ประโยชน์ที่ได้รับ

- ✓ เพิ่มความปลอดภัยของระบบและข้อมูล
- ✓ ช่วยให้การจัดการระบบมีประสิทธิภาพ
- ✓ ลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต
- ✓ สามารถตรวจสอบและติดตามการใช้งานได้
- ✓ สอดคล้องกับนโยบายและมาตรฐานขององค์กร

8. สรุป

- ✓ การวางแผนการจัดการผู้ใช้งานและสิทธิ์การเข้าถึงที่ดี ต้องเริ่มจากการเข้าใจโครงสร้างองค์กร กำหนดบทบาทและกลุ่มผู้ใช้ กำหนดสิทธิ์ตามหลักความปลอดภัย จัดทำเอกสารและทบทวนอย่างสม่ำเสมอ เพื่อให้ระบบปลอดภัย มีประสิทธิภาพ และยั่งยืน



จำไว้เสมอ : “ให้สิทธิ์เท่าที่จำเป็น ตรวจสอบได้ และทบทวนอย่างสม่ำเสมอ” จะช่วยให้องค์กรของคุณปลอดภัยและน่าเชื่อถือ

ในความรู้ที่ 2

กำหนดค่าพื้นฐานของระบบและเครือข่าย



จุดประสงค์

- เพื่อให้ผู้เรียนสามารถกำหนดค่าพื้นฐานของระบบปฏิบัติการเครื่องแม่ข่ายและเครือข่ายได้อย่างถูกต้อง ปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ

1. ความสำคัญ

การกำหนดค่าพื้นฐานของระบบและเครือข่าย เป็นขั้นตอนแรกหลังจากติดตั้งระบบปฏิบัติการ ซึ่งมีผลต่อความเสถียร ความปลอดภัย และประสิทธิภาพในการให้บริการของเครื่องแม่ข่าย รวมถึงการเชื่อมต่อและสื่อสารในเครือข่ายอย่างถูกต้อง

2. องค์ประกอบที่ต้องกำหนดค่าพื้นฐาน



ระบบปฏิบัติการ
และชื่อเครื่อง



การตั้งค่า
เครือข่าย



วันที่และเวลา



ผู้ใช้และสิทธิ์
เริ่มต้น



ความปลอดภัย
ขั้นพื้นฐาน



บริการและ
การอัปเดตระบบ

3. การกำหนดค่าพื้นฐานของระบบปฏิบัติการ (ตัวอย่าง: Windows Server / Linux)



3.1 Windows Server

- ตั้งชื่อเครื่อง (Computer Name) System > About > Rename this PC
- ตั้งค่าเวลาภูมิภาค Settings > Time & Language
- ตั้งค่า IP Address (IPv4) Control Panel > Network and Sharing Center > Change adapter settings
- เปิดใช้งานไฟร์วอลล์ Windows Defender Firewall
- เปิดการอัปเดตอัตโนมัติ Windows Update > Change active hours
- ตรวจสอบบริการที่จำเป็น Services.msc (เช่น DHCP, DNS, File Server)

3.2 Linux (Ubuntu Server)



- ตั้งชื่อเครื่อง (Hostname) `sudo hostnamectl set-hostname server01`
- ตั้งค่าเวลาภูมิภาค `sudo timedatectl set-timezone Asia/Bangkok`
- ตั้งค่า IP Address (IPv4) `sudo nano /etc/netplan/01-netcfg.yaml`
`sudo netplan apply`
- เปิดใช้งานไฟร์วอลล์ (UFW) `sudo ufw enable`
- อัปเดตระบบ `sudo apt update && sudo apt upgrade -y`
- ตรวจสอบบริการที่จำเป็น `systemctl status` (ชื่อบริการ)

4. การตั้งค่าเครือข่าย (TCP/IP)

รายการ	คำอธิบาย
IP Address	ที่อยู่ประจำเครื่องในเครือข่าย (IPv4/IPv6)
Subnet Mask	กำหนดขอบเขตเครือข่ายย่อย
Default Gateway	ที่อยู่เกตเวย์สำหรับออกสู่อินเทอร์เน็ต/เครือข่ายอื่น
DNS Server	เซิร์ฟเวอร์สำหรับแปลงชื่อโดเมนเป็น IP Address
Preferred DNS	DNS หลักที่ใช้ในการค้นหา
Alternate DNS	DNS สำรอง (ใช้เมื่อ DNS หลักใช้งานไม่ได้)

คำแนะนำ : ควรได้รับค่าจากแผนผังเครือข่าย (Network Plan) ขององค์กร หรือผู้ดูแลระบบเครือข่าย

ตัวอย่างการกำหนดค่าเครือข่าย



Server
192.168.1.10

IP Address : 192.168.1.10
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
Preferred DNS : 192.168.1.2
Alternate DNS : 8.8.8.8

5. ความปลอดภัยขั้นพื้นฐาน

- เปลี่ยนรหัสผ่านผู้ดูแลระบบเริ่มต้นให้แข็งแรง
- ปิดบริการที่ไม่จำเป็นเพื่อลดช่องโหว่
- เปิดใช้งานไฟร์วอลล์และกำหนดกฎที่เหมาะสม
- อัปเดตระบบปฏิบัติการและโปรแกรมอย่างสม่ำเสมอ
- สำรองข้อมูลระบบและการตั้งค่าอย่างสม่ำเสมอ

6. การตรวจสอบค่าที่ตั้งแล้ว

รายการตรวจสอบ	Windows	Linux
ตรวจสอบ IP Address	<code>ipconfig</code>	<code>ip a</code>
ตรวจสอบเส้นทางเครือข่าย	<code>route print</code>	<code>ip route</code>
ตรวจสอบการเชื่อมต่อ	<code>ping, tracert</code>	<code>ping, traceroute</code>
ตรวจสอบ DNS	<code>nslookup</code>	<code>dig / nslookup</code>
ตรวจสอบเวลาระบบ	<code>date / time</code>	<code>date</code>
ตรวจสอบสถานะบริการ	<code>services.msc</code>	<code>systemctl status</code>

7. ข้อควรระวัง

- ห้ามกำหนดค่า IP Address ซ้ำกับเครื่องอื่นในเครือข่าย
- ตรวจสอบความถูกต้องของ Gateway และ DNS
- การเปลี่ยนแปลงค่าระบบควรบันทึกและทดสอบก่อนนำไปใช้งานจริง
- การกำหนดค่าที่ไม่ถูกต้องอาจทำให้ระบบไม่สามารถเชื่อมต่อเครือข่ายได้
- ปฏิบัติตามนโยบายความปลอดภัยขององค์กรอย่างเคร่งครัด

8. สรุป



การกำหนดค่าพื้นฐานของระบบและเครือข่ายเป็นขั้นตอนสำคัญที่ทำให้เครื่องแม่ข่ายสามารถทำงานได้อย่างเสถียร ปลอดภัย และเชื่อมต่อเครือข่ายได้อย่างถูกต้อง ผู้ดูแลระบบควรตรวจสอบและบันทึกค่าที่ตั้งทุกครั้ง พร้อมทดสอบการใช้งานก่อนให้บริการจริง



จำไว้เสมอ : “กำหนดค่าถูกต้อง ปลอดภัย และตรวจสอบได้ คือรากฐานของระบบที่มั่นคง”

ในความรู้ที่ 3

การจัดการผู้ใช้งานและกลุ่มผู้ใช้งาน



จุดประสงค์

- เพื่อให้ผู้เรียนสามารถจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งาน สร้าง แก้ไข ลบ และกำหนดคุณสมบัติของผู้ใช้ รวมถึงการจัดการกลุ่มผู้ใช้ได้อย่างถูกต้อง ปลอดภัย และเหมาะสมกับนโยบายขององค์กร

1. ความสำคัญของการจัดการผู้ใช้งานและกลุ่มผู้ใช้งาน

การจัดการผู้ใช้งานและกลุ่มผู้ใช้งานอย่างเป็นระบบ ช่วยให้การควบคุม การเข้าถึงทรัพยากรมีประสิทธิภาพ ลดความเสี่ยงด้านความปลอดภัย และสะดวกต่อการบริหารจัดการ เมื่อมีผู้ใช้งานจำนวนมาก



เพิ่มความปลอดภัย
ควบคุมการเข้าถึง
อย่างเหมาะสม



บริหารจัดการง่าย
ใช้กลุ่มช่วยลด
ความซับซ้อน



ตรวจสอบได้
ติดตามการใช้งาน
และการเปลี่ยนแปลง



ประหยัดเวลา
กำหนดสิทธิ์เป็นกลุ่ม
ได้รวดเร็ว

2. หลักการจัดการผู้ใช้งานและกลุ่มผู้ใช้งาน



กำหนดเฉพาะสิ่งที่จำเป็น
สร้างบัญชีผู้ใช้และกลุ่มเฉพาะที่จำเป็นในการใช้งาน



ใช้กลุ่มแทนผู้ใช้รายบุคคล
กำหนดสิทธิ์ให้กลุ่ม เพื่อลดงานและลดความผิดพลาด



สิทธิ์ตามหน้าที่
กำหนดสิทธิ์อย่างเหมาะสมตามบทบาทและหน้าที่



ตรวจสอบและบำรุงรักษา
ทบทวนบัญชีผู้ใช้และกลุ่มเป็นประจำ

3. การจัดการผู้ใช้งานและกลุ่มผู้ใช้งาน (ตัวอย่างคำสั่ง)

3.1 Windows Server (PowerShell / Command Prompt)

3.1.1 การจัดการผู้ใช้งาน

การดำเนินการ	คำสั่งตัวอย่าง
สร้างผู้ใช้	New-LocalUser -Name "user01" -Password (ConvertTo-SecureString "P@ssw0rd!" -AsPlainText -Force) -User01 -Description "พนักงานทั่วไป"
ลบผู้ใช้	Remove-LocalUser -Name "user01"
ปิดการใช้งานผู้ใช้	Disable-LocalUser -Name "user01"
เปิดการใช้งานผู้ใช้	Enable-LocalUser -Name "user01"
เปลี่ยนรหัสผ่าน	Set-LocalUser -Name "user01" -Password (ConvertTo-SecureString "NewP@ss!" -AsPlainText -Force)
แสดงรายชื่อผู้ใช้	Get-LocalUser

3.1.2 การจัดการกลุ่มผู้ใช้

การดำเนินการ	คำสั่งตัวอย่าง
สร้างกลุ่ม	New-LocalGroup -Name "IT_Users" -Description "กลุ่มผู้ใช้ฝ่ายไอที"
ลบกลุ่ม	Remove-LocalGroup -Name "IT_Users"
เพิ่มผู้ใช้เข้ากลุ่ม	Add-LocalGroupMember -Group "IT_Users" -Member "user01"
ลบผู้ใช้จากกลุ่ม	Remove-LocalGroupMember -Group "IT_Users" -Member "user01"
แสดงรายชื่อกลุ่ม	Get-LocalGroup
แสดงสมาชิกในกลุ่ม	Get-LocalGroupMember -Group "IT_Users"

3.2 Linux (Ubuntu Server)

3.2.1 การจัดการผู้ใช้งาน

การดำเนินการ	คำสั่งตัวอย่าง
สร้างผู้ใช้	sudo adduser user01
ลบผู้ใช้	sudo deluser --remove-home user01
ปิดการใช้งานผู้ใช้	sudo usermod -L user01
เปิดการใช้งานผู้ใช้	sudo usermod -U user01
เปลี่ยนรหัสผ่าน	sudo passwd user01
แสดงรายชื่อผู้ใช้	cat /etc/passwd หรือ getent passwd

3.2.2 การจัดการกลุ่มผู้ใช้

การดำเนินการ	คำสั่งตัวอย่าง
สร้างกลุ่ม	sudo groupadd IT_Users
ลบกลุ่ม	sudo groupdel IT_Users
เพิ่มผู้ใช้เข้ากลุ่ม	sudo usermod -aG IT_Users user01
ลบผู้ใช้จากกลุ่ม	sudo gpasswd -d user01 IT_Users
แสดงรายชื่อกลุ่ม	cat /etc/group หรือ getent group
แสดงสมาชิกในกลุ่ม	getent group IT_Users

4. คุณสมบัติของบัญชีผู้ใช้ (User Attributes)

คุณสมบัติ	คำอธิบาย
Username	ชื่อบัญชีผู้ใช้ ใช้สำหรับเข้าสู่ระบบ
Password	รหัสผ่านในการยืนยันตัวตน
Full Name / GECOS	ชื่อจริง-นามสกุล / รายละเอียดผู้ใช้
Home Directory	ไดเรกทอรีส่วนตัวของผู้ใช้
Shell / Logon Script	โปรแกรมเชลล์หรือสคริปต์เมื่อเข้าสู่ระบบ
Account Status	สถานะบัญชี (ใช้งาน / ปิดใช้งาน / หมดอายุ)
Group Membership	กลุ่มที่ผู้ใช้เป็นสมาชิก
Permissions	สิทธิ์การเข้าถึงไฟล์/โฟลเดอร์/ทรัพยากร

หมายเหตุ : ควรกำหนดคุณสมบัติผู้ใช้ให้เหมาะสมกับหน้าที่และสิทธิ์ที่จำเป็นเท่านั้น

6. แนวปฏิบัติที่ดี (Best Practices)

- ✓ สร้างเฉพาะบัญชีผู้ใช้ที่จำเป็น
- ✓ ใช้กลุ่มในการกำหนดสิทธิ์แทนการกำหนดให้ผู้ใช้รายบุคคล
- ✓ กำหนดรหัสผ่านที่รัดกุมและเปลี่ยนรหัสผ่านเป็นระยะ
- ✓ ปิดการใช้งานบัญชีที่ไม่ใช้งาน และลบบัญชีที่ไม่จำเป็น
- ✓ ตรวจสอบสมาชิกกลุ่มและสิทธิ์อย่างสม่ำเสมอ
- ✓ บันทึกการเปลี่ยนแปลงและตรวจสอบเหตุการณ์ (Audit Log)
- ✓ ปฏิบัติตามนโยบายความปลอดภัยขององค์กรอย่างเคร่งครัด



5. ตัวอย่างการใช้กลุ่มผู้ใช้ตามหน้าที่

กลุ่มผู้ใช้	หน้าที่โดยย่อ	ตัวอย่างสิทธิ์ที่กำหนด
Admins	ผู้ดูแลระบบ	- สิทธิ์เต็มในการจัดการระบบ - ติดตั้งโปรแกรม / เปลี่ยนแปลงการตั้งค่า
IT_Users	พนักงานฝ่ายไอที	- เข้าถึงไฟล์ระบบและเครื่องมือไอที - จัดการผู้ใช้บางส่วน, สำรองข้อมูล
Staff	พนักงานทั่วไป	- ใช้งานไฟล์และโปรแกรมทั่วไป - เข้าถึงโฟลเดอร์ที่ได้รับอนุญาต
Guests	ผู้เยี่ยมชม/ชั่วคราว	- เข้าถึงเฉพาะทรัพยากรที่กำหนด - ไม่สามารถเปลี่ยนแปลงระบบ

ข้อแนะนำ : ใช้กลุ่มช่วยลดความซับซ้อนในการกำหนดสิทธิ์และการบำรุงรักษาระบบ

7. สรุป



การจัดการผู้ใช้งานและกลุ่มผู้ใช้งานอย่างเป็นระบบ ช่วยให้การควบคุมการเข้าถึง ทรัพยากรได้อย่างปลอดภัย มีประสิทธิภาพ และสะดวกต่อการบริหารจัดการ ควรปฏิบัติตามแนวทางที่ดีและตรวจสอบอย่างสม่ำเสมอ เพื่อป้องกัน ความเสี่ยงและรักษาความปลอดภัยของระบบ



จำไว้เสมอ : "บัญชีผู้ใช้ทุกบัญชีคือประตูสู่ระบบ จงเปิดให้เฉพาะผู้ที่จำเป็น และปิดเมื่อไม่ใช้งาน"

ในความรู้ที่ 4

Windows Server 2019

กำหนดสิทธิ์การเข้าถึงทรัพยากรบนเครื่องแม่ข่าย



จุดประสงค์

- เพื่อให้ผู้เรียนสามารถกำหนดสิทธิ์การเข้าถึงไฟล์ โฟลเดอร์ และทรัพยากรต่าง ๆ บน Windows Server 2019 ได้อย่างถูกต้อง ปลอดภัย และเหมาะสมกับนโยบายขององค์กร

1. ความหมายของสิทธิ์การเข้าถึง (Permissions)

สิทธิ์การเข้าถึง คือ การกำหนดว่าผู้ใช้หรือกลุ่มผู้ใช้สามารถทำอะไรกับทรัพยากรนั้นได้บ้าง เช่น อ่าน แก้ไข ลบ หรือไม่สามารถเข้าถึงได้ การกำหนดสิทธิ์แบ่งออกเป็น 2 ระดับ

1. สิทธิ์บนไฟล์/โฟลเดอร์ (NTFS Permissions)



ควบคุมการเข้าถึงไฟล์ และโฟลเดอร์โดยตรง เช่น Read, Write, Modify

2. สิทธิ์การแชร์ (Share Permissions)



ควบคุมการเข้าถึงเมื่อมีการแชร์ทรัพยากรผ่านเครือข่าย เช่น Full Control, Change, Read

หมายเหตุ : สิทธิ์ที่มีผลจริง = สิทธิ์ Share Permissions ร่วมกับ NTFS Permissions โดยจะใช้สิทธิ์ที่ "เข้มงวดกว่า" (Deny > Allow)

2. ทรัพยากรที่สามารถกำหนดสิทธิ์ได้

- ไฟล์และโฟลเดอร์
- เครื่องพิมพ์ (Printers)
- การแชร์โฟลเดอร์ (Shares)
- บริการต่าง ๆ เช่น IIS, SQL Server



3. หลักการกำหนดสิทธิ์

- กำหนดสิทธิ์ตาม "กลุ่มผู้ใช้" แทนการกำหนดสิทธิ์รายบุคคล เพื่อง่ายต่อการบริหารจัดการ
- ให้สิทธิ์เท่าที่จำเป็น (Least Privilege)
- ตรวจสอบและทบทวนสิทธิ์อย่างสม่ำเสมอ
- บันทึกการเปลี่ยนแปลงสิทธิ์ (Audit) เพื่อตรวจสอบย้อนหลัง



4. ขั้นตอนการกำหนดสิทธิ์การเข้าถึงโฟลเดอร์ที่แชร์ (ตัวอย่าง: แชร์โฟลเดอร์ "DATA")

1 สร้างโฟลเดอร์
สร้างโฟลเดอร์ที่ต้องการแชร์ เช่น D:\DATA

2 กำหนดสิทธิ์ NTFS
คลิกขวาโฟลเดอร์ > Properties > แท็บ Security > Edit...

3 เพิ่มผู้ใช้หรือกลุ่ม
คลิก Add... > พิมพ์ชื่อผู้ใช้หรือกลุ่ม > Check Names > OK

4 กำหนดสิทธิ์ NTFS
เลือกผู้ใช้/กลุ่ม > กำหนดสิทธิ์ตามความเหมาะสม > OK

5 แชร์โฟลเดอร์
แท็บ Sharing > Advanced Sharing > ตีถูก Share this folder > ตั้งชื่อ Share Name > Permissions

6 กำหนดสิทธิ์การแชร์ (Share)
เลือกผู้ใช้/กลุ่ม > กำหนดสิทธิ์ เช่น Change หรือ Full Control

ข้อควรจำ : เมื่อแชร์แล้ว ผู้ใช้จะต้องมีสิทธิ์ทั้ง Share Permissions และ NTFS Permissions จึงจะเข้าถึงทรัพยากรได้สำเร็จ

5. ตัวอย่างสิทธิ์ที่ใช้บ่อย

สิทธิ์	ความหมาย
NTFS Permissions	
Full Control	ควบคุมได้ทั้งหมด (อ่าน เขียน แก้ไข ลบ เปลี่ยนสิทธิ์)
Modify	แก้ไข สร้าง ลบไฟล์ได้ แต่เปลี่ยนสิทธิ์ไม่ได้
Read & Execute	อ่านและเรียกใช้งานไฟล์ได้
List Folder Contents	แสดงรายชื่อไฟล์และโฟลเดอร์ในโฟลเดอร์นั้น
Read	อ่านไฟล์ได้
Write	เขียนไฟล์ได้
Deny	ปฏิเสธการเข้าถึง (มีผลเหนือกว่า Allow)
Share Permissions	
Full Control	ควบคุมได้ทั้งหมด
Change	เพิ่ม แก้ไข ลบไฟล์ได้
Read	อ่านไฟล์และแสดงรายชื่อได้
Deny	ปฏิเสธการเข้าถึง

6. การตรวจสอบสิทธิ์ที่กำหนด

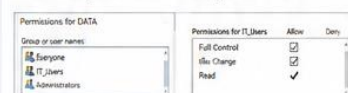
6.1 ตรวจสอบ NTFS Permissions

คลิกขวาโฟลเดอร์ > Properties > Security



6.2 ตรวจสอบ Share Permissions

คลิกขวาโฟลเดอร์ > Properties > แท็บ Sharing > Advanced Sharing > Permissions



6.3 ทดสอบการเข้าถึง

- ✓ เข้าสู่ระบบด้วยผู้ใช้ที่ต้องการทดสอบ
- ✓ เข้าถึงโฟลเดอร์ผ่าน \\Server\DATA
- ✓ ตรวจสอบว่าสามารถอ่าน/เขียนได้ตามสิทธิ์ที่กำหนดหรือไม่

7. ข้อควรระวัง

- ✗ อย่าให้สิทธิ์ Full Control กับทุกคน
- ✗ หลีกเลี่ยงการใช้สิทธิ์กับผู้ใช้รายบุคคล
- ✗ ใช้กลุ่มผู้ใช้ในการกำหนดสิทธิ์แทน
- ✗ ตรวจสอบการทำงานของสิทธิ์หลังจากแชร์ทุกครั้ง
- ✗ หากเข้าถึงไม่ได้ ให้ตรวจสอบสิทธิ์ทั้ง Share และ NTFS และลำดับ Deny ก่อน Allow
- ✗ สำรองข้อมูลก่อนการเปลี่ยนแปลงสิทธิ์สำคัญ

เทคนิคเพิ่มเติม

- ✓ ใช้คำสั่ง PowerShell ตรวจสอบสิทธิ์ เช่น Get-Acl "D:\DATA"
- ✓ จัดทำเอกสารนโยบายการกำหนดสิทธิ์ และทบทวนอย่างสม่ำเสมอ

```
PS C:\> Get-Acl "D:\DATA" | Format-List
Path       : Microsoft.PowerShell.Core\FileSystem::D:\DATA
Owner      : BUILTIN\Administrators
Access     :
            NT AUTHORITY\SYSTEM Allow FullControl
            SERVER\IT_Users Allow Modify
```



สรุป

การกำหนดสิทธิ์การเข้าถึงทรัพยากรบน Windows Server 2019 ควรพิจารณาทั้ง Share Permissions และ NTFS Permissions ร่วมกัน เพื่อควบคุมการเข้าถึงอย่างปลอดภัยและมีประสิทธิภาพ สอดคล้องกับนโยบายความปลอดภัยขององค์กร

★ จำไว้เสมอ

"ให้สิทธิ์เท่าที่จำเป็น ตรวจสอบสม่ำเสมอ ปลอดภัยแน่นอน"



ใบความรู้ที่ 5 การตั้งค่าการควบคุมเครื่องแม่ข่ายระยะไกล

การควบคุมเครื่องแม่ข่ายระยะไกล (Remote Administration) ช่วยให้ผู้ใช้และระบบสามารถเข้าถึงและจัดการเครื่องแม่ข่ายจากคอมพิวเตอร์เครื่องอื่นได้อย่างสะดวกและปลอดภัย โดยใช้เครื่องมือ Remote Desktop และการตั้งค่าที่เกี่ยวข้องใน Windows Server 2019



ประโยชน์

- ✓ เข้าถึงและจัดการเครื่องแม่ข่ายจากระยะไกล
- ✓ ลดค่าใช้จ่ายและเวลาในการเดินทาง
- ✓ แก้ไขปัญหาและดูแลระบบได้อย่างรวดเร็ว
- ✓ เพิ่มประสิทธิภาพในการบริหารจัดการระบบ

สิ่งที่ต้องมี

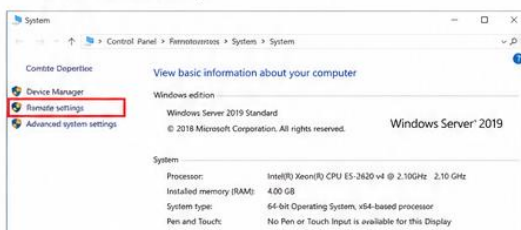
- Windows Server 2019 ที่ติดตั้งและพร้อมใช้งาน (มี IP Address ที่แน่นอน)
- คอมพิวเตอร์ปลายทางที่ใช้สำหรับเชื่อมต่อ
- เครือข่ายที่เชื่อมต่อกันได้ (LAN หรือ VPN)
- มีสิทธิ์ผู้ดูแลระบบ (Administrator) บนเครื่องแม่ข่าย



ขั้นตอนการตั้งค่าการควบคุมเครื่องแม่ข่ายระยะไกล (Remote Desktop)

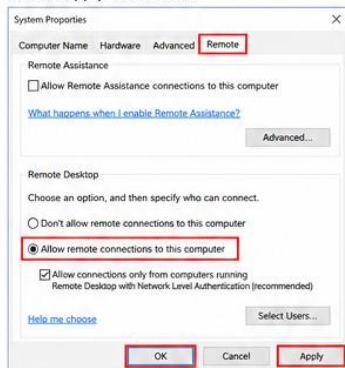
1 เปิดการใช้งาน Remote Desktop

1. คลิกขวาที่ This PC หรือ Computer แล้วเลือก Properties
2. คลิก Remote settings



2 อนุญาตการเชื่อมต่อระยะไกล

1. ในหน้าต่าง System Properties แท็บ Remote
2. เลือก Allow remote connections to this computer
3. คลิก Apply แล้วคลิก OK



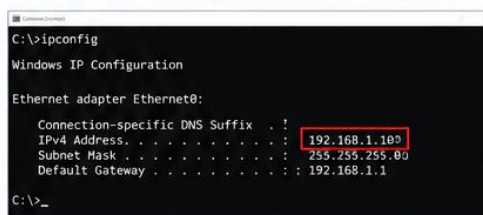
3 เปิดไฟร์วอลล์สำหรับ Remote Desktop

1. เปิด Windows Defender Firewall with Advanced Security
2. คลิก Inbound Rules
3. ตรวจสอบว่าเปิดใช้งานกฎต่อไปนี้
 - Remote Desktop – User Mode (TCP-In)
 - Remote Desktop – User Mode (UDP-In)
 (หากปิดใช้งาน ให้คลิกขวาแล้วเลือก Enable Rule)



4 ตรวจสอบ IP Address ของเครื่องแม่ข่าย

1. เปิด Command Prompt
2. พิมพ์คำสั่ง ipconfig แล้วกด Enter
3. จดจำค่า IPv4 Address (เช่น 192.168.1.10) สำหรับใช้เชื่อมต่อ



5 การเชื่อมต่อด้วย Remote Desktop

1. ที่เครื่องคอมพิวเตอร์ปลายทาง กดปุ่ม Windows + R
2. พิมพ์ mstsc, แล้วกด Enter
3. ในช่อง Computer พิมพ์ IP Address ของเครื่องแม่ข่าย แล้วคลิก Connect
4. กรอกรหัสผู้ใช้และรหัสผ่านของบัญชีที่มีสิทธิ์บนเครื่องแม่ข่าย



💡 ข้อแนะนำด้านความปลอดภัย

- ควรใช้ Network Level Authentication (NLA) (ค่าเริ่มต้นและเปิดใช้งาน)
- ใช้รหัสผ่านที่รัดกุมและเปลี่ยนรหัสผ่านสม่ำเสมอ
- จำกัดการเข้าถึงเฉพาะ IP หรือกลุ่มผู้ใช้ที่เชื่อถือได้
- หากเชื่อมต่อผ่านอินเทอร์เน็ต ควรใช้ VPN เพื่อความปลอดภัย

สรุป

การตั้งค่าการควบคุมเครื่องแม่ข่ายระยะไกลใน Windows Server 2019 ทำได้โดย เปิดใช้งาน Remote Desktop, อนุญาตการเชื่อมต่อ, เปิดไฟร์วอลล์, ตรวจสอบ IP Address และเชื่อมต่อจากเครื่องปลายทาง จะช่วยให้ผู้ใช้และระบบสามารถบริหารจัดการเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ สะดวก และปลอดภัย

การตรวจสอบและบันทึกการตั้งค่าระบบ

(ชิ้นงาน: แผนการจัดการผู้ใช้และสิทธิ์, รายงานการตั้งค่าระบบ)



1. วัตถุประสงค์

- ตรวจสอบการตั้งค่าระบบของ Windows Server 2019 ได้อย่างถูกต้อง
- บันทึกข้อมูลการตั้งค่าระบบเป็นเอกสาร/รายงานได้ครบถ้วน
- จัดทำแผนการจัดการผู้ใช้และสิทธิ์ได้เหมาะสมตามความต้องการขององค์กร



2. ความสำคัญ

- ช่วยให้ทราบสถานะและความถูกต้องของการตั้งค่าระบบ
- ใช้เป็นข้อมูลอ้างอิงสำหรับการดูแลรักษาและแก้ไขปัญหา
- ช่วยวางแผนการจัดการผู้ใช้และสิทธิ์อย่างเป็นระบบ
- สนับสนุนการปฏิบัติตามนโยบายความปลอดภัยขององค์กร



3. รายการที่ควรตรวจสอบและบันทึก

- ข้อมูลทั่วไปของระบบ
 - ชื่อเซิร์ฟเวอร์, ชื่อโดเมน/เวิร์กกรุ๊ป, IP Address, เวอร์ชัน OS
- การตั้งค่าเครือข่าย
 - IP Address, Subnet Mask, Default Gateway, DNS
- การตั้งค่าเวลาและโซนเวลา
 - Time Zone, NTP Server, การซิงโครไนซ์เวลา
- บทบาทและฟีเจอร์ (Roles and Features)
 - รายการบทบาทและฟีเจอร์ที่ติดตั้งและสถานะ
- การตั้งค่าความปลอดภัย
 - นโยบายรหัสผ่าน, Account Lockout, Windows Firewall
- การตั้งค่าการอัปเดต
 - Windows Update, การติดตั้งอัปเดตล่าสุด
- การสำรองข้อมูล
 - วิธีการสำรองข้อมูล, ตำแหน่งจัดเก็บ, กำหนดการสำรอง
- บันทึกเหตุการณ์ระบบ (Event Logs)
 - ตรวจสอบและบันทึกค่าที่สำคัญ เช่น System, Security



4. วิธีการตรวจสอบและบันทึกข้อมูล

รายการ	วิธีการตรวจสอบ	เครื่องมือ/คำสั่งที่ใช้
ข้อมูลทั่วไปของระบบ	ดูชื่อเครื่อง, โดเมน/เวิร์กกรุ๊ป, เวอร์ชัน OS	System > About หรือคำสั่ง: systeminfo
การตั้งค่าเครือข่าย	ดูค่าการตั้งค่า IP, DNS, Gateway	Network and Sharing Center หรือคำสั่ง: ipconfig /all
การตั้งค่าเวลาและโซนเวลา	ตรวจสอบ Time Zone และการซิงโครไนซ์เวลา	Date and Time หรือคำสั่ง: w32tm /query /status
บทบาทและฟีเจอร์	ดูบทบาทและฟีเจอร์ที่ติดตั้ง	Server Manager > Manage > Add Roles and Features หรือคำสั่ง: Get-WindowsFeature
การตั้งค่าความปลอดภัย	ตรวจสอบนโยบายความปลอดภัย	Local Security Policy หรือคำสั่ง: secedit /export /cfg security.inf
การตั้งค่าการอัปเดต	ดูสถานะการอัปเดตล่าสุด	Settings > Update & Security หรือคำสั่ง: Get-WindowsUpdateLog
การสำรองข้อมูล	ตรวจสอบสถานะและกำหนดการสำรอง	Windows Server Backup หรือ wadmin get status
บันทึกเหตุการณ์ระบบ	ตรวจสอบเหตุการณ์สำคัญ	Event Viewer (eventvwr.msc)

5. ชิ้นงานที่ต้องจัดทำ



- แผนการจัดการผู้ใช้และสิทธิ์ (User & Permission Management Plan)
 - ระบุผู้ใช้/กลุ่มผู้ใช้
 - กำหนดบทบาทหน้าที่
 - กำหนดสิทธิ์การเข้าถึงทรัพยากร
 - แนวทางการสร้าง, ปรับปรุง, ลบผู้ใช้



- รายงานการตั้งค่าระบบ (System Configuration Report)
 - สรุปผลการตรวจสอบตามรายการในข้อ 3
 - ระบุวันที่ตรวจสอบและผู้จัดทำ
 - จัดทำรูปแบบรายงานที่ชัดเจน

6. ตัวอย่างโครงสร้างรายงานการตั้งค่าระบบ

- ข้อมูลทั่วไป

ชื่อเซิร์ฟเวอร์	:	
โดเมน/เวิร์กกรุ๊ป	:	
เวอร์ชันระบบปฏิบัติการ	:	
วันที่ตรวจสอบ	:	
ผู้จัดทำ	:	

2. ผลการตรวจสอบและการตั้งค่าระบบ

รายการ	ค่าที่ตรวจพบ	หมายเหตุ

3. สรุปและข้อเสนอแนะ

.....



หมายเหตุ

- ✓ ควรบันทึกข้อมูลให้ครบถ้วนและเป็นปัจจุบัน
- เก็บรักษารายงานไว้ในที่ปลอดภัย และสำรองข้อมูลไว้ด้วย
- ทบทวนและปรับปรุงแผนการจัดการผู้ใช้และสิทธิ์เป็นประจำ

6. แบบฝึกหัด

แบบฝึกหัดหน่วยที่ 2

1. หลักใดที่กำหนดสิทธิ์ขั้นต่ำตามหน้าที่ของผู้ใช้
 - ก. Least Privilege
 - ข. Load Balancing
 - ค. Fault Tolerance
 - ง. High Availability
2. วิธีใดช่วยให้บริหารสิทธิ์ผู้ใช้จำนวนมากได้สะดวก
 - ก. ให้สิทธิ์ทีละไฟล์
 - ข. ให้สิทธิ์ผ่านกลุ่ม
 - ค. ใช้บัญชีร่วมกัน
 - ง. เพิ่มทุกคนเป็นผู้ดูแล
3. คำสั่งใดใช้แสดงบัญชี Local user ใน Command Prompt
 - ก. net user
 - ข. net share
 - ค. net start
 - ง. net session
4. เมื่อบุคลากรพ้นสภาพ วิธีใดหยุดการเข้าสู่ระบบและยังคงข้อมูลบัญชีไว้
 - ก. Rename
 - ข. Disable
 - ค. Delete
 - ง. Duplicate
5. NTFS Permissions ถูกกำหนดจากแท็บใดของโฟลเดอร์
 - ก. General
 - ข. Sharing
 - ค. Security
 - ง. Customize
6. หาก Share เป็น Read แต่ NTFS เป็น Modify ผู้ใช้ผ่านเครือข่ายทำอะไรได้
 - ก. อ่านข้อมูล
 - ข. ลบข้อมูล
 - ค. แก้ไขข้อมูล
 - ง. เปลี่ยนสิทธิ์

7. เครื่องมือใดใช้ตรวจสอบสิทธิ์รวมของผู้ใช้ต่อโพลเดอร์

- ก. Event Viewer
- ข. Effective Access
- ค. Task Scheduler
- ง. Device Manager

8. คำสั่งใดใช้ตรวจสอบค่า IPv4, Gateway และ DNS ของ Adapter

- ก. hostname
- ข. whoami
- ค. ipconfig /all
- ง. net localgroup

9. การตั้งค่าใดควรเปิดร่วมกับ Remote Desktop เมื่อ Client รองรับ

- ก. NLA
- ข. DHCP
- ค. SMB
- ง. Telnet

10. หลักฐานใดเหมาะสำหรับยืนยันว่าเชื่อมต่อ Remote Desktop ด้วยบัญชีที่กำหนด

- ก. ผล whoami ใน Session
- ข. ภาพหน้าจอ Desktop เป้า
- ค. รายชื่อไฟล์ในเครื่อง Client
- ง. หมายเลข Serial ของเครื่อง Host

ตอนที่ 2 แบบอัตนัย (5 ข้อ)

1. จากสถานการณ์โรงเรียนที่มีผู้บริหาร ครู และเจ้าหน้าที่ จงออกแบบบัญชี กลุ่ม และสิทธิ์อย่างย่อ

.....

.....

.....

2. อธิบายวงจรชีวิตบัญชีตั้งแต่การขอสร้างจนถึงการปิดใช้งาน พร้อมเหตุผลที่ควร Disable ก่อน Delete

.....

.....

.....

3. อธิบายความแตกต่างระหว่าง Share Permissions และ NTFS Permissions พร้อมยกตัวอย่างสิทธิ์ที่มีผลจริง

.....

.....

.....

4. เขียนลำดับตรวจสอบก่อนเปิด Remote Desktop และเมื่อ Client เชื่อมต่อไม่ได้อย่างน้อย 5 ขั้นตอน

.....

.....

.....

5. ระบุองค์ประกอบรายการงานการตั้งค่าระบบอย่างน้อย 6 รายการ และข้อมูลที่ต้องปิดบัง

.....

.....

.....

7. เอกสารอ้างอิง

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

8. ภาคผนวก

8.1 เฉลย แบบฝึกหัดบทเรียนที่ 2

เฉลยแบบฝึกหัด ตอนที่ 1

ข้อ	1	2	3	4	5	6	7	8	9	10
คำตอบ	ก	ข	ก	ข	ค	ก	ข	ค	ก	ก

แนวคำตอบแบบฝึกหัด ตอนที่ 2

ข้อ	แนวคำตอบสำคัญ
1	กำหนดบัญชีรายบุคคล; จัดกลุ่มตามบทบาท; ให้ Teachers_RW แก้ไขพื้นที่ครู, Staff_R อ่านพื้นที่เจ้าหน้าที่, ผู้ดูแลและผู้ใช้ RDP แยกกลุ่ม; ทดสอบทั้ง Allow/Deny
2	ขอและอนุมัติ > สร้าง > จัดกลุ่ม/ให้สิทธิ์ > ใช้งานและติดตาม > ทบทวน > Disable เมื่อย้าย/พ้นสภาพ > ลบเมื่อพ้นระยะเก็บ; Disable หยุดการเข้าสู่ระบบแต่ยังคงข้อมูลสำหรับตรวจสอบ
3	Share ใช้เมื่อเข้าผ่านเครือข่าย; NTFS ใช้ทั้งหน้าเครื่องและเครือข่าย; ผ่านเครือข่ายต้องผ่านทั้งสองชั้น เช่น Share Read + NTFS Modify มีผลเป็นอ่านได้
4	ตรวจ IP/เวลา/เครือข่าย > เปิด RDP > NLA > ผู้ได้รับอนุญาต > Firewall/Profile/Scope > ทดสอบ mstsc > whoami > Sign out; เมื่อผิดให้แยกตรวจ Network, Service/Setting, Account และ Firewall
5	ผู้ปฏิบัติ/เวลา, วัตถุประสงค์, แผนผู้ใช้-กลุ่ม-สิทธิ์, ค่าระบบ/เครือข่าย, ผลทดสอบ, ปัญหาและผลทดสอบซ้ำ, ข้อเสนอแนะ/ส่งมอบ; ปิดบังรหัสผ่าน Product Key Token และข้อมูลลับ

	ใบงานที่ 1		หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชาระบบปฏิบัติการเครื่องแม่ข่าย		สอนครั้งที่ 5
	ชื่อหน่วยการเรียนรู้	ทฤษฎี 1 ชม.	
	งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	ปฏิบัติ 4 ชม.	
ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น			

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถวางแผน สร้าง และบริหารจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานบนระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างถูกต้อง พร้อมกำหนดสิทธิ์การใช้งานเบื้องต้นได้อย่างเหมาะสมและปลอดภัย

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับหลักการบริหารจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานบนระบบปฏิบัติการเครื่องแม่ข่าย
2. ปฏิบัติการสร้าง แก้ไข และจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานได้อย่างถูกต้อง
3. กำหนดสิทธิ์การเข้าถึงทรัพยากรเบื้องต้นได้เหมาะสมกับหน้าที่ของผู้ใช้งาน

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายหลักการบริหารจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานได้
2. บอกหน้าที่ของบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานประเภทต่าง ๆ ได้ถูกต้อง
3. วิเคราะห์ความสำคัญของการกำหนดสิทธิ์ผู้ใช้งานได้อย่างเหมาะสม

4.2 ทักษะพิสัย

1. สร้างบัญชีผู้ใช้งานบนระบบปฏิบัติการเครื่องแม่ข่ายได้ถูกต้อง
2. สร้างและจัดการกลุ่มผู้ใช้งานได้ถูกต้อง
3. เพิ่มและนำสมาชิกออกจากกลุ่มผู้ใช้งานได้ถูกต้อง

4.3 จิตพิสัย

1. มีความรับผิดชอบ รอบคอบ และปฏิบัติตามขั้นตอนการทำงาน
2. ตระหนักถึงความสำคัญของความปลอดภัยในการจัดการบัญชีผู้ใช้งาน

4.4 ประยุกต์ใช้และรับผิดชอบ

ประยุกต์ใช้การจัดการบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานให้เหมาะสมกับสถานการณ์จำลองขององค์กรขนาดเล็กได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์หรือโน้ตบุ๊ก
2. โปรแกรม VMware Workstation / VMware Player
3. ระบบปฏิบัติการ Windows Server 2019
4. คู่มือปฏิบัติการหรือใบความรู้

6. คำแนะนำ/ข้อควรระวัง

1. ศึกษาใบความรู้ก่อนลงมือปฏิบัติงานทุกครั้ง
2. ตรวจสอบชื่อบัญชีผู้ใช้งานก่อนบันทึกข้อมูล
3. กำหนดรหัสผ่านตามหลักความปลอดภัยของระบบ
4. ใช้บัญชี Administrator เท่านั้น
5. บันทึกผลการปฏิบัติงานทุกขั้นตอน
6. ปฏิบัติงานด้วยความรอบคอบและรับผิดชอบ

7. ขั้นตอนการปฏิบัติงาน

สถานการณ์จำลอง : โรงเรียนแห่งหนึ่งต้องการจัดการบัญชีผู้ใช้งานสำหรับบุคลากร โดยแบ่งออกเป็น 3 กลุ่ม ได้แก่ ผู้บริหาร ครู และเจ้าหน้าที่

ให้ผู้เรียนปฏิบัติดังนี้

1. เปิดเครื่องเสมือน Windows Server 2019
2. วางแผนกำหนดบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานที่กำหนด
3. สร้างกลุ่มผู้ใช้งาน ได้แก่
Administrators
Teachers
Staff
4. สร้างบัญชีผู้ใช้งานจำนวนอย่างน้อย 3 บัญชี
5. กำหนดรหัสผ่านให้กับบัญชีผู้ใช้งาน
6. เพิ่มสมาชิกเข้าสู่กลุ่มที่เกี่ยวข้อง
7. ตรวจสอบความถูกต้องของบัญชีและสมาชิกในแต่ละกลุ่ม
8. บันทึกภาพหน้าจอผลการปฏิบัติงาน
9. สรุปผลการปฏิบัติงานและปัญหาที่พบ

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การวางแผนและเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ขั้นตอนและความถูกต้อง	ครบ ถูกลำดับ ทำได้อิสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกกรณี มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านเพียงบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ ชัดเจน ย้อนตรงได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ	ไม่มีหลักฐานตรงได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 2		หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย		สอนครั้งที่ 6
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
	ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถกำหนดและบริหารจัดการสิทธิ์การเข้าถึงทรัพยากรบนระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างถูกต้อง เหมาะสม และปลอดภัยตามบทบาทหน้าที่ของผู้ใช้งาน

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับหลักการกำหนดสิทธิ์การเข้าถึงทรัพยากรบนเครื่องแม่ข่าย
2. ปฏิบัติการกำหนดสิทธิ์การเข้าถึงแฟ้มข้อมูลและโฟลเดอร์ได้อย่างถูกต้อง
3. ตรวจสอบและประเมินผลการกำหนดสิทธิ์ให้เหมาะสมกับการใช้งานจริง

4. จุดประสงค์เชิงพฤติกรรม

4.1 ทักษะพิสัย

1. อธิบายความหมายและประเภทของสิทธิ์การเข้าถึงทรัพยากรได้
2. จำแนกสิทธิ์การใช้งาน เช่น Read, Modify และ Full Control ได้ถูกต้อง
3. วิเคราะห์ผลกระทบจากการกำหนดสิทธิ์ที่ไม่เหมาะสมได้

4.2 ทักษะพิสัย (Psychomotor Domain)

1. สร้างโฟลเดอร์สำหรับใช้งานร่วมกันบนเครื่องแม่ข่ายได้
2. กำหนด NTFS Permissions ได้ถูกต้อง
3. กำหนด Share Permissions ได้เหมาะสมกับกลุ่มผู้ใช้งาน
4. ทดสอบการเข้าถึงทรัพยากรด้วยบัญชีผู้ใช้แต่ละกลุ่มได้

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้การกำหนดสิทธิ์การเข้าถึงทรัพยากรให้เหมาะสมกับโครงสร้างการทำงานของหน่วยงานขนาดเล็กได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. สมุดจด
2. คอมพิวเตอร์ / สมาร์ทโฟน
3. อินเทอร์เน็ต
4. USB Boot windows 10

6. คำแนะนำ/ข้อควรระวัง

1. ตรวจสอบชื่อกลุ่มผู้ใช้งานก่อนกำหนดสิทธิ์ทุกครั้ง
2. หลีกเลี่ยงการกำหนดสิทธิ์ Full Control โดยไม่จำเป็น
3. ทดสอบสิทธิ์การเข้าถึงหลังการตั้งค่าทุกครั้ง
4. บันทึกผลการปฏิบัติงานและภาพหน้าจอเป็นหลักฐาน
5. ปฏิบัติงานด้วยความรับผิดชอบและรักษาความลับของข้อมูล

7. ขั้นตอนการปฏิบัติงาน

สถานการณ์จำลอง

โรงเรียนแห่งหนึ่งต้องการจัดเก็บข้อมูลกลางบนเครื่องแม่ข่าย โดยกำหนดสิทธิ์การเข้าถึงให้เหมาะสมกับหน้าที่ของบุคลากร ดังนี้

- กลุ่ม Teachers : อ่านและแก้ไขข้อมูลได้
- กลุ่ม Staff : อ่านข้อมูลได้เท่านั้น
- กลุ่ม Administrators : จัดการข้อมูลได้ทั้งหมด

ให้ผู้เรียนปฏิบัติดังนี้

1. เปิดเครื่องเสมือน Windows Server 2019
2. สร้างโฟลเดอร์ชื่อ SchoolData
3. สร้างโฟลเดอร์ย่อย ได้แก่
 Teachers
 Staff
 Shared
4. แชร์โฟลเดอร์ SchoolData ให้สามารถเข้าถึงผ่านเครือข่ายได้
5. กำหนด Share Permissions ให้เหมาะสม
6. กำหนด NTFS Permissions ตามเงื่อนไขที่กำหนด
7. ทดสอบการเข้าใช้งานด้วยบัญชีผู้ใช้จากแต่ละกลุ่ม

8.บันทึกผลการทดสอบและภาพหน้าจอ

9.สรุปปัญหาที่พบและแนวทางแก้ไข

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การวางแผนและเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ขั้นตอนและความถูกต้อง	ครบ ถูกลำดับ ทำได้อิสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกกรณี มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านเพียงบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ ชัดเจน ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ	ไม่มีหลักฐานตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 3	หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 7
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถกำหนดค่าพื้นฐานที่จำเป็นของระบบปฏิบัติการเครื่องแม่ข่าย และตั้งค่าการควบคุมเครื่องแม่ข่ายจากระยะไกลได้อย่างถูกต้อง เหมาะสม และปลอดภัย พร้อมตรวจสอบและบันทึกผลการตั้งค่าระบบได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับการกำหนดค่าพื้นฐานของระบบปฏิบัติการเครื่องแม่ข่ายและการควบคุมจากระยะไกล
2. ปฏิบัติการกำหนดค่าพื้นฐานของระบบและเครือข่ายได้อย่างถูกต้อง
3. ตั้งค่าและทดสอบการควบคุมเครื่องแม่ข่ายจากระยะไกลได้อย่างปลอดภัย
4. ตรวจสอบ บันทึก และจัดทำรายงานผลการตั้งค่าระบบได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายหลักการกำหนดค่าพื้นฐานของระบบปฏิบัติการเครื่องแม่ข่ายได้
2. อธิบายหลักการทำงานของเครื่องแม่ข่ายจากระยะไกลได้
3. วิเคราะห์ข้อดี ข้อจำกัด และความเสี่ยงด้านความปลอดภัยของการบริหารจัดการเครื่องแม่ข่ายจากระยะไกลได้

4.2 ทักษะพิสัย

1. กำหนดชื่อเครื่องแม่ข่าย (Computer Name) ได้ถูกต้อง
2. กำหนดค่าเครือข่ายพื้นฐาน เช่น IP Address, Subnet Mask, Default Gateway และ DNS ได้ถูกต้อง
3. ตรวจสอบการเชื่อมต่อเครือข่ายด้วยคำสั่งที่เหมาะสมได้
4. เปิดใช้งานและตั้งค่า Remote Desktop ได้ถูกต้อง
5. ทดสอบการเชื่อมต่อและควบคุมเครื่องแม่ข่ายจากระยะไกลได้สำเร็จ

4.3 จิตพิสัย

1. มีความรับผิดชอบ รอบคอบ และคำนึงถึงความปลอดภัยของระบบขณะกำหนดค่าพื้นฐานและควบคุมเครื่องแม่ข่ายจากระยะไกลปฏิบัติตามขั้นตอนการทำงานและใช้งานบัญชีผู้ดูแลระบบอย่างเหมาะสม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1.ประยุกต์ใช้ความรู้และทักษะในการกำหนดค่าพื้นฐานและควบคุมเครื่องแม่ข่ายจากระยะไกล เพื่อสนับสนุนการบริหารจัดการระบบขององค์กรขนาดเล็กได้อย่างมีประสิทธิภาพและปลอดภัย

5. เครื่องมือ วัสดุ และอุปกรณ์

- 1.เครื่องคอมพิวเตอร์หรือโน้ตบุ๊ก จำนวน 1 เครื่องต่อผู้เรียน
- 2.โปรแกรม VMware Workstation / VMware Player
- 3.ระบบปฏิบัติการ Windows Server 2019
- 4.เครื่องลูกข่าย (Client) หรือเครื่องเสมือนสำหรับทดสอบ Remote Desktop
- 5.สายสัญญาณเครือข่ายหรือระบบเครือข่ายภายในห้องปฏิบัติการ
- 6.คู่มือปฏิบัติการหรือใบความรู้
- 7.แบบบันทึกผลการปฏิบัติงาน

6. คำแนะนำ/ข้อควรระวัง

- 1.ตรวจสอบความถูกต้องของค่าการตั้งค่าเครือข่ายก่อนบันทึกทุกครั้ง
- 2.ระมัดระวังการเปลี่ยนแปลงค่าที่มีผลต่อการเชื่อมต่อระบบ
- 3.ใช้บัญชี Administrator เฉพาะเมื่อจำเป็นเท่านั้น
- 4.กำหนดสิทธิ์ผู้ที่สามารถใช้งาน Remote Desktop อย่างเหมาะสม
- 5.ออกจากระบบ (Sign Out) หลังจากใช้งาน Remote Desktop เสร็จสิ้น
- 6.บันทึกผลการปฏิบัติงานและภาพหน้าจอทุกขั้นตอน
- 7.ปฏิบัติงานด้วยความรอบคอบและรับผิดชอบต่อความปลอดภัยของระบบ

7. ขั้นตอนการปฏิบัติงาน

สถานการณ์จำลอง

โรงเรียนแห่งหนึ่งมีความต้องการให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศสามารถบริหารจัดการเครื่องแม่ข่ายจากห้องทำงานได้ โดยต้องกำหนดค่าพื้นฐานของเครื่องแม่ข่ายและเปิดใช้งานการควบคุมระยะไกลอย่างปลอดภัย

ให้ผู้เรียนปฏิบัติดังนี้

- 1.เปิดเครื่องเสมือน Windows Server 2019
- 2.เปลี่ยนชื่อเครื่องแม่ข่ายเป็น SERVER-01
- 3.กำหนดค่าเครือข่าย ดังนี้
 - IP Address : 192.168.1.10
 - Subnet Mask : 255.255.255.0
 - Default Gateway : 192.168.1.1
 - Preferred DNS Server : 8.8.8.8
- 4.ตรวจสอบการเชื่อมต่อเครือข่ายด้วยคำสั่ง ping และ ipconfig

- 5.เปิดใช้งาน Remote Desktop บนเครื่องแม่ข่าย
- 6.กำหนดบัญชีผู้ใช้ที่ได้รับอนุญาตให้เชื่อมต่อจากระยะไกล
- 7.ใช้เครื่องลูกข่ายทดสอบเชื่อมต่อผ่าน Remote Desktop
- 8.บันทึกภาพหน้าจอผลการตั้งค่าและการเชื่อมต่อ

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

8. การประเมินผล

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การวางแผนและเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ขั้นตอนและความถูกต้อง	ครบ ถูกลำดับ ทำได้อิสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกกรณี มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านเพียงบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ ชัดเจน ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ	ไม่มีหลักฐานตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 4	หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 7
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถตรวจสอบสถานะของระบบปฏิบัติการเครื่องแม่ข่าย บันทึกผลการตั้งค่าระบบ และจัดทำรายงานสรุปผลการบริหารจัดการระบบได้อย่างถูกต้อง เป็นระบบ และสามารถนำข้อมูลไปใช้ในการตรวจสอบหรือแก้ไขปัญหาได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับการตรวจสอบและบันทึกข้อมูลการตั้งค่าระบบปฏิบัติการเครื่องแม่ข่าย
2. ปฏิบัติการตรวจสอบสถานะและการตั้งค่าของระบบได้อย่างถูกต้อง
3. จัดทำรายงานผลการบริหารจัดการระบบเพื่อใช้เป็นเอกสารอ้างอิงและการบำรุงรักษาระบบได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายความสำคัญของการตรวจสอบและบันทึกการตั้งค่าระบบได้
2. ระบุข้อมูลที่จำเป็นสำหรับการจัดทำรายงานการบริหารจัดการระบบได้
3. วิเคราะห์ประโยชน์ของเอกสารบันทึกการตั้งค่าระบบต่อการบำรุงรักษาและแก้ไขปัญหาได้

4.2 ทักษะพิสัย

1. ตรวจสอบข้อมูลพื้นฐานของระบบปฏิบัติการเครื่องแม่ข่ายได้
2. ตรวจสอบบัญชีผู้ใช้งาน กลุ่มผู้ใช้งาน และสิทธิ์การเข้าถึงได้
3. ตรวจสอบค่าการตั้งค่าเครือข่ายและการเชื่อมต่อจากระยะไกลได้
4. บันทึกข้อมูลและภาพหน้าจอผลการปฏิบัติงานได้อย่างครบถ้วน
5. จัดทำรายงานสรุปผลการบริหารจัดการระบบได้ถูกต้อง

4.3 จิตพิสัย

1. มีความรับผิดชอบ รอบคอบ และคำนึงถึงความปลอดภัยของระบบขณะกำหนดค่าพื้นฐานและควบคุมเครื่องแม่ข่ายจากระยะไกลปฏิบัติตามขั้นตอนการทำงานและใช้งานบัญชีผู้ดูแลระบบอย่างเหมาะสม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1. ประยุกต์ใช้ข้อมูลจากรายงานเพื่อสนับสนุนการบำรุงรักษา การแก้ไขปัญหา และการส่งมอบงานด้านระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์หรือโน้ตบุ๊ก
2. โปรแกรม VMware Workstation / VMware Player
3. ระบบปฏิบัติการ Windows Server 2019
4. เครื่องลูกข่ายสำหรับทดสอบระบบ (ถ้ามี)
5. ใบงานที่ 1-3 และผลการปฏิบัติงานที่ผ่านมา
6. โปรแกรมประมวลผลคำ เช่น Microsoft Word หรือ Google Docs

6. คำแนะนำ/ข้อควรระวัง

1. ตรวจสอบความถูกต้องของข้อมูลก่อนบันทึกลงในรายงาน
2. บันทึกข้อมูลตามสภาพจริงของระบบ ห้ามปลอมแปลงข้อมูล
3. จัดเก็บภาพหน้าจอและเอกสารประกอบให้เป็นระเบียบ
4. ไม่เปิดเผยข้อมูลสำคัญของระบบแก่บุคคลที่ไม่เกี่ยวข้อง
5. ส่งรายงานภายในเวลาที่กำหนด

7. ขั้นตอนการปฏิบัติงาน

สถานการณ์จำลอง

1. เปิดเครื่องเสมือน Windows Server 2019 ที่ได้ดำเนินการจากใบงานที่ 1-3
2. ตรวจสอบและบันทึกข้อมูลทั่วไปของระบบ ได้แก่
 - ชื่อเครื่องแม่ข่าย
 - เวอร์ชันของระบบปฏิบัติการ
 - วันที่ตรวจสอบระบบ
3. ตรวจสอบบัญชีผู้ใช้งานและกลุ่มผู้ใช้งานที่สร้างไว้
4. ตรวจสอบสิทธิ์การเข้าถึงโฟลเดอร์และทรัพยากรที่กำหนดไว้
5. ตรวจสอบค่าการตั้งค่าเครือข่าย
6. ตรวจสอบสถานะการเปิดใช้งาน Remote Desktop
7. บันทึกภาพหน้าจอผลการตรวจสอบในแต่ละหัวข้อ
8. จัดทำรายงานสรุปผลการบริหารจัดการระบบ ประกอบด้วย
 - บทนำ
 - รายละเอียดการตรวจสอบ
 - ผลการตรวจสอบ
 - ปัญหาที่พบ
 - แนวทางแก้ไข
 - ข้อเสนอแนะ
9. จัดพิมพ์รายงานและส่งให้ครูผู้สอน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9.การประเมินผล

รายการประเมิน	4 คะแนน	3 คะแนน	2 คะแนน	1 คะแนน
การวางแผนและเตรียมงาน	ครบ ถูกต้อง พร้อมปฏิบัติ	ขาดเล็กน้อยไม่กระทบงาน	ขาดหลายรายการ ต้องแนะนำ	ไม่พร้อมหรือใช้ข้อมูลผิด
ขั้นตอนและความถูกต้อง	ครบ ถูกลำดับ ทำได้อิสระ	ผิดเล็กน้อย แก้ได้เอง	ต้องช่วยเหลือหลายครั้ง	ไม่สำเร็จ/ข้ามจุดสำคัญ
ผลลัพธ์และการทดสอบ	ผ่านทุกกรณี มีผลยืนยัน	ผ่านเกือบทั้งหมด	ผ่านเพียงบางส่วน	ไม่ผ่านจุดสำคัญ
หลักฐานและรายงาน	ครบ ชัดเจน ย้อนตรวจได้	ขาดรายละเอียดเล็กน้อย	หลักฐานไม่ครบ	ไม่มีหลักฐานตรวจได้
ความปลอดภัยและรับผิดชอบ	รอบคอบ ตรงเวลา	บกพร่องเล็กน้อย	ต้องเตือนหลายครั้ง	ละเมิดข้อกำหนด

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	แผนการจัดการเรียนรู้	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 9-12
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 4 ชม. ปฏิบัติ 16 ชม.
ชื่อเรื่อง/งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

จัดตั้งและบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่ายหลัก เช่น DNS, DHCP, File/Resource Sharing ให้พร้อมใช้งานได้อย่างมีประสิทธิภาพและปลอดภัย พร้อมตรวจสอบและรายงานผล

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย
2. จัดตั้ง บริหารจัดการ ตรวจสอบ และรายงานผลบริการโครงสร้างพื้นฐานเครือข่ายหลัก เช่น DNS, DHCP, File/Resource Sharing ให้พร้อมใช้งาน

4. จุดประสงค์เชิงพฤติกรรม (เขียนให้ครบด้าน พุทธิพิสัย ทักษะพิสัย จิตพิสัย และ ประยุกต์ใช้)

4.1 พุทธิพิสัย (Cognitive Domain)

1. อธิบายหลักการทำงานของบริการ DNS Server, DHCP Server และ File/Resource Sharing Server ได้ถูกต้อง
2. เลือกใช้เครื่องมือและคำสั่งในการตั้งค่าบริการโครงสร้างพื้นฐานเครือข่ายตามข้อกำหนดได้ถูกต้อง
3. วิเคราะห์ปัญหาที่อาจเกิดขึ้นกับการทำงานของบริการ DNS, DHCP หรือ File/Resource Sharing ได้ถูกต้อง
4. ออกแบบการจัดสรร IP Address โดยใช้บริการ DHCP Server สำหรับเครือข่ายภายในองค์กรได้ถูกต้อง

4.2 ทักษะพิสัย (Psychomotor Domain)

1. จัดตั้งและกำหนดค่าบริการ DNS Server ตามความต้องการได้ถูกต้อง
2. จัดตั้งและกำหนดค่าบริการ DHCP Server เพื่อจัดสรรหมายเลข IP Address ได้ถูกต้อง
3. จัดตั้งและกำหนดค่าบริการ File and Resource Sharing Server ได้ถูกต้อง
4. บริหารจัดการและแก้ไขปัญหาบริการ DNS, DHCP และ File/Resource Sharing ได้ถูกต้อง
5. ตรวจสอบสถานะและประสิทธิภาพการทำงานของบริการโครงสร้างพื้นฐานเครือข่ายได้ถูกต้อง
6. จัดทำรายงานผลการบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่ายได้ถูกต้อง

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการวางแผน บริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง และควบคุมระบบปฏิบัติการเครือข่ายจากระยะไกลด้วยความละเอียดรอบคอบและรับผิดชอบ

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ความรู้และทักษะในการจัดตั้งและบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่ายเพื่อให้ระบบเครือข่ายทำงานได้อย่างมีประสิทธิภาพและปลอดภัย

5. สารการเรียนรู้

1. วิเคราะห์ความต้องการและออกแบบบริการเครือข่ายพื้นฐาน (DNS, DHCP, File/Resource Sharing)
2. วางแผน ติดตั้งและตั้งค่าบริการ DNS Server
3. วางแผน ติดตั้งและตั้งค่าบริการ DHCP Server
4. วางแผน ติดตั้งและตั้งค่าบริการ File and Resource Sharing Server
5. ทดสอบการทำงานของบริการโครงสร้างพื้นฐานเครือข่าย
6. จัดทำรายงานผลการให้บริการ (ชิ้นงาน: รายงานผลการให้บริการเครือข่ายพื้นฐาน)
7. จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (ชิ้นงาน: บริการเครือข่ายพื้นฐานที่ติดตั้งและทำงานได้)

6. กิจกรรมการเรียนรู้

1. ขั้นเตรียมความพร้อม

1. สอบความพร้อมของห้องปฏิบัติการ เครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบปฏิบัติการเครือข่าย
2. ครูชี้แจงผลลัพธ์การเรียนรู้ สมรรถนะประจำหน่วย จุดประสงค์การเรียนรู้ และเกณฑ์การประเมินผล
3. นักเรียนเข้าสู่ระบบปฏิบัติการเครือข่ายและตรวจสอบความพร้อมของเครื่องแม่ข่ายและเครื่องลูกข่าย
4. ทบทวนความรู้เดิมเกี่ยวกับระบบเครือข่าย TCP/IP การกำหนด IP Address และบทบาทของเครื่องแม่ข่ายในระบบเครือข่าย

2. ขั้นนำเข้าสู่บทเรียน

1. นำเสนอกรณีศึกษาการบริหารเครือข่ายภายในองค์กรที่มีผู้ใช้งานจำนวนมาก
2. ชักถามนักเรียนเกี่ยวกับปัญหาที่อาจเกิดขึ้นเมื่อไม่มีบริการ DNS Server, DHCP Server และ File Sharing Server
3. ครูเชื่อมโยงเนื้อหาเข้าสู่การติดตั้งและบริหารจัดการบริการ DNS, DHCP และ File/Resource Sharing บนเครื่องแม่ข่าย

3. ขั้นให้เนื้อหา

1. หลักการทำงานและหน้าที่ของ DNS Server
2. หลักการทำงานและหน้าที่ของ DHCP Server
3. หลักการทำงานและหน้าที่ของ File and Resource Sharing
4. การติดตั้งและกำหนดค่าบริการ DNS Server

5. ครูสาธิตการติดตั้งและกำหนดค่าบริการ DHCP Server
6. ครูสาธิตการสร้าง Shared Folder และกำหนดสิทธิ์การเข้าถึงทรัพยากร
7. ครูอธิบายการตรวจสอบสถานะ การบำรุงรักษา และการแก้ไขปัญหาเบื้องต้นของบริการโครงสร้างพื้นฐานเครือข่าย
8. นักเรียนศึกษาจากเอกสารประกอบการสอน ใบความรู้ และสื่อการเรียนรู้ออนไลน์

4. ขั้นฝึกปฏิบัติ

1. นักเรียนติดตั้งและกำหนดค่าบริการ DNS Server ตามใบงาน
2. นักเรียนสร้าง Forward Lookup Zone และทดสอบการแปลงชื่อโดเมน
3. นักเรียนติดตั้งและกำหนดค่าบริการ DHCP Server
4. นักเรียนสร้าง Scope และกำหนดช่วงหมายเลข IP Address สำหรับเครือข่ายภายใน
5. นักเรียนทดสอบการแจกจ่าย IP Address ให้กับเครื่องลูกข่าย
6. นักเรียนสร้าง Shared Folder และกำหนด Share Permission และ NTFS Permission
7. นักเรียนทดสอบการเข้าถึงทรัพยากรจากเครื่องลูกข่าย
8. นักเรียนตรวจสอบสถานะการทำงานของบริการ DNS, DHCP และ File Sharing
9. นักเรียนวิเคราะห์และแก้ไขปัญหาตามสถานการณ์ที่กำหนด
10. นักเรียนบันทึกผลการปฏิบัติงานและจัดทำรายงานผลการดำเนินงาน

5. ขั้นสรุปและประเมินผล

1. ครูและนักเรียนร่วมกันสรุปหลักการทำงานของ DNS Server, DHCP Server และ File Sharing Server
2. นักเรียนนำเสนอผลการปฏิบัติงานและแลกเปลี่ยนความคิดเห็น
3. ครูซักถามและอภิปรายปัญหาที่พบระหว่างการปฏิบัติงาน
4. ครูประเมินผลจาก

การตอบคำถามระหว่างเรียน

แบบทดสอบหลังเรียน

การปฏิบัติงานตามใบงาน

ชิ้นงานและรายงานผลการปฏิบัติงาน

พฤติกรรมการทำงานและการทำงานร่วมกับผู้อื่น

6. คำแนะนำ/ข้อควรระวัง

1. ควรสำรองข้อมูลหรือสร้าง Snapshot ของเครื่องเสมือนก่อนดำเนินการติดตั้งหรือปรับแต่งระบบ
2. ตรวจสอบการกำหนดค่า IP Address ให้ถูกต้องก่อนติดตั้งบริการ DNS และ DHCP
3. ควรระมัดระวังการกำหนดสิทธิ์การเข้าถึงไฟล์และทรัพยากรเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
4. ตรวจสอบความถูกต้องของชื่อโดเมนและข้อมูล DNS Records ก่อนบันทึกการตั้งค่า
5. หลีกเลี่ยงการกำหนดช่วง IP Address ซ้ำซ้อนกับอุปกรณ์อื่นในเครือข่าย
6. บันทึกขั้นตอนการปฏิบัติงานทุกครั้งเพื่อใช้ในการตรวจสอบและแก้ไขปัญหาในภายหลัง
7. ปฏิบัติตามหลักความปลอดภัยด้านสารสนเทศและจริยธรรมในการใช้งานระบบเครือข่าย

7. สื่อและแหล่งเรียนรู้

1. เอกสารประกอบการสอนหน่วยที่ 3 งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย
2. ใบความรู้ เรื่อง DNS Server, DHCP Server และ File and Resource Sharing
3. ใบงานปฏิบัติการติดตั้งและกำหนดค่าบริการโครงสร้างพื้นฐานเครือข่าย
4. เครื่องคอมพิวเตอร์หรือเครื่องเสมือน (Virtual Machine)
5. ระบบปฏิบัติการ Windows Server 2019 หรือรุ่นที่เหมาะสม
6. เครื่องลูกข่ายสำหรับทดสอบระบบ
7. Windows Server 2019 Documentation และคู่มือการใช้งาน

8. หลักฐานการเรียนรู้

1. หลักฐานความรู้
คะแนนจากการทำแบบฝึกหัด และแบบทดสอบในหนังสือประกอบการเรียน
2. หลักฐานการปฏิบัติงาน
คะแนนการทำการกิจกรรมการเรียนรู้ และภาพถ่ายการทำการกิจกรรมของผู้เรียน

9. การวัดและประเมินผล

1. เกณฑ์การปฏิบัติงาน
ตอบคำถามหรือแบบทดสอบได้อย่างถูกต้อง ไม่น้อยกว่า 80%
ปฏิบัติตามขั้นตอนกิจกรรม และใช้เทคโนโลยีได้อย่างเหมาะสมถูกต้อง
เข้าร่วม สื่อสาร และร่วมมือกับสมาชิกในกลุ่มได้ดี มีความรับผิดชอบ
2. วิธีการประเมิน
แบบฝึกหัดหลังเรียน ตรวจสอบความเข้าใจในเนื้อหา
แบบทดสอบหลังเรียนถูกต้อง ไม่น้อยกว่า 80%
3. เครื่องมือประเมิน
แบบทดสอบหลังเรียน

10. บันทึกผลหลังจัดการเรียนรู้

1. ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

2. ปัญหา อุปสรรคที่พบ

3. การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

11. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบความรู้ ที่ 1	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 9-12
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 4 ชม. ปฏิบัติ 16 ชม.
	ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

จัดตั้งและบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่ายหลัก เช่น DNS, DHCP, File/Resource Sharing ให้พร้อมใช้งานได้อย่างมีประสิทธิภาพและปลอดภัย พร้อมตรวจสอบและรายงานผล

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย
2. จัดตั้ง บริหารจัดการ ตรวจสอบ และรายงานผลบริการโครงสร้างพื้นฐานเครือข่ายหลัก เช่น DNS, DHCP, File/Resource Sharing ให้พร้อมใช้งาน

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย (Cognitive Domain)

1. อธิบายหลักการทำงานของบริการ DNS Server, DHCP Server และ File/Resource Sharing Server ได้ถูกต้อง
2. เลือกใช้เครื่องมือและคำสั่งในการตั้งค่าบริการโครงสร้างพื้นฐานเครือข่ายตามข้อกำหนดได้ถูกต้อง
3. วิเคราะห์ปัญหาที่อาจเกิดขึ้นกับการทำงานของบริการ DNS, DHCP หรือ File/Resource Sharing ได้ถูกต้อง
4. ออกแบบการจัดสรร IP Address โดยใช้บริการ DHCP Server สำหรับเครือข่ายภายในองค์กรได้ถูกต้อง

4.2 ทักษะพิสัย (Psychomotor Domain)

1. จัดตั้งและกำหนดค่าบริการ DNS Server ตามความต้องการได้ถูกต้อง
2. จัดตั้งและกำหนดค่าบริการ DHCP Server เพื่อจัดสรรหมายเลข IP Address ได้ถูกต้อง
3. จัดตั้งและกำหนดค่าบริการ File and Resource Sharing Server ได้ถูกต้อง
4. บริหารจัดการและแก้ไขปัญหาบริการ DNS, DHCP และ File/Resource Sharing ได้ถูกต้อง
5. ตรวจสอบสถานะและประสิทธิภาพการทำงานของบริการโครงสร้างพื้นฐานเครือข่ายได้ถูกต้อง

6. จัดทำรายงานผลการบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่ายได้ถูกต้อง

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการวางแผน บริหารจัดการผู้ใช้งาน สิทธิการเข้าถึง และควบคุมระบบปฏิบัติการเครื่องแม่ข่ายจากระยะไกลด้วยความละเอียดรอบคอบและรับผิดชอบ

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ความรู้และทักษะในการจัดตั้งและบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่ายเพื่อให้ระบบเครือข่ายทำงานได้อย่างมีประสิทธิภาพและปลอดภัย

5. เนื้อหาสาระ

1. วิเคราะห์ความต้องการและออกแบบบริการเครือข่ายพื้นฐาน (DNS, DHCP, File/Resource Sharing)
2. วางแผน ติดตั้งและตั้งค่าบริการ DNS Server
3. วางแผน ติดตั้งและตั้งค่าบริการ DHCP Server
4. วางแผน ติดตั้งและตั้งค่าบริการ File and Resource Sharing Server
5. ทดสอบการทำงานของบริการโครงสร้างพื้นฐานเครือข่าย
6. จัดทำรายงานผลการให้บริการ (ชิ้นงาน: รายงานผลการให้บริการเครือข่ายพื้นฐาน)
7. จัดเก็บและดูแลรักษาเครื่องมืออุปกรณ์ (ชิ้นงาน: บริการเครือข่ายพื้นฐานที่ติดตั้งและทำงานได้)

งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย

1. ภาพรวมและสถานการณ์ปฏิบัติ

บริการโครงสร้างพื้นฐานทำให้ผู้ใช้เข้าถึงทรัพยากรด้วยชื่อที่จำง่าย รับค่าการเชื่อมต่ออัตโนมัติ และใช้ไฟล์ร่วมกันโดยควบคุมสิทธิ์ได้ หากบริการหนึ่งผิดพลาด ผลกระทบอาจดูเหมือนเกิดจากอีกบริการ เช่น ผู้ใช้เปิดโฟลเดอร์ด้วย IP ได้แต่เปิดด้วยชื่อไม่ได้ สาเหตุหลักย่อมชี้ไปที่ DNS มากกว่า SMB ดังนั้นผู้ดูแลต้องเข้าใจความสัมพันธ์และตรวจสอบจากชั้นพื้นฐานขึ้นไป

1.1 สถานการณ์กลางของหน่วย

รายการ	ค่าทดลอง	เหตุผล/การใช้
เครือข่าย	192.168.30.0/24	เครือข่ายเสมือนแยก ไม่เชื่อมกับเครือข่ายจริง
Gateway	192.168.30.1	ค่าจำลองตามโจทย์ หากไม่มี Router ให้บันทึกว่าไม่ทดสอบภายนอก
Server	SRV-INFRA / 192.168.30.10	Static IP เพื่อให้ Client อ้างอิง DNS/DHCP/SMB ได้คงที่
DNS Zone	training.example	ใช้โดเมน example ที่สงวนสำหรับเอกสารและการทดลอง
DNS Records	srv-infra → .10; files → .10	A Record สำหรับ Server และชื่อบริการไฟล์
DHCP Pool	192.168.30.100-199	ช่วง Dynamic สำหรับ Client
Exclusion	192.168.30.100-109	กันพื้นที่สำหรับการสาธิต/อุปกรณ์ที่กำหนดเอง
DHCP Options	003=.1, 006=.10, 015=training.example	ส่ง Gateway, DNS และ DNS suffix ให้ Client
SMB Share	\\SRV-INFRA\Department	ใช้ทดสอบการเข้าถึงด้วยชื่อและสิทธิ์

ข้อสำคัญ: ถ้าห้องปฏิบัติการใช้ค่าคนละชุด ให้ผู้สอนเปลี่ยนค่าทั้งตาราง ไปงาน และเฉลยก่อนสอน ห้ามแก้ไขเฉพาะบางหน้า เพราะจะทำให้การทดสอบไม่สอดคล้องกัน

2. การวางแผนก่อนติดตั้ง

2.1 ตรวจสอบความพร้อม

- 1.สร้าง Snapshot ของ Server และ Client และตรวจสอบว่าทั้งสองเครื่องอยู่ Virtual Network เดียวกัน
- 2.กำหนด Static IP ให้ Server; ตรวจสอบ IP, Prefix/Subnet, Gateway และ DNS ไม่ให้ชนกับ DHCP Pool
- 3.ปิด DHCP ของ Virtualization Platform ในเครือข่ายทดลอง หากต้องการทดสอบ Windows DHCP เพื่อป้องกัน Rogue DHCP
- 4.กำหนดเกณฑ์ผ่านล่วงหน้า เช่น Client ต้องได้รับ IP ในช่วงที่กำหนด ใช้ DNS .10 และเปิด Share ด้วยชื่อได้
- 5.กำหนดบัญชี/กลุ่มทดสอบและข้อมูลที่ไม่ใช่ข้อมูลจริง

2.2 คำสั่งตรวจสอบพื้นฐาน

คำสั่ง	ใช้ตรวจ	สิ่งที่ต้องสังเกต
hostname	ชื่อเครื่อง	Server ต้องเป็น SRV-INFRA
ipconfig /all	ค่าการ์ดเครือข่าย	IP, Mask, Gateway, DNS, DHCP Enabled, Lease
ping <IP>	การเข้าถึงระดับ IP	ใช้ยืนยันเครือข่ายก่อนสรุปว่า DNS เสีย
Get-Service DNS,DHCPserver,Lan manServer	สถานะบริการ	ควรเป็น Running ตามบทบาทที่ติดตั้ง

3. DNS Server

3.1 หลักการทำงาน

DNS แปลงชื่อเป็นข้อมูลที่เครื่องใช้สื่อสาร เช่น A Record เชื่อมชื่อ IPv4 กับที่อยู่ IPv4 และ PTR Record เชื่อม IPv4 กลับไปยังชื่อ การค้นชื่อปกติเริ่มที่ Client Resolver ซึ่งตรวจ Cache และส่งคำถามไปยัง DNS Server ที่กำหนด หาก Server เป็นผู้มีอำนาจของ Zone จะตอบจาก Zone; หากไม่ใช่ อาจใช้ Forwarder หรือ Root Hints ตามการกำหนด

3.2 Zone และ Record ที่ใช้ในหน่วย

- 1.Forward Lookup Zone `training.example`: ใช้ค้นจากชื่อไปยัง IP
- 2.Reverse Lookup Zone สำหรับ 192.168.30.0/24: ใช้ค้นจาก IP ไปยังชื่อ
- 3.A Record `srv-infra.training.example` และ `files.training.example` → 192.168.30.10
- 4.PTR Record 192.168.30.10 → srv-infra.training.example

5.CNAME เป็นชื่อแฝงที่ชี้ไปยังชื่อหลัก แต่ในหน่วยนี้ใช้ A Record เพื่อให้เห็นความสัมพันธ์โดยตรง

3.3 การติดตั้งและกำหนดค่า

- 1.เปิด Server Manager > Manage > Add Roles and Features > Role-based or feature-based installation
- 2.เลือกเครื่องปลายทาง เลือก DNS Server และ Management Tools แล้วติดตั้ง
- 3.เปิด DNS Manager ตรวจสอบ Server และ Event ที่เกี่ยวข้อง
- 4.สร้าง Primary Forward Lookup Zone ชื่อ training.example; สำหรับห้องทดลอง Workgroup เลือก 5.Zone file และกำหนด Dynamic Update ตามนโยบายผู้สอน
- 6.สร้าง A Record สำหรับ srv-infra และ files เป็น 192.168.30.10
- 7.สร้าง Reverse Lookup Zone สำหรับ Network ID 192.168.30 และสร้าง/ตรวจสอบ PTR Record

3.4 การทดสอบ DNS

ลำดับ	คำสั่ง/การตรวจ	เกณฑ์ผ่าน
1	ipconfig /all	Client ใช้ DNS Server 192.168.30.10
2	ping 192.168.30.10	เข้าถึง Server ระดับ IP ได้
3	nslookup srv-infra.training.example 192.168.30.10	ตอบ 192.168.30.10 จาก Server ที่ระบุ
4	nslookup 192.168.30.10 192.168.30.10	ตอบ PTR เป็น srv-infra.training.example
5	ping files.training.example	ชื่อถูกแปลงเป็น .10; การตอบ Echo ขึ้นกับ Firewall

3.5 การแก้ปัญหา DNS อย่างเป็นลำดับ

- 1.ถ้า IP ยัง ping ไม่ถึง ให้แก้เครือข่ายก่อน DNS
- 2.ถ้า IP ถึงแต่ชื่อไม่ถึง ตรวจสอบ DNS Server ใน ipconfig /all ว่าชี้ .10
- 3.ใช้ nslookup ระบุ DNS Server โดยตรงเพื่อแยกปัญหา Client Cache ออกจาก Server
- 4.ตรวจสอบ DNS Service, Zone loading, ชื่อ Zone, Record, Firewall UDP/TCP 53 และ Event Viewer
- 5.หลังแก้ Client Cache อาจยังเก็บผลลบ ใช้ ipconfig /flushdns แล้วทดสอบซ้ำ

4. DHCP Server

4.1 หลักการ DORA

Client ที่ตั้งรับค่าอัตโนมัติเริ่มจาก DHCPDISCOVER เพื่อค้นหา Server; Server ส่ง DHCPOFFER; Client เลือกและส่ง DHCPREQUEST; Server ยืนยันด้วย DHCPACK กระบวนการนี้ทำให้ Client ได้ IP, Subnet

Mask และ Options ที่เกี่ยวข้อง หาก Client ได้ 169.254.x.x (APIPA) แสดงว่าไม่ได้รับ Lease จาก DHCP ที่ใช้งานได้

4.2 องค์ประกอบของ Scope

องค์ประกอบ	ค่าหน่วยนี้	คำอธิบาย
Range	192.168.30.100-199	ช่วงที่ Server สามารถแจก
Exclusion	192.168.30.100-109	ที่อยู่ใน Range แต่ห้ามแจก
Lease Duration	8 ชั่วโมง (ห้องเรียน)	ระยะเวลาที่ Client ใช้ Address ก่อนต่ออายุ
Option 003	192.168.30.1	Default Router/Gateway
Option 006	192.168.30.10	DNS Server; จำเป็นต่อการใช้ชื่อในหน่วย
Option 015	training.example	DNS Domain Name/Suffix
Reservation	กำหนดเมื่อผู้สอนให้ MAC	ผูก MAC กับ IP เฉพาะ โดยยังบริหารผ่าน DHCP

4.3 การติดตั้งและสร้าง Scope

1. ยืนยันว่า Server ใช้ Static IP และไม่มี DHCP อื่นใน Virtual Network เดียวกัน
2. ติดตั้ง DHCP Server Role พร้อม Management Tools ผ่าน Server Manager
3. ถ้าอยู่ใน Active Directory Domain ให้ทำ Post-install Configuration และ Authorize
4. ด้วยสิทธิ์ที่เหมาะสม; ถ้าเป็น Standalone Workgroup ไม่ต้อง Authorize ใน AD
5. เปิด DHCP Manager > IPv4 > New Scope ตั้งชื่อ LAB-30
6. กำหนด Range, Mask, Exclusion และ Lease Duration ตามตาราง
7. กำหนด Scope Options 003, 006 และ 015 แล้ว Activate Scope

4.4 การทดสอบ DHCP

1. ตั้ง Client เป็น Obtain an IP address automatically และ Obtain DNS server address automatically
2. เปิด Command Prompt แล้วใช้ ipconfig /release จากนั้น ipconfig /renew
3. ใช้ ipconfig /all ตรวจสอบว่า IP อยู่ 192.168.30.110-199 ไม่ใช่ Exclusion, DHCP Server เป็น .10, DNS เป็น .10 และ Suffix ถูกต้อง
4. ตรวจสอบ Address Leases ใน DHCP Manager ให้ตรงกับ Client ID/MAC
5. ทดสอบ nslookup และเปิด Share ด้วยชื่อ เพื่อยืนยันว่า DHCP Options ทำงานร่วมกับ DNS

4.5 การแก้ปัญหา DHCP

1. APIPA 169.254.x.x: ตรวจสอบ Network Segment, DHCP Service, Scope Active, Address Pool เหลือ และ Firewall

- 2.ได้ IP แต่ DNS ผิด: ตรวจสอบ Option 006 ระดับ Server/Scope และต่อ Lease ใหม่
- 3.ได้ IP ชั่ว: ตรวจสอบ Static Address ที่อยู่ใน Pool, Exclusion และ Rogue DHCP
- 4.ไม่มี Lease ใน Console: ตรวจสอบว่า Client ต่อ Network เดียวกัน; ถ้าคนละ Subnet ต้องมี DHCP Relay ซึ่งอยู่นอกขอบเขตปฏิบัติการหน่วยนี้

5. File and Resource Sharing

5.1 SMB และ UNC Path

SMB เป็นโพรโทคอลสำหรับเข้าถึงไฟล์และทรัพยากรผ่านเครือข่าย เมื่อผู้ใช้เปิด `\\SRV-INFRA\Department` เครื่อง Client จะต้องแปลงชื่อ SRV-INFRA ให้เป็น IP ก่อน แล้วจึงเชื่อมต่อบริการ SMB บน Server ดังนั้นการทดสอบด้วยทั้งชื่อและ IP ช่วยแยกปัญหา DNS ออกจากปัญหา SMB

5.2 Share Permissions และ NTFS Permissions

Share Permissions มีผลเมื่อเข้าถึงผ่านเครือข่าย ส่วน NTFS Permissions มีผลกับไฟล์และโฟลเดอร์ทั้งการใช้งานภายในเครื่องและผ่านเครือข่าย เมื่อเข้าผ่าน Share ต้องผ่านทั้งสองชั้น โดยผลที่ใช้จริงถูกจำกัดจากสิทธิ์ทั้งสองชุด ผู้ดูแลควรกำหนดสิทธิ์ผ่านกลุ่ม หลีกเลี่ยง Deny หากไม่จำเป็น และทดสอบด้วยบัญชีจริงของแต่ละบทบาท

กลุ่ม	Share Permission	NTFS Permission	ผลที่คาดหวัง
Administrators	Full Control	Full Control	บริหารทุกอย่าง
GG-IT	Change	Modify	อ่าน สร้าง แก้ไข และลบ
GG-HR	Change	Modify เฉพาะ HR	แก้ไขใน HR; ไม่มีสิทธิ์ใน Accounting
GG-Accounting	Change	Modify เฉพาะ Accounting	แก้ไขใน Accounting; ไม่มีสิทธิ์ใน HR
Authenticated Users	Read (ถ้าจำเป็น)	Read เฉพาะโฟลเดอร์กลาง	อ่านตามนโยบาย ไม่แก้ไข

5.3 ขั้นตอนสร้าง Share

- 1.สร้าง D:\Shares\Department และโฟลเดอร์ย่อย Common, IT, HR, Accounting
- 2.สร้างหรือยืนยันกลุ่มทดสอบ แล้วเพิ่มบัญชีให้ตรงบทบาท
- 3.เปิด Properties > Sharing > Advanced Sharing > Share this folder และตั้ง Share name เป็น Department
- 4.กำหนด Share Permissions ตามตาราง; จากนั้นกำหนด NTFS Security แยกแต่ละโฟลเดอร์
- 5.จาก Client ใช้ `\\SRV-INFRA\Department` และทดสอบ Read/Create/Edit/Delete ด้วยแต่ละบัญชี

6.บันทึกผลตามตาราง ไม่ใช้การทดสอบด้วยบัญชี Administrator แทนผู้ใช้ทั่วไป

ข้อควรระวัง: อย่าทดสอบกับข้อมูลจริง อย่าให้ Everyone: Full Control เพื่อให้ผ่านชั่วคราว และอย่าลบการสืบทอดสิทธิ์โดยไม่บันทึกค่าก่อนแก้

6. การตรวจระบบรวมและการวิเคราะห์ปัญหา

อาการ	การแยกปัญหา	รายการตรวจตามลำดับ
เปิด Share ด้วย IP ได้ แต่ด้วยชื่อไม่ได้	ชี้ไปที่ DNS	ipconfig /all → ping IP → nslookup ชื่อ → Zone/Record/Port 53
Client ได้ APIPA	ชี้ไปที่ DHCP/เครือข่าย	Segment → Service → Scope Active → Pool/Exclusion → Firewall
ได้ IP แต่เปิด Share ไม่ได้	ตรวจ DNS แล้ว SMB/สิทธิ์	nslookup → ping → Server service/Firewall → Share → NTFS → Credential
บางกลุ่มอ่านได้แต่แก้ไขไม่ได้	ชี้ไปที่สิทธิ์	Membership → Share Permission → NTFS Permission → Sign out/in → ทดสอบซ้ำ

6.1 หลักการแก้ปัญหา

- 1.บันทึกอาการและเงื่อนไขก่อนแก้ เช่น ผู้ใช้ เครื่อง เวลา และข้อความผิดพลาด
- 2.เริ่มตรวจ Physical/Virtual Network และ IP ก่อนบริการระดับชื่อหรือไฟล์
- 3.เปลี่ยนทีละค่าและบันทึกเหตุผล เพื่อทราบว่าการแก้ไขได้ให้ผล
- 4.ทดสอบซ้ำด้วยเงื่อนไขเดิมและตรวจผลข้างเคียงกับบริการอื่น
- 5.คืนค่าที่ทดลองชั่วคราวและสรุปหลักฐานก่อนส่งมอบ

7. ความปลอดภัย การสำรอง และการบันทึกหลักฐาน

- 1.สร้าง Snapshot ก่อนติดตั้ง Role หรือเปลี่ยนค่าขนาดใหญ่ แต่ไม่ใช่ Snapshot แทนระบบสำรองข้อมูลจริง
- 2.ใช้ Static IP สำหรับ Server และกัน IP นั้นออกจาก DHCP Pool
- 3.เปิดเฉพาะ Role/Port ที่จำเป็น ไม่ปิด Firewall ทั้งหมดเพื่อแก้ปัญหา
- 4.ใช้กลุ่มในการให้สิทธิ์และหลัก Least Privilege; ตรวจสิทธิ์หลังเปลี่ยนสมาชิกกลุ่ม
- 5.ปิดบังรหัสผ่าน Product Key และข้อมูลลับในภาพ; ภาพต้องมีวันเวลาและคำบรรยาย
- 6.บันทึก Before/After, คำสั่ง, ผลลัพธ์, ปัญหา, วิธีแก้ และผลทดสอบซ้ำ

8. รูปแบบรายงานผลการให้บริการ

1. ปกและข้อมูลผู้ปฏิบัติงาน
2. วัตถุประสงค์ ขอบเขต และผังเครือข่าย
3. ตารางค่ากำหนด Server, DNS, DHCP และ Share
4. ขั้นตอนดำเนินงานพร้อมภาพจุดตรวจที่มีคำบรรยาย
5. ตารางผลทดสอบ DNS, DHCP, SMB และสิทธิ์
6. ปัญหา อาการ หลักฐาน สาเหตุ วิธีแก้ และผลหลังแก้
7. สรุปความพร้อม ความเสี่ยงที่เหลือ และข้อเสนอแนะ

9. เอกสารอ้างอิงของใบความรู้

Microsoft Learn. Quickstart: Install and configure DNS Server.

<https://learn.microsoft.com/windows-server/networking/dns/quickstart-install-configure-dns-server>

Microsoft Learn. Quickstart: Install and configure DHCP Server.

<https://learn.microsoft.com/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server>

Microsoft Learn. Troubleshooting DNS clients. <https://learn.microsoft.com/windows-server/networking/dns/troubleshoot/troubleshoot-dns-client>

Microsoft Learn. What is SMB File Sharing for Windows and Windows Server?

<https://learn.microsoft.com/windows-server/storage/file-server/file-server-smb-overview>

Microsoft Learn. NTFS overview. <https://learn.microsoft.com/windows-server/storage/file-server/ntfs-overview>



Windows Server 2019



ใบความรู้ที่ 1

วิเคราะห์ความต้องการและออกแบบบริการเครือข่ายพื้นฐาน (DNS, DHCP, File/Resource Sharing)

1. วัตถุประสงค์

เพื่อให้นักเรียนสามารถวิเคราะห์ความต้องการขององค์กร และออกแบบบริการเครือข่ายพื้นฐาน ได้แก่ DNS, DHCP และ File/Resource Sharing บน Windows Server 2019 ได้อย่างเหมาะสม

2. ความหมายของบริการ



DNS (Domain Name System)

บริการแปลงชื่อโดเมน (เช่น www.company.local) ให้เป็นหมายเลข IP Address เพื่อให้อุปกรณ์ในเครือข่ายสามารถสื่อสารกันได้



DHCP (Dynamic Host Configuration Protocol)

บริการจัดสรร IP Address และค่าการตั้งค่าเครือข่ายให้อุปกรณ์ในเครือข่ายโดยอัตโนมัติ



File/Resource Sharing

บริการแชร์ไฟล์และทรัพยากรต่าง ๆ เช่น โฟลเดอร์, เครื่องพิมพ์ เพื่อให้ผู้ใช้ในเครือข่ายเข้าถึงและใช้งานร่วมกันได้

3. การวิเคราะห์ความต้องการ (ตัวอย่างองค์กร)

ตัวอย่าง: บริษัท ABC จำกัด

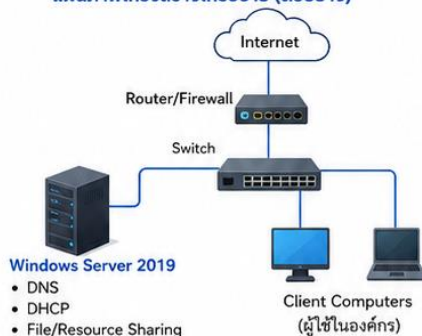
	จำนวนผู้ใช้	50 คน
	จำนวนเครื่องลูกข่าย	50 เครื่อง
	รูปแบบเครือข่าย	เครือข่ายภายในองค์กร (LAN)
	โดเมนที่ใช้	abc.local
	เซิร์ฟเวอร์	Windows Server 2019

ความต้องการบริการ

- ใช้ DNS สำหรับแปลงชื่อโดเมนภายในองค์กร
- ใช้ DHCP สำหรับแจกจ่าย IP Address ให้อุปกรณ์อัตโนมัติ
- ใช้ File/Resource Sharing สำหรับแชร์ไฟล์และเครื่องพิมพ์ให้พนักงานใช้งานร่วมกัน

4. การออกแบบบริการเครือข่ายพื้นฐาน

แผนภาพโครงสร้างเครือข่าย (ตัวอย่าง)



บริการ	การออกแบบ
DNS	• ติดตั้ง DNS Server บน Windows Server 2019 • สร้าง Zone ชื่อ "abc.local" • ใช้ Server เป็น DNS สำหรับเครื่องในองค์กร
DHCP	• ติดตั้ง DHCP Server บน Windows Server 2019 • สร้าง Scope: 192.168.10.0/24 • ช่วงแจกจ่าย IP: 192.168.10.100 – 192.168.10.200 • Default Gateway: 192.168.10.1 • DNS Server: 192.168.10.10
File/Resource Sharing	• สร้างโฟลเดอร์สำหรับแชร์ เช่น Share\Data, Share\Doc • กำหนดสิทธิ์การเข้าถึงตามกลุ่มผู้ใช้ • แชร์เครื่องพิมพ์ให้ผู้ใช้ในเครือข่าย

5. ประโยชน์ที่ได้รับ

- ✓ ช่วยให้อุปกรณ์ในเครือข่ายเชื่อมต่อและสื่อสารกันได้อย่างมีประสิทธิภาพ
- ✓ ลดภาระการตั้งค่าเครือข่ายด้วยตนเองของผู้ใช้
- ✓ เพิ่มความสะดวกในการเข้าถึงและใช้ทรัพยากรร่วมกันอย่างปลอดภัย
- ✓ ช่วยให้องค์กรบริหารจัดการเครือข่ายได้ง่ายและเป็นระบบ



ข้อควรจำ

ก่อนออกแบบระบบ ควรวิเคราะห์ความต้องการขององค์กรให้ชัดเจน เพื่อเลือกใช้บริการและกำหนดค่าที่เหมาะสมกับสภาพแวดล้อมจริง



ใบความรู้ที่ 2

วางแผน ติดตั้งและตั้งค่าบริการ DNS Server



จุดประสงค์การเรียนรู้

1. อธิบายหลักการทำงานและหน้าที่ของ DNS Server ได้
2. วางแผนการติดตั้งและตั้งค่าบริการ DNS Server ได้อย่างเหมาะสม
3. ติดตั้งและตั้งค่าบริการ DNS Server บน Windows Server 2019 ได้
4. ทดสอบการทำงานของ DNS Server ได้อย่างถูกต้อง

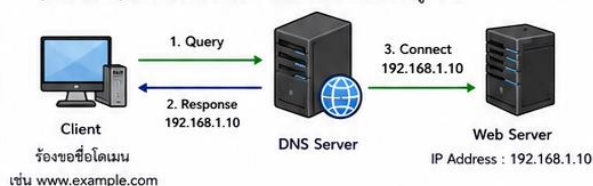


ความหมายของ DNS

DNS (Domain Name System) คือ ระบบที่ทำหน้าที่แปลงชื่อโดเมน (Domain Name) ที่มนุษย์เข้าใจ เช่น `www.example.com` ให้เป็นหมายเลข IP Address ที่เครื่องคอมพิวเตอร์เข้าใจ เช่น `192.168.1.10` และยังสามารถแปลงจาก IP Address กลับเป็นชื่อโดเมนได้ (Reverse Lookup)

1. หลักการทำงานของ DNS Server

DNS Server ทำหน้าที่เหมือน “สมุดโทรศัพท์” ของเครือข่าย เมื่อมีการร้องขอชื่อโดเมน DNS Server จะค้นหาข้อมูลในฐานข้อมูล (DNS Zone) แล้วตอบกลับด้วย IP Address ให้กับเครื่องลูกข่าย



2. ประเภทของ DNS Zone

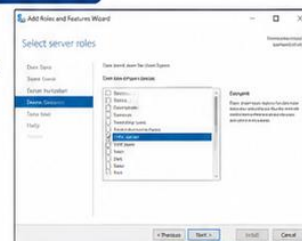
- Primary Zone : Zone หลักที่เก็บข้อมูลจริง สามารถแก้ไขได้
- Secondary Zone : Zone สำรองที่รับข้อมูลมาจาก Primary Zone
- Stub Zone : เก็บเพียงข้อมูลบางส่วนของ Zone
- Forward Lookup Zone : ใช้แปลงชื่อโดเมนเป็น IP Address
- Reverse Lookup Zone : ใช้แปลง IP Address เป็นชื่อโดเมน

3. การวางแผนติดตั้ง DNS Server

1. กำหนดชื่อโดเมนขององค์กร (เช่น `example.com`)
2. กำหนดโครงสร้าง DNS Zone (Forward และ Reverse Lookup)
3. กำหนด IP Address คงที่ให้กับ DNS Server
4. กำหนดสิทธิ์และการเข้าถึง DNS Server
5. วางแผนการสร้างข้อมูลและความปลอดภัย

4. การติดตั้งบริการ DNS Server บน Windows Server 2019

1. เปิด Server Manager → คลิก Add roles and features
2. เลือก Role-based or feature-based installation → Next
3. เลือกเซิร์ฟเวอร์ปลายทาง → Next
4. ดักเลือก DNS Server → Next
5. คลิก Add Features → Next
6. ตรวจสอบข้อมูล → Install
7. รอการติดตั้งเสร็จสิ้น → คลิก Close



5. การตั้งค่า DNS Server (การสร้าง Forward Lookup Zone)

1. เปิด DNS Manager
ไปที่ Tools > DNS

2. สร้าง Forward Lookup Zone
คลิกขวาที่ Forward Lookup Zones → New Zone...

3. เลือกประเภท Zone
เลือก Primary zone → Next

4. กำหนดชื่อ Zone
พิมพ์ชื่อโดเมนขององค์กร เช่น `example.com` → Next

5. เสร็จสิ้นการสร้าง Zone
ตรวจสอบข้อมูล → Finish

6. ตรวจสอบผลลัพธ์
จะปรากฏชื่อ Zone ที่สร้างใน Forward Lookup Zones

6. การเพิ่ม DNS Record ที่สำคัญ

ชนิดของ Record	คำอธิบาย	ตัวอย่างการใช้งาน
A (Host)	แปลงชื่อโฮสต์เป็น IP Address	<code>www.example.com</code> → <code>192.168.1.10</code>
AAAA (IPv6)	แปลงชื่อโฮสต์เป็น IPv6 Address	<code>www.example.com</code> → <code>2001:db8::10</code>
CNAME (Alias)	สร้างชื่ออื่นอ้างอิงไปยังชื่อหลัก	<code>mail.example.com</code> → <code>www.example.com</code>
MX (Mail Exchanger)	กำหนดเมลเซิร์ฟเวอร์ของโดเมน	<code>example.com</code> → <code>mail.example.com</code>
PTR (Pointer)	ใช้ใน Reverse Lookup Zone	<code>10.1.168.192</code> in <code>addr.arpa</code> → <code>server.example.com</code>

7. การทดสอบการทำงานของ DNS Server

1. ทดสอบด้วยคำสั่ง nslookup
 - `nslookup www.example.com`
 - `nslookup 192.168.1.10`
2. ทดสอบด้วยคำสั่ง ping
 - `ping www.example.com`
3. ทดสอบจากเครื่องลูกข่าย
 - ตั้งค่า DNS Server เป็น IP ของ DNS Server ที่สร้าง
 - ทดสอบเปิดเว็บไซต์หรือใช้คำสั่ง nslookup

```

C:\>nslookup www.example.com
Server: SERVER2019
Address: 192.168.1.1

Name: www.example.com
Address: 192.168.1.10
  
```



ข้อควรระวัง

- กำหนด IP Address แบบคงที่ให้กับ DNS Server
- ตรวจสอบชื่อโดเมนและการตั้งค่า DNS Record ให้ถูกต้อง
- สร้างข้อมูล DNS Zone อย่างสม่ำเสมอ
- ตรวจสอบการเชื่อมต่อเครือข่ายก่อนเริ่มใช้งาน
- ควรทดสอบจากเครื่องลูกข่ายทุกครั้งหลังการตั้งค่า



ใบความรู้ที่ 3

วางแผน ติดตั้งและตั้งค่าบริการ DHCP Server



จุดประสงค์การเรียนรู้

- อธิบายหลักการทำงานและหน้าที่ของ DHCP Server ได้
- วางแผนการติดตั้งและตั้งค่าบริการ DHCP Server ได้อย่างเหมาะสม
- ติดตั้งและตั้งค่าบริการ DHCP Server บน Windows Server 2019 ได้
- ทดสอบการแจกจ่าย IP Address ให้กับเครื่องลูกข่ายได้อย่างถูกต้อง



ความหมายของ DHCP

DHCP (Dynamic Host Configuration Protocol) คือ โปรโตคอลที่ใช้สำหรับจัดการการตั้งค่าเครือข่ายให้กับเครื่องลูกข่ายแบบอัตโนมัติ เช่น IP Address, Subnet Mask, Default Gateway, DNS Server และอื่น ๆ ช่วยลดความยุ่งยากในการกำหนดค่าเครือข่ายและลดข้อผิดพลาด

1. หลักการทำงานของ DHCP Server

DHCP Server จะจัดสรร IP Address และข้อมูลการตั้งค่าเครือข่ายให้กับ DHCP Client แบบอัตโนมัติ เมื่อเครื่องลูกข่ายร้องขอ โดยใช้กระบวนการ DORA



DORA Process

- Discover** : Client ค้นหา DHCP Server
- Offer** : Server เสนอ IP Address ให้ Client
- Request** : Client ขอรับ IP Address ที่เสนอ
- Acknowledge** : Server ยืนยันการจัดสรร IP Address

2. องค์ประกอบของ DHCP

- Scope** : กลุ่มของ IP Address ที่จัดสรรให้กับเครื่องลูกข่าย
- Exclusion Range** : ช่วง IP Address ที่ไม่ต้องการให้มีการแจกจ่าย
- Lease Duration** : ระยะเวลาในการเช่า IP Address
- Reservation** : การจอง IP Address ให้กับเครื่องลูกข่ายที่มี MAC Address เฉพาะ
- DHCP Options** : ข้อมูลการตั้งค่าเครือข่ายเพิ่มเติม เช่น Default Gateway, DNS Server

ข้อมูล DHCP Server แจกจ่ายให้ Client

- ✓ IP Address
- ✓ Subnet Mask
- ✓ Default Gateway
- ✓ DNS Server
- ✓ Domain Name
- ✓ อื่น ๆ (WINS, NTP, ฯลฯ)

3. การวางแผนก่อนติดตั้ง DHCP Server

- กำหนดช่วง IP Address ที่จะใช้ในเครือข่าย
- กำหนด Scope สำหรับแจกจ่าย IP Address
- กำหนดค่า Exclusion Range (ถ้ามี)
- กำหนดระยะเวลา Lease Duration ที่เหมาะสม
- กำหนด DHCP Options เช่น Gateway, DNS
- ตรวจสอบ IP Address ที่อุปกรณ์อื่นใช้งานอยู่เพื่อหลีกเลี่ยงการซ้ำซ้อน

ตัวอย่างการวางแผน

Network	: 192.168.1.0 /24
Usable Range	: 192.168.1.1 - 192.168.1.254
Scope Range	: 192.168.1.100 - 192.168.1.200
Exclusion Range	: 192.168.1.1 - 192.168.1.99
Default Gateway	: 192.168.1.1
DNS Server	: 192.168.1.10
Lease Duration	: 8 Days

4. ขั้นตอนการติดตั้งและตั้งค่าบริการ DHCP Server บน Windows Server 2019

1. เปิด Server Manager
คลิก Manage >
Add Roles and Features

2. เลือก Role-based or feature-based installation
คลิก Next

3. เลือก Server ที่จะติดตั้ง
แล้วคลิก Next

4. เลือก DHCP Server
แล้วคลิก Next

5. เพิ่ม Features ที่เกี่ยวข้อง
ตามที่ระบบแนะนำ
แล้วคลิก Next

6. ตรวจสอบข้อมูลให้ถูกต้อง
แล้วคลิก Install

7. ติดตั้งเสร็จสิ้น
คลิก Close

5. การตั้งค่า DHCP Server (สร้าง Scope)

1. เปิด DHCP Manager
ที่ Tools > DHCP

2. คลิกขวาที่ IPv4
เลือก New Scope...

3. New Scope Wizard
คลิก Next

4. ตั้งชื่อ Scope และ
คำอธิบาย คลิก Next

5. กำหนดช่วง IP Address
แล้วคลิก Next

6. กำหนด Exclusion Range
(ถ้ามี) แล้วคลิก Next

(นำเสนอขั้นตอนที่เหลือ เช่น Lease Duration, Options, Activation ต่อไป)

6. การทดสอบการทำงานของ DHCP Server

- ตั้งค่าเครื่องลูกข่ายให้รับ IP Address แบบอัตโนมัติ (DHCP)
- ตรวจสอบ IP Address ที่ได้รับ

วิธีการตรวจสอบ	ตัวอย่าง
Windows (CMD)	ipconfig /all
Windows (PowerShell)	Get-NetIPConfiguration
ผลลัพธ์ที่ควรได้รับ	ได้รับ IP Address, Subnet Mask, Gateway, DNS ตามที่กำหนด

7. คำสั่งที่เกี่ยวข้อง

- ipconfig /release # คืนค่า IP Address
- ipconfig /renew # ขอรับ IP Address ใหม่
- ipconfig /all # แสดงรายละเอียดการตั้งค่า IP
- netsh dhcp server show scope # แสดงข้อมูล Scope
- netsh dhcp server show binding # แสดงรายการการแจกจ่าย IP

8. เคล็ดลับและข้อควรระวัง

- ✓ ตรวจสอบ IP Address ไม่ให้ซ้ำกับอุปกรณ์อื่นในเครือข่าย
- ✓ กำหนดค่า Exclusion Range สำหรับ IP ที่ต้องการจองไว้
- ✓ ตรวจสอบการตั้งค่า Gateway และ DNS ให้ถูกต้อง
- ✓ บันทึกการเปลี่ยนแปลงและสำรองข้อมูลการตั้งค่า DHCP
- ✓ ตรวจสอบ Log Event Viewer หากเกิดปัญหา



ข้อควรระวัง

- หลีกเลี่ยงการติดตั้ง DHCP Server มากกว่าหนึ่งเครื่อง ในเครือข่ายเดียวกัน (ยกเว้นมีการจัดการ Failover)
- ตรวจสอบการตั้งค่า Firewall ให้เปิดพอร์ตที่จำเป็น (UDP 67, 68)
- บันทึกขั้นตอนการตั้งค่าและแผนผังเครือข่ายเพื่อการตรวจสอบและแก้ไขปัญหาในอนาคต

ในความรู้ที่ 4 **งานวางแผน ติดตั้งและตั้งค่าบริการ** **File and Resource Sharing Server** **Windows Server 2019**



บริการ File and Resource Sharing ช่วยให้ผู้ใช้ในเครือข่ายสามารถจัดเก็บ แชร์ และเข้าถึงไฟล์หรือทรัพยากรต่าง ๆ ได้อย่างปลอดภัยและมีประสิทธิภาพ

1. การวางแผน (Planning)

- 1.1 กำหนดวัตถุประสงค์**
 - เพื่อจัดเก็บและแชร์ไฟล์ให้ผู้ใช้ในองค์กร
 - เพื่อควบคุมการเข้าถึงข้อมูลอย่างปลอดภัย
- 1.2 วิเคราะห์ความต้องการ**
 - ปริมาณข้อมูลและจำนวนผู้ใช้
 - ประเภทข้อมูลที่จัดเก็บ
 - ระดับความปลอดภัยที่ต้องการ
- 1.3 ออกแบบโครงสร้าง**
 - โครงสร้างโฟลเดอร์ (Folder Structure)
 - การตั้งชื่อ (Naming Convention)
 - การกำหนดสิทธิ์การเข้าถึง (NTFS & Share Permission)
- 1.4 วางแผนพื้นที่จัดเก็บ**
 - เลือกใช้ RAID ที่เหมาะสม
 - เผื่อพื้นที่สำหรับการขยายในอนาคต
 - สำรองข้อมูลอย่างสม่ำเสมอ
- 1.5 กำหนดนโยบายและความปลอดภัย**
 - นโยบายการเข้าถึงข้อมูล
 - การเข้ารหัส (BitLocker / EFS)
 - การสำรองข้อมูลและการกู้คืน

การติดตั้งบริการ (Installation)

- 2.1 เพิ่มบทบาทและคุณลักษณะ (Add Roles and Features)**
 - เปิด Server Manager > Manage > Add Roles and Features
 - เลือก Role-based or feature-based installation
 - เลือกเซิร์ฟเวอร์เป้าหมาย
 - เลือก File and Storage Services > File and iSCSI Services
 - เลือก File Server
 - ดำเนินการติดตั้งจนเสร็จสิ้น
- 2.2 ตรวจสอบบริการที่ติดตั้ง**
 - ตรวจสอบใน Server Manager > Local Server > Roles and Features
 - บริการที่สำคัญ : Server, File and Storage Services

การตั้งค่า (Configuration)

- 3.1 สร้างโฟลเดอร์สำหรับแชร์**
 - สร้างโฟลเดอร์ตามโครงสร้างที่วางแผนไว้
- 3.2 กำหนดสิทธิ์ NTFS (Security)**
 - คลิกขวาที่โฟลเดอร์ > Properties > Security > Edit
 - กำหนดสิทธิ์กับกลุ่มผู้ใช้ (Domain Groups)
- 3.3 แชร์โฟลเดอร์ (Share)**
 - คลิกขวาที่โฟลเดอร์ > Give access to > Specific people
 - กำหนดชื่อแชร์และสิทธิ์การใช้งาน (Read / Change / Full Control)
- 3.4 ตรวจสอบการเข้าถึง**
 - ทดสอบเข้าถึงจากเครื่องลูกข่ายในเครือข่าย
 - ใช้ \\ชื่อเซิร์ฟเวอร์\ชื่อแชร์ หรือ Map Network Drive

4 การใช้งานและการจัดการ (Operation & Management)

- 4.1 ตรวจสอบการใช้งานพื้นที่**
ผ่าน Server Manager > File and Storage Services > Shares
- 4.2 จัดการโควตา (Quota)**
ควบคุมขนาดพื้นที่ที่ผู้ใช้หรือกลุ่มสามารถใช้งานได้
- 4.3 จัดการ File Screening**
ควบคุมประเภทไฟล์ที่อนุญาตหรือไม่อนุญาต
- 4.4 ตรวจสอบการเชื่อมต่อ**
ใช้คำสั่ง net share หรือ Computer Management
- 4.5 สำรองข้อมูลและกู้คืน**
ใช้ Windows Server Backup หรือเครื่องมืออื่น

5 ความปลอดภัย (Security)

- ✓ 5.1 ใช้หลักการ Least Privilege ให้สิทธิ์เท่าที่จำเป็น
- ✓ 5.2 กำหนดสิทธิ์ด้วยกลุ่ม (Groups) แทนผู้ใช้รายบุคคล
- ✓ 5.3 เปิดใช้งาน Windows Defender Firewall
- ✓ 5.4 เปิดใช้งานการเข้ารหัส (EFS / BitLocker) สำหรับข้อมูลสำคัญ
- ✓ 5.5 ตรวจสอบและบันทึกเหตุการณ์การเข้าถึง (Event Logging)

คำสั่งที่เกี่ยวข้อง (Useful Commands)

คำสั่ง	คำอธิบาย
net share	แสดงรายการการแชร์ทั้งหมด
net share ชื่อแชร์ /delete	ลบการแชร์
net use	แสดงการเชื่อมต่อไดรฟ์เครือข่าย
net use Z: \\Server\Share	เชื่อมต่อไดรฟ์เครือข่าย
icacls "D:\Share"	จัดการสิทธิ์ NTFS ผ่านบรรทัดคำสั่ง



หมายเหตุ : การวางแผน ติดตั้ง และตั้งค่าบริการ File and Resource Sharing Server ที่ดี จะช่วยให้การจัดเก็บและแชร์ข้อมูลมีประสิทธิภาพ ปลอดภัย และพร้อมใช้งานอย่างต่อเนื่อง



จุดประสงค์การเรียนรู้

1. ทดสอบการทำงานของบริการ DNS Server ได้
2. ทดสอบการทำงานของบริการ DHCP Server ได้
3. ทดสอบการทำงานของบริการ File/Resource Sharing ได้
4. วิเคราะห์และแก้ไขปัญหาที่เกิดขึ้นจากบริการเครือข่ายได้อย่างถูกต้อง



ความหมาย

การทดสอบการทำงานของบริการโครงสร้างพื้นฐานเครือข่าย คือ การตรวจสอบว่า บริการ DNS, DHCP และ File/Resource Sharing ทำงานได้ถูกต้องและสามารถให้บริการแก่เครื่องลูกข่ายได้ตามที่กำหนด โดยใช้เครื่องมือและคำสั่งเพื่อตรวจสอบความถูกต้อง ประสิทธิภาพ และการเข้าถึงทรัพยากรของระบบ

1 ทดสอบ DNS Server

1. ทดสอบการแปลงชื่อโดเมน (Forward Lookup)
 - nslookup www.example.com
 - nslookup -type=A www.example.com
2. ทดสอบการแปลง IP เป็นชื่อโดเมน (Reverse Lookup)
 - nslookup 192.168.1.10
 - nslookup -type=PTR 192.168.1.10
3. ทดสอบด้วยคำสั่ง Ping
 - ping www.example.com

ตัวอย่างผลลัพธ์

```
C:\>nslookup www.example.com
Server: SERVER2019
Address: 192.168.1.10

Name: www.example.com
Address: 192.168.1.20
```



ผลลัพธ์
ถูกต้อง

สิ่งที่ควรตรวจสอบ

- ✓ DNS Server ตอบกลับได้
- ✓ ชื่อโดเมนแปลงเป็น IP ได้ถูกต้อง
- ✓ IP แปลงเป็นชื่อโดเมนได้ถูกต้อง
- ✓ ไม่มี Error เช่น "Non-existent domain"

2 ทดสอบ DHCP Server

1. ตรวจสอบการรับ IP Address อัตโนมัติ
 - ipconfig /release
 - ipconfig /renew
2. ตรวจสอบข้อมูล IP Address ที่ได้รับ
 - ipconfig /all
3. ตรวจสอบการต่ออายุ Lease
 - รอจนกว่า Lease ใกล้เคียงแล้วตรวจสอบว่าได้รับ IP เดิมต่ออายุอัตโนมัติ

ตัวอย่างผลลัพธ์

```
C:\>ipconfig /all

Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : example.com
IP Address . . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.10
Lease Obtained . . . . . : 10/05/2024 09:30:00
Lease Expires . . . . . : 10/05/2024 17:30:00
```



ผลลัพธ์
ถูกต้อง

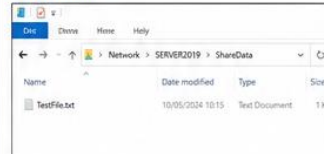
สิ่งที่ควรตรวจสอบ

- ✓ ได้รับ IP Address จาก DHCP Server
- ✓ ค่า Subnet Mask, Default Gateway, DNS ถูกต้อง
- ✓ Lease Time ถูกต้องและต่ออายุได้
- ✓ ไม่มี IP ซ้ำกันอุปกรณ์อื่น

3 ทดสอบ File/Resource Sharing

1. ทดสอบการเข้าถึง Shared Folder
 - จากเครื่องลูกข่าย พิมพ์ \\ชื่อเซิร์ฟเวอร์หรือ IP\ชื่อแชร์ เช่น \\SERVER2019\ShareData
2. ทดสอบการอ่าน/เขียนไฟล์
 - สร้างไฟล์ ทดสอบแก้ไขไฟล์ และบันทึกไฟล์
3. ตรวจสอบสิทธิ์การเข้าถึง
 - ทดสอบด้วยบัญชีผู้ใช้ที่มีสิทธิ์และไม่มีสิทธิ์

ตัวอย่างผลลัพธ์



ผลลัพธ์
ถูกต้อง

สิ่งที่ควรตรวจสอบ

- ✓ สามารถเชื่อมต่อและเห็น Shared Folder
- ✓ สามารถสร้าง/แก้ไข/ลบไฟล์ได้ตามสิทธิ์
- ✓ บัญชีที่ไม่มีสิทธิ์ไม่สามารถเข้าถึงได้
- ✓ ไม่มี Error เช่น "Access is denied"

4 เครื่องมือที่ใช้ในการทดสอบ

เครื่องมือ / คำสั่ง	ใช้สำหรับ
nslookup	ทดสอบการแปลงชื่อ DNS
ping	ทดสอบการเชื่อมต่อเครือข่าย
ipconfig	ตรวจสอบและจัดการ IP Address
tracert	ตรวจสอบเส้นทางในการเชื่อมต่อ
net use	เชื่อมต่อไดรฟ์เครือข่าย

5 ตัวอย่างการทดสอบครบทุกบริการ

บริการ	คำสั่ง/วิธีการทดสอบ	ผลลัพธ์ที่คาดหวัง
DNS Server	nslookup www.example.com nslookup 192.168.1.10 ping www.example.com	• ได้ IP Address ที่ถูกต้อง • ได้ชื่อโดเมนที่ถูกต้อง • Ping สำเร็จ (Reply)
DHCP Server	ipconfig /release ipconfig /renew ipconfig /all	• ได้รับ IP Address ใหม่ • ค่า IP, Mask, Gateway, DNS ถูกต้อง • Lease Time แสดงค่าถูกต้อง
File Sharing	\\SERVER2019\ShareData สร้าง/แก้ไข/ลบไฟล์	• เข้าถึงโฟลเดอร์ได้ • สามารถอ่าน/เขียนไฟล์ได้ตามสิทธิ์

6 แนวทางแก้ไขปัญหาเบื้องต้น

ปัญหา	สาเหตุที่เป็นไปได้	แนวทางแก้ไข
nslookup ไม่ได้ผล	• DNS Server ไม่ทำงาน • DNS Client ตั้งค่าไม่ถูกต้อง	• ตรวจสอบบริการ DNS บนเซิร์ฟเวอร์ • ตรวจสอบค่า DNS Server บนเครื่องลูกข่าย
ไม่ได้รับ IP จาก DHCP	• บริการ DHCP ไม่ทำงาน • Scope หมดช่วง IP • เครื่องลูกข่ายไม่ได้ตั้งเป็น DHCP	• ตรวจสอบบริการ DHCP • ขยายช่วง IP ใน Scope หรือสร้าง Scope ใหม่ • ตั้งค่า IPv4 เป็น Obtain an IP address automatically
เข้าถึง Shared Folder ไม่ได้	• พิมพ์ชื่อหรือ IP ผิด • สิทธิ์การเข้าถึงไม่เพียงพอ • ไฟร์วอลล์บล็อกการเชื่อมต่อ	• ตรวจสอบชื่อเซิร์ฟเวอร์หรือ IP • ตรวจสอบสิทธิ์ Share และ NTFS • ปิดไฟร์วอลล์หรือ SMB (TCP 445)

7 สรุป

การทดสอบบริการโครงสร้างพื้นฐานเครือข่ายเป็นขั้นตอนสำคัญเพื่อให้มั่นใจว่าบริการต่าง ๆ ทำงานได้อย่างถูกต้องและพร้อมให้บริการแก่ผู้ใช้งาน โดยควรทดสอบอย่างเป็นระบบ ตรวจสอบผลลัพธ์ และบันทึกผลการทดสอบทุกครั้ง เพื่อใช้ในการตรวจสอบและแก้ไขปัญหาในอนาคต



ข้อควรระวัง

- ตรวจสอบการเชื่อมต่อเครือข่ายก่อนทำการทดสอบทุกครั้ง
- ใช้บัญชีผู้ใช้ที่มีสิทธิ์เพียงพอในการทดสอบ
- บันทึกผลการทดสอบและข้อผิดพลาดเพื่อใช้ในการวิเคราะห์ปัญหา
- ปฏิบัติตามนโยบายความปลอดภัยขององค์กรในการเข้าถึงระบบ

6. แบบฝึกหัด

แบบฝึกหัดหน่วยที่ 3

1. เหตุใดเครื่อง SRV-INFRA ต้องใช้ Static IP

ก. เพื่อให้เปลี่ยน IP ทุกครั้ง

ข. เพื่อให้ Client อ้างอิงบริการได้คงที่

ค. เพื่อปิด DNS

ง. เพื่อเพิ่ม RAM

2. ค่าใดเป็น Network Address ของ 192.168.30.0/24

ก. 192.168.30.0

ข. 192.168.30.1

ค. 192.168.30.10

ง. 192.168.30.255

3. เหตุใดต้องปิด DHCP อื่นใน Virtual Network ทดลอง

ก. ป้องกัน Client รับค่าจาก Server ผิดตัว

ข. ทำให้ DNS เร็วขึ้น

ค. เพิ่มพื้นที่ดิสก์

ง. เปิด SMB

4. A Record ใช้ทำอะไร

ก. ชี้ไป IPv4

ข. IPv4 ไปชื่อ

ค. แจก IP

ง. กำหนดสิทธิ์ไฟล์

5. PTR Record อยู่ใน Zone ประเภทใด

ก. Forward Lookup

ข. Reverse Lookup

ค. DHCP Scope

ง. SMB Share

6. คำสั่งใดทดสอบ DNS โดยระบุ Server ได้โดยตรง

ก. hostname

ข. nslookup

ค. net user

ง. format

7. ลำดับ DHCP ที่ถูกต้องคือข้อใด

ก. Discover-Offer-Request-Ack

ข. Offer-Discover-Ack-Request

ค. Request-Ack-Discover-Offer

- ง. Ack-Request-Offer-Discover
- 8. Exclusion ใช้ทำอะไร
- ก. เพิ่ม IP นอกเครือข่าย
- ข. กัน IP ในช่วงไม่ให้ DHCP แจก
- ค. ลบ DNS
- ง. ปิด Scope
- 9. DHCP Option 006 คือค่าใด
- ก. Router
- ข. DNS Server
- ค. Domain Name
- ง. Lease Duration
- 10. Client ได้ 169.254.x.x สื่อถึงอะไร
- ก. ได้ Lease ปกติ
- ข. APIPA เพราะไม่ได้รับ DHCP
- ค. DNS ตอบถูกต้อง
- ง. Share Full Control
- 11. เส้นทางใดเป็น UNC Path
- ก. C:\Department
- ข. \\SRV-INFRA\Department
- ค. https://server
- ง. 192.168.30.0/24
- 12. เมื่อเข้าผ่านเครือข่าย สิทธิ์ใดเกี่ยวข้อง
- ก. Share เท่านั้น
- ข. NTFS เท่านั้น
- ค. Share และ NTFS
- ง. DHCP เท่านั้น
- 13. วิธีใดสอดคล้อง Least Privilege
- ก. Everyone Full Control
- ข. ให้สิทธิ์ผ่านกลุ่มตามหน้าที่
- ค. เพิ่มทุกคนเป็น Administrator
- ง. ปิด Firewall
- 14. เปิด Share ด้วย IP ได้แต่ด้วยชื่อไม่ได้ ควรตรวจสอบอะไรเป็นหลัก
- ก. DNS
- ข. RAM
- ค. Keyboard
- ง. Product Key

15. หลักฐานที่ดีคือข้อใด

ก. ภาพไม่มีคำบรรยาย

ข. รหัสผ่านจริง

ค. ผลทดสอบพร้อมค่าที่ตรวจและวันเวลา

ง. ข้อสรุปโดยไม่ทดสอบ

ตอนที่ 2 คำถามอัตนัย (5 ข้อ)

1. อธิบายความสัมพันธ์ของ DNS, DHCP และ SMB ตั้งแต่ Client เปิดเครื่องจนเข้าถึง Shared Folder ด้วยชื่อ

.....

.....

2. ออกแบบ DHCP Scope สำหรับเครือข่าย 192.168.30.0/24 โดยอธิบาย Range, Exclusion และ Options 003/006/015

.....

.....

3. อธิบายลำดับตรวจสอบเมื่อ nslookup ชื่อภายในไม่สำเร็จ แต่ ping IP ของ Server สำเร็จ

.....

.....

4. เปรียบเทียบ Share Permissions กับ NTFS Permissions และยกตัวอย่างสิทธิ์ของกลุ่ม HR

.....

.....

5. ออกแบบรายการหลักฐานอย่างน้อย 8 รายการสำหรับรายงานผล โดยคำนึงถึงการรักษาความลับ

.....

.....

7. เอกสารอ้างอิง

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

8. ภาคผนวก

8.1 เฉลย แบบฝึกหัดบทเรียนที่ 3

เฉลยแบบฝึกหัด ตอนที่ 1

1 ข, 2 ก, 3 ก, 4 ก, 5 ข, 6 ข, 7 ก, 8 ข, 9 ข, 10 ข, 11 ข, 12 ค, 13 ข, 14 ก, 15 ค

แนวคำตอบแบบฝึกหัด ตอนที่ 2

1. Client รับ IP/Mask/Gateway/DNS จาก DHCP จากนั้นใช้ DNS แปลงชื่อ Server หรือชื่อบริการเป็น IP แล้ว SMB จึงเชื่อมต่อ Share และตรวจสอบสิทธิ์
2. Range .100-.199, Exclusion .100-.109, 003=.1, 006=.10, 015=training.example โดย Server .10 อยู่นอก Pool
3. ตรวจสอบ DNS ใน ipconfig /all, ใช้ nslookup ระบุ .10, ตรวจสอบ DNS Service, Zone/Record, Port 53 และ Cache แล้วทดสอบซ้ำ
4. Share Permission ควบคุมการเข้าผ่านเครือข่าย; NTFS ควบคุมไฟล์/โฟลเดอร์ทุกช่องทาง; HR ควรได้ Change ที่ Share และ Modify เฉพาะโฟลเดอร์ HR
5. ตัวอย่าง: ผัง, ตารางค่า, Snapshot, Zone, Records, Scope, Options, Lease, ipconfig /all, nslookup, สิทธิ์, ผลทดสอบ, ปัญหา/วิธีแก้ โดยปิดบังรหัสผ่าน

	ใบงานที่ 1	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 9
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
	ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

จัดตั้งและกำหนดค่าบริการ DNS Server บนระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างถูกต้อง สามารถทดสอบ ตรวจสอบ และรายงานผลการการทำงานของระบบได้ พร้อมประยุกต์ใช้ในการบริหารจัดการเครือข่ายองค์กรได้อย่างมีประสิทธิภาพและปลอดภัย

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ติดตั้งและกำหนดค่าบริการ DNS Server ได้ถูกต้อง
2. สร้างและบริหารจัดการ DNS Zone และ Resource Record ได้
3. ตรวจสอบและแก้ไขปัญหาการทำงานของ DNS Server เบื้องต้นได้
4. จัดทำรายงานผลการปฏิบัติงานได้ถูกต้อง

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายหลักการทำงานและความสำคัญของ DNS Server ได้
2. อธิบายหน้าที่ของ DNS Zone และ Resource Record ได้
3. วิเคราะห์การทำงานของระบบแปลงชื่อโดเมนเป็น IP Address ได้

4.2 ทักษะพิสัย

1. ติดตั้ง DNS Server ได้ถูกต้อง
2. สร้าง Forward Lookup Zone ได้ถูกต้อง
3. สร้าง Host Record (A Record) ได้ถูกต้อง
4. ทดสอบการทำงานของ DNS Server ด้วยคำสั่งที่เหมาะสมได้

4.3 จิตพิสัย

1. มีความรับผิดชอบในการปฏิบัติงาน
2. มีความละเอียดรอบคอบในการกำหนดค่าระบบ
3. ปฏิบัติตามข้อกำหนดด้านความปลอดภัยของระบบเครือข่าย

4.4 ประยุกต์ใช้และรับผิดชอบ

ประยุกต์ใช้บริการ DNS Server ในการบริหารจัดการระบบเครือข่ายองค์กรได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์แม่ข่าย (Server)
2. เครื่องคอมพิวเตอร์ลูกข่าย (Client)
3. ระบบปฏิบัติการ Windows Server 2019
4. โปรแกรม VMware Workstation หรือ VirtualBox
5. ระบบเครือข่าย LAN
6. ใบความรู้และเอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1. ตรวจสอบการกำหนดค่า IP Address ของเครื่องแม่ข่ายก่อนติดตั้ง DNS Server
2. ตรวจสอบการเชื่อมต่อเครือข่ายให้พร้อมใช้งาน
3. กำหนดชื่อโดเมนให้ถูกต้องและเป็นมาตรฐาน
4. บันทึกขั้นตอนการปฏิบัติงานทุกครั้ง
5. ห้ามเปลี่ยนแปลงค่าระบบอื่นที่ไม่เกี่ยวข้องกับการใช้งาน
6. ควรสร้าง Snapshot ก่อนเริ่มปฏิบัติงาน

7. ขั้นตอนการปฏิบัติงาน

ตอนที่ 1 ติดตั้ง DNS Server

1. เปิด Server Manager
2. เลือก Add Roles and Features
3. เลือก DNS Server
4. ดำเนินการติดตั้งจนเสร็จสมบูรณ์

ตอนที่ 2 สร้าง DNS Zone

1. เปิด DNS Manager
2. เลือก Forward Lookup Zones
3. สร้าง New Zone
4. กำหนดชื่อ Zone ตามที่ครูกำหนด
5. บันทึกการตั้งค่า

ตอนที่ 3 สร้าง Resource Record

1. เลือก Zone ที่สร้างขึ้น
2. สร้าง Host (A) Record
3. กำหนดชื่อ Host
4. กำหนดหมายเลข IP Address
5. บันทึกการตั้งค่า

ตอนที่ 4 ทดสอบการทำงาน

1. เปิด Command Prompt
2. ใช้คำสั่ง nslookup
3. ใช้คำสั่ง ping ชื่อ Host
4. บันทึกผลการทดสอบ

ตอนที่ 5 สรุปผล

1. บันทึกภาพหน้าจอการตั้งค่า
2. สรุปผลการปฏิบัติงาน
3. วิเคราะห์ปัญหาและแนวทางแก้ไข (ถ้ามี)
4. ส่งรายงานผลการปฏิบัติงาน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

รายการประเมิน	ดีเยี่ยม (4)	ดี (3)	พอใช้ (2)	ปรับปรุง (1)	คะแนน
ความรู้ความเข้าใจเกี่ยวกับ DNS Server	อธิบายได้ถูกต้องครบถ้วน	อธิบายได้ถูกต้องเกือบทั้งหมด	อธิบายได้บางส่วน	อธิบายไม่ถูกต้อง	4
การติดตั้ง DNS Server	ติดตั้งได้ถูกต้องสมบูรณ์	ผิดพลาดเล็กน้อย	ต้องได้รับคำแนะนำ	ไม่สามารถติดตั้งได้	4
การสร้าง DNS Zone	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การสร้าง Resource Record	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การทดสอบและตรวจสอบระบบ	ทดสอบครบทุกขั้นตอน	ทดสอบได้เกือบครบ	ทดสอบได้บางส่วน	ไม่สามารถทดสอบได้	4

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 2		หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย		สอนครั้งที่ 10
	ชื่อหน่วยการเรียนรู้	งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
	ชื่อเรื่อง/งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

จัดตั้งและกำหนดค่าบริการ DHCP Server บนระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างถูกต้อง สามารถแจกจ่ายหมายเลข IP Address ให้กับเครื่องลูกข่ายอัตโนมัติ ตรวจสอบและรายงานผลการทำงานได้ พร้อมประยุกต์ใช้ในการบริหารจัดการเครือข่ายองค์กรได้อย่างมีประสิทธิภาพ

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับหลักการทำงานของ DHCP Server
2. ติดตั้งและกำหนดค่าบริการ DHCP Server ได้ถูกต้อง
3. สร้างและกำหนดค่า DHCP Scope ได้ถูกต้อง
4. ทดสอบการแจกจ่าย IP Address ให้เครื่องลูกข่ายได้
5. ตรวจสอบและแก้ไขปัญหาเบื้องต้นของ DHCP Server ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายหลักการทำงานของ DHCP Server ได้
2. อธิบายความหมายของ Scope, Lease และ Reservation ได้
3. วิเคราะห์การจัดสรรหมายเลข IP Address ในระบบเครือข่ายได้

4.2 ทักษะพิสัย (Psychomotor Domain)

1. ติดตั้ง DHCP Server ได้ถูกต้อง
2. สร้างและกำหนดค่า Scope ได้ถูกต้อง
3. กำหนดค่า Gateway และ DNS Server ได้ถูกต้อง
4. ทดสอบการรับ IP Address ของเครื่องลูกข่ายได้
5. ตรวจสอบสถานะการทำงานของ DHCP Server ได้

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการจัดเตรียม ติดตั้ง ตรวจสอบ และจัดทำรายงานระบบปฏิบัติการเครื่องแม่ข่ายด้วยความละเอียดรอบคอบ รับผิดชอบ และทำงานเป็นทีม

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ DHCP Server ในการบริหารจัดการเครือข่ายองค์กรได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์แม่ข่าย (Server)
2. เครื่องคอมพิวเตอร์ลูกข่าย (Client)
3. ระบบปฏิบัติการ Windows Server 2019
4. โปรแกรม VMware Workstation หรือ VirtualBox
5. ระบบเครือข่าย LAN
6. ใบความรู้และเอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1. กำหนด IP Address แบบ Static ให้เครื่องแม่ข่ายก่อนติดตั้ง DHCP Server
2. ตรวจสอบช่วง IP Address ที่จะนำมาใช้งานไม่ให้ซ้ำกับอุปกรณ์อื่น
3. ตรวจสอบค่า Gateway และ DNS Server ให้ถูกต้อง
4. รมั้ดระวังการกำหนด Scope ให้ครอบคลุมจำนวนผู้ใช้งาน
5. บันทึกผลการปฏิบัติงานทุกขั้นตอน
6. ควรสร้าง Snapshot ก่อนดำเนินการติดตั้งระบบ

7. ขั้นตอนการปฏิบัติงาน

ตอนที่ 1 ติดตั้ง DHCP Server

1. เปิด Server Manager
2. เลือก Add Roles and Features
3. เลือก DHCP Server
4. ดำเนินการติดตั้งจนเสร็จสมบูรณ์
5. ทำการ Authorize DHCP Server

ตอนที่ 2 สร้าง DHCP Scope

1. เปิด DHCP Manager
2. เลือก IPv4
3. เลือก New Scope
4. กำหนดชื่อ Scope
5. กำหนดช่วง IP Address ตัวอย่าง
6. Start IP : 192.168.1.100
7. End IP : 192.168.1.200
8. กำหนด Subnet Mask
9. กำหนด Lease Duration

ตอนที่ 3 กำหนด DHCP Options

1. กำหนด Default Gateway
2. กำหนด DNS Server
3. กำหนด Domain Name (ถ้ามี)
4. เปิดใช้งาน Scope

ตอนที่ 4 ทดสอบการทำงาน

1. ตั้งค่าเครื่องลูกข่ายให้รับ IP Address อัตโนมัติ
2. ใช้คำสั่ง ipconfig /release
3. ใช้คำสั่ง ipconfig /renew
4. ใช้คำสั่ง ipconfig /all
5. บันทึกผลการรับ IP Address

ตอนที่ 5 สรุปผลการปฏิบัติงาน

1. บันทึกภาพหน้าจอการสร้าง Scope
2. บันทึกภาพหน้าจอผลการรับ IP Address
3. สรุปผลการดำเนินงาน
4. วิเคราะห์ปัญหาและแนวทางแก้ไข (ถ้ามี)
5. จัดทำรายงานส่งผู้สอน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

รายการประเมิน	ดีเยี่ยม (4)	ดี (3)	พอใช้ (2)	ปรับปรุง (1)	คะแนน
ความรู้เกี่ยวกับ DHCP Server	อธิบายได้ถูกต้องครบถ้วน	อธิบายได้ถูกต้องเกือบทั้งหมด	อธิบายได้บางส่วน	อธิบายไม่ถูกต้อง	4
การติดตั้ง DHCP Server	ติดตั้งได้ถูกต้องสมบูรณ์	ผิดพลาดเล็กน้อย	ต้องได้รับคำแนะนำ	ไม่สามารถติดตั้งได้	4
การสร้าง Scope	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การกำหนด DHCP Options	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4

การทดสอบการ แจกจ่าย IP Address	ทดสอบครบทุก ขั้นตอน	ทดสอบได้เกือบ ครบ	ทดสอบได้ บางส่วน	ไม่สามารถ ทดสอบได้	4
-----------------------------------	------------------------	----------------------	---------------------	-----------------------	---

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 3	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชาระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 11
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

จัดตั้งและกำหนดค่าบริการ File and Resource Sharing บนระบบปฏิบัติการเครื่องแม่ข่ายได้อย่างถูกต้อง สามารถกำหนดสิทธิ์การเข้าถึงทรัพยากร ทดสอบการใช้งาน ตรวจสอบ และรายงานผลการปฏิบัติงานได้ พร้อมประยุกต์ใช้ในการบริหารจัดการทรัพยากรเครือข่ายขององค์กรได้อย่างมีประสิทธิภาพและปลอดภัย

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับหลักการทำงานของ File and Resource Sharing
2. สร้างและกำหนดค่า Shared Folder ได้ถูกต้อง
3. กำหนด Share Permissions และ NTFS Permissions ได้ถูกต้อง
4. ทดสอบการเข้าถึงทรัพยากรจากเครื่องลูกข่ายได้
5. ตรวจสอบและแก้ไขปัญหาเบื้องต้นเกี่ยวกับการแชร์ไฟล์ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายหลักการทำงานของ File and Resource Sharing ได้
2. อธิบายความแตกต่างระหว่าง Share Permission และ NTFS Permission ได้
3. วิเคราะห์การกำหนดสิทธิ์การเข้าถึงทรัพยากรในองค์กรได้

4.2 ทักษะพิสัย

1. สร้าง Shared Folder ได้ถูกต้อง
2. กำหนด Share Permission ได้ถูกต้อง
3. กำหนด NTFS Permission ได้ถูกต้อง
4. ทดสอบการเข้าถึงทรัพยากรผ่านระบบเครือข่ายได้
5. ตรวจสอบและแก้ไขปัญหาการแชร์ไฟล์เบื้องต้นได้

4.3 จิตพิสัย

1. มีความรับผิดชอบในการปฏิบัติงาน

2. มีความละเอียดรอบคอบในการกำหนดสิทธิ์การเข้าถึงข้อมูล
3. ตระหนักถึงความสำคัญของความปลอดภัยของข้อมูลในระบบเครือข่าย

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1. ประยุกต์ใช้บริการ File and Resource Sharing ในการทำงานขององค์กรได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์แม่ข่าย (Server)
2. เครื่องคอมพิวเตอร์ลูกข่าย (Client)
3. ระบบปฏิบัติการ Windows Server 2019
4. โปรแกรม VMware Workstation หรือ VirtualBox
5. ระบบเครือข่าย LAN
6. ใบความรู้และเอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1. ตรวจสอบชื่อโฟลเดอร์และตำแหน่งจัดเก็บก่อนทำการแชร์
2. กำหนดสิทธิ์ผู้ใช้งานตามหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege)
3. หลีกเลี่ยงการกำหนดสิทธิ์ Full Control ให้กับผู้ใช้ทุกคน
4. ตรวจสอบความถูกต้องของ Share Permission และ NTFS Permission ก่อนใช้งานจริง
5. ระมัดระวังการลบหรือแก้ไขข้อมูลที่ใช้งานร่วมกัน

7. ขั้นตอนการปฏิบัติงาน

ตอนที่ 1 สร้างโฟลเดอร์สำหรับแชร์

1. สร้างโฟลเดอร์ชื่อ "Department"
2. สร้างโฟลเดอร์ย่อยดังนี้

Accounting

HR

IT

3. บันทึกภาพหน้าจอผลการสร้างโฟลเดอร์

ตอนที่ 2 กำหนดค่า Shared Folder

1. คลิกขวาที่โฟลเดอร์ Department
2. เลือก Properties
3. เลือกแท็บ Sharing
4. เลือก Advanced Sharing
5. ตี勾 Share this folder
6. กำหนดชื่อ Share เป็น Department
7. กด Apply และ OK

ตอนที่ 3 กำหนด Share Permission

กำหนดสิทธิ์ดังนี้

1. กลุ่มผู้ใช้ สิทธิ์
 Administrators Full Control
 IT Change
 HR Read
 Accounting Read
2. บันทึกภาพหน้าจอการกำหนดสิทธิ์

ตอนที่ 4 กำหนด NTFS Permission

1. เปิดแท็บ Security
2. เพิ่มกลุ่มผู้ใช้ที่กำหนด
3. กำหนดสิทธิ์ตามนโยบายขององค์กร
4. ตรวจสอบผลการกำหนดสิทธิ์
5. บันทึกภาพหน้าจอการตั้งค่า

ตอนที่ 5 ทดสอบการเข้าถึงทรัพยากร

1. เข้าใช้งานจากเครื่องลูกข่าย
2. เปิด Run และพิมพ์

`\ServerName\Department`

3. ทดสอบการเข้าถึงด้วยบัญชีผู้ใช้แต่ละกลุ่ม
 4. บันทึกผลการทดสอบลงตาราง
- | กลุ่มผู้ใช้ | อ่านข้อมูล | แก้ไขข้อมูล | ลบข้อมูล |
|-------------|------------|-------------|----------|
| IT | | | |
| HR | | | |
| Accounting | | | |

ตอนที่ 6 สรุปผลการปฏิบัติงาน

1. สรุปผลการสร้าง Shared Folder
2. สรุปผลการกำหนดสิทธิ์
3. วิเคราะห์ปัญหาที่พบระหว่างปฏิบัติงาน
4. เสนอแนวทางแก้ไขปัญหา
5. จัดทำรายงานผลการปฏิบัติงานส่งผู้สอน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9.การประเมินผล

รายการประเมิน	ดีเยี่ยม (4)	ดี (3)	พอใช้ (2)	ปรับปรุง (1)	คะแนน
ความรู้เกี่ยวกับ File and Resource Sharing	อธิบายได้ถูกต้องครบถ้วน	อธิบายได้ถูกต้องเกือบทั้งหมด	อธิบายได้บางส่วน	อธิบายไม่ถูกต้อง	4
การสร้าง Shared Folder	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การกำหนด Share Permission	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การกำหนด NTFS Permission	ถูกต้องครบถ้วน	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การทดสอบการเข้าถึงทรัพยากร	ทดสอบครบทุกขั้นตอน	ทดสอบได้เกือบครบ	ทดสอบได้บางส่วน	ไม่สามารถทดสอบได้	4

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 4	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชาระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 12
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

ตรวจสอบ วิเคราะห์ และแก้ไขปัญหาการทำงานของบริการ DNS Server, DHCP Server และ File and Resource Sharing ได้อย่างถูกต้อง สามารถจัดทำรายงานผลการบริหารจัดการบริการ โครงสร้างพื้นฐานเครือข่ายได้อย่างเป็นระบบ และนำเสนอผลการดำเนินงานได้อย่างมีประสิทธิภาพ

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับการตรวจสอบและแก้ไขปัญหาบริการโครงสร้างพื้นฐานเครือข่าย
2. ตรวจสอบสถานะการทำงานของ DNS Server, DHCP Server และ File Sharing ได้
3. วิเคราะห์สาเหตุของปัญหาและกำหนดแนวทางแก้ไขได้
4. ใช้เครื่องมือและคำสั่งในการตรวจสอบระบบได้ถูกต้อง
5. จัดทำรายงานผลการดำเนินงานและนำเสนอข้อมูลได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายแนวทางการตรวจสอบการทำงานของ DNS, DHCP และ File Sharing ได้
2. วิเคราะห์สาเหตุของปัญหาที่เกิดขึ้นในระบบเครือข่ายได้
3. อธิบายวิธีการแก้ไขปัญหาพื้นฐานของบริการโครงสร้างพื้นฐานเครือข่ายได้

4.2 ทักษะพิสัย

1. ใช้เครื่องมือสำหรับตรวจสอบสถานะบริการต่าง ๆ ได้
2. ใช้คำสั่งในการวิเคราะห์ปัญหาเครือข่ายได้
3. แก้ไขปัญหาการทำงานของ DNS, DHCP และ File Sharing ได้
4. จัดทำรายงานสรุปผลการดำเนินงานได้ถูกต้อง

4.3 จิตพิสัย

1. มีความรับผิดชอบต่อการปฏิบัติงาน
2. มีความละเอียดรอบคอบในการตรวจสอบระบบ

3.มีเจตคติที่ดีต่อการแก้ไขปัญหาอย่างเป็นระบบ

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1.ประยุกต์ใช้กระบวนการวิเคราะห์และแก้ไขปัญหาในสถานการณ์จริงได้

5. เครื่องมือ วัสดุ และอุปกรณ์

- 1.เครื่องคอมพิวเตอร์แม่ข่าย (Server)
- 2.เครื่องคอมพิวเตอร์ลูกข่าย (Client)
- 3.ระบบปฏิบัติการ Windows Server 2019
- 4.โปรแกรม VMware Workstation หรือ VirtualBox
- 5.ระบบเครือข่าย LAN
- 3.ใบความรู้และคู่มือการปฏิบัติงาน

6. คำแนะนำ/ข้อควรระวัง

- 1.ตรวจสอบข้อมูลก่อนดำเนินการแก้ไขระบบทุกครั้ง
- 2.สำรองข้อมูลหรือสร้าง Snapshot ก่อนปรับแต่งค่าระบบ
- 3.บันทึกผลการตรวจสอบและการแก้ไขปัญหาอย่างละเอียด
- 4.ไม่แก้ไขค่าระบบที่ไม่เกี่ยวข้องกับปัญหาที่พบ
- 5.ปฏิบัติตามหลักความปลอดภัยด้านสารสนเทศ

7. ขั้นตอนการปฏิบัติงาน

ตอนที่ 1 ตรวจสอบบริการ DNS Server

ตรวจสอบสถานะ DNS Service

ใช้คำสั่ง nslookup ทดสอบการแปลงชื่อโดเมน

ใช้คำสั่ง ping ทดสอบการเชื่อมต่อ

ตัวอย่างแบบบันทึกผลการตรวจสอบ

ลำดับ	รายการตรวจสอบ	คำสั่งที่ใช้	ผลการตรวจสอบ	หมายเหตุ
1	ตรวจสอบ DNS Service	Get-Service DNS หรือ services.msc		
2	ตรวจสอบการทำงานของ DNS	nslookup server01.local		

3	ทดสอบการเชื่อมต่อผ่านชื่อเครื่อง	ping server01.local		
---	----------------------------------	---------------------	--	--

ตอนที่ 2 ตรวจสอบบริการ DHCP Server

- 1.ตรวจสอบสถานะ DHCP Service
- 2.ตรวจสอบ Scope ที่กำหนด
- 3.ตรวจสอบ Address Lease
- 4.ทดสอบรับ IP Address จากเครื่องลูกข่าย
- 5.บันทึกผลการตรวจสอบ

ตัวอย่างแบบบันทึกผลการตรวจสอบ

ลำดับ	รายการตรวจสอบ	วิธีตรวจสอบ/คำสั่ง	ผลการตรวจสอบ	หมายเหตุ
1	DHCP Service	Get-Service DHCPService หรือ services.msc		
2	Scope	DHCP Manager → IPv4 → Scope		
3	Lease	DHCP Manager → Address Leases		
4	การรับ IP Address	ipconfig /all หรือ ipconfig /renew		

ตอนที่ 3 ตรวจสอบบริการ File Sharing

- 1.ตรวจสอบ Shared Folder
- 2.ตรวจสอบ Share Permission
- 3.ตรวจสอบ NTFS Permission
- 4.ทดสอบการเข้าถึงจากเครื่องลูกข่าย

5.บันทึกผลการตรวจสอบ

ตัวอย่างแบบบันทึกผลการตรวจสอบ

ลำดับ	รายการตรวจสอบ	วิธีตรวจสอบ	ผลการตรวจสอบ	หมายเหตุ
1	Shared Folder	File Explorer → Properties → Sharing		
2	Share Permission	Advanced Sharing → Permissions		
3	NTFS Permission	Properties → Security		
4	การเข้าถึงข้อมูล	ทดสอบเข้าใช้งานผ่าน \\ServerName\ShareName และทดลอง อ่าน/สร้าง/แก้ไข/ลบไฟล์		

ตอนที่ 4 วิเคราะห์และแก้ไขปัญหา

ให้นักศึกษาวิเคราะห์ปัญหาจากสถานการณ์ที่กำหนด

กรณีศึกษา 1

เครื่องลูกข่ายไม่สามารถแปลงชื่อโดเมนเป็น IP Address ได้
สาเหตุที่คาดว่าเป็นไปได้

.....
แนวทางแก้ไข

.....

กรณีศึกษา 2

เครื่องลูกข่ายไม่ได้รับ IP Address อัตโนมัติ
สาเหตุที่คาดว่าจะเป็นไปได้

.....

แนวทางแก้ไข

.....

กรณีศึกษา 3

ผู้ใช้ไม่สามารถเปิด Shared Folder ได้
สาเหตุที่คาดว่าจะเป็นไปได้

.....

แนวทางแก้ไข

.....

ตอนที่ 5 จัดทำรายงานผลการปฏิบัติงาน

ให้นักศึกษาจัดทำรายงานประกอบด้วย

- 1.วัตถุประสงค์ของการปฏิบัติงาน
- 2.เครื่องมือและอุปกรณ์ที่ใช้
- 3.ขั้นตอนการดำเนินงาน
- 4.ผลการตรวจสอบระบบ
- 5.ปัญหาที่พบ
- 6.แนวทางแก้ไข
- 7.สรุปผลการดำเนินงาน

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9.การประเมินผล

รายการประเมิน	ดีเยี่ยม (4)	ดี (3)	พอใช้ (2)	ปรับปรุง (1)	คะแนน
ความรู้เกี่ยวกับการตรวจสอบและแก้ไขปัญหา	อธิบายได้ถูกต้องครบถ้วน	อธิบายได้ถูกต้องเกือบทั้งหมด	อธิบายได้บางส่วน	อธิบายไม่ถูกต้อง	4
การตรวจสอบบริการ DNS	ตรวจสอบได้ครบถ้วนและถูกต้อง	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การตรวจสอบบริการ DHCP	ตรวจสอบได้ครบถ้วนและถูกต้อง	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การตรวจสอบ File Sharing	ตรวจสอบได้ครบถ้วนและถูกต้อง	ผิดพลาดเล็กน้อย	ทำได้บางส่วน	ไม่สามารถดำเนินการได้	4
การวิเคราะห์และแก้ไขปัญหา	วิเคราะห์ได้ถูกต้องและเป็นระบบ	วิเคราะห์ได้ดี	วิเคราะห์ได้บางส่วน	ไม่สามารถวิเคราะห์ได้	4

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	แผนการจัดการเรียนรู้	หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 13-15
	ชื่อหน่วยการเรียนรู้	ทฤษฎี 3 ชม.
	งานรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ	ปฏิบัติ 12 ชม.
ชื่อเรื่อง/งานรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

ประเมินความเสี่ยง กำหนดมาตรการความปลอดภัย เช่น Firewall, SSL Certificate และ AAA Server เพื่อปกป้องระบบเครื่องแม่ข่ายและบริการจากภัยคุกคาม พร้อมจัดทำรายงาน

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ
2. ประเมินความเสี่ยง กำหนดมาตรการความปลอดภัยเพื่อปกป้องระบบเครื่องแม่ข่ายและบริการจากภัยคุกคาม และจัดทำรายงาน

4. จุดประสงค์เชิงพฤติกรรม (เขียนให้ครบด้าน พุทธิพิสัย ทักษะพิสัย จิตพิสัย และ ประยุกต์ใช้)

4.1 พุทธิพิสัย (Cognitive Domain)

1. บอกประเภทของภัยคุกคามและช่องโหว่ทางความปลอดภัยของระบบเครื่องแม่ข่ายได้ถูกต้อง
2. อธิบายหลักการทำงานของ Firewall, SSL Certificate และ AAA Server ได้ถูกต้อง
3. เลือกใช้เครื่องมือหรือเทคนิคในการรักษาความปลอดภัยของระบบเครื่องแม่ข่ายและบริการตามสถานการณ์ได้ถูกต้อง
4. วิเคราะห์ความเสี่ยงและผลกระทบของภัยคุกคามต่อระบบเครื่องแม่ข่ายได้ถูกต้อง
5. ประเมินประสิทธิภาพของมาตรการความปลอดภัยที่นำมาใช้กับระบบเครื่องแม่ข่ายได้ถูกต้อง
6. วางแผนการป้องกันระบบเครื่องแม่ข่ายจากภัยคุกคามทางไซเบอร์เบื้องต้นได้ถูกต้อง

4.2 ทักษะพิสัย (Psychomotor Domain)

1. ประเมินความเสี่ยงและช่องโหว่ด้านความปลอดภัยของระบบเครื่องแม่ข่ายและบริการได้ถูกต้อง
2. กำหนดและตั้งค่า Firewall เพื่อป้องกันระบบเครื่องแม่ข่ายได้ถูกต้อง
3. สร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัยได้ถูกต้อง
4. กำหนดค่าและบริหารจัดการ AAA Server เพื่อการตรวจสอบยืนยันตัวตนได้ถูกต้อง
5. บำรุงรักษาและอัปเดตระบบรักษาความปลอดภัยของเครื่องแม่ข่ายเป็นประจำได้ถูกต้อง
6. จัดทำรายงานผลการประเมินความเสี่ยงและมาตรการความปลอดภัยได้ถูกต้อง

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการด้วยความละเอียดรอบคอบ มีความรับผิดชอบ และตระหนักถึงความสำคัญของข้อมูล

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ความรู้และทักษะในการประเมินความเสี่ยงและกำหนดมาตรการความปลอดภัยเพื่อปกป้องระบบเครื่องแม่ข่ายและบริการจากภัยคุกคามได้อย่างมีประสิทธิภาพ

5. สารการเรียนรู้

1. ประเมินความเสี่ยงและภัยคุกคามต่อระบบ
2. วางแผนการตั้งค่าและมาตรการความปลอดภัย
3. กำหนดการทำงานของ Firewall เบื้องต้น
4. สร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัย
5. ตั้งค่าการตรวจสอบยืนยันตัวตนและการอนุญาต (AAA Server)
6. ตรวจสอบและทดสอบมาตรการความปลอดภัย
7. จัดทำรายงานการประเมินความปลอดภัย (ชิ้นงาน: รายงานการประเมินความปลอดภัย, ระบบที่ได้รับการรักษาความปลอดภัย)

6. กิจกรรมการเรียนรู้

1. ขั้นเตรียมความพร้อม

1. ครูตรวจสอบความพร้อมของห้องปฏิบัติการคอมพิวเตอร์ ระบบเครือข่าย และเครื่องแม่ข่ายที่ใช้ในการฝึกปฏิบัติ
2. ผู้เรียนเปิดเครื่องคอมพิวเตอร์และเตรียมระบบปฏิบัติการเครื่องแม่ข่ายสำหรับการเรียน
3. ครูชี้แจงจุดประสงค์การเรียนรู้ สมรรถนะประจำหน่วย และภาระงานที่ต้องปฏิบัติ
4. ผู้เรียนทบทวนความรู้เดิมเกี่ยวกับระบบเครือข่าย การจัดการผู้ใช้ และบริการของเครื่องแม่ข่าย

2. ขั้นนำเข้าสู่บทเรียน

1. ครูนำเสนอกรณีศึกษาการถูกโจมตีระบบสารสนเทศ เช่น การโจมตีด้วย Malware, Ransomware หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต
2. ครูตั้งคำถามกระตุ้นความคิด เช่น
หากเครื่องแม่ข่ายขององค์กรถูกโจมตีจะเกิดผลกระทบอย่างไร
ข้อมูลขององค์กรควรได้รับการป้องกันด้วยวิธีใด
3. ผู้เรียนร่วมอภิปรายเกี่ยวกับภัยคุกคามทางไซเบอร์ที่พบในชีวิตประจำวัน
4. ครูเชื่อมโยงเข้าสู่เนื้อหาเรื่องการรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ

3. ขั้นให้เนื้อหา

- 1 การประเมินความเสี่ยงและภัยคุกคาม
ประเภทของภัยคุกคามทางไซเบอร์
ช่องโหว่ของระบบเครื่องแม่ข่าย
การวิเคราะห์ความเสี่ยงด้านความปลอดภัย
- 2 การวางแผนมาตรการรักษาความปลอดภัย
หลักการป้องกันเชิงรุก
แนวคิด Defense in Depth

การกำหนดนโยบายความปลอดภัย

3 การกำหนดค่า Firewall

หลักการทำงานของ Firewall

การกำหนดกฎ (Rule)

การอนุญาตและปฏิเสธการเข้าถึง

4 การสร้างและติดตั้ง SSL Certificate

ความสำคัญของ SSL/TLS

การสร้าง Self-Signed Certificate

การติดตั้ง Certificate บน Web Server

5 การตั้งค่า AAA Server

Authentication

Authorization

Accounting

การจัดการบัญชีผู้ใช้งาน

6 การตรวจสอบและทดสอบระบบรักษาความปลอดภัย

การทดสอบการเข้าถึงระบบ

การตรวจสอบ Log

การประเมินผลการป้องกัน

4. ขั้นฝึกปฏิบัติ

กิจกรรมที่ 1 วิเคราะห์ความเสี่ยงของระบบ

1. ผู้เรียนศึกษาสถานการณ์จำลองที่กำหนด
2. ระบุทรัพย์สินสารสนเทศ ภัยคุกคาม และช่องโหว่
3. จัดทำตารางประเมินความเสี่ยง

กิจกรรมที่ 2 การกำหนดค่า Firewall

1. ติดตั้งและเปิดใช้งาน Firewall
2. สร้างกฎการอนุญาตและปฏิเสธการเข้าถึง
3. ทดสอบผลการทำงานของ Firewall

กิจกรรมที่ 3 การสร้าง SSL Certificate

1. สร้าง SSL Certificate
2. ติดตั้ง Certificate บน Web Server
3. ทดสอบการเชื่อมต่อผ่าน HTTPS

กิจกรรมที่ 4 การกำหนดค่า AAA Server

1. สร้างบัญชีผู้ใช้งาน
2. กำหนดสิทธิ์การเข้าถึง
3. ทดสอบการยืนยันตัวตนและการอนุญาต

กิจกรรมที่ 5 การตรวจสอบระบบ

1. ตรวจสอบบันทึกเหตุการณ์ (Log)
2. วิเคราะห์ผลการทำงานของระบบรักษาความปลอดภัย

3. สรุปผลการทดสอบ

กิจกรรมที่ 6 จัดทำรายงาน

1. จัดทำรายงานการประเมินความเสี่ยง
2. บันทึกขั้นตอนการกำหนดค่าระบบ
3. สรุปผลการดำเนินงานและข้อเสนอแนะ

5. ขั้นสรุปและประเมินผล

1. ผู้เรียนร่วมกันสรุปความรู้เกี่ยวกับการรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ
2. ผู้เรียนนำเสนอผลการปฏิบัติงานและรายงานที่จัดทำ
3. ครูซักถามและอภิปรายปัญหาที่พบระหว่างการปฏิบัติงาน
 - ประเมินผลจาก
 - การสังเกตพฤติกรรมการปฏิบัติงาน
 - ใบงานและรายงาน
 - ผลการตั้งค่าระบบ
 - แบบทดสอบหลังเรียน

6. คำแนะนำ/ข้อควรระวัง

1. สำรองข้อมูลก่อนดำเนินการปรับแต่งระบบเครื่องแม่ข่ายทุกครั้ง
2. ตรวจสอบความถูกต้องของการกำหนดค่า Firewall ก่อนนำไปใช้งานจริง
3. รักษาความลับของบัญชีผู้ใช้ รหัสผ่าน และ Certificate
4. ระวังการกำหนดสิทธิ์ผู้ใช้งานไม่ให้มากเกินไปจนเกิดความจำเป็น
5. ศึกษาขั้นตอนการติดตั้งและกำหนดค่าระบบให้เข้าใจก่อนปฏิบัติ
6. บันทึกขั้นตอนการดำเนินงานทุกครั้งเพื่อใช้ในการตรวจสอบย้อนหลัง
7. ปฏิบัติตามหลักจริยธรรมและความมั่นคงปลอดภัยทางสารสนเทศอย่างเคร่งครัด

7. สื่อและแหล่งเรียนรู้

1. เอกสารประกอบการสอน เรื่อง การรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ
2. ใบความรู้หน่วยที่ 4
3. ใบงานหน่วยที่ 4
4. แบบฝึกหัดและแบบทดสอบ
5. เครื่องคอมพิวเตอร์และระบบเครือข่าย
6. Windows Server 2019
7. โปรแกรม Web Browser
8. Firewall Software
9. SSL Certificate Tools
10. ระบบ AAA Server

8. หลักฐานการเรียนรู้

1. หลักฐานความรู้
 - คะแนนจากการทำแบบฝึกหัด และแบบทดสอบในหนังสือประกอบการเรียน

2. หลักฐานการปฏิบัติงาน

คะแนนการทำกิจกรรมการเรียนรู้ และภาพถ่ายการทำกิจกรรมของผู้เรียน

9. การวัดและประเมินผล

1. เกณฑ์การปฏิบัติงาน

ตอบคำถามหรือแบบทดสอบได้อย่างถูกต้อง ไม่น้อยกว่า 80%

ปฏิบัติตามขั้นตอนกิจกรรม และใช้เทคโนโลยีได้อย่างเหมาะสมถูกต้อง

เข้าร่วม สื่อสาร และร่วมมือกับสมาชิกในกลุ่มได้ดี มีความรับผิดชอบ

2. วิธีประเมิน

แบบฝึกหัดหลังเรียน ตรวจสอบความเข้าใจในเนื้อหา

แบบทดสอบหลังเรียนถูกต้อง ไม่น้อยกว่า 80%

3. เครื่องมือประเมิน

แบบทดสอบหลังเรียน

10. บันทึกผลหลังจัดการเรียนรู้

1. ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

2. ปัญหา อุปสรรคที่พบ

3. การแก้ไขปัญหา

5) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

6) แนวทางแก้ปัญหาในครั้งต่อไป

11. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”

2. เว็บไซต์: classroom <https://learn.microsoft.com/>

3. YouTube

4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบความรู้ ที่ 1	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 9-12
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย	ทฤษฎี 4 ชม. ปฏิบัติ 16 ชม.
	ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียนรู้

ประเมินความเสี่ยง กำหนดมาตรการความปลอดภัย เช่น Firewall, SSL Certificate และ AAA Server เพื่อปกป้องระบบเครื่องแม่ข่ายและบริการจากภัยคุกคาม พร้อมจัดทำรายงาน

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะประจำหน่วย

1. ประมวลความรู้เกี่ยวกับหลักการรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ
2. ประเมินความเสี่ยง กำหนดมาตรการความปลอดภัยเพื่อปกป้องระบบเครื่องแม่ข่ายและบริการจากภัยคุกคาม และจัดทำรายงาน

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย (Cognitive Domain)

1. บอกประเภทของภัยคุกคามและช่องโหว่ทางความปลอดภัยของระบบเครื่องแม่ข่ายได้ถูกต้อง
2. อธิบายหลักการทำงานของ Firewall, SSL Certificate และ AAA Server ได้ถูกต้อง
3. เลือกใช้เครื่องมือหรือเทคนิคในการรักษาความปลอดภัยของระบบเครื่องแม่ข่ายและบริการตามสถานการณ์ได้ถูกต้อง
4. วิเคราะห์ความเสี่ยงและผลกระทบของภัยคุกคามต่อระบบเครื่องแม่ข่ายได้ถูกต้อง
5. ประเมินประสิทธิภาพของมาตรการความปลอดภัยที่นำมาใช้กับระบบเครื่องแม่ข่ายได้ถูกต้อง
6. วางแผนการป้องกันระบบเครื่องแม่ข่ายจากภัยคุกคามทางไซเบอร์เบื้องต้นได้ถูกต้อง

4.2 ทักษะพิสัย (Psychomotor Domain)

1. ประเมินความเสี่ยงและช่องโหว่ด้านความปลอดภัยของระบบเครื่องแม่ข่ายและบริการได้ถูกต้อง
2. กำหนดและตั้งค่า Firewall เพื่อป้องกันระบบเครื่องแม่ข่ายได้ถูกต้อง
3. สร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัยได้ถูกต้อง
4. กำหนดค่าและบริหารจัดการ AAA Server เพื่อการตรวจสอบยืนยันตัวตนได้ถูกต้อง
5. บำรุงรักษาและอัปเดตระบบรักษาความปลอดภัยของเครื่องแม่ข่ายเป็นประจำได้ถูกต้อง
6. จัดทำรายงานผลการประเมินความเสี่ยงและมาตรการความปลอดภัยได้ถูกต้อง

4.3 จิตพิสัย (Affective Domain)

1. มีเจตคติและกิจนิสัยที่ดีเกี่ยวกับการรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการด้วยความละเอียดรอบคอบ มีความรับผิดชอบ และตระหนักถึงความสำคัญของข้อมูล

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ความรู้และทักษะในการประเมินความเสี่ยงและกำหนดมาตรการความปลอดภัยเพื่อปกป้องระบบเครื่องแม่ข่ายและบริการจากภัยคุกคามได้อย่างมีประสิทธิภาพ

5. สารการเรียนรู้

1. ประเมินความเสี่ยงและภัยคุกคามต่อระบบ
2. วางแผนการตั้งค่าและมาตรการความปลอดภัย
3. กำหนดการทำงานของ Firewall เบื้องต้น
4. สร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัย
5. ตั้งค่าการตรวจสอบยืนยันตัวตนและการอนุญาต (AAA Server)
6. ตรวจสอบและทดสอบมาตรการความปลอดภัย
7. จัดทำรายงานการประเมินความปลอดภัย (ชิ้นงาน: รายงานการประเมินความปลอดภัย, ระบบที่ได้รับการรักษาความปลอดภัย)

การรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ

1. สถานการณ์กลางและขอบเขต

องค์กรทดลองมีเครื่อง SRV-SEC ที่ให้บริการเว็บไซต์ IIS และอาจทำหน้าที่ NPS

ห้องปฏิบัติการต้องลดพื้นผิวโจมตี เปิดเฉพาะบริการจำเป็น ใช้ HTTPS

และออกแบบการควบคุมการเข้าถึงแบบ AAA โดยเก็บหลักฐานก่อนและหลัง

รายการ	ค่าทดลอง	การใช้
Server	SRV-SEC / 192.168.40.10/24	Windows Server 2019, Static IP
Client	CLIENT-SEC / DHCP หรือ 192.168.40.20	ใช้ทดสอบจากเครือข่ายเดียวกัน
Web name	secure.training.example	ชื่อใน Certificate/Host record ตามที่ผู้สอนเตรียม
Allowed management subnet	192.168.40.0/24	จำกัด Remote IP ของ Rule ทดลอง
HTTP/HTTPS	TCP 80 / TCP 443	ทดสอบก่อนและหลัง HTTPS
NPS/RADIUS	UDP 1812/1813	เปิดเมื่อมี RADIUS Client/NAS ที่อนุญาตเท่านั้น

2. การประเมินความเสี่ยง

2.1 คำศัพท์

- Asset: สิ่งที่มีคุณค่า เช่น Server, Service, Account, Certificate, Log และข้อมูล
- Threat: เหตุหรือผู้กระทำที่อาจก่อผลเสีย เช่น Malware, Credential theft, Misconfiguration
- Vulnerability: จุดอ่อนที่ Threat ใช้ได้ เช่น Patch ล้าหลัง Port เปิดกว้าง รหัสผ่านอ่อน
- Control: มาตรการลดโอกาสหรือผลกระทบ เช่น Firewall, TLS, MFA, Backup, Logging
- Risk: ความเป็นไปได้ที่ Threat ใช้ Vulnerability และสร้างผลกระทบต่อ Asset

2.2 Risk Matrix

Likelihood \ Impact	1 ต่ำ	2 ปานกลาง	3 สูง
1 ต่ำ	1 ต่ำ	2 ต่ำ	3 ปานกลาง

Likelihood \ Impact	1 ต่ำ	2 ปานกลาง	3 สูง
2 ปานกลาง	2 ต่ำ	4 ปานกลาง	6 สูง
3 สูง	3 ปานกลาง	6 สูง	9 วิกฤต

สูตรฝึกปฏิบัติ: Risk Score = Likelihood × Impact. คะแนน 1-2 ต่ำ, 3-4 ปานกลาง, 6 สูง, 9 วิกฤต
ผู้เรียนต้องให้เหตุผลของคะแนนและระบุ Control owner/กำหนดเสร็จ ไม่ใช่คะแนนโดยเดา

2.3 กระบวนการ

37. กำหนด Scope และผู้อนุมัติ

38. จัดทำ Asset Register และเจ้าของทรัพย์สิน

39. ระบุ Threat/Vulnerability/Existing Control จากหลักฐาน

40. ให้คะแนน Likelihood/Impact และจัดลำดับ

41. เลือก Treatment: Avoid, Reduce, Transfer หรือ Accept

42. กำหนด Control, Owner, Due date และประเมิน Residual Risk หลังทดสอบ

3. Defense in Depth และ Baseline

การป้องกันที่ดีไม่พึ่ง Control เดียว ชั้นสำคัญได้แก่ Physical/Virtual isolation, Network firewall, Host hardening, Identity/least privilege, Application/TLS, Data protection/backup และ Monitoring/logging หาก Firewall ผิดพลาด TLS และสิทธิ์ยังช่วยลดผลกระทบ และ Log ช่วยตรวจสอบย้อนหลัง

- อัปเดตระบบและซอฟต์แวร์ก่อนเปิดบริการ
- ถอน Role/Feature ที่ไม่ใช่และหยุด Service ที่ไม่จำเป็น
- ใช้บัญชีผู้ดูแลเฉพาะงานและไม่แชร์รหัสผ่าน
- สำรอง Configuration และตรวจสอบว่าสามารถ Restore ได้
- ตั้งเวลาให้ตรงเพื่อให้ Log และ Certificate ตรวจสอบได้
- เก็บ Baseline ของ Port, Firewall Profile, Rules และ Event ก่อนเปลี่ยน

4. Windows Defender Firewall with Advanced Security

4.1 องค์ประกอบ Rule

องค์ประกอบ	คำถามที่ต้องตอบ	ตัวอย่าง
Direction	Inbound หรือ Outbound	Inbound HTTPS
Action	Allow, Block หรือ Allow if secure	Allow
Protocol/Port	บริการใดจำเป็น	TCP 443

องค์ประกอบ	คำถามที่ต้องตอบ	ตัวอย่าง
Profile	Domain, Private, Public ไต	Private/Domain ตาม Lab
Scope	Local/Remote IP ไต	Remote 192.168.40.0/24
Program/Service	ผูกกับโปรแกรมหรือ Service หรือไม่	World Wide Web Publishing Service

4.2 หลักการออกแบบ

- ใช้ Inbound default block และสร้าง Allow เฉพาะบริการจำเป็น
- จำกัด Profile และ Remote IP ให้แคบที่สุด
- ตั้งชื่อ Rule มีระบบ เช่น LAB-Allow-HTTPS-443-Subnet40
- บันทึก Owner, เหตุผล, วันที่ และผลทดสอบ
- ระวัง Block rule มีลำดับเหนือ Allow rule เมื่อเงื่อนไขตรงกัน
- ห้ามปิด Firewall ทั้งหมดเพื่อแก้ปัญหา

4.3 Backup, สร้าง Rule และทดสอบ

43. เปิด wf.msc แล้ว Export Policy เป็นไฟล์ก่อนแก้ หรือใช้ netsh advfirewall export ตามที่ผู้สอนกำหนด
44. บันทึก Profile state และ Inbound default action
45. สร้าง Inbound Custom/Port Rule สำหรับ TCP 443 จำกัด Remote IP 192.168.40.0/24 และ Profile ตามแผน
46. ใช้ Test-NetConnection 192.168.40.10 -Port 443 จาก Client ก่อน/หลัง
47. ตรวจสอบ Monitoring > Firewall และ Event/Logging ตามที่เปิดใช้
48. หากสูญเสียการเชื่อมต่อ ให้ใช้ Console ของ VM และ Restore Policy/Disable เฉพาะ Rule ที่สร้าง

ช่องทางกู้คืน: อย่าสร้าง Block rule ที่อาจตัด RDP/WinRM ก่อนยืนยันว่ามี Console ของ VM หรือ Out-of-band access และ Backup Policy

5. TLS Certificate และ HTTPS บน IIS

5.1 TLS ช่วยอะไร

TLS ให้การเข้ารหัสระหว่างทาง ความถูกต้องของข้อมูล และการยืนยันตัวตนของ Server ผ่าน Certificate แต่ Self-Signed Certificate ไม่ได้ได้รับความไว้วางใจอัตโนมัติ เหมาะสำหรับห้องทดลองเท่านั้น ระบบจริงควรใช้ Certificate จาก CA ที่เชื่อถือได้และมีขั้นตอนจัดการอายุ/การต่ออายุ

5.2 สิ่งที่ต้องตรวจใน Certificate

- Subject หรือ SAN ต้องตรงชื่อที่ Client ใช้ เช่น secure.training.example

- Validity ต้องยังไม่หมดอายุและเวลาเครื่องต้องถูกต้อง
- Enhanced Key Usage ควรรองรับ Server Authentication
- Certificate ต้องมี Private Key บน Server
- Client ต้อง Trust Issuer จึงจะไม่เตือน; การกดยอมรับคำเตือนไม่เท่ากับ Trust ที่ถูกต้อง

5.3 ขั้นตอน IIS

- ติดตั้ง Web Server (IIS) และ Management Tools แล้วสร้างหน้า Test ที่ไม่มีข้อมูลลับ
- เปิด IIS Manager > Server Certificates > Create Self-Signed Certificate ตั้ง Friendly name 'LAB-SRV-SEC-HTTPS'
- เปิด Sites > Default Web Site > Bindings > Add > https > Port 443 > เลือก Certificate
- ตรวจสอบ Windows Firewall Rule TCP 443 ให้ตรง Scope
- จาก Client เปิด https://secure.training.example และตรวจสอบ Certificate details
- บันทึกว่า Browser เตือนเพราะ Self-Signed หรือไม่ หากนำ Certificate เข้า Trusted Root ต้องทำเฉพาะ Lab และลบเมื่อจบ
- ใช้ Test-NetConnection และ Browser/Invoke-WebRequest ตามคำสั่งผู้สอนเพื่อยืนยัน Port และ TLS

5.4 แยกอาการ

อาการ	สาเหตุที่เป็นไปได้	ตรวจสอบ
Timeout/ต่อไม่ได้	Network/Firewall/Binding/Service	ping, Test-NetConnection, IIS site, binding
Name not resolved	DNS/Hosts file	nslookup, ipconfig /all
Certificate name mismatch	Subject/SAN ไม่ตรง URL	Certificate details และ URL
Untrusted issuer	Self-signed หรือ CA ไม่ trusted	Certification Path/Trusted Root
Expired/not yet valid	Validity หรือเวลาเครื่องผิด	Date/Time และ Valid from/to

6. AAA และ Network Policy Server (NPS)

6.1 AAA

- Authentication: ยืนยันว่าเป็นใคร
- Authorization: หลังยืนยันแล้วอนุญาตทำอะไร/เข้าเครือข่ายใด

- Accounting: บันทึกว่าใคร เชื่อมต่อเมื่อใด นานเท่าใด และผลเป็นอย่างไร

NPS เป็นการใช้งาน RADIUS ของ Microsoft สำหรับรวม Authentication, Authorization และ Accounting ของการเชื่อมต่อเครือข่าย เช่น VPN, Wireless AP หรือ Switch ที่รองรับ 802.1X อุปกรณ์เหล่านี้คือ RADIUS Client/NAS ไม่ใช่เครื่องผู้ใช้งานปลายทางโดยตรง

6.2 องค์ประกอบ NPS

องค์ประกอบ	หน้าที่	จุดเสี่ยง
RADIUS Client	NAS ที่ส่ง Access-Request	IP/Shared secret ผิดหรือเปิดกว้าง
Connection Request Policy	กำหนดว่าจะประมวลผล/ส่งต่อคำขออย่างไร	ลำดับหรือเงื่อนไขกว้างเกินไป
Network Policy	กำหนดเงื่อนไข การอนุญาต และวิธียืนยัน	Allow กว้าง/วิธียืนยันไม่ปลอดภัย
Account database	AD DS หรือ Local SAM ตามสถาปัตยกรรม	บัญชี/กลุ่ม/สิทธิ์ผิด
Accounting	เขียน Text/SQL log และ Event	ไม่เปิด Log หรือเวลาไม่ตรง

6.3 ขั้นตอนห้องปฏิบัติการ

- ติดตั้ง Network Policy and Access Services > Network Policy Server (Desktop Experience)
- เปิด nps.msc และบันทึก/Export Configuration ตามคำแนะนำผู้สอน; ไฟล์ Export อาจมี Shared Secret แบบไม่เข้ารหัส ต้องเก็บเป็นความลับ
- สร้าง RADIUS Client ด้วย IP ของ NAS/Simulator ที่ผู้สอนอนุญาตและ Shared Secret สำหรับ Lab เท่านั้น
- สร้างกลุ่มผู้ใช้ทดสอบและ Network Policy ที่จำกัดกลุ่ม ประเภท NAS และวิธียืนยันตามโจทย์
- กำหนด Accounting เป็น Local file หรือ Event ตาม Lab และตรวจตำแหน่งจัดเก็บ
- ถ้ามี NAS/Simulator ให้ส่ง Access-Request และตรวจ Event/Accounting; หากไม่มี ให้ประเมิน Configuration เท่านั้นและระบุข้อจำกัด ห้ามอ้างว่าทดสอบ End-to-end สำเร็จ

ข้อจำกัดการทดสอบ NPS: NPS จะทดสอบ AAA แบบครบวงจรได้เมื่อมี RADIUS Client/NAS ที่ส่งคำขอจริง เช่น VPN Server, AP หรือ Switch หากไม่มี ให้ส่งหลักฐานการติดตั้งและ Policy พร้อมแผนทดสอบ แต่ต้องระบุว่า End-to-end ยังไม่ได้ยืนยัน

7. Logging การทดสอบ และความเสี่ยงคงเหลือ

- กำหนดเวลาและ Time zone ให้ถูกต้องก่อนทดสอบ
- บันทึก Event ID/Source/Time/Account/Client IP และ Result โดยปิดบัง Secret

- เก็บ Before/After เพื่อแสดงว่า Control ทำให้ Risk ลดลงจริง
- ทดสอบทั้งกรณีควรอนุญาตและควรปฏิเสธ
- ไม่ลบ Log เพื่อให้รายงานดูผ่าน และไม่เก็บรหัสผ่าน/Private key ในรายงาน
- ประเมิน Residual Risk พร้อม Owner และแผนติดตาม

8. รูปแบบรายงานการประเมินความปลอดภัย

- ขอบเขตและข้อจำกัดการทดสอบ
- Asset Register และผังระบบ
- Risk Register ก่อนใช้ Control
- รายละเอียด Firewall, TLS และ AAA/NPS Control
- Test matrix: Test case, Expected, Actual, Evidence, Pass/Fail
- เหตุการณ์/Log ที่เกี่ยวข้องและการวิเคราะห์
- Residual Risk, ข้อเสนอแนะ, Owner และ Due date
- ภาควงภาพหลักฐานโดยปิดบังข้อมูลลับ

9. เอกสารอ้างอิงของใบความรู้

Microsoft Learn. Windows Firewall rules.

<https://learn.microsoft.com/windows/security/operating-system-security/network-security/windows-firewall/rules>

Microsoft Learn. Windows Firewall with Advanced Security troubleshooting guidance.

<https://learn.microsoft.com/troubleshoot/windows-server/networking/troubleshoot-windows-firewall-with-advanced-security-guidance>

Microsoft Learn. How to Set Up SSL on IIS.

<https://learn.microsoft.com/iis/manage/configuring-security/how-to-set-up-ssl-on-iis>

Microsoft Learn. Network Policy Server overview. <https://learn.microsoft.com/windows-server/networking/technologies/nps/nps-top>

Microsoft Learn. Network Policy Server best practices. <https://learn.microsoft.com/windows-server/networking/technologies/nps/nps-best-practices>

NIST SP 800-115. Technical Guide to Information Security Testing and Assessment.

<https://csrc.nist.gov/pubs/sp/800/115/final>



ในความรู้ที่ 1

การประเมินความเสี่ยงและ ภัยคุกคามต่อระบบ Windows Server 2019





หมายเหตุสำคัญ

การประเมินความเสี่ยงคือการระบุการระบุ วิเคราะห์ และจัดลำดับความเสี่ยงที่อาจส่งผลกระทบต่อระบบ เพื่อกำหนดแนวทางการควบคุมและลดความเสี่ยงอย่างเหมาะสม ช่วยให้ระบบ Windows Server 2019 มีความมั่นคง ปลอดภัย และพร้อมให้บริการอย่างต่อเนื่อง


1. ความหมาย

การประเมินความเสี่ยง (Risk Assessment) คือ การระบุ ปัจจัยเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นกับระบบ วิเคราะห์ โอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) หากเกิดเหตุการณ์นั้น แล้วจัดลำดับความสำคัญของความเสี่ยง เพื่อนำไปสู่การวางแผนควบคุมและป้องกัน


2. วัตถุประสงค์

- ✓ ระบุความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นกับระบบ Windows Server 2019
- ✓ ประเมินระดับความรุนแรงของความเสี่ยง
- ✓ จัดลำดับความสำคัญของความเสี่ยง
- ✓ กำหนดแนวทางการควบคุมและลดความเสี่ยงอย่างเหมาะสม
- ✓ เสริมสร้างความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการ


3. ทรัพย์สินที่ต้องปกป้อง (Assets)

- ฮาร์ดแวร์เซิร์ฟเวอร์ (Server Hardware)
- ระบบปฏิบัติการ Windows Server 2019
- ข้อมูลและฐานข้อมูล (Data & Database)
- บริการและบทบาทต่าง ๆ (Roles & Services) เช่น AD DS, DNS, DHCP, File Services, Web Server
- บัญชีผู้ใช้และสิทธิ์การเข้าถึง (User Accounts & Permissions)
- เครือข่ายและอุปกรณ์ที่เกี่ยวข้อง (Network & Devices)
- การสำรองข้อมูลและการกู้คืน (Backup & Recovery)




4. ภัยคุกคามที่พบบ่อยต่อ Windows Server 2019

- 1 มัลแวร์และไวรัส (Malware & Virus) เช่น Ransomware, Trojan
- 2 การโจมตีจากภายนอก (External Attack) เช่น Brute Force, Exploit
- 3 การใช้รหัสผ่านที่อ่อนแอ (Weak Password) หรือการเดาห้รหัสผ่าน
- 4 ช่องโหว่ของระบบ (Vulnerability) ที่ยังไม่ได้อัปเดต
- 5 การตั้งค่าความปลอดภัยไม่เหมาะสม (Misconfiguration)
- 6 การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access)
- 7 ความผิดพลาดจากมนุษย์ (Human Error) เช่น ลบข้อมูลสำคัญ
- 8 ภัยคุกคามจากภายใน (Insider Threat) เช่น การใช้สิทธิ์เกินความจำเป็น



5. การประเมินความเสี่ยง (Risk Assessment Matrix)

5.1 โอกาสที่จะเกิด (Likelihood)

ระดับ	คำอธิบาย	คะแนน
5	เกิดขึ้นได้บ่อยมาก	5
4	เกิดขึ้นได้บ่อย	4
3	เกิดขึ้นเป็นบางครั้ง	3
2	เกิดขึ้นได้บ้าง	2
1	เกิดขึ้นได้ไม่บ่อย	1

X

5.2 ผลกระทบ (Impact)

ระดับ	คำอธิบาย	คะแนน
5	กระทบรุนแรงมาก (ระบบหยุดทำงานทั้งหมด/ข้อมูลสูญหาย)	5
4	กระทบรุนแรงสูง (บริการหยุดชะงักนาน/สูญเสียบางข้อมูลสำคัญ)	4
3	กระทบปานกลาง (บริการบางส่วนหยุดชะงัก/ข้อมูลเสียหายบางส่วน)	3
2	กระทบน้อย (บริการชะงักระยะสั้น/แก้ไขได้ง่าย)	2
1	กระทบน้อยมาก (ไม่มีผลต่อการให้บริการ)	1

=

5.3 ระดับความเสี่ยง (Risk Level)

คะแนนรวม (L x I)	ระดับความเสี่ยง	การดำเนินการ
20 - 25	สูงมาก (Critical)	ต้องดำเนินการทันที
15 - 19	สูง (High)	ควรดำเนินการโดยเร็ว
8 - 14	ปานกลาง (Medium)	วางแผนควบคุม
1 - 7	ต่ำ (Low)	เฝ้าระวังอย่างต่อเนื่อง



ตัวอย่าง: ความเสี่ยงจาก Ransomware

โอกาสเกิด = 4 (เกิดบ่อย) ผลกระทบ = 5 (รุนแรงมาก) คะแนนรวม = 4 x 5 = 20 ระดับความเสี่ยง = สูงมาก (ต้องดำเนินการทันที)

6. แนวทางการควบคุมและลดความเสี่ยง



การอัปเดตและแพตช์ระบบ

- อัปเดต Windows Server 2019 และซอฟต์แวร์ที่เชื่อมต่อ
- ปิดช่องโหว่ที่รู้จักทุกจุด



การจัดการบัญชีผู้ใช้และสิทธิ์การเข้าถึง

- ใช้หลักการ Least Privilege
- ใช้รหัสผ่านที่แข็งแรงและเปลี่ยนเป็นระยะ



การตั้งค่าความปลอดภัยของเครือข่าย

- เปิดใช้งาน Windows Firewall
- จำกัดพอร์ตและบริการที่ไม่จำเป็น



การสำรองข้อมูลและการกู้คืน

- สำรองข้อมูลอย่างสม่ำเสมอ
- ทดสอบการกู้คืนข้อมูลเป็นประจำ



การเฝ้าระวังและตรวจสอบ

- ตรวจสอบ Event Logs เป็นประจำ
- ใช้เครื่องมือ Monitoring เพื่อตรวจหาความผิดปกติ



การสร้างความรู้ให้ผู้ใช้งาน

- อบรมความปลอดภัยไซเบอร์
- ป้องกันการคลิกลิงก์หรือไฟล์ที่น่าสงสัย



สรุป

การประเมินความเสี่ยงและภัยคุกคามเป็นขั้นตอนสำคัญในการบริหารจัดการความปลอดภัยของระบบ Windows Server 2019 ช่วยให้สามารถป้องกัน ลดผลกระทบ และฟื้นฟูระบบได้อย่างมีประสิทธิภาพ

ใบความรู้ที่

2

วางแผนการตั้งค่าและมาตรการความปลอดภัย

Windows Server 2019



การวางแผนการตั้งค่าและมาตรการความปลอดภัยที่ดี จะช่วยให้ระบบ Windows Server 2019 มีความเสถียร ปลอดภัย และพร้อมให้บริการอย่างมีประสิทธิภาพ

1 การวางแผนการตั้งค่า (Planning)



1.1 กำหนดวัตถุประสงค์ของเซิร์ฟเวอร์

ระบุบทบาทของเซิร์ฟเวอร์ เช่น File Server, DNS Server, DHCP Server, Web Server, Domain Controller เป็นต้น



1.2 ประเมินทรัพยากรที่ต้องการ

พิจารณา CPU, RAM, พื้นที่จัดเก็บข้อมูล, เครือข่าย ให้เหมาะสมกับบริการที่จะติดตั้ง



1.3 ออกแบบโครงสร้างเครือข่าย

กำหนด IP Address, Subnet, Gateway, DNS และการแบ่ง VLAN (ถ้ามี)



1.4 กำหนดบทบาทและสิทธิ์ผู้ใช้งาน

วางแผนโครงสร้างผู้ใช้และกลุ่ม (Group) และกำหนดสิทธิ์ การเข้าถึงทรัพยากรตามความเหมาะสม



1.5 วางแผนการสำรองข้อมูลและกู้คืนระบบ

กำหนดวิธีการสำรองข้อมูล ความถี่ และสถานที่จัดเก็บ เพื่อให้สามารถกู้คืนได้เมื่อเกิดเหตุการณ์ไม่คาดคิด

2 มาตรการความปลอดภัย (Security Measures)



2.1 การตั้งรหัสผ่านที่ปลอดภัย

- ใช้รหัสผ่านที่ยาวและซับซ้อน (อย่างน้อย 12 ตัวอักษร)
- เปิดใช้นโยบายรหัสผ่าน (Password Policy)



2.2 การควบคุมสิทธิ์การเข้าถึง

- ใช้หลักการ Least Privilege (ให้สิทธิ์เท่าที่จำเป็น)
- แยกบัญชีผู้ดูแลระบบ (Administrator Account) ออกจากบัญชีผู้ใช้ทั่วไป



2.3 การตั้งค่าไฟร์วอลล์

- เปิดใช้งาน Windows Defender Firewall
- อนุญาตเฉพาะพอร์ตและบริการที่จำเป็น



2.4 การอัปเดตระบบและแพตช์ความปลอดภัย

- ติดตั้ง Windows Update อย่างสม่ำเสมอ
- อัปเดตบทบาทและคุณลักษณะ (Roles and Features) ให้เป็นเวอร์ชันล่าสุด



2.5 การตรวจสอบและบันทึกเหตุการณ์

- เปิดใช้งานการบันทึกเหตุการณ์ (Event Logging)
- ตรวจสอบ Event Viewer อย่างสม่ำเสมอ



2.6 การสำรองข้อมูลและกู้คืนระบบ

- สำรองข้อมูลตามกำหนดเวลา
- ทดสอบการกู้คืนข้อมูลเป็นระยะเพื่อความมั่นใจ

3 การตั้งค่าพื้นฐานที่ควรดำเนินการหลังการติดตั้ง Windows Server 2019



3.1 ตั้งชื่อเซิร์ฟเวอร์ (Rename)



3.2 ตั้งค่าเครือข่าย (IP Address, DNS)



3.3 ตั้งวันที่และเวลาให้ถูกต้อง



3.4 ตั้งค่า Region และ Language



3.5 ตั้งค่า Roles และ Features



3.6 เปิดใช้งาน Windows Defender

4 ข้อควรจำ

- ✓ ความปลอดภัยต้องเริ่มตั้งแต่การวางแผน ออกแบบ และตั้งค่าอย่างรอบคอบ
- ✓ ใช้สิทธิ์ผู้ดูแลระบบเท่าที่จำเป็น และหลีกเลี่ยงการใช้งานบัญชี Administrator ในงานทั่วไป
- ✓ ตรวจสอบระบบอย่างสม่ำเสมอ และตอบสนองต่อเหตุการณ์ผิดปกติทันที
- ✓ สำรองข้อมูลเสมอ เพราะข้อมูลคือทรัพย์สินที่สำคัญที่สุดขององค์กร



หมายเหตุ : การกำหนดค่าที่เหมาะสมและมาตรการความปลอดภัยที่รัดกุม จะช่วยลดความเสี่ยงจากภัยคุกคามและทำให้ระบบ Windows Server 2019 ทำงานได้อย่างมั่นคงและปลอดภัย

ในความรู้ที่
3

การกำหนดการทำงานของ Firewall

Windows Server 2019



Firewall (ไฟร์วอลล์) คือระบบรักษาความปลอดภัยที่ทำหน้าที่ควบคุมการรับ-ส่งข้อมูลเครือข่าย โดยอนุญาตหรือบล็อกทราฟฟิกตามกฎหมาย (Rule) ที่กำหนดไว้ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต และลดความเสี่ยงจากภัยคุกคามทางเครือข่าย



1. ความสำคัญของ Firewall

- ✔ ป้องกันการเข้าถึงระบบจากผู้ไม่หวังดี
- ✔ ควบคุมการใช้งานบริการและพอร์ตที่จำเป็น
- ✔ ลดความเสี่ยงจากไวรัส เวิร์ม และการโจมตีทางเครือข่าย
- ✔ ช่วยแยกเครือข่ายภายในให้ปลอดภัยยิ่งขึ้น
- ✔ รองรับนโยบายความปลอดภัยขององค์กร



2. ประเภทของ Firewall บน Windows Server 2019

- Windows Defender Firewall (ไฟร์วอลล์ในตัวของ Windows Server 2019)
- สามารถกำหนดกฎให้กับโปรไฟล์เครือข่ายได้ 3 แบบ Domain, Private, Public
- ทำงานร่วมกับ IPsec เพื่อเพิ่มความปลอดภัย



3. หลักการทำงานของ Firewall

Firewall จะตรวจสอบแพ็กเก็ตข้อมูลที่ได้รับเข้าหรือส่งออก
ตามกฎ (Rule) ที่กำหนดไว้ โดยพิจารณาจาก

- IP Address ต้นทางและปลายทาง
- Port และ Protocol (TCP, UDP, ICMP)
- ทิศทางของการสื่อสาร (Inbound / Outbound)
- โปรไฟล์เครือข่าย (Domain / Private / Public)
- การดำเนินการ (Allow หรือ Block)

ลำดับการประมวลผลกฎ

- 1) กฎที่กำหนดเอง (Custom Rule)
- 2) กฎในตัวของ Windows
- 3) ค่าตั้งต้น (Default Rule)

4. โปรไฟล์เครือข่าย (Network Profile)

โปรไฟล์	ลักษณะการใช้งาน	ตัวอย่างการเชื่อมต่อ	ค่าตั้งต้นของ Firewall
 Domain (โดเมน)	ใช้ในเครือข่ายองค์กรที่มี Domain Controller	เชื่อมต่อกับเครือข่ายภายในองค์กรที่เข้าร่วมโดเมน	Inbound: Block (ยกเว้นที่อนุญาต) Outbound: Allow
 Private (ส่วนตัว)	ใช้กับเครือข่ายที่เชื่อถือได้ เช่น บ้าน หรือสำนักงานย่อย	เชื่อมต่อกับเครือข่ายภายในที่เชื่อถือได้	Inbound: Block (ยกเว้นที่อนุญาต) Outbound: Allow
 Public (สาธารณะ)	ใช้กับเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต หรือ Wi-Fi สาธารณะ	เชื่อมต่ออินเทอร์เน็ตจากภายนอกองค์กร	Inbound: Block (เข้มงวด) Outbound: Allow

5. ชนิดของกฎ (Firewall Rule)

-  **Inbound Rule (กฎขาเข้า)**
ควบคุมการรับข้อมูลเข้าสู่เครื่องแม่ข่าย
 -  **Outbound Rule (กฎขาออก)**
ควบคุมการส่งข้อมูลออกจากเครื่องแม่ข่าย
 -  **Connection Security Rule**
ใช้ร่วมกับ IPsec เพื่อกำหนดการเข้ารหัสและการยืนยันตัวตน
 -  **Monitoring Rule**
ใช้สำหรับตรวจสอบหาฟลักที่ตรงตามเงื่อนไข

6. การสร้างกฎ Firewall เบื้องต้น

1. เปิด Windows Defender Firewall with Advanced Security
2. เลือกประเภทกฎ (Inbound / Outbound)
3. เลือก Action (Allow the connection หรือ Block the connection)
4. เลือก Protocol และระบุ Port (เช่น TCP 80)
5. ระบุ Scope (Remote IP Address)
6. ตั้งชื่อและคำอธิบายกฎ แล้วคลิก Finish

7. ตัวอย่างการใช้งาน

วัตถุประสงค์	ตัวอย่างกฎ
อนุญาตให้ใช้บริการเว็บ (HTTP)	Inbound, Allow, TCP, Port 80
อนุญาตให้ใช้บริการรีโมต (RDP)	Inbound, Allow, TCP, Port 3389 เฉพาะ IP ที่กำหนด
บล็อกการเข้าจากทก IP	Inbound, Block, Any, Any

8. แนวทางปฏิบัติที่ดี (Best Practice)

- ✓ เปิดใช้ Firewall เฉพาะโปรไฟล์ที่เหมาะสม
- ✓ อนุญาตเฉพาะบริการและพอร์ตที่จำเป็น
- ✓ ใช้ IP Address กำหนดขอบเขตให้แคบที่สุด
- ✓ ตรวจสอบ Log อย่างสม่ำเสมอ
- ✓ อัปเดตระบบและกฎ Firewall ให้เป็นปัจจุบัน
- ✓ ทดสอบการทำงานของกฎหลังการเปลี่ยนแปลงทุกครั้ง
- ✓ จัดทำเอกสารกฎ Firewall ของระบบ

>.. คำสั่งที่เกี่ยวข้อง (Command)

```
ตรวจสอบสถานะ Firewall
netsh advfirewall show allprofiles

เปิด/ปิด Firewall
netsh advfirewall set allprofiles state on/off

รีเซ็ตกฎทั้งหมดเป็นค่าเริ่มต้น
netsh advfirewall reset
```



Firewall เป็นด่านแรกที่สำคัญในการป้องกันระบบเครือข่าย การกำหนดกฎที่เหมาะสมจะช่วยให้ระบบปลอดภัย
โดยยังคงให้บริการที่จำเป็นได้อย่างมีประสิทธิภาพ

ใบความรู้ที่

4

การสร้างและติดตั้ง SSL Certificate เพื่อการเชื่อมต่อที่ปลอดภัย

Windows Server 2019



SSL (Secure Sockets Layer) / TLS (Transport Layer Security) คือเทคโนโลยีที่ใช้เข้ารหัสข้อมูลระหว่างผู้ใช้และเซิร์ฟเวอร์ เพื่อป้องกันการดักฟัง การปลอมแปลงข้อมูล และสร้างความน่าเชื่อถือในการให้บริการผ่านเว็บไซต์หรือแอปพลิเคชัน



1. ความสำคัญของ SSL Certificate

- ✓ เข้ารหัสข้อมูลในการรับส่ง (Encryption) ป้องกันการดักฟัง
- ✓ ยืนยันตัวตนของเว็บไซต์หรือเซิร์ฟเวอร์ (Authentication)
- ✓ สร้างความน่าเชื่อถือให้กับผู้ใช้ (Trust & Confidence)
- ✓ ช่วยให้เว็บไซต์รองรับ HTTPS และแสดงกุญแจสีเขียวในเบราว์เซอร์
- ✓ จำเป็นสำหรับบริการออนไลน์ เช่น เว็บไซต์ อีเมล VPN เป็นต้น



2. ประเภทของ SSL Certificate

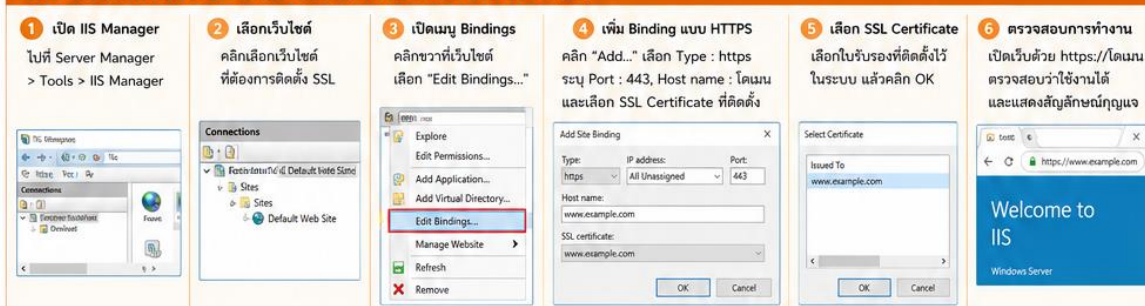
ประเภท	ระดับการตรวจสอบ	เหมาะสำหรับ
Domain Validation (DV)	ตรวจสอบความเป็นเจ้าของโดเมน	เว็บไซต์ทั่วไป, บล็อก, องค์กรขนาดเล็ก
Organization Validation (OV)	ตรวจสอบความเป็นเจ้าของโดเมน และข้อมูลขององค์กร	องค์กร, บริษัท, หน่วยงานต่าง ๆ
Extended Validation (EV)	ตรวจสอบเข้มงวดที่สุด	องค์กรขนาดใหญ่, ธนาคาร, อีคอมเมิร์ซ



3. ขั้นตอนการขอและเตรียม SSL Certificate (ตัวอย่าง: ขอจาก Let's Encrypt)



4. ขั้นตอนการติดตั้ง SSL Certificate บน Windows Server 2019 (IIS)



5. เครื่องมือที่ใช้ในการขอ SSL Certificate ฟรี

	เครื่องมือ	รายละเอียด
Let's Encrypt	Let's Encrypt	ให้ใบรับรองฟรี ใช้งานง่าย ไม่เสียค่าใช้จ่าย อายุใบรับรอง 90 วัน ต้องต่ออายุอัตโนมัติ
	Win-ACME	เครื่องมือช่วยขอและติดตั้ง Let's Encrypt บน Windows Server (รองรับ IIS)
Certbot	Certbot	เครื่องมือจาก Let's Encrypt (สำหรับ Windows ต้องใช้ร่วมกับ WSL หรือ Docker)

6. การตรวจสอบข้อมูล SSL Certificate

สามารถตรวจสอบได้จากเว็บเบราว์เซอร์ หรือใช้เครื่องมือออนไลน์ เช่น

- <https://www.ssllabs.com/ssltest/>
- <https://www.digicert.com/help/>
- Certificate > View Certificate ในเบราว์เซอร์

7. ข้อควรปฏิบัติ

ใช้ใบรับรองจาก CA ที่น่าเชื่อถือ หรือ Let's Encrypt

ต่ออายุใบรับรองก่อนหมดอายุ (ทุก 90 วันสำหรับ Let's Encrypt)

บังคับใช้ HTTPS ทั้งระบบ (Redirect HTTP to HTTPS)

ตรวจสอบการตั้งค่า SSL/TLS และความปลอดภัยอย่างสม่ำเสมอ



สรุป : การใช้ SSL Certificate ช่วยให้การเชื่อมต่อระหว่างผู้ใช้กับเซิร์ฟเวอร์มีความปลอดภัย ป้องกันการดักฟังข้อมูล และสร้างความน่าเชื่อถือให้กับระบบและองค์กรของคุณ



ใบความรู้ที่ 5

การตั้งค่าการตรวจสอบยืนยันตัวตน และการอนุญาต (AAA Server)

รายวิชา : ระบบปฏิบัติการเครื่องแม่ข่าย
รหัสวิชา : 20204-2105
ระดับชั้น : ปวส.
สาขาวิชา : เทคโนโลยีสารสนเทศ
ระบบปฏิบัติการ : Windows Server 2019

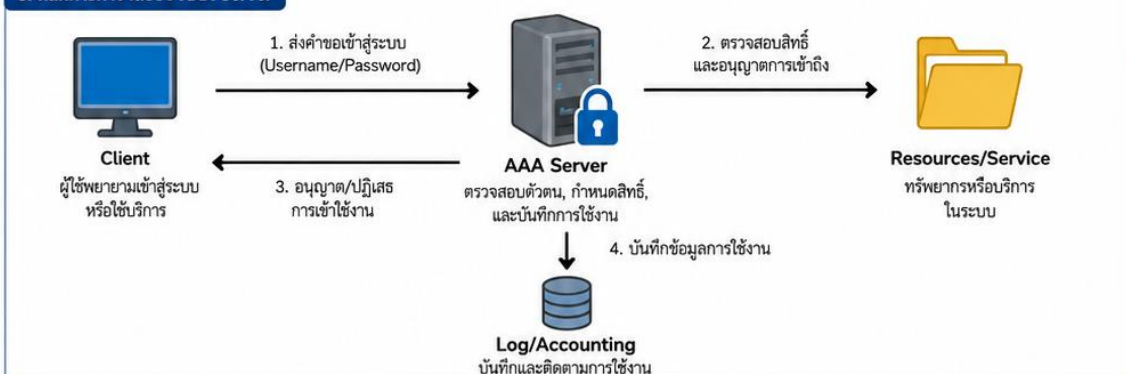
1. ความหมาย

AAA Server ย่อมาจาก Authentication, Authorization and Accounting Server คือ เซิร์ฟเวอร์ที่ทำหน้าที่ในการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) กำหนดสิทธิ์และอนุญาตการเข้าใช้ทรัพยากร (Authorization) และบันทึก/ติดตามการใช้งาน (Accounting) เพื่อเพิ่มความปลอดภัยและสามารถตรวจสอบการใช้งานในระบบได้

2. องค์ประกอบของ AAA

- **Authentication** (การตรวจสอบยืนยันตัวตน) ตรวจสอบว่าผู้ใช้เป็นใคร โดยใช้ชื่อผู้ใช้และรหัสผ่าน
- **Authorization** (การอนุญาต) กำหนดสิทธิ์ในการเข้าถึงทรัพยากรหรือบริการต่าง ๆ
- **Accounting** (การบันทึกและติดตามการใช้งาน) บันทึกข้อมูลการใช้งาน เช่น เวลาเข้าใช้, บริการที่ใช้, ปริมาณข้อมูล เป็นต้น

3. หลักการทำงานของ AAA Server



4. บทบาทของ AAA Server ในระบบเครือข่าย

- ✓ เพิ่มความปลอดภัยในการเข้าถึงระบบและข้อมูล
- ✓ ควบคุมสิทธิ์การใช้งานตามนโยบายขององค์กร
- ✓ สามารถตรวจสอบและติดตามการใช้งานย้อนหลังได้
- ✓ รองรับการใช้งานร่วมกับอุปกรณ์เครือข่าย เช่น Router, Switch, Firewall, VPN และ Wireless Access Point
- ✓ ลดภาระการจัดการผู้ใช้จากอุปกรณ์ปลายทาง

5. ตัวอย่างโปรโตคอลที่ใช้ใน AAA

โปรโตคอล	หน้าที่
RADIUS	ใช้สำหรับ Authentication, Authorization และ Accounting ผ่านเครือข่าย
TACACS+	ใช้สำหรับควบคุมการเข้าถึงอุปกรณ์เครือข่าย (Cisco อุปกรณ์เป็นหลัก)
LDAP	ใช้สำหรับการจัดการและค้นหาข้อมูลผู้ใช้ในไดเรกทอรี
Kerberos	ใช้สำหรับการยืนยันตัวตนในระบบ Windows (Active Directory)

6. ขั้นตอนการติดตั้งและตั้งค่า AAA Server ด้วย RADIUS บน Windows Server 2019 (NPS)

1. ติดตั้ง Role NPS

ไปที่ Server Manager > Add Roles and Features > เลือก Network Policy and Access Services > Next > Install

2. เปิด NPS

เมื่อติดตั้งเสร็จแล้ว ไปที่ Tools > Network Policy Server (NPS)

3. เพิ่ม RADIUS Client

คลิก RADIUS Clients > คลิกขวา > New > ใส่ IP อุปกรณ์ที่ต้องการให้ตรวจสอบ (เช่น Router, AP) > ใส่ Shared Secret

4. สร้าง Network Policy

คลิก Network Policies > New > เลือก Network Access Protection (NAP) > Next

5. กำหนดเงื่อนไข

กำหนด Conditions เช่น NAS Identifier, User Groups และกำหนดการอนุญาต

6. ทดสอบการใช้งาน

ทดสอบการเชื่อมต่อจากอุปกรณ์ปลายทางและตรวจสอบผลลัพธ์ใน NPS/Event Viewer



ข้อควรจำ

- Shared Secret ต้องตั้งให้ตรงกันระหว่าง AAA Server และอุปกรณ์ที่ร้องขอ
- ควรใช้การเชื่อมต่อที่ปลอดภัย (เช่น ใช้ IPsec หรือ TLS) เพื่อป้องกันการดักจับข้อมูล
- ควรสำรองข้อมูลการตั้งค่าและฐานข้อมูลผู้ใช้อย่างสม่ำเสมอ



ประโยชน์ที่ได้รับ

- ระบบปลอดภัยและน่าเชื่อถือมากขึ้น
- ควบคุมสิทธิ์การเข้าถึงได้อย่างมีประสิทธิภาพ
- สามารถตรวจสอบและติดตามการใช้งานย้อนหลังได้



แหล่งอ้างอิง

- Microsoft Docs: Network Policy Server (NPS) in Windows Server 2019
- คู่มือการใช้งาน Windows Server 2019



ใบความรู้ที่ 5

6. งานตรวจสอบและทดสอบ มาตรการความปลอดภัย

รายวิชา : ระบบปฏิบัติการเครื่องแม่ข่าย
รหัสวิชา : 20204-2105
ระดับชั้น : ปวส.
สาขาวิชา : เทคโนโลยีสารสนเทศ
ระบบปฏิบัติการ : Windows Server 2019

1. ความหมาย

การตรวจสอบและทดสอบมาตรการความปลอดภัย คือ กระบวนการตรวจสอบความถูกต้องและความมีประสิทธิภาพของมาตรการรักษาความปลอดภัยที่ได้กำหนดและใช้งานอยู่ในระบบ เพื่อให้มั่นใจว่าสามารถป้องกันความเสี่ยงและภัยคุกคามได้อย่างเหมาะสม และสอดคล้องกับนโยบายและข้อกำหนดขององค์กร

3. สิ่งที่ต้องตรวจสอบ

- นโยบายและการตั้งค่าความปลอดภัย**
ตรวจสอบการตั้งค่าตามนโยบาย เช่น Password Policy, Account Lockout, Audit Policy, Firewall Policy
- สิทธิ์การเข้าถึงและการอนุญาต**
ตรวจสอบสิทธิ์กลุ่มผู้ใช้ สิทธิไฟล์เดสก์ท็อป และสิทธิ์บนระบบ
- ไฟร์วอลล์และการเชื่อมต่อเครือข่าย**
ตรวจสอบกฎไฟร์วอลล์ พอร์ตที่เปิดใช้งาน และการเข้าถึงจากภายนอก
- การอัปเดตและแพตช์ความปลอดภัย**
ตรวจสอบสถานะการอัปเดตระบบปฏิบัติการและโปรแกรมสำคัญ
- การบันทึกและตรวจสอบเหตุการณ์ (Logging)**
ตรวจสอบการตั้งค่าการบันทึกเหตุการณ์ (Event Log) และการเก็บรักษาข้อมูล
- การสำรองข้อมูลและการกู้คืน**
ตรวจสอบการสำรองข้อมูลและทดสอบการกู้คืนข้อมูล
- มัลแวร์และโปรแกรมไม่พึงประสงค์**
ตรวจสอบการทำงานของ Antivirus และสแกนหาไวรัส

6. ขั้นตอนการตรวจสอบและทดสอบมาตรการความปลอดภัย

1. กำหนดขอบเขตและวัตถุประสงค์ : ระบุระบบ เป้าหมาย และสิ่งที่ต้องการตรวจสอบ
2. รวบรวมข้อมูลและวิเคราะห์ระบบ : เก็บข้อมูลระบบ เครือข่าย ผู้ใช้ และการตั้งค่าปัจจุบัน
3. ดำเนินการตรวจสอบ/ทดสอบ : ใช้วิธีการและเครื่องมือที่เหมาะสมในการตรวจสอบ
4. วิเคราะห์ผลและประเมินความเสี่ยง : ประเมินความรุนแรงของช่องโหว่และผลกระทบ
5. จัดทำรายงานและข้อเสนอแนะ : สรุปผลการตรวจสอบ พร้อมแนวทางการแก้ไข
6. ปรับปรุงและติดตามผล : ดำเนินการแก้ไขและติดตามผลการปรับปรุงอย่างต่อเนื่อง

7. ตัวอย่างรายการตรวจสอบ (Checklist)

รายการตรวจสอบ	ตรวจสอบแล้ว (✓)	ไม่พบปัญหา	พบปัญหา	หมายเหตุ
1. ตั้งค่านโยบายรหัสผ่าน (Password Policy) ถูกต้อง	☐	☐	☐	
2. บัญชีผู้ใช้ที่ไม่ใช้แล้วถูกปิดหรือถอนสิทธิ์	☐	☐	☐	
3. เปิดใช้งาน Firewall และกำหนดกฎอย่างเหมาะสม	☐	☐	☐	
4. ระบบได้รับการอัปเดตและติดตั้งแพตช์ล่าสุด	☐	☐	☐	
5. มีการบันทึกเหตุการณ์ (Event Log) และเก็บรักษาอย่างเหมาะสม	☐	☐	☐	
6. ทดสอบการกู้คืนข้อมูลสำรองได้สำเร็จ	☐	☐	☐	
7. ไม่พบมัลแวร์หรือโปรแกรมที่ไม่พึงประสงค์	☐	☐	☐	
8. สิทธิ์การเข้าถึงทรัพยากรสอดคล้องกับหน้าที่ผู้ใช้	☐	☐	☐	

2. วัตถุประสงค์

- ✓ เพื่อยืนยันว่ามาตรการความปลอดภัยทำงานได้ตามที่กำหนด
- ✓ เพื่อค้นหาช่องโหว่และจุดอ่อนที่อาจถูกโจมตี
- ✓ เพื่อประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- ✓ เพื่อปรับปรุงและยกระดับมาตรการความปลอดภัยให้เหมาะสมยิ่งขึ้น
- ✓ เพื่อให้เป็นไปตามข้อกำหนดทางกฎหมายและมาตรฐานความปลอดภัย

4. วิธีการทดสอบ

วิธีการทดสอบ	รายละเอียด
การตรวจสอบการตั้งค่า (Configuration Review)	ตรวจสอบการตั้งค่าระบบตามแนวปฏิบัติที่ดี (Best Practice) และนโยบายขององค์กร
การทดสอบการเจาะระบบ (Penetration Test)	จำลองการโจมตีจากผู้ไม่หวังดี เพื่อค้นหาช่องโหว่ที่สามารถถูกใช้โจมตีระบบได้
การสแกนช่องโหว่ (Vulnerability Scan)	ใช้เครื่องมือสแกนเพื่อค้นหาจุดอ่อนของระบบบริการ และแอปพลิเคชัน
การทดสอบสิทธิ์การเข้าถึง (Access Control Test)	ทดสอบสิทธิ์ของผู้ใช้ เพื่อยืนยันว่ามีมาตรการควบคุมการเข้าถึงที่เหมาะสม
การทดสอบเครือข่าย (Network Security Test)	ทดสอบการเชื่อมต่อ พอร์ต และกฎไฟร์วอลล์ว่ามีความปลอดภัยเพียงใด
การทดสอบการสำรองข้อมูล (Backup/Recovery Test)	ทดสอบการกู้คืนข้อมูลจากสำเนาสำรอง เพื่อให้แน่ใจว่าสามารถกู้คืนได้เมื่อเกิดเหตุการณ์

5. เครื่องมือที่ใช้ในการตรวจสอบและทดสอบ

Windows Server Tools	Event Viewer, Local Security Policy, Group Policy Result
PowerShell	ใช้คำสั่งสำหรับตรวจสอบการตั้งค่าและสถานะระบบ
Windows Defender / Microsoft Defender	สแกนมัลแวร์ ตรวจสอบการป้องกันแบบเรียลไทม์
Microsoft Baseline Security Analyzer (MBSA)	ตรวจสอบการตั้งค่าความปลอดภัยและช่องโหว่ในระบบ
Nmap	สแกนพอร์ตและบริการบนเครือข่าย
Nessus / OpenVAS	สแกนช่องโหว่ขั้นสูงและให้คำแนะนำในการแก้ไข



ข้อควรจำ

- ตรวจสอบและทดสอบอย่างสม่ำเสมอ เพื่อให้ระบบปลอดภัยอยู่เสมอ
- บันทึกผลการตรวจสอบและเก็บหลักฐานประกอบ
- จัดลำดับความสำคัญของช่องโหว่ตามความรุนแรง
- ปรับปรุงมาตรการความปลอดภัยอย่างต่อเนื่อง



ประโยชน์ที่ได้รับ

- ลดความเสี่ยงจากการถูกโจมตี
- เพิ่มความเชื่อมั่นต่อระบบและบริการ
- สอดคล้องกับมาตรฐานและกฎหมาย
- ช่วยให้องค์กรดำเนินงานได้อย่างมั่นคงและปลอดภัย



แหล่งอ้างอิง

- Microsoft Docs: Security, Compliance, and Identity in Windows Server 2019
- NIST SP 800-53 Rev.5 Security and Privacy Controls
- CIS Benchmarks for Windows Server 2019

6. แบบฝึกหัด

แบบฝึกหัดหน่วยที่ 4

1. Vulnerability คือข้อใด

ก. ทรัพย์สิน

ข. จุดอ่อนที่ภัยคุกคามใช้ได้

ค. เจ้าของระบบ

ง. รายงาน

2. คะแนน Risk 3x3 เท่ากับเท่าใด

ก. 3

ข. 6

ค. 9

ง. 12

3. Residual Risk คือข้อใด

ก. ก่อนใช้ Control

ข. ความเสี่ยงที่เหลือหลังใช้ Control

ค. ไม่มีความเสี่ยง

ง. Asset

4. Defense in Depth หมายถึงอะไร

ก. ฝั่ง Firewall เดียว

ข. ใช้มาตรการหลายชั้น

ค. ปิด Log

ง. แฮร์รหัสผ่าน

5. Inbound Rule TCP 443 ใช้กับบริการใด

ก. DNS

ข. HTTPS

ค. DHCP

ง. RADIUS Accounting

6. เหตุใดต้องจำกัด Remote IP

ก. เพิ่ม RAM

ข. ลดแหล่งที่เชื่อมต่อได้

ค. ปิด TLS

ง. เพิ่ม Lease

7. ก่อนแก้ Firewall ควรทำอะไร

ก. Export Policy และมี Console คุ้มค่าน

ข. ปิดทุก Profile

ค. ลบ Rule เดิม

- ง. เปิด Any/Any
- 8. Self-Signed Certificate เหมาะกับอะไร
 - ก. ระบบจริงสาธารณะโดยไม่ตรวจ
 - ข. Lab/ทดสอบ
 - ค. DHCP
 - ง. NTFS
- 9. Name mismatch เกิดเมื่อใด
 - ก. URL ไม่ตรง Subject/SAN
 - ข. Port เปิด
 - ค. NPS Log เขียนได้
 - ง. Risk ต่ำ
- 10. HTTPS Binding ต้องมีอะไร
 - ก. Port 443 และ Certificate
 - ข. DHCP Scope
 - ค. Share Permission
 - ง. RADIUS Client
- 11. Authentication ตอบคำถามใด
 - ก. เป็นใคร
 - ข. ทำอะไรได้
 - ค. บันทึกอะไร
 - ง. เสียงเท่าใด
- 12. Authorization คือข้อใด
 - ก. ยืนยันตัวตน
 - ข. กำหนดสิ่งที่ได้รับอนุญาต
 - ค. บันทึก Session
 - ง. เข้ารหัส TLS
- 13. Accounting ทำหน้าที่ใด
 - ก. บันทึกการเชื่อมต่อ/ผล
 - ข. สร้าง Certificate
 - ค. เปิด Port 443
 - ง. ลบ Risk
- 14. RADIUS Client คือใคร
 - ก. NAS เช่น AP/VPN/Switch
 - ข. Browser ทุกเครื่องโดยตรง
 - ค. Certificate
 - ง. Firewall Profile

15. หากไม่มี NAS ควรรายงานอย่างไร

- ก. อ้างว่าผ่าน End-to-end
- ข. ระบุว่าตรวจ Configuration แต่ยังไม่ยืนยัน End-to-end
- ค. ปิด Log
- ง. ใช้ระบบจริง

ตอนที่ 2 คำถามอัตนัย (5 ข้อ)

1. จัดทำตัวอย่าง Risk Register 1 รายการสำหรับ IIS ที่เปิด HTTP ต่อเครือข่ายกว้าง

.....

.....

2. ออกแบบ Firewall Rule สำหรับ HTTPS ที่อนุญาตเฉพาะ 192.168.40.0/24 พร้อมแผนภูมิกำหนด

.....

.....

3. อธิบายความแตกต่างระหว่าง Encryption, Server Authentication และ Trust ของ Certificate

.....

.....

4. อธิบายลำดับ RADIUS จาก NAS ไป NPS และบทบาท Authentication/Authorization/Accounting

.....

.....

5. ออกแบบ Test matrix อย่างน้อย 6 กรณีสำหรับ Firewall, HTTPS และ AAA/NPS

.....

.....

7. เอกสารอ้างอิง

- 1. หนังสือ “ติดตั้งและบริหาร network ในองค์กร ด้วย windowserver 2019”
- 2. เว็บไซต์: classroom <https://learn.microsoft.com/>
- 3. YouTube
- 4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

8. ภาคผนวก

8.1 เฉลย แบบฝึกหัดบทเรียนที่ 4

1 ข, 2 ค, 3 ข, 4 ข, 5 ข, 6 ข, 7 ก, 8 ข, 9 ก, 10 ก, 11 ก, 12 ข, 13 ก, 14 ก, 15 ข

แนวคำตอบอันทัน

1. ระบุ Asset IIS, Threat การดักข้อมูล/แก้ไข, Vulnerability HTTP, Control HTTPS/Firewall, L/I/Score และ Residual Risk
2. Inbound TCP 443, Profile ตาม Lab, Remote 192.168.40.0/24, Export Policy, มี Console และ Test case Allow/Block
3. Encryption ป้องกันการอ่านระหว่างทาง; Certificate ยืนยัน Server; Trust คือ Client เชื่อถือ Issuer และชื่อ/เวลา Certificate ถูกต้อง
4. NAS ส่ง Access-Request; NPS ตรวจสอบ Authentication, Network Policy ทำ Authorization, Accounting บันทึกผล
5. ต้องมีกรณีควรผ่านและควรปฏิเสธของ 443, HTTPS name/trust และ NPS Allow/Deny พร้อม Expected/Actual/Evidence

	ใบงานที่ 1		หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย		สอนครั้งที่ 13
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการบริการโครงสร้างพื้นฐานเครือข่าย		ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
	ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถวิเคราะห์และประเมินความเสี่ยงด้านความปลอดภัยของระบบเครื่องแม่ข่ายและบริการได้ ระบุภัยคุกคามและช่องโหว่ของระบบเครื่องแม่ข่ายได้อย่างถูกต้อง เสนอแนวทางป้องกันและลดความเสี่ยงของระบบได้อย่างเหมาะสม

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. ประมวลความรู้เกี่ยวกับหลักการรักษาความปลอดภัยของระบบเครื่องแม่ข่ายและบริการ
2. ประเมินความเสี่ยงและวิเคราะห์ภัยคุกคามที่อาจส่งผลกระทบต่อระบบเครื่องแม่ข่าย
3. เสนอแนวทางป้องกันและลดความเสี่ยงตามหลักการรักษาความปลอดภัยสารสนเทศ
4. จัดทำรายงานผลการประเมินความปลอดภัยของระบบได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายความหมายของความเสี่ยง ภัยคุกคาม และช่องโหว่ได้
2. จำแนกประเภทของภัยคุกคามต่อระบบเครื่องแม่ข่ายได้
3. วิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามได้

4.2 ทักษะพิสัย

1. ประเมินความเสี่ยงของระบบเครื่องแม่ข่ายตามสถานการณ์ที่กำหนดได้
2. จัดทำตารางวิเคราะห์ความเสี่ยงได้ถูกต้อง
3. จัดทำรายงานผลการประเมินความเสี่ยงได้

4.3 จิตพิสัย

1. มีความรับผิดชอบในการปฏิบัติงาน
2. มีความละเอียดรอบคอบในการวิเคราะห์ข้อมูล
3. ตระหนักถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศ

4.4 ประยุกต์ใช้และรับผิดชอบ

ประยุกต์ใช้ความรู้ด้านการรักษาความปลอดภัยในการวิเคราะห์ความเสี่ยงของระบบจริงได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์แม่ข่าย (Server)
2. เครื่องคอมพิวเตอร์ลูกข่าย (Client)
3. ระบบปฏิบัติการ Windows Server 2019
4. โปรแกรม VMware Workstation หรือ VirtualBox
5. ระบบเครือข่าย LAN
6. ใบความรู้และเอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1. ศึกษากรณีตัวอย่างให้ครบถ้วนก่อนวิเคราะห์
2. ตรวจสอบข้อมูลก่อนบันทึกผลการประเมิน
3. ใช้หลักการประเมินความเสี่ยงอย่างเป็นระบบ
4. ไม่แก้ไขค่าการตั้งค่าของเครื่องแม่ข่ายจริงโดยไม่ได้รับอนุญาต
5. บันทึกข้อมูลและจัดเก็บเอกสารอย่างเป็นระเบียบ

7. ขั้นตอนการปฏิบัติงาน

1. ศึกษากรณีตัวอย่างที่ได้รับมอบหมาย
2. ระบุนิยามสิ่งที่ต้องการปกป้อง
3. ระบุนักคุกคามที่อาจเกิดขึ้น
4. ระบุนโยบายของระบบ
5. ประเมินระดับความเสี่ยง
6. เสนอแนวทางป้องกันและลดความเสี่ยง
7. จัดทำรายงานสรุปผล
8. ส่งผลงานและนำเสนอผลการวิเคราะห์

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

ตารางประเมินผลการปฏิบัติงาน (Rubric Assessment)					
เกณฑ์การประเมิน	4 ดีเยี่ยม	3 ดี	2 พอใช้	1 ต้องปรับปรุง	คะแนน
การวิเคราะห์ทรัพยากร และภัยคุกคาม	ถูกต้องครบถ้วน	ถูกต้องเกือบทั้งหมด	ถูกต้องบางส่วน	ไม่ถูกต้อง	
การระบุช่องโหว่	ครบถ้วนและชัดเจน	ค่อนข้างครบถ้วน	ยังไม่ครบถ้วน	ไม่สามารถระบุได้	
การประเมินความเสี่ยง	ถูกต้องตามหลักการ	ผิดพลาดเล็กน้อย	ผิดพลาดหลายจุด	ไม่ถูกต้อง	
แนวทางป้องกันความเสี่ยง	เหมาะสมและเป็นไปได้	เหมาะสมส่วนใหญ่	เหมาะสมบางส่วน	ไม่เหมาะสม	
ความสมบูรณ์ของรายงาน	สมบูรณ์ เป็นระเบียบ	ค่อนข้างสมบูรณ์	ขาดรายละเอียดบางส่วน	ไม่สมบูรณ์	
ความรับผิดชอบและการตรงต่อเวลา	ดีเยี่ยม	ดี	พอใช้	ต้องปรับปรุง	

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows 10”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 2		หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย		สอนครั้งที่ 13
	ชื่อหน่วยการเรียนรู้	งานรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
	ชื่อเรื่อง/งานรักษาความปลอดภัยระบบเครื่องแม่ข่ายและบริการ		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถกำหนดค่า Firewall เพื่อป้องกันการเข้าถึงระบบเครื่องแม่ข่ายจากผู้ที่ไม่ได้รับอนุญาตได้
สร้างกฎ (Firewall Rules) สำหรับควบคุมการรับส่งข้อมูลผ่านเครือข่ายได้ทดสอบและตรวจสอบผลการ
ทำงานของ Firewall จัดทำรายงานผลการกำหนดค่าและทดสอบระบบ Firewall ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. แสดงความรู้เกี่ยวกับหลักการทำงานของ Firewall
2. กำหนดค่า Firewall เพื่อควบคุมการรับส่งข้อมูลผ่านเครือข่ายได้
3. ตรวจสอบและแก้ไขปัญหาการทำงานของ Firewall ได้
4. จัดทำเอกสารสรุปผลการกำหนดค่า Firewall ได้อย่างถูกต้อง

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายหลักการทำงานของ Firewall ได้
2. จำแนกประเภทของ Firewall ได้
3. อธิบายความสำคัญของการควบคุมการเข้าถึงระบบเครือข่ายได้

4.2 ทักษะพิสัย (Psychomotor Domain)

1. เปิดใช้งาน Firewall บนเครื่องแม่ข่ายได้
2. สร้างกฎการอนุญาต (Allow Rule) และปฏิเสธ (Block Rule) ได้
3. ทดสอบการเข้าถึงบริการหลังการกำหนดค่า Firewall ได้
4. บันทึกผลการปฏิบัติงานได้ถูกต้อง

4.3 จิตพิสัย (Affective Domain)

1. มีความรับผิดชอบในการปฏิบัติงานมีความละเอียดรอบคอบในการกำหนดค่าระบบ

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ (Application)

1. ประยุกต์ใช้ Firewall เพื่อป้องกันระบบเครื่องแม่ข่ายตามสถานการณ์จริงได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์แม่ข่าย (Server)
2. เครื่องคอมพิวเตอร์ลูกข่าย (Client)
3. ระบบปฏิบัติการ Windows Server 2019
4. โปรแกรม VMware Workstation หรือ VirtualBox
5. ระบบเครือข่าย LAN
6. ใบความรู้และเอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1. ตรวจสอบหมายเลข Port ก่อนสร้างกฎทุกครั้ง
2. หลีกเลี่ยงการบล็อกบริการที่จำเป็นต่อการบริหารจัดการระบบ
3. สำรองค่าการตั้งค่าก่อนปรับแต่งระบบ
4. ทดสอบผลการทำงานทุกครั้งหลังสร้างกฎใหม่
5. บันทึกขั้นตอนการดำเนินงานอย่างละเอียด

7. ขั้นตอนการปฏิบัติงาน

1. เปิด Windows Defender Firewall
2. ตรวจสอบ Firewall Rules ที่มีอยู่
3. สร้าง Allow Rule สำหรับ Web Server
4. สร้าง Block Rule สำหรับบริการที่ไม่จำเป็น
5. ทดสอบการเชื่อมต่อจากเครื่อง Client
6. บันทึกผลการทดสอบ
7. วิเคราะห์ผลการทำงานของ Firewall
8. จัดทำรายงานสรุปผล

ตัวอย่างตารางผลการดำเนินงาน

ลำดับ	รายการ	วิธีตรวจสอบ	ผลการดำเนินงาน	หมายเหตุ
1	เปิดใช้งาน Firewall	Windows Defender Firewall หรือ wf.msc		
2	สร้าง Allow Rule	Inbound/Outbound Rules		
3	สร้าง Block Rule	Inbound/Outbound Rules		
4	ผลการทดสอบจาก Client	ping, Remote Desktop, Web Browser หรือบริการที่ กำหนด		
5	ปัญหาที่พบ	บันทึกปัญหาระหว่างการ ทดสอบ		
6	วิธีแก้ไข	บันทึกแนวทางการแก้ไข		

8. สรุปและวิจารณ์ผล

- สรุปสิ่งที่ได้เรียนรู้
- ปัญหาหรืออุปสรรคที่พบ
- วิธีแก้ไขและการพัฒนาตนเอง
- ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9. การประเมินผล

เกณฑ์การประเมิน	4 ดีเยี่ยม	3 ดี	2 พอใช้	1 ต้องปรับปรุง	คะแนน
การเปิดใช้งาน Firewall	ถูกต้องครบถ้วน	ถูกต้องเกือบทั้งหมด	ผิดพลาดเล็กน้อย	ไม่สามารถปฏิบัติได้	
การสร้าง Firewall Rule	ถูกต้องครบถ้วน	ถูกต้องส่วนใหญ่	ผิดพลาดบางส่วน	ไม่ถูกต้อง	
การทดสอบระบบ	ทดสอบครบทุกขั้นตอน	ทดสอบเกือบครบ	ทดสอบบางส่วน	ไม่ทดสอบ	
การวิเคราะห์ผล	วิเคราะห์ได้ถูกต้อง	วิเคราะห์ได้ดี	วิเคราะห์ได้บางส่วน	ไม่สามารถวิเคราะห์ได้	

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows 10”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 3	หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชาการระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 14
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น		

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถติดตั้ง SSL Certificate บน Web Server ได้ถูกต้อง ทดสอบการเชื่อมต่อผ่าน HTTPS ได้ ตรวจสอบสถานะและความถูกต้องของ Certificate จัดทำรายงานผลการปฏิบัติงานได้ครบถ้วน

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. แสดงความรู้เกี่ยวกับหลักการทำงานของ SSL/TLS และการเข้ารหัสข้อมูล
2. สร้างและติดตั้ง SSL Certificate บนเครื่องแม่ข่ายได้
3. ทดสอบและตรวจสอบความปลอดภัยของการเชื่อมต่อผ่าน HTTPS ได้
4. จัดทำเอกสารสรุปผลการติดตั้งและทดสอบระบบได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายความสำคัญของ SSL/TLS ได้
2. อธิบายหน้าที่ของ SSL Certificate ได้
3. อธิบายความแตกต่างระหว่าง HTTP และ HTTPS ได้
4. อธิบายกระบวนการเข้ารหัสข้อมูลเบื้องต้นได้

4.2 ทักษะพิสัย

1. สร้าง SSL Certificate ได้
2. ติดตั้ง Certificate บน Web Server ได้
3. กำหนดค่าเว็บไซต์ให้รองรับ HTTPS ได้
4. ทดสอบการทำงานของ SSL Certificate ได้
5. ตรวจสอบรายละเอียดของ Certificate ได้

4.3 จิตพิสัย

1. มีความรับผิดชอบในการปฏิบัติงาน
2. มีความละเอียดรอบคอบในการกำหนดสิทธิ์การเข้าถึงข้อมูล
3. ตระหนักถึงความสำคัญของความปลอดภัยของข้อมูลในระบบเครือข่าย

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1. ประยุกต์ใช้ SSL Certificate เพื่อเพิ่มความปลอดภัยให้กับบริการบนเครื่องแม่ข่ายได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1. เครื่องคอมพิวเตอร์แม่ข่าย (Server)
2. เครื่องคอมพิวเตอร์ลูกข่าย (Client)
3. ระบบปฏิบัติการ Windows Server 2019
4. โปรแกรม VMware Workstation หรือ VirtualBox
5. ระบบเครือข่าย LAN
6. ใบความรู้และเอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1. ตรวจสอบชื่อโดเมนหรือชื่อเครื่องแม่ข่ายให้ถูกต้องก่อนสร้าง Certificate
2. เก็บรักษา Private Key อย่างปลอดภัย
3. ตรวจสอบวันหมดอายุของ Certificate
4. ทดสอบการเชื่อมต่อ HTTPS ทุกครั้งหลังติดตั้ง
5. บันทึกขั้นตอนการดำเนินงานอย่างละเอียด
6. หลีกเลี่ยงการแก้ไขค่าระบบโดยไม่มีการสำรองข้อมูล

7. ขั้นตอนการปฏิบัติงาน

1. ศึกษาหลักการทำงานของ SSL/TLS
2. เปิดโปรแกรม IIS Manager
3. สร้าง Self-Signed Certificate
4. ผูก Certificate กับเว็บไซต์ (Binding HTTPS)
5. กำหนดค่า Port 443
6. ทดสอบการเชื่อมต่อ HTTPS
7. ตรวจสอบรายละเอียด Certificate
8. บันทึกผลการทดสอบ
9. จัดทำรายงานสรุปผล

ตัวอย่างแบบบันทึกผลการปฏิบัติงาน

ลำดับ	รายการตรวจสอบ	วิธีตรวจสอบ	ผลการดำเนินงาน	หมายเหตุ
1	สร้าง SSL Certificate สำเร็จ	IIS Manager → Server Certificates		
2	ติดตั้ง Certificate สำเร็จ	certlm.msc หรือ IIS Manager		
3	กำหนดค่า HTTPS สำเร็จ	IIS Manager → Site → Bindings → HTTPS		
4	ทดสอบการเชื่อมต่อ HTTPS	Web Browser เข้า https://ชื่อเครื่อง หรือ https://IP Address		
5	ตรวจสอบรายละเอียด Certificate	คลิกไอคอนรูปแม่กุญแจ → Certificate หรือ certlm.msc		
6	ปัญหาที่พบ	บันทึกปัญหาที่เกิดขึ้น		
7	วิธีแก้ไข	บันทึกแนวทางการแก้ไข		

ตัวอย่างตารางระบุผลการทดสอบ

ลำดับ	รายการทดสอบ	วิธีทดสอบ	ผลการทดสอบ	หมายเหตุ
1	เปิดเว็บไซต์ผ่าน HTTP	เปิดเว็บเบราว์เซอร์ และเข้า http://ชื่อ เครื่อง หรือ http://IP Address		
2	เปิดเว็บไซต์ผ่าน HTTPS	เปิดเว็บเบราว์เซอร์ และเข้า https://ชื่อ เครื่อง หรือ https://IP Address		
3	ตรวจสอบสัญลักษณ์ ความปลอดภัยบน Browser	ตรวจสอบการแสดง รูปแม่กุญแจที่แถบที่ อยู่ (Address Bar)		
4	ตรวจสอบข้อมูล Certificate	คลิกสัญลักษณ์แม่ กุญแจ → ดู รายละเอียด Certificate		

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9.การประเมินผล

เกณฑ์การประเมิน	5 ดีเยี่ยม	3 ดี	2 พอใช้	1 ต้องปรับปรุง	คะแนน
ความเข้าใจหลักการ SSL/TLS	อธิบายได้ครบถ้วน	อธิบายได้ดี	อธิบายได้บางส่วน	อธิบายไม่ได้	
การสร้าง SSL Certificate	ถูกต้องครบถ้วน	ถูกต้องเกือบทั้งหมด	ผิดพลาดเล็กน้อย	ไม่สามารถดำเนินการได้	
การติดตั้งและกำหนดค่า HTTPS	ถูกต้องครบถ้วน	ถูกต้องส่วนใหญ่	ผิดพลาดบางส่วน	ไม่ถูกต้อง	
การทดสอบระบบ	ทดสอบครบทุกขั้นตอน	ทดสอบเกือบครบ	ทดสอบบางส่วน	ไม่ทดสอบ	

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

	ใบงานที่ 4	หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชาระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 15
	ชื่อหน่วยการเรียนรู้ งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	ทฤษฎี 1 ชม. ปฏิบัติ 4 ชม.
	ชื่อเรื่อง/งานบริหารจัดการระบบปฏิบัติการเครื่องแม่ข่ายเบื้องต้น	

1. ผลลัพธ์การเรียนรู้จากการปฏิบัติงาน

สามารถกำหนดค่า AAA Server สำหรับการตรวจสอบยืนยันตัวตนผู้ใช้งานได้ กำหนดสิทธิ์การเข้าถึงทรัพยากรของผู้ใช้งานได้อย่างเหมาะสม บันทึกและตรวจสอบข้อมูลการใช้งานของผู้ใช้ได้ทดสอบการทำงานของระบบ Authentication, Authorization และ Accounting จัดทำรายงานผลการกำหนดค่าและทดสอบระบบ AAA Server ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

1. มาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ รหัส 40106 อาชีพ ช่างสนับสนุนด้านเทคนิค ระดับ 5

3. สมรรถนะการปฏิบัติงาน

1. แสดงความรู้เกี่ยวกับหลักการทำงานของ AAA Server
2. กำหนดค่า Authentication, Authorization และ Accounting ได้
3. จัดการบัญชีผู้ใช้และสิทธิ์การใช้งานระบบได้
4. ตรวจสอบและวิเคราะห์ข้อมูลการใช้งานจาก Log ได้
5. จัดทำเอกสารสรุปผลการดำเนินงานได้อย่างถูกต้อง

4. จุดประสงค์เชิงพฤติกรรม

4.1 พุทธิพิสัย

1. อธิบายความหมายของ AAA ได้
2. อธิบายหลักการ Authentication, Authorization และ Accounting ได้
3. อธิบายความสำคัญของการจัดการบัญชีผู้ใช้และสิทธิ์การเข้าถึงได้
4. วิเคราะห์ความเสี่ยงจากการกำหนดสิทธิ์ผู้ใช้งานที่ไม่เหมาะสมได้

4.2 ทักษะพิสัย

1. สร้างบัญชีผู้ใช้งานบนเครื่องแม่ข่ายได้
2. กำหนดสิทธิ์การเข้าถึงทรัพยากรได้
3. กำหนดนโยบายการเข้าสู่ระบบได้
4. ตรวจสอบข้อมูลการใช้งานจากระบบ Log ได้
5. ทดสอบการทำงานของระบบ AAA ได้

4.3 จิตพิสัย

1. มีความรับผิดชอบต่อการปฏิบัติงาน

2.มีความละเอียดรอบคอบในการตรวจสอบระบบ

3.มีเจตคติที่ดีต่อการแก้ไขปัญหาอย่างเป็นระบบ

4.4 ความสามารถประยุกต์ใช้และรับผิดชอบ

1.ประยุกต์ใช้ระบบ AAA เพื่อควบคุมการเข้าถึงทรัพยากรขององค์กรได้

5. เครื่องมือ วัสดุ และอุปกรณ์

1.เครื่องคอมพิวเตอร์แม่ข่าย

2.เครื่องคอมพิวเตอร์ลูกข่าย

3.ระบบปฏิบัติการ Windows Server 2019

4.Active Directory Domain Services (AD DS)

5.Event Viewer

6.ระบบเครือข่าย LAN

7.เอกสารประกอบการเรียน

6. คำแนะนำ/ข้อควรระวัง

1.กำหนดรหัสผ่านให้มีความซับซ้อนตามนโยบายความปลอดภัย

2.กำหนดสิทธิ์ตามหลัก Least Privilege (ให้สิทธิ์เท่าที่จำเป็น)

3.ตรวจสอบบัญชีผู้ใช้งานก่อนบันทึกข้อมูล

4.หลีกเลี่ยงการมอบสิทธิ์ Administrator โดยไม่จำเป็น

5.สำรองข้อมูลก่อนปรับแต่งระบบ

6.บันทึกผลการปฏิบัติงานทุกขั้นตอน

7. ขั้นตอนการปฏิบัติงาน

1.เปิด Server Manager

2.สร้างบัญชีผู้ใช้งานใน Active Directory

3.สร้างกลุ่มผู้ใช้งาน

4.เพิ่มสมาชิกเข้ากลุ่ม

5.กำหนดสิทธิ์การเข้าถึงทรัพยากร

6.กำหนด Password Policy

7.ทดสอบการ Login ของผู้ใช้งาน

8.ตรวจสอบ Log การเข้าใช้งาน

9.บันทึกผลการทดสอบ

10.จัดทำรายงานสรุปผล

แบบบันทึกผลการปฏิบัติงาน		
ข้อมูลบัญชีผู้ใช้งาน		
ชื่อผู้ใช้	กลุ่มผู้ใช้	สิทธิ์ที่ได้รับ

ผลการทดสอบ Authentication			
ชื่อผู้ใช้	Login สำเร็จ	Login ไม่สำเร็จ	หมายเหตุ

ผลการทดสอบ Authorization			
รายการทรัพยากร	เข้าถึงได้	เข้าถึงไม่ได้	หมายเหตุ

ผลการตรวจสอบ Accounting	
รายการตรวจสอบ	ผลการตรวจสอบ
พบข้อมูลการ Login	
พบข้อมูลการ Logout	
พบข้อมูลการเข้าถึงทรัพยากร	
ปัญหาที่พบ	
วิธีแก้ไข	

8. สรุปและวิจารณ์ผล

1. สรุปสิ่งที่ได้เรียนรู้
2. ปัญหาหรืออุปสรรคที่พบ
3. วิธีแก้ไขและการพัฒนาตนเอง
4. ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

9.การประเมินผล

ตารางประเมินผลการปฏิบัติงาน (Rubric Assessment)					
เกณฑ์การประเมิน	4 ดีเยี่ยม	3 ดี	2 พอใช้	1 ต้องปรับปรุง	คะแนน
ความเข้าใจหลักการ AAA	อธิบายได้ครบถ้วน	อธิบายได้ดี	อธิบายได้บางส่วน	อธิบายไม่ได้	
การสร้างบัญชีผู้ใช้งาน	ถูกต้องครบถ้วน	ถูกต้องส่วนใหญ่	ผิดพลาดบางส่วน	ไม่ถูกต้อง	
การกำหนดสิทธิ์ผู้ใช้งาน	เหมาะสมและถูกต้อง	ถูกต้องเกือบทั้งหมด	มีข้อผิดพลาดบางส่วน	ไม่ถูกต้อง	
การกำหนด Password Policy	ถูกต้องครบถ้วน	ถูกต้องส่วนใหญ่	ผิดพลาดเล็กน้อย	ไม่สามารถดำเนินการได้	
การทดสอบและตรวจสอบ Log	ครบทุกขั้นตอน	เกือบครบถ้วน	บางส่วน	ไม่ดำเนินการ	

10. เอกสารอ้างอิง /เอกสารค้นคว้าเพิ่มเติม

1. หนังสือ “windows server 2019”
2. เว็บไซต์: classroom <https://learn.microsoft.com/>
3. YouTube
4. เอกสารประกอบการสอน / PowerPoint ครูผู้สอน

