Power Systems

การติดตั้งและตั้งค่าคอนโซลการจัดการฮาร์ดแวร์

ข้อมูลบันทึก

ก่อนการใช้ข้อมูลนี้และผลิตภัณฑ์ที่ข้อมูลนี้ สนับสนุน โปรดอ่านข้อมูลใน “ประกาศด้านความปลอดภัย” ในหน้า v, “หมายเหตุ” ในหน้า 89, คู่มือ *IBM Systems Safety Notices*, G229-9054 และ *IBM Environmental Notices and User Guide*, Z125–5823

เอดิชันนี้ใช้กับ IBM® Hardware Management Console เวอร์ชัน 9 รีลีส 2 ระดับการซ่อมบำรุง 950 และรีลีสและโมดิฟิเคชัน ถัดมาทั้งหมด จนกว่าจะระบุไว้เป็นอย่างอื่นในเอดิชันใหม่

สารบัญ

ประกาศด้านความปลอดภัย

ประกาศด้านความปลอดภัยอาจพิมพ์อยู่ในคำแนะนำนี้โดยตลอด:

- ประกาศ **อันตราย** เป็นการแจ้งถึงสถานการณ์ที่อาจเกิดอันตรายร้ายแรงถึงชีวิตหรืออันตรายร้ายแรงต่อผู้คน
- ประกาศ **ข้อควรระวัง** เป็นการแจ้งถึงสถานการณ์ที่อาจเกิดอันตรายกับคน เนื่องจากสภาวะที่เป็นอยู่บางอย่าง
- ประกาศ **ข้อควรพิจารณา** เป็นการแจ้งถึงความเป็นไปได้ของความเสียหายที่เกิดกับโปรแกรม อุปกรณ์ ระบบ หรือข้อมูล

ข้อมูลด้านความปลอดภัยเกี่ยวกับการค้าระดับโลก

หลายประเทศต้องการข้อมูลด้านความปลอดภัยที่มีอยู่ในเอกสารผลิตภัณฑ์ในภาษาประจำชาติของตนเอง หากประเทศของคุณมีความต้องการตามนี้ หนังสือข้อมูลด้านความปลอดภัยจะถูกบรรจุอยู่ในหีบห่อเอกสารที่จัดส่งพร้อมกับผลิตภัณฑ์ (เช่น ในหนังสือข้อมูลที่ตีพิมพ์ ใน DVD หรือเป็นส่วนหนึ่งของผลิตภัณฑ์) หนังสือนี้จะประกอบด้วยข้อมูลด้านความปลอดภัยในภาษาประจำชาติของคุณพร้อมกับการอ้างอิงกับต้นฉบับภาษาอังกฤษ ก่อนใช้เอกสารภาษาอังกฤษในการติดตั้ง ปฏิบัติงาน หรือให้บริการผลิตภัณฑ์นี้ คุณต้องทำความคุ้นเคยกับข้อมูลด้านความปลอดภัยที่เกี่ยวข้องที่มีอยู่ในหนังสือ คุณควรอ้างอิงถึงหนังสือนี้ทุกครั้งที่คุณไม่เข้าใจข้อมูลด้านความปลอดภัยที่มีอยู่ในเอกสารภาษาอังกฤษอย่างชัดเจน

ขอรับเอกสารแทนที่หรือเอกสารชุดใหม่ได้โดยการโทรศัพท์ไปที่ IBM Hotline เบอร์ 1-800-300-8751

ข้อมูลด้านความปลอดภัยในภาษาเยอรมัน

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

ข้อมูลด้านความปลอดภัยเกี่ยวกับเลเซอร์

IBM เซิร์ฟเวอร์สามารถใช้การ์ด I/O หรือคุณลักษณะที่อิงกับเส้นใยนำแสงและใช้เลเซอร์หรือหลอดไฟ LED

ความสอดคล้องเกี่ยวกับเลเซอร์

เซิร์ฟเวอร์ IBM สามารถติดตั้งได้ทั้งภายในและภายนอกของชั้นวางอุปกรณ์ IT

อันตราย: เมื่อทำงานเกี่ยวกับระบบหรือแวดล้อมไปด้วยระบบ ให้สังเกตข้อควรระวังต่อไปนี้:

กำลังไฟและกระแสไฟที่มาจากสายไฟ, สายโทรศัพท์, และสายสื่อสาร เป็นอันตราย เพื่อหลีกเลี่ยงอันตรายจากไฟช็อต: หาก IBM จัดเตรียมสายไฟไว้ให้ ให้เชื่อมต่อไฟเข้ากับยูนิตนี้ด้วยสายไฟที่ IBM จัดให้ ห้ามใช้สายไฟของ IBM สำหรับผลิตภัณฑ์อื่นใด ห้ามเปิดหรือให้บริการตัวจ่ายไฟ ห้ามเชื่อมต่อ หรือปลดการเชื่อมต่อสายเคเบิลใด ๆ หรือทำการติดตั้ง, บำรุงรักษา, หรือตั้งค่าคอนฟิกูเรชันผลิตภัณฑ์นี้ใหม่ในระหว่างที่มีพายุฟ้าคะนอง

-  ผลิตภัณฑ์อาจมีสายไฟหลายเส้น เมื่อต้องการขจัดแรงดันไฟฟ้าที่เป็นอันตรายทั้งหมด ให้ถอดสายไฟทั้งหมดออก สำหรับไฟกระแสสลับ ถอดสายไฟทั้งหมดออกจากแหล่งจ่ายไฟกระแสสลับ สำหรับชั้นวางที่มี DC power distribution panel (PDP) ให้ถอดแหล่งจ่ายไฟกระแสตรงของลูกค้า เป็น PDP
- เมื่อเชื่อมต่อไฟฟ้ากับผลิตภัณฑ์ ตรวจสอบให้แน่ใจว่าสายไฟทั้งหมดเชื่อมต่อเหมาะสม สำหรับชั้นวางที่มีไฟกระแสสลับ เชื่อมต่อสายไฟทั้งหมดกับเต้ารับที่ต่อสายไฟและสายดิน อย่างเหมาะสม ตรวจสอบให้แน่ใจว่าเต้ารับไฟฟ้าจ่ายไฟที่มีกำลังเหมาะสมและมีการหมุนเฟสตรงตามค่ากำหนดบนแผ่นโลหะของระบบ สำหรับชั้นวางที่มี DC power distribution panel (PDP) ให้เชื่อมต่อแหล่งจ่ายไฟกระแสตรงของลูกค้า เป็น PDP ตรวจสอบให้แน่ใจว่าใช้ขั้วเหมาะสมเมื่อต่อเชื่อมต่อสายไฟกระแสตรงและส่งกลับ ไฟกระแสตรง
- เชื่อมต่ออุปกรณ์ใด ๆ ที่จะพ่วงต่อกับผลิตภัณฑ์นี้กับเต้ารับไฟฟ้าที่เดินสายไฟอย่างเหมาะสม
- หากเป็นไปได้ ควรใช้มือเพียงข้างเดียวในการเชื่อมต่อ หรือปลดการเชื่อมต่อสายเคเบิลสัญญาณ
- ห้ามเปิดอุปกรณ์ใด ๆ เมื่อพบว่ามีไฟ, น้ำ, หรือโครงสร้างได้รับความเสียหาย
- อย่าพยายามเปิดเครื่อง จนกว่าแก้ไขสภาพที่ไม่ปลอดภัย ทั้งหมดแล้ว
- เมื่อทำการตรวจสอบเครื่อง: ให้ถือว่ามีอันตรายด้านความปลอดภัยทางไฟฟ้า ทำการตรวจสอบความต่อเนื่อง การต่อสายดิน และกำลังไฟทั้งหมดที่ระบุระหว่างโพรซีเดอร์ การติดตั้งระบบย่อย เพื่อให้แน่ใจว่าเครื่องตรงกับข้อกำหนดด้าน

ความปลอดภัย อย่าพยายามเปิดเครื่อง จนกว่าสภาพที่ไม่ปลอดภัยที่เป็นไปได้ทั้งหมดได้รับการแก้ไขแล้ว ก่อนคุณเปิดฝาอุปกรณ์ ยกเว้นว่ามีการแนะนำเป็นอย่างอื่นในโพรซีเดอร์ การติดตั้งและการกำหนดคอนฟิก: ให้ถอดสายไฟกระแสตรงที่เสียบอยู่ ปิดตัวตัดวงจร ที่มีอยู่ใน rack power distribution panel (PDP) และถอดระบบ สื่อสารทางไกล เครือข่าย และโมเด็มที่มี

- เชื่อมต่อและปลดการเชื่อมต่อสายเคเบิลตามที่ได้อธิบายไว้ในขั้นตอนต่อไปนี้ เมื่อติดตั้ง, เคลื่อนย้าย, หรือเปิดฝาครอบผลิตภัณฑ์หรืออุปกรณ์ที่ต่อพ่วง

  เมื่อต้องการตัดการเชื่อมต่อ: 1) ให้ปิดอุปกรณ์ทุกอย่าง (เว้นแต่มีคำแนะนำไว้เป็นอย่างอื่น) 2) สำหรับไฟกระแสสลับ ให้ถอดสายไฟออกจากเต้ารับ 3) สำหรับ ชั้นวางที่มี DC power distribution panel (PDP) ให้ปิดตัวตัดวงจรที่อยู่ใน PDP และถอดสายไฟออกจากแหล่งจ่ายไฟกระแสตรงของลูกค้า 4) ถอดสายสัญญาณออกจาก ตัวเชื่อมต่อ 5) ถอดสายเคเบิลทั้งหมดออกจากอุปกรณ์

  เมื่อต้องการเชื่อมต่อ: 1) ให้ปิดอุปกรณ์ทุกอย่าง (เว้นแต่ มีคำแนะนำไว้เป็นอย่างอื่น) 2) เสียบสายเคเบิลทั้งหมดเข้ากับอุปกรณ์ 3) เสียบสายสัญญาณเข้ากับ ตัวเชื่อมต่อ 4) สำหรับไฟกระแสสลับ เสียบสายไฟเข้ากับเต้ารับ 5) สำหรับชั้นวางที่มี DC power distribution panel (PDP), ให้เชื่อมต่อกับแหล่งจ่ายไฟกระแสตรงของลูกค้า และเปิด ตัวตัดวงจรที่อยู่ใน PDP 6) เปิดอุปกรณ์

-  อาจมีขอบ มุม และข้อต่อที่แหลมคมอยู่ภายในและโดยรอบระบบ ใช้ความระมัดระวังเมื่อจัดการกับเครื่องมือเพื่อหลีกเลี่ยงการบาด การถลอก และการหนีบ (D005)

(R001 ส่วน 1 จากทั้งหมด 2):

อันตราย: ขณะที่ทำงานอยู่กับชั้นวางระบบ IT หรือในบริเวณที่มีชั้นวางระบบ IT ของคุณ ให้สังเกตข้อควรระวังต่อไปนี้:

- อุปกรณ์หนัก–อาจทำให้เกิดการบาดเจ็บของบุคคลหรือความเสียหายของอุปกรณ์ได้ถ้ายกไม่ระวัง
- ลดการวางระดับเสริมบนตู้ชั้นวางให้อยู่ต่ำเสมอ
- ติดตั้งโครงยึดสเตบิไลเซอร์บนตู้อุปกรณ์ชั้นวางเสมอ ยกเว้นว่ามีการติดตั้ง อุปกรณ์ป้องกันแผ่นดินไหว
- ติดตั้งอุปกรณ์ที่มีน้ำหนักมากที่สุดไว้ที่ด้านล่างสุดของตู้ชั้นวาง เพื่อหลีกเลี่ยง สภาวะการจัดวางเครื่องจักรที่ไม่สม่ำเสมอ ควรติดตั้งเซิร์ฟเวอร์และอุปกรณ์เสริมโดยเริ่มจาก ด้านล่างสุดของตู้ชั้นวางเสมอ
- ไม่ควรใช้อุปกรณ์ที่ประกอบเข้ากับชั้นวางเป็นชั้นวางหรือเป็นพื้นที่ใช้งาน ห้ามวางอ็อบเจ็กต์ต่าง ๆ ที่ด้านบนของอุปกรณ์ที่ประกอบเข้ากับชั้นวาง นอกจากนั้น อย่าพิงอุปกรณ์ที่ติดตั้งบนแร็ค และอย่าใช้ อุปกรณ์นั้นเพื่อให้ตำแหน่งร่างกายของคุณมีความเสถียร (ตัวอย่างเช่น เมื่อทำงานบนบันได)

- อันตรายเกี่ยวกับความเสถียร:
  - ชั้นวางอาจพลิกคว่ำทำให้ได้รับบาดเจ็บสาหัสได้
  - ก่อนที่จะยึดชั้นวางไปยังตำแหน่งการติดตั้ง โปรดอ่านคำแนะนำในการติดตั้ง
  - อย่าวางโหลดใดๆ บนอุปกรณ์ที่ติดตั้งรางสไลด์ซึ่งติดตั้งอยู่ในตำแหน่ง ติดตั้ง
  - อย่าปล่อยอุปกรณ์ที่ติดตั้งรางสไลด์ไว้ในตำแหน่งติดตั้ง
- ตู้ชั้นวางแต่ละตู้อาจมีสายไฟมากกว่าหนึ่งสาย
  - สำหรับชั้นว่างที่มีไฟกระแสสลับ ตรวจสอบให้แน่ใจว่าได้ดึงสายไฟทั้งหมดในตู้ชั้นวางออกแล้ว เมื่อได้รับคำสั่งให้ปลดการเชื่อมต่อกำลังไฟในระหว่างให้บริการ
  - สำหรับชั้นวางที่มี DC power distribution panel (PDP) ปิดตัวตัดวงจรที่ควบคุม กระแสไฟไปยังหน่วยอุปกรณ์ระบบ หรือถอดแหล่งจ่ายไฟกระแสตรงของลูกค้า เมื่อได้รับคำสั่ง ให้ถอดสายไฟระหว่างการให้บริการ
- เชื่อมต่ออุปกรณ์ทั้งหมดที่ติดตั้งในตู้ชั้นวางกับอุปกรณ์ไฟฟ้าที่ติดตั้งในตู้ชั้นวาง เดียวกัน ห้ามเสียบปลั๊กสายไฟจากอุปกรณ์ที่ติดตั้งในตู้ชั้นวางตู้หนึ่งกับอุปกรณ์ไฟฟ้า ที่ติดตั้งในตู้ชั้นวางอื่น
- เต้ารับไฟฟ้าที่ต่อสายไฟไม่ถูกต้องสามารถทำให้เกิดอันตรายจากกำลังไฟต่อระบบ หรืออุปกรณ์ที่พ่วงต่อกับระบบที่เป็นโลหะ ลูกค้ามีหน้าที่รับผิดชอบในการตรวจสอบจนแน่ใจว่า มีการต่อเต้ารับไฟฟ้าและสายดินถูกต้องเพื่อป้องกันไฟฟ้าช็อต (R001 ส่วน 1 จาก 2)

(R001 ส่วน 2 จากทั้งหมด 2):

ข้อควรระวัง:

- ห้ามติดตั้งยูนิตในชั้นวางซึ่งมีอุณหภูมิภายในสูงกว่าอุณหภูมิ ที่ผู้ผลิตแนะนำไว้สำหรับอุปกรณ์ที่ประกอบเข้ากับชั้นวาง
- ห้ามติดตั้งยูนิตในชั้นวางซึ่งมีการไหลเวียนอากาศที่ไม่เหมาะสม ตรวจสอบให้แน่ใจว่า การไหลเวียนอากาศตามช่องสำหรับใช้ระบายอากาศที่ด้านข้าง, ด้านหน้า หรือด้านหลังของยูนิตไม่ได้ถูกกีดขวางหรือลดลง
- ในการเชื่อมต่ออุปกรณ์เข้ากับวงจรจ่ายไฟฟ้า ควรพิจารณาให้ดีว่าการใช้งานวงจร จนเกินพิกัดจะไม่ทำให้ความสามารถในการป้องกันสายจ่ายไฟหรือการป้องกันกระแสไฟเกินด้อยลง หากต้องการ เตรียมการเชื่อมต่อสายไฟกับชั้นวางที่ถูกต้อง โปรดอ้างอิงถึงแถบป้ายการกำหนดค่าที่อยู่บนอุปกรณ์ ในชั้นวางเพื่อกำหนดความต้องการกำลังไฟทั้งหมดของวงจรจ่ายไฟฟ้า
- *(สำหรับลิ้นชักแบบเลื่อน)* ห้ามดึงหรือติดตั้งลิ้นชักหรือคุณลักษณะใด ๆ หากไม่ได้ติดตั้ง เหล็กฉากถ่วงดุลย์เข้ากับชั้นวาง หรือถ้าไม่ได้ยึดชั้นวางติดกับพื้น ห้ามดึง ลิ้นชักออกมากกว่าหนึ่งลิ้นชักในหนึ่งครั้ง แร็คอาจไม่เสถียรถ้าคุณดึงลิ้นชักออกมากกว่า หนึ่งลิ้นชักในแต่ละครั้ง

- *(สำหรับลิ้นชักแบบยึดตายตัว)* ลิ้นชักนี้เป็นลิ้นชักแบบยึดตายตัว และห้ามไม่ให้เคลื่อนย้ายเพื่อรับบริการ ยกเว้นได้รับการระบุโดยผู้ผลิต ความพยายามในการเคลื่อนย้ายลิ้นชักบางส่วน หรือทั้งหมดออกจากชั้นวาง อาจเป็นสาเหตุทำให้ชั้นวางไม่มั่นคง หรือเป็นสาเหตุทำให้ลิ้นชักตกลงมาจากชั้นวาง (R001 ส่วน 2 จาก 2)

ข้อควรระวัง: การถอดส่วนประกอบออกจากตำแหน่งด้านบนในตู้ชั้นวาง จะช่วยให้ชั้นวางมีความมั่นคงระหว่างที่มีการย้ายตำแหน่งใหม่ โปรดปฏิบัติตามคำแนะนำทั่วไปเหล่านี้ ในทุกครั้งที่คุณเปลี่ยนตำแหน่ง ตู้ชั้นวางภายในห้องหรืออาคาร

- ลดน้ำหนักของตู้ชั้นวางโดยการถอดอุปกรณ์โดยเริ่มต้นจากด้านบนสุดของ ตู้ชั้นวาง หากเป็นไปได้ ให้จัดตู้ชั้นวางคืนสภาพตามคอนฟิกูเรชันเดิมตั้งแต่ ที่คุณได้รับมา ถ้าไม่ทราบคอนฟิกูเรชันดังกล่าว คุณต้องปฏิบัติตามข้อควรระวังดังต่อไปนี้:
  - ถอดอุปกรณ์ทั้งหมดในตำแหน่ง 32U และด้านบนออก
  - ตรวจสอบให้แน่ใจว่า ได้ติดตั้งอุปกรณ์ที่หนักสุดไว้ที่ด้านล่างของตู้ชั้นวาง
  - ตรวจสอบให้แน่ใจว่า มีน้อยมากหรือไม่มีระดับ U ที่ว่างระหว่างอุปกรณ์ต่างๆ ซึ่งติดตั้งในตู้ชั้นวาง ต่ำกว่าระดับ 32U ยกเว้นว่าคอนฟิกูเรชันที่ได้รับอนุญาตเช่นนั้นเป็นพิเศษ
- ถ้าตู้ชั้นวางที่คุณจัดตำแหน่งใหม่คือส่วนของห้องชุดของตู้ชั้นวาง ให้ดึงตู้ชั้นวางออกจากห้องชุด
- ถ้าตู้ชั้นวางที่คุณกำลังเปลี่ยนตำแหน่งมีการจัดส่งมาพร้อมกับแขนค้ำซึ่ง ถอดออกได้ ต้องติดตั้งแขนค้ำนั้นอีกครั้งก่อนจะเปลี่ยนตำแหน่งตู้
- ตรวจสอบเราต์ที่คุณวางแผนที่จะกำจัดอันตรายที่อาจเกิดขึ้นได้
- ตรวจสอบว่าเราต์ที่คุณเลือกสามารถรองรับน้ำหนักของตู้ชั้นวางที่โหลดได้ อ้างอิงถึง เอกสารที่มาพร้อมกับตู้ชั้นวางของคุณเพื่อทราบข้อมูลเกี่ยวกับน้ำหนักของตู้ชั้นวางที่โหลด
- ตรวจสอบว่าประตูเปิดทั้งหมดมีขนาดอย่างน้อย 760 x 2083 มม. (30 x 82 นิ้ว).
- ตรวจสอบให้แน่ใจว่าได้เก็บอุปกรณ์, ชั้น, ลิ้นชัก, ประตู, และสายเคเบิลทั้งหมดอยู่ในสภาพที่เรียบร้อย

- ตรวจสอบให้แน่ใจว่า การวางระดับเสริมทั้งสี่ระดับถูกยกไว้ที่ตำแหน่งสูงสุด
- ตรวจสอบให้แน่ใจว่า ไม่มีแท่นยึดสเตบิไลเซอร์ที่ติดตั้งบนตู้ชั้นวางในขณะทำการเคลื่อนย้าย
- ห้ามใช้ทางลาดที่เอียงเกิน 10 องศา
- เมื่อตู้ชั้นวางอยู่ในตำแหน่งใหม่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้โดยสมบูรณ์:
  - ลดการวางระดับเสริมทั้งสี่ระดับให้ต่ำลง
  - ติดตั้งแท่นยึดบนตู้ชั้นวาง หรือในสภาพแวดล้อมที่มีแผ่นดินไหวที่ยึดชั้นวาง กับพื้น
  - ถ้าคุณถอดอุปกรณ์ใด ๆ ออกจากตู้ชั้นวาง ให้ประกอบเข้าในตู้ชั้นวางใหม่จากตำแหน่งล่างสุด ไปยังตำแหน่งบนสุด
- หากจำเป็นต้องย้ายตำแหน่งเป็นระยะทางไกล ๆ ให้จัดตู้ชั้นวาง คืนสภาพตามคอนฟิกูเรชันเดิมตั้งแต่ที่คุณได้รับมา บรรจุตู้ชั้นวางด้วยบรรจุภัณฑ์วัสดุเดิม หรือเทียบเท่า ลดการวางระดับเสริมให้ต่ำลง เพื่อยกฐานล้อให้ออกนอกพาเลตและเลื่อนตู้ชั้นวาง ไปยังพาเลต

(R002)

(L001)

อันตราย: แรงดันไฟ กระแสไฟ หรือระดับพลังงานที่เป็นอันตรายจะแสดงอยู่ภายในส่วนประกอบต่าง ๆ ที่มีเลเบลนี้ติดอยู่ ห้ามเปิดฝาครอบ หรือแผงกั้นที่ติดเลเบลนี้อยู่ (L001)

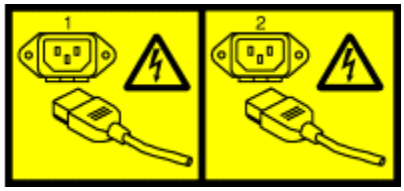
(L002)

อันตราย: ไม่ควรใช้อุปกรณ์ที่ประกอบเข้ากับชั้นวางเป็นชั้นวางหรือเป็นพื้นที่ใช้งาน ห้ามวางอ็อบเจ็กต์ต่าง ๆ ที่ด้านบนของอุปกรณ์ที่ประกอบเข้ากับชั้นวาง นอกจากนั้น อย่าพิงกับอุปกรณ์ที่เมาท์กับชั้นวาง และอย่าใช้อุปกรณ์นั้นเพื่อสร้างความเสถียรให้กับตำแหน่งร่างกายของคุณ (ตัวอย่างเช่น เมื่อทำงานจากบันได) อันตรายเกี่ยวกับความเสถียร:

- ชั้นวางอาจพลิกคว่ำทำให้ได้รับบาดเจ็บสาหัสได้
- ก่อนที่จะยึดชั้นวางไปยังตำแหน่งการติดตั้ง โปรดอ่านคำแนะนำในการติดตั้ง
- อย่าวางโหลดใดๆ บนอุปกรณ์ที่ติดตั้งรางสไลด์ซึ่งติดตั้งอยู่ในตำแหน่ง ติดตั้ง
- อย่าปล่อยอุปกรณ์ที่ติดตั้งรางสไลด์ไว้ในตำแหน่งติดตั้ง

(L002)

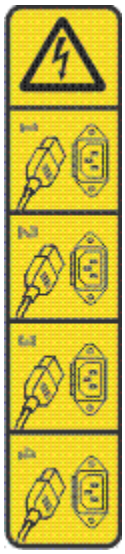
(L003)



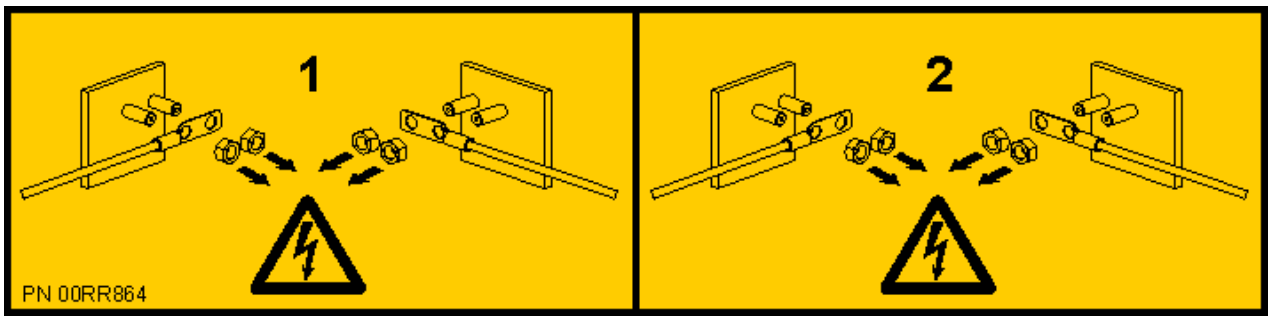
หรือ

หรือ

หรือ



หรือ



อันตราย: สายไฟหลายเส้น ผลิตภัณฑ์อาจมากับสายไฟกระแสตรง หลายเส้น หรือสายไฟกระแสสลับหลายเส้น ปลดการเชื่อมต่อสายไฟทั้งหมดเพื่อถอดสายไฟ และสายเคเบิลที่เป็นอันตรายออกไป (L003)

(L007)

ข้อควรระวัง: พื้นผิวบริเวณใกล้เคียง ร้อน (L007)

(L008)

ข้อควรระวัง: ชิ้นส่วนที่เคลื่อนไหวที่เป็นอันตรายในบริเวณใกล้เคียง (L008)

เลเซอร์ทั้งหมดได้รับการรับรองในประเทศสหรัฐอเมริกาตามข้อกำหนดของ DHHS 21 CFR Subchapter J สำหรับผลิตภัณฑ์เลเซอร์ class 1 นอกประเทศสหรัฐอเมริกา เลเซอร์ทั้งหมดจะได้รับการรับรองตาม IEC 60825 ว่าเป็นผลิตภัณฑ์เลเซอร์ class 1 ศึกษาแถบป้ายบนชิ้นส่วนแต่ละชิ้นสำหรับข้อมูลหมายเลขใบรับรองเลเซอร์และการอนุมัติ

ข้อควรระวัง: ผลิตภัณฑ์นี้อาจมีอุปกรณ์ต่อไปนี้ตั้งแต่หนึ่งตัวขึ้นไป: ซีดีรอมไดร์ฟ, ดีวีดีรอมไดร์ฟ, ดีวีดีแรมไดร์ฟ, หรือโมดูลเลเซอร์ ซึ่งเป็นผลิตภัณฑ์เลเซอร์ Class 1 หมายเหตุ ให้จดจำข้อมูลต่อไปนี้:

- ห้ามถอดฝาครอบออก การถอดฝาครอบของผลิตภัณฑ์เลเซอร์อาจเป็นผลทำให้เกิดการสัมผัสกับการแผ่รังสีเลเซอร์ที่เป็นอันตราย ไม่มีชิ้นส่วนที่สามารถถอดเปลี่ยนได้ภายในอุปกรณ์
- การใช้ตัวควบคุม หรือตัวปรับเปลี่ยน หรือใช้ประสิทธิภาพของขั้นตอนที่แตกต่างไปจากที่ระบุไว้ในที่นี้ อาจเป็นสาเหตุทำให้เกิดการสัมผัสกับการแผ่รังสีที่เป็นอันตราย

(C026)

ข้อควรระวัง: สภาพแวดล้อมการประมวลผลข้อมูลสามารถประกอบด้วยอุปกรณ์ซึ่งส่งผ่านบนระบบ ที่เชื่อมต่อกับโมดูลเลเซอร์ซึ่งปฏิบัติงานด้วยกำลังไฟมากกว่าระดับกำลังไฟของ Class 1 ด้วยเหตุนี้ จึงห้ามมองที่ส่วนปลายของเส้นใยแก้วนำแสงหรือเต้ารับที่เปิดอยู่ แม้ว่าการส่องไฟเข้าใน ปลายด้านหนึ่ง และการมองเข้าในปลายอีกด้านหนึ่งของเส้นใยแก้วนำแสงที่ไม่ได้เชื่อมต่อเพื่อตรวจสอบความต่อเนื่องของ เส้นใยแก้วนำแสงอาจไม่ทำร้ายดวงตา แต่โพรซีเดอร์นี้อาจเป็นอันตรายได้ ดังนั้น จึงไม่แนะนำ การตรวจสอบความต่อเนื่องของเส้นใยแก้วนำแสงโดยการส่องไฟเข้าในปลายด้านหนึ่ง และการมองที่ ปลายอีกด้านหนึ่ง เมื่อต้องการตรวจสอบความต่อเนื่องของสายเส้นใยแก้วนำแสง ให้ใช้แหล่งไฟออปติคัลและ มิเตอร์วัดพลังงาน (C027)

ข้อควรระวัง: ผลิตภัณฑ์นี้ประกอบด้วยเลเซอร์ Class 1M ห้ามมองที่อุปกรณ์ออพติคัลโดยตรง (C028)

ข้อควรระวัง: ผลิตภัณฑ์เลเซอร์บางชนิดประกอบด้วยเลเซอร์ไดโอด Class 3A หรือ Class 3B ฝังอยู่ หมายเหตุ ให้จดจำข้อมูลต่อไปนี้:

- การแผ่รังสีเลเซอร์เมื่อเปิด
- ห้ามจ้องมองลำแสง, ห้ามใช้อุปกรณ์ออพติคัลในการมองโดยตรง, และหลีกเลี่ยงการสัมผัสกับลำแสงโดยตรง (C030)

(C030)

ข้อควรระวัง: แบตเตอรี่ประกอบด้วยลิเธียม หากต้องการหลีกเลี่ยงการระเบิดที่อาจเกิดขึ้นได้ ห้ามเผา หรือชาร์จแบตเตอรี่

ห้าม:

- ขว้าง หรือทิ้งลงในน้ำ
- ทำให้ร้อนจนมีอุณหภูมิสูงกว่า 100 องศาเซลเซียส (212 องศาฟาเรนไฮต์)
- ซ่อมหรือถอดแยก

ให้แลกเปลี่ยนกับชิ้นส่วนที่ IBM เท่านั้น นำไปรีไซเคิล หรือทิ้งแบตเตอรี่ตามกฎข้อบังคับท้องถิ่นของคุณ ในประเทศสหรัฐอเมริกา IBM มีขั้นตอนสำหรับการเก็บรวบรวมแบตเตอรี่นี้ สำหรับข้อมูลเพิ่มเติม โปรดโทรศัพท์ติดต่อที่ 1-800-426-4333 คุณต้องทราบหมายเลขชิ้นส่วนของแบตเตอรี่ ขณะที่คุณโทรศัพท์ติดต่อ (C003)

ข้อควรระวัง: เกี่ยวกับ ที่จัดเตรียมโดย IBM เครื่องมือยกของผู้จัดจำหน่าย:

- การใช้งานเครื่องมือยกควรทำโดยบุคลากรที่ได้รับอนุญาตเท่านั้น
- เครื่องมือยกใช้สำหรับการช่วยเหลือ ยก ติดตั้ง ถอดยูนิต (โหลด) เข้าในการยก ชั้นวาง ไม่ได้ใช้สำหรับการขนส่งปริมาณมากบนทางลาด และไม่ได้ใช้แทน เครื่องมือที่กำหนด เช่น รถลากพาเลท, walkies, รถยก และแนวปฏิบัติในการย้ายตำแหน่งที่เกี่ยวข้อง เมื่อ ไม่สามารถปฏิบัติได้ ต้องใช้บุคคลที่ผ่านการฝึกอบรมมาเป็นพิเศษ หรือเซอร์วิส (เช่น ผู้ควบคุมการยก หรือบริษัทรับจ้างย้ายของ)
- อ่าน และทำความเข้าใจกับเนื้อหาของคู่มือผู้ใช้งานเครื่องมือยกโดยสมบูรณ์ก่อนจะใช้ การไม่อ่าน ไม่ทำความเข้าใจ ไม่เชื่อฟังกฎด้านความปลอดภัย และไม่ปฏิบัติตามคำแนะนำอาจส่งผล ให้ทรัพย์สินเสียหาย และ/หรือ บาดเจ็บ หากมีคำถาม โปรดติดต่อเซอร์วิสและฝ่ายสนับสนุนของผู้จัดจำหน่าย เอกสารคู่มือต้องเก็บไว้กับเครื่องในพื้นที่ช่องเก็บซึ่งจัดเตรียมไว้ คู่มือฉบับแก้ไขล่าสุด มีอยู่บนเว็บไซต์ของผู้จัดจำหน่าย
- ทดสอบฟังก์ชันเบรกขาค้ำยันก่อนการใช้งานแต่ละครั้ง อย่าย้ายหรือเลื่อน เครื่องมือยกแรงเกินไปขณะใช้เบรกขาค้ำยัน
- อย่ายก กด หรือเลื่อนเชลฟ์โหลดแพล็ตฟอร์มยกเว้นสเตบิไลเซอร์ (brake pedal jack) ยึด ติดแน่น ให้ใช้เบรกสเตบิไลเซอร์เมื่อไม่ได้ใช้งานหรือมีการเคลื่อนไหว
- อย่าย้ายเครื่องมือยกขณะยกแพล็ตฟอร์มขึ้น ยกเว้นสำหรับการจัดตำแหน่งเล็กน้อย
- อย่าบรรทุกเกินความจุน้ำหนักบรรทุกที่กำหนด โปรดดูแผนภูมิความจุน้ำหนักบรรทุกเกี่ยวกับน้ำหนักบรรทุกสูงสุดที่ ศูนย์กลาง และที่ขอบของแพล็ตฟอร์มซึ่งขยาย
- เพิ่มน้ำหนักบรรทุกเฉพาะถ้าจัดตำแหน่งศูนย์กลางบนแพล็ตฟอร์มอย่างถูกต้อง อย่าวางของมากกว่า 200 ปอนด์ (91 กก.) บน ขอบของชั้นแพล็ตฟอร์มที่เลื่อนได้ และพิจารณาถึงแรงโน้มถ่วง (CoG) ของน้ำหนักบรรทุกด้วย
- อย่าวางแพล็ตฟอร์ม ด้วยกมุมเอียง ลิ่มติดตั้งอุปกรณ์เข้ามุม หรืออ็อพชัน เสริมอื่น ๆ ยึดแพล็ตฟอร์ม -- ด้วยกเอียง ลิ่ม หรืออ็อพชันอื่น ๆ กับเชลฟ์ยกหลัก หรือ อุปกรณ์ยกในตำแหน่งทั้งสี่ (4x หรือการเมาท์ที่จัดเตรียมอื่น ๆ ทั้งหมดด้วยฮาร์ดแวร์ที่จัดเตรียมให้เท่านั้น ก่อนที่จะใช้งาน อ็อบเจ็กต์ ที่บรรทุกได้รับการออกแบบมาเพื่อเลื่อนเข้า/ออกแพล็ตฟอร์มอย่างราบรื่นโดยไม่ต้องใช้แรง ดังนั้น ระวังอย่า ผลักหรือเอียง ให้อ็อพชันด้วยกเอียง [แพล็ตฟอร์มที่ปรับมุมเอียงได้] อยู่ในแนวราบตลอด เวลา ยกเว้นสำหรับการปรับมุมเพียงเล็กน้อยครั้งสุดท้ายเมื่อจำเป็น
- อย่ายืนใต้น้ำหนักบรรทุกที่ยื่นออกมา
- อย่าใช้บนพื้นผิวที่ไม่ราบ เอียงขึ้น หรือเอียงลง (ทางลาดมาก)
- อย่าซ้อนทับน้ำหนักบรรทุก
- อย่าใช้งานขณะรับประทานยาหรือแอลกอฮอล์
- อย่าพาดบันไดกับเครื่องมือยก (ยกเว้นมีการอนุญาตเป็นการเฉพาะ สำหรับหนึ่งในขั้นตอนที่ได้รับอนุญาตต่อไปนี้สำหรับการทำงานในการยกด้วยเครื่องมือนี้)
- อันตรายจากการหนีบ อย่าผลักหรือพิงน้ำหนักบรรทุกด้วยแพล็ตฟอร์มที่ยกขึ้น

- อย่าใช้เป็นแพล็ตฟอร์มยกส่วนบุคคล หรือขั้นบันได ห้ามนั่งคร่อม
- อย่ายืนบนส่วนใด ๆ ของเครื่องมือยก ไม่ใช่ขั้นบันได
- อย่าปีนบนเสา
- อย่าใช้เครื่องมือยกที่เสียหายหรือทำงานผิดปกติ
- จุดที่ขรุขระและไม่เรียบเป็นอันตรายต่อแพล็ตฟอร์มด้านล่าง บรรทุกสิ่งของด้านล่างในพื้นที่ซึ่งไม่มีบุคคลและสิ่งกีดขวางเท่านั้น มือและเท้าไม่ควรมีสิ่งกีดขวางระหว่างการใช้งาน
- ไม่ใช่รถยก ห้ามยกหรือย้ายเครื่องมือยกเปล่าด้วยรถลากพาเลท, jack หรือ รถยก
- เสาขยายได้มากกว่าแพล็ตฟอร์ม ระวังความสูงของเพดาน ถาดสายเคเบิล หัวฉีดดับเพลิง ดวงไฟ และอ็อบเจ็กต์เหนือศีรษะอื่น
- อย่าปล่อยเครื่องมือยกที่มีน้ำหนักบรรทุกยกขึ้นโดยไม่มีการควบคุม
- เฝ้าดู และอย่าให้มือ นิ้ว และเสื้อผ้ามีสิ่งกีดขวางเมื่อเครื่องมือเคลื่อนไหว
- ปรับเครื่องยกด้วยมือเท่านั้น ถ้าไม่สามารถหมุนที่จับเครื่องยกได้ง่ายด้วยมือเดียว แสดงว่า อาจบรรทุกเกินน้ำหนัก อย่าหมุนเครื่องยกต่อไปจนผ่านระดับบนสุดหรือล่างสุดของแพล็ตฟอร์ม การคลายออกมากเกินไปจะถอดที่จับ และทำให้สายเคเบิลเสียหาย จับที่จับไว้เสมอเมื่อลดระดับ หรือคลายออก ตรวจสอบให้แน่ใจเสมอว่าเครื่องยกมีน้ำหนักบรรทุกอยู่ก่อนจะปล่อยที่จับเครื่องยก
- อุบัติเหตุเกี่ยวกับเครื่องยกอาจทำให้บาดเจ็บร้ายแรง ไม่เหมาะสำหรับสถานที่ที่มีผู้คนพลุกพล่าน ส่งเสียงสัญญาณ ให้ได้ยินขณะเครื่องมือกำลังยก ตรวจสอบให้แน่ใจว่าเครื่องยกถูกล็อคไว้ในตำแหน่งก่อน จะปล่อยที่จับ อ่านหน้าคำแนะนำก่อนจะใช้เครื่องยกนี้ ห้ามปล่อยให้เครื่องยกคลายออก อย่างอิสระ ล้อที่หมุนอย่างอิสระจะทำให้สายเคเบิลพันรอบดรัมเครื่องยกอย่างไม่เท่าเทียมกัน ทำให้สายเคเบิลเสียหาย และอาจเป็นสาเหตุให้เกิดการบาดเจ็บร้ายแรง
- เครื่องมือนี้ต้องได้รับการดูแลรักษาอย่างเหมาะสมสำหรับให้เจ้าหน้าที่ IBM Service ใช้งาน IBM จะ ตรวจสอบสภาพ และยืนยันความถูกต้องในประวัติการดูแลรักษาก่อนการดำเนินงาน เจ้าหน้าที่ขอสงวนสิทธิ์ที่จะไม่ใช้ เครื่องมือหากไม่เหมาะสม (C048)

ข้อมูลกำลังไฟฟ้าและการวางสายเคเบิลสำหรับ NEBS (Network Equipment-Building System) GR-1089-CORE

ข้อสังเกตต่อไปนี้ใช้กับเซิร์ฟเวอร์ IBM ที่ได้รับการออกแบบมาให้สอดคล้องกับ NEBS (Network Equipment-Building System) GR-1089-CORE:

อุปกรณ์เหมาะกับการติดตั้งในสถานที่ต่อไปนี้:

- สถานที่อำนวยความสะดวกด้านเครือข่ายโทรคมนาคม
- ตำแหน่งที่สามารถใช้ NEC (National Electrical Code) ได้

พอร์ตภายในอาคารของอุปกรณ์นี้เหมาะกับการเชื่อมต่อภายในอาคาร หรือการวางสายไฟหรือสายเคเบิลที่มีฉนวนห่อหุ้มเท่านั้น พอร์ตภายในอาคารของอุปกรณ์นี้ *ต้องไม่* เชื่อมต่อแบบโลหะกับอินเตอร์เฟสที่เชื่อมต่อกับ OSP (outside plant) หรือสายไฟของอุปกรณ์เอง อินเตอร์เฟสเหล่านี้ได้รับการออกแบบมาเพื่อใช้เป็นอินเตอร์เฟสภายในอาคารเท่านั้น (พอร์ตชนิด 2 หรือชนิด 4 ตามที่อธิบายใน GR-1089-CORE) และต้องมีการแยก จากสายเคเบิล OSP แบบเปลือย การเพิ่มตัวปกป้องหลักไม่ใช่การปกป้องที่เพียงพอสำหรับการเชื่อมต่อ อินเตอร์เฟสเหล่านี้ในแบบโลหะเข้ากับสาย OSP

หมายเหตุ: สายเคเบิลอีเทอร์เน็ตทั้งหมด ต้องมีฉนวนหุ้มและต่อสายดินที่ปลายทั้งสองด้าน

ระบบไฟฟ้ากระแสสลับไม่จำเป็นต้องใช้อุปกรณ์ป้องกันไฟกระชากหรือ surge protection device (SPD)ภายนอก

ส่วนระบบไฟฟ้ากระแสตรงใช้รูปแบบ DC return แบบแยกออก หรือ isolated DC return (DC-I) ขั้วต่อกลับของแบตเตอรี่กระแสตรง *ต้องไม่* เชื่อมต่อกับโครงเครื่องหรือกรอบสายดิน

ระบบกำลังไฟกระแสตรงมีเจตนาที่จะติดตั้งไว้ใน common bonding network (CBN) ตามที่กล่าวไว้ใน GR-1089-CORE

การติดตั้งและการตั้งค่าคอนฟิก คอนโซลการจัดการฮาร์ดแวร์

ศึกษาวิธีการติดตั้งฮาร์ดแวร์ คอนโซลการจัดการฮาร์ดแวร์ (HMC) เชื่อมต่อกับระบบที่ถูกจัดการของคุณ และ กำหนดค่าเพื่อใช้งาน คุณสามารถดำเนินการกับงานเหล่านี้ได้ด้วยตนเอง หรือติดต่อผู้ให้บริการเพื่อดำเนินการกับงานเหล่านี้ให้คุณ คุณอาจถูกเรียกเก็บค่า ธรรมเนียมจากผู้ให้บริการสำหรับการให้บริการนี้

มีอะไรใหม่สำหรับการติดตั้งและการกำหนดคอนฟิก HMC

อ่านข้อมูลที่มีการเปลี่ยนแปลงหรือข้อมูลใหม่ที่เกี่ยวกับหัวข้อการติดตั้งและกำหนดคอนฟิก HMC เมื่อมีการอัพเดตการรวบรวมหัวข้อก่อนหน้า

เมษายน 2021

- เพิ่มหัวข้อต่อไปนี้ :
  - “การติดตั้ง IBM Power Systems HMC (7063-CR2) เข้ากับชั้นวาง” ในหน้า 4
  - “สิ่งที่จำเป็นต้องมีสำหรับการติดตั้งระบบ 7063-CR2 บนชั้นวาง” ในหน้า 4
  - “การจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ” ในหน้า 4
  - “การกำหนดและทำเครื่องหมายตำแหน่งในชั้นวางสำหรับระบบ 7063-CR2” ในหน้า 5
  - “การยึดรางแบบปรับได้กับแชสซีระบบและยึดกับชั้นวาง” ในหน้า 6
  - “การยึดรางกับโครงเครื่องและยึดกับชั้นวาง” ในหน้า 8
  - “การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ” ในหน้า 9
  - “การเดินสายเคเบิล 7063-CR2 HMC ที่ติดตั้งในชั้นวาง” ในหน้า 10
  - “การกำหนดคอนฟิก 7063-CR2 HMC” ในหน้า 11

พฤศจิกายน 2020

- อัพเดตหัวข้อต่อไปนี้:
  - “ภารกิจการติดตั้งและการกำหนดคอนฟิก” ในหน้า 2
  - “การรักษาความปลอดภัย HMC” ในหน้า 78
  - “ตำแหน่งพอร์ตของ HMC” ในหน้า 85

กรกฎาคม 2020

- อัพเดตหัวข้อต่อไปนี้:
  - “การติดตั้ง เครื่องมือเสมือน HMC ” ในหน้า 22
  - “ตำแหน่งพอร์ตของ HMC” ในหน้า 85

ตุลาคม 2019

- อัพเดตหัวข้อต่อไปนี้:
  - “การติดตั้ง เครื่องมือเสมือน HMC ” ในหน้า 22
  - “การรักษาความปลอดภัย HMC” ในหน้า 78

กุมภาพันธ์ 2019

- เพิ่มหัวข้อต่อไปนี้:
  - “การรักษาความปลอดภัย HMC” ในหน้า 78
  - “นโยบายรหัสผ่านที่ได้รับการพัฒนา” ในหน้า 80

- “การแก้ไขปัญหาทั่วไปขณะรักษาความปลอดภัย HMC” ในหน้า 83
- “โปรไฟล์ความปลอดภัย: Global Data Protection Regulation (GDPR) และ Payment Card Industry Data Security Standard (PCI-DSS) ” ในหน้า 81

สิงหาคม 2018

- อัพเดตหัวข้อต่อไปนี้:
  - “การกำหนดคอนฟิก 7063-CR1 HMC” ในหน้า 20
  - “ตำแหน่งพอร์ตของ HMC” ในหน้า 85

ธันวาคม 2017

- เพิ่มข้อมูลสำหรับเซิร์ฟเวอร์ IBM Power Systems ที่มีตัวประมวลผล POWER9

ภารกิจการติดตั้งและการกำหนดคอนฟิก

ศึกษาเกี่ยวกับภารกิจที่เชื่อมโยงกับการติดตั้งและภารกิจกำหนดคอนฟิก HMC ที่แตกต่างกัน

ศึกษาเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการเมื่อคุณติดตั้งและกำหนดคอนฟิก HMC คุณสามารถติดตั้งและกำหนดคอนฟิก HMC ในวิธีที่แตกต่างกัน ค้นหาสถานการณ์ที่เหมาะสมที่สุด กับงานที่คุณต้องการดำเนินการ

Notes:

- หากคุณกำลังจัดการเวอร์ชันที่ใช้ตัวประมวลผล POWER9 HMC ต้องเป็นเวอร์ชัน 9.1.0 หรือใหม่กว่า สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดเวอร์ชันและรีลีสของรหัสเครื่อง HMC ของคุณ” ในหน้า 69
- Hardware Management Console เวอร์ชัน 9.2.950 หรือใหม่กว่าไม่สนับสนุนบนชนิดเครื่อง HMC 7042 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเวอร์ชันของ HMC สำหรับ 7042 HMC ของคุณ โปรดดูที่หมายเหตุรีลีส HMC ที่ พร้อมใช้งานในเว็บไซต์ Fix Central

การติดตั้งและการกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

ศึกษาเกี่ยวกับภารกิจขั้นสูงที่คุณต้องดำเนินการเมื่อคุณติดตั้งและกำหนดคอนฟิก HMC ใหม่กับเซิร์ฟเวอร์ใหม่

Table 1. ภารกิจที่คุณต้องดำเนินการเมื่อคุณติดตั้งและกำหนดคอนฟิก HMC ใหม่กับ เซิร์ฟเวอร์ใหม่

ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. รวบรวมข้อมูลและป้อนข้อมูลในเวิร์กชีตการกำหนดคอนฟิก ก่อนการติดตั้ง	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42 “การจัดเตรียมสำหรับการตั้งค่าของ HMC” on page 41
2. แกะกล่องบรรจุฮาร์ดแวร์	
3. ต่อสายเคเบิลฮาร์ดแวร์ HMC	“การเดินสายเคเบิล 7063-CR1 HMC ที่ติดตั้งในชั้นวาง” on page 18
4. เปิดกำลังไฟ HMC โดยกดปุ่มเปิดกำลังไฟ	
5. ล็อกอินและเริ่มต้นเว็บแอ็พพลิเคชัน HMC	
6. เข้าใช้วิซาร์ดตั้งค่าที่แนะนำ หรือใช้เมนู HMC เพื่อกำหนดคอนฟิก HMC	“การกำหนดคอนฟิก HMC โดย ใช้พาธด่วนผ่านทางวิซาร์ดเซ็ตอัพที่แนะนำ” on page 49 “การกำหนดค่า HMC โดยใช้เมนู ” on page 49
7. ต่อเซิร์ฟเวอร์เข้ากับ HMC	

การอัพเดตและอัพเกรดรหัส HMC ของคุณ

ศึกษาเพิ่มเติมเกี่ยวกับภารกิจขั้นสูงที่คุณต้องดำเนินการเมื่อคุณอัพเดตและอัพเกรด โค้ด HMC ของคุณ

หากคุณมี HMC ที่มีอยู่ และต้องการอัพเดตหรืออัพเกรด รหัส HMC ของคุณ คุณต้องทำภารกิจขั้นสูงต่อไปนี้ให้เสร็จสิ้น:

Table 2. ภารกิจที่คุณต้องดำเนินการเมื่อคุณอัพเดตหรืออัพเกรดโค้ด HMC	
ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. ขอรับอัพเกรด	“การอัพเกรดซอฟต์แวร์ HMC ของคุณ” on page 73
2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	
3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ	
4. สำรองข้อมูล HMC	
5. บันทึกข้อมูลการกำหนดคอนฟิก HMC ปัจจุบัน	
6. บันทึกสถานะคำสั่งรีโมต	
7. จัดเก็บข้อมูลอัพเกรด	
8. อัพเกรดซอฟต์แวร์ HMC	
9. ตรวจสอบว่ามีการติดตั้งการอัพเกรดรหัสเครื่อง HMC เรียบร้อยแล้ว	

การเพิ่ม HMC ตัวที่สองในการติดตั้งที่มีอยู่

ศึกษาเพิ่มเติมเกี่ยวกับภารกิจขั้นสูงที่คุณต้องดำเนินการเมื่อคุณเพิ่ม HMC ตัวที่สองเข้ากับ ระบบที่ถูกจัดการของคุณ

หากคุณมี HMC และระบบที่ถูกจัดการอยู่แล้วและต้องการเพิ่ม HMC ตัวที่สองเข้ากับ การกำหนดคอนฟิกนี้ ให้ทำตามขั้นตอนต่อไปนี้:

Table 3. ภารกิจที่คุณต้องดำเนินการเมื่อคุณเพิ่ม HMC ตัวที่สองเข้ากับการติดตั้งที่มีอยู่	
ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. ตรวจสอบให้แน่ใจว่าฮาร์ดแวร์ HMC ของคุณสนับสนุนโค้ด HMC เวอร์ชัน 7	
2. รวบรวมข้อมูล และกรอกข้อมูลในเวิร์กชีต การกำหนดคอนฟิกก่อนการติดตั้ง	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42
3. แกะกล่องบรรจุฮาร์ดแวร์	
4. ต่อสายเคเบิลฮาร์ดแวร์ HMC	“การเดินสายเคเบิล 7063-CR1 HMC ที่ติดตั้งในชั้นวาง” on page 18
5. เปิดกำลังไฟ HMC โดยกดปุ่มเปิดกำลังไฟ	
6. ล็อกอินเข้าสู่ HMC	
7. ระดับโค้ด HMC ต้องตรงกัน เปลี่ยนโค้ดบน เครื่องหนึ่งให้ตรงกับโค้ดบน HMC เครื่องอื่น	“การกำหนดเวอร์ชันและรีลีสของรหัสเครื่อง HMC ของคุณ” on page 69 “การอัพเกรดซอฟต์แวร์ HMC ของคุณ” on page 73
8. เข้าใช้วิซาร์ดตั้งค่าที่แนะนำ หรือใช้เมนู HMC เพื่อกำหนดคอนฟิก HMC	“การกำหนดค่า HMC โดยใช้เมนู ” on page 49
9. กำหนดคอนฟิก HMC นี้สำหรับการให้บริการโดยใช้วิซาร์ดการตั้งค่า Call-Home	“การกำหนดค่า HMC เพื่อให้สามารถเชื่อมต่อกับฝ่ายบริการและสนับสนุนโดยใช้วิซาร์ดการตั้งค่า call-home” on page 62
10. ต่อเซิร์ฟเวอร์เข้ากับ HMC	

การตั้งค่า HMC

คุณต้องตั้งค่าฮาร์ดแวร์ HMC ก่อนตั้งค่าซอฟต์แวร์ HMC ศึกษาเพิ่มเติมเกี่ยวกับการตั้งค่า HMC ที่มีดิสก์หรือ HMC ที่ติดตั้งชั้นวาง

การติดตั้ง IBM Power Systems HMC (7063-CR2) เข้ากับชั้นวาง

ศึกษาเกี่ยวกับการติดตั้ง IBM Power Systems HMC (7063-CR2) เข้ากับชั้นวาง

คุณสามารถดูเอกสารคู่มือการติดตั้งแบบออนไลน์ หรือคุณสามารถพิมพ์ ข้อมูลเดียวกันในเวอร์ชัน PDF เมื่อต้องการดูหรือพิมพ์เวอร์ชัน PDF โปรดดูที่ การติดตั้งและ การกำหนดค่า Hardware Management Console

สิ่งที่จำเป็นต้องมีสำหรับการติดตั้งระบบ 7063-CR2 บนชั้นวาง

ใช้ข้อมูลเพื่อทำความเข้าใจกับสิ่งที่จำเป็นต้องมีที่จำเป็นสำหรับการติดตั้ง ระบบ

เกี่ยวกับภารกิจนี้

ข้อควรระวัง: ชิ้นส่วนหรือยูนิตนี้หนักมาก แต่มีน้ำหนักน้อยกว่า 18 กก. (39.7 ปอนด์) โปรดใช้ความระมัดระวังขณะยก, ถอด, หรือติดตั้งชิ้นส่วนหรือยูนิตนี้ (C008)

คุณอาจต้องอ่าน เอกสารต่อไปนี้ก่อนที่คุณจะเริ่มต้นการติดตั้งเซิร์ฟเวอร์:

- เวอร์ชันล่าสุดของเอกสารนี้ถูกเก็บไว้แบบออนไลน์ โปรดดูที่ การติดตั้ง 7063-CR2 เข้ากับชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm)
- เมื่อต้องการวางแผนการติดตั้งเซิร์ฟเวอร์ของคุณ โปรดดูที่ การวางแผนไซต์และฮาร์ดแวร์

กระบวนการ

1. ตรวจสอบให้แน่ใจว่า คุณมีรายการต่อไปนี้ก่อนที่จะเริ่มต้นการติดตั้ง:
   - ไขควงแฉกเบอร์ 2
   - ไขควงแบบแบน
   - ไขควง T25
   - ที่ตัดกล่อง
   - สายรัดข้อมือป้องกันไฟฟ้าสถิต (ESD)
   - ชั้นวางที่มีที่ว่างหนึ่งหน่วย Electronic Industries Association (EIA) (1U)

   Notes:

   - หากคุณไม่ได้ติดตั้งชั้นวาง ให้ติดตั้งชั้นวาง สำหรับคำแนะนำ โปรดดูที่ ชั้นวางและคุณลักษณะชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm)
   - พิกัดของแหล่งจ่ายไฟคือ 100 ถึง 127 V ac, 9 A (x2), 200 ถึง 240 V ac, 4.5 A (x2); 50 หรือ 60 Hz.
2. ดำเนินการต่อกับ “การจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ” ในหน้า 4

การจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ

ใช้ข้อมูลนี้เพื่อจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ

กระบวนการ

1. ตรวจสอบว่าคุณได้รับทุกกล่อง ที่คุณสั่งซื้อ
2. นำคอมโพเนนต์เซิร์ฟเวอร์ออกจากกล่องตามต้องการ
3. รายการชิ้นส่วนและตรวจสอบว่าคุณได้รับชิ้นส่วนทั้งหมดที่คุณสั่งซื้อ ก่อนที่คุณจะติดตั้งแต่ละคอมโพเนนต์ของเซิร์ฟเวอร์

   หมายเหตุ:

ข้อมูลใบสั่งซื้อ รวมอยู่กับผลิตภัณฑ์ของคุณ คุณยังสามารถได้รับข้อมูลการสั่งซื้อจาก ตัวแทนด้านการตลาดของคุณ หรือ IBM Business Partner

ถ้าชิ้นส่วนไม่ถูกต้อง หายไป หรือเสียหาย ให้ติดต่อรีซอร์สใด ๆ ต่อไปนี้:

- ตัวแทนจำหน่าย IBM
- สายข้อมูลอัตโนมัติเกี่ยวกับการผลิต IBM Rochester ที่ 1-800-300-8751 (สหรัฐอเมริกาเท่านั้น)
- เว็บไซต์ ไดเร็กทอรีของ ผู้ติดต่อทั่วโลก (http://www.ibm.com/planetwide) เลือก ที่ตั้งของคุณเพื่อดูข้อมูลผู้ติดต่อฝ่ายสนับสนุนและบริการ

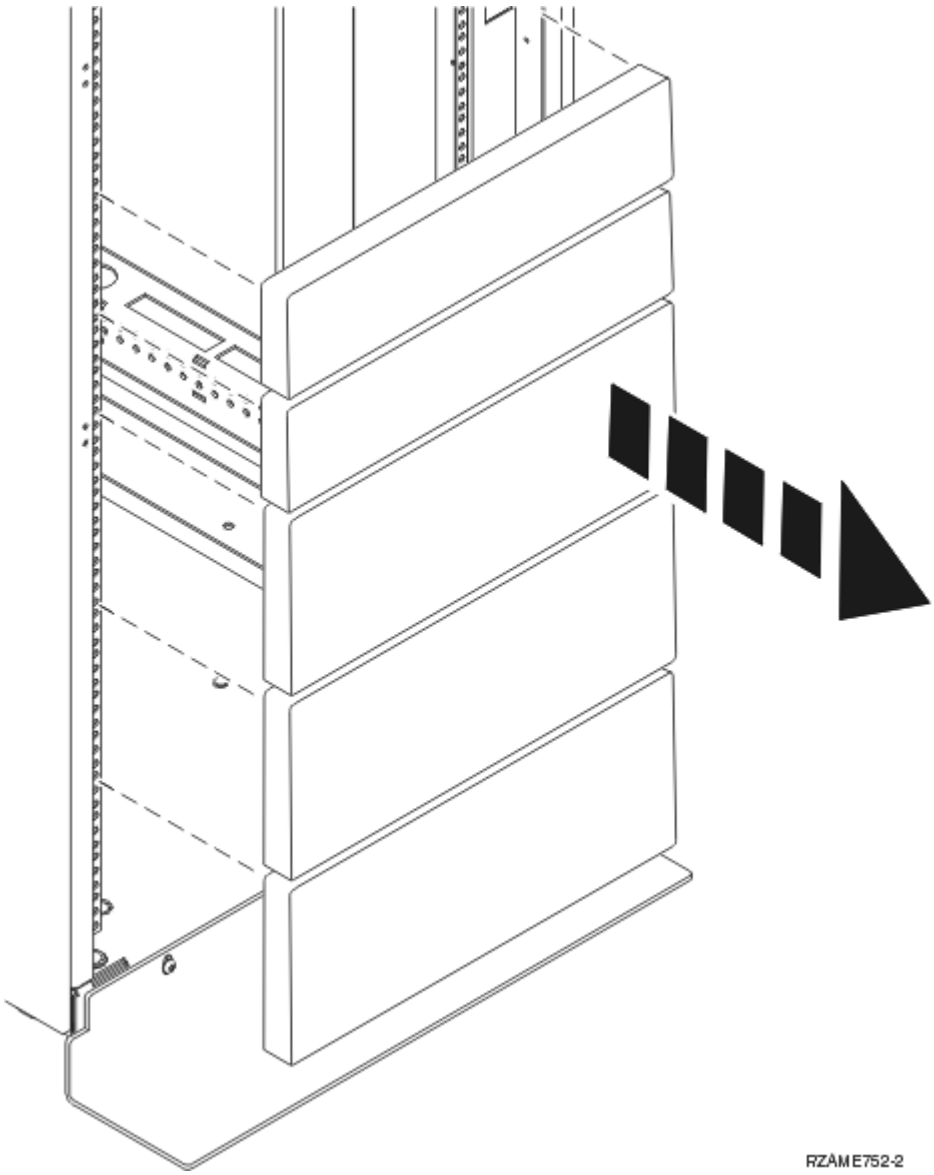
4. ดำเนินการต่อด้วย “การกำหนดและทำเครื่องหมายตำแหน่งในชั้นวางสำหรับระบบ 7063-CR2” ในหน้า 5

การกำหนดและทำเครื่องหมายตำแหน่งในชั้นวางสำหรับระบบ 7063-CR2

คุณต้องกำหนดตำแหน่งที่จะติดตั้งยูนิตระบบลงในชั้นวาง

กระบวนการ

1. อ่าน หมายเหตุความปลอดภัยของชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm)
2. ระบุตำแหน่งที่จะวาง ยูนิตระบบในชั้นวาง เมื่อคุณวางแผนสำหรับการติดตั้งยูนิต ระบบในชั้นวาง ให้พิจารณาข้อมูลต่อไปนี้:
   - วางยูนิตที่ใหญ่กว่าและหนักกว่าใน ส่วนล่างของชั้นวาง
   - วางแผนติดตั้งยูนิตระบบในส่วนล่างของชั้นวางก่อน
   - บันทึกตำแหน่ง Electronic Industries Alliance (EIA) ในแผนของคุณ
3. ถ้าจำเป็น ให้ถอดพาเนลฟิลเลอร์ออก เพื่อให้สามารถเข้าถึงด้านในของส่วนแนบชั้นวางที่คุณวางแผนจะ วางยูนิตดังแสดงใน รูปที่ 1 ในหน้า 6



รูปที่ 1. การถอดพาเนลฟิลเลอร์

4. กำหนดตำแหน่งที่จะวางระบบในชั้นวาง บันทึกตำแหน่ง EIA
5. ห้นหน้าเข้าหาชั้นวางและทำงานจากด้านขวา ใช้เทป ปากกาทำเครื่องหมาย หรือดินสอ เพื่อทำเครื่องหมายที่รูด้านล่างของยูนิต EIA แต่ละตัว
6. ทำซ้ำขั้นตอน “5” ในหน้า 6 สำหรับรูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
7. ไปที่ด้านหลังของชั้นวาง
8. ที่ด้านขวา, ให้หายูนิต EIA ที่ตรงกับยูนิต EIA ด้านล่างซึ่งทำเครื่องหมายอยู่บนด้านหน้าของชั้นวาง
9. ทำเครื่องหมายที่ยูนิต EIA ด้านล่าง
10. ทำเครื่องหมายรูที่ตรงกันทางด้านซ้ายของชั้นวาง
11. ดำเนินการต่อกับ “การยึดรางแบบปรับได้กับแชสซีระบบและยึดกับชั้นวาง” ในหน้า 6 เพื่อยึด รางแบบปรับได้ หรือดำเนินการต่อกับ “การยึดรางกับโครงเครื่องและยึดกับชั้นวาง” ในหน้า 8 เพื่อยึด รางแบบยึดตายตัว

การยึดรางแบบปรับได้กับแชสซีระบบและยึดกับชั้นวาง

คุณต้องติดตั้งรางบนแชสซีและยึดกับชั้นวาง ใช้โพรซีเดอร์นี้ เพื่อดำเนินการกับภารกิจนี้

เกี่ยวกับภารกิจนี้

ข้อควรสนใจ: เพื่อหลีกเลี่ยงความล้มเหลวของรางและอันตรายที่อาจเกิดขึ้นต่อตัวคุณเอง และเครื่อง ตรวจสอบให้แน่ใจว่าคุณมีรางและอุปกรณ์ติดตั้งที่ถูกต้อง สำหรับชั้นวาง ถ้าชั้นวางมีช่องค้ำรูปสี่เหลี่ยม หรือช่องค้ำ screw-thread ตรวจสอบให้แน่ใจว่า รางและอุปกรณ์ติดตั้งตรงกับช่องค้ำที่ใช้บน ชั้นวาง อย่าติดตั้งฮาร์ดแวร์ที่ไม่ตรงกันโดยใช้แหวนรองหรือ ตัวรอง หากคุณไม่มีรางและอุปกรณ์ติดตั้ง ที่ถูกต้องสำหรับชั้นวางของคุณ ให้ติดต่อผู้ตัวแทนจำหน่าย IBM ของคุณ

หมายเหตุ: หน่วย EIA 1 หน่วยในชั้นวางวัดโดยเพิ่มขึ้นตามแนวตั้งที่ 44.45 มม. (1.75 นิ้ว) ต่อหน่วย การเพิ่มขึ้น แต่ละ 44.45 มม. (1.75 นิ้ว) เรียกว่า “EIA.” ในบางประเทศ การเพิ่มที่เท่ากัน สามารถเรียกว่า “U.”

หมายเหตุ: ระบบต้องการพื้นที่ว่างยูนิตชั้นวาง 1 EIA (1U)

ตรวจสอบว่า คุณมีชิ้นส่วนที่จำเป็นเพื่อติดตั้งราง ชิ้นส่วนต่อไปนี้ ถูกรวมกับชุดของราง:

- 4 - สกรูหัวแฉก 6.35 มม. (0.25 นิ้ว)
- 2 - ชั้นวางและชุดรางยึดสไลด์
- 2 - ตัวยึดสไลด์ HMC
- 10 - nut clips สำหรับรูยึด EIA แบบสี่เหลี่ยม
- 10 - nut clips สำหรับรูยึด EIA แบบวงกลม
- 10 - สกรูหน้าแปลนหกเหลี่ยม M5

กระบวนการ

1. ถอดส่วนของรางออกจากแพ็กเกจและวางลงบนพื้นที่งาน
2. ระบุช่องว่าง 1U ในชั้นวางของ HMC
3. เมื่อต้องการยึดตัวยึดสไลด์เข้ากับ HMC ให้ดำเนินการดังต่อไปนี้:
   a. ระบุตัวยึดสไลด์ด้านขวา
   b. จัดแนวรูบนตัวยึดสไลด์ด้านขวาด้วยหมุดยึดสไลด์ที่อยู่ทางด้านขวา ของ HMC ตรวจสอบให้แน่ใจว่าหมุดทั้งหมดอยู่ในแนวเดียวกันกับรูยึด
   c. ดันตัวยึดสไลด์ HMC ไปทางด้านหลังของ HMC จนกระทั่งล็อคเข้าที่ จนสุด
   d. ยึดตัวยึดสไลด์ด้านขวากับด้านขวาของเวิร์กสเตชัน HMC โดยติดตั้ง สกรูแฉก 6.35 มม. (0.25 นิ้ว) สองตัวเข้ากับรูสกรู
   e. ทำซ้ำขั้นตอน “3.a” ในหน้า 7 - “3.d” ในหน้า 7 เพื่อติดตั้งตัวยึดสไลด์ด้านซ้ายกับ ด้านซ้ายของเวิร์กสเตชัน HMC
4. ย้ายไปยังด้านหน้าของชั้นวาง
   a. ทางด้านซ้าย ให้ติดตั้ง nut clips สามตัวลงในรูสามรูที่ขอบด้านหน้า ของชั้นวางในสล็อต 1U ที่กำหนดไว้สำหรับ HMC

      หมายเหตุ: ชุดรางประกอบด้วย nut clip สำหรับ รูทั้งแบบเหลี่ยมและแบบกลมของชั้นวาง ตรวจสอบให้แน่ใจว่าคุณใช้ nut clip ที่เหมาะสมที่เข้ากับรูในชั้นวาง
   b. ทำซ้ำขั้นตอน “4.a” ในหน้า 7 กับทางด้านขวาของ ชั้นวาง
5. ย้ายไปยังด้านหลังของชั้นวาง
   a. ทางด้านซ้าย ให้ติดตั้ง nut clips สองตัวลงในรูด้านบนและด้านล่างที่ ขอบด้านหน้าของชั้นวางในสล็อต 1U ที่กำหนดไว้สำหรับ HMC

      หมายเหตุ: ส่วนรูตรงกลางให้ ปล่อยว่างไว้
   b. ทำซ้ำขั้นตอน “5.a” ในหน้า 7 กับทางด้านขวาของ ชั้นวาง
6. เมื่อต้องการติดตั้งรางสไลด์ของ HMC เข้ากับชั้นวาง ให้ดำเนินการขั้นตอนต่อไปนี้:
   a. วัดความลึกของชั้นวาง ความลึกต้องอยู่ระหว่าง 558.8 มม. (22 นิ้ว) ถึง 863.6 มม. (34 นิ้ว).
   b. วางรางสไลด์ HMC บนพื้นผิวเรียบและค้นหาสกรูที่ติดตั้งไว้ล่วงหน้า

      หมายเหตุ: รางสไลด์ มีรูสกรูสี่รู
   c. คลายสกรูที่ติดตั้งไว้ล่วงหน้าบนรางสไลด์ออกให้เพียงพอที่จะเคลื่อนย้ายเข้าและออก ได้ง่าย

d. ขึ้นอยู่กับความลึกของชั้นวางที่วัดได้ในขั้นตอน “6.a” ในหน้า 7 คุณต้องปรับสกรูบนราง

i) ถ้าความลึกของชั้นวางอยู่ระหว่าง 558.8 มม. (22 นิ้ว) ถึง 698.5 มม. (27.5 นิ้ว) ให้ขันสกรูเข้ากับรูแรก และรูที่สาม

ii) ถ้าความลึกของชั้นวางอยู่ระหว่าง 698.5 มม. (27.5 นิ้ว) ถึง 863.6 มม. (34 นิ้ว) ให้ขันสกรูเข้ากับ รูที่สอง และรูที่สี่

Notes:

- รูแรกคือรูที่อยู่ใกล้กับปลายรางเลื่อนที่สุดเสมอ รูที่สามและสี่ จะอยู่ติดกัน
- ตรวจสอบให้แน่ใจว่าสกรูหลวมเพียงพอเพื่อให้สามารถปรับความยาวของรางสไลด์ ได้เล็กน้อยในขณะที่ติดตั้งในชั้นวาง

7. ที่ด้านหน้าของชั้นวาง ให้ติดตั้งรางสไลด์ HMC ในชั้นวางโดย ทำตามขั้นตอนต่อไปนี้:
   a. ค้นหาชุดรางสไลด์ด้านซ้าย
   b. จัดแนวชุดรางเพื่อให้ปลายที่มีรูสกรูที่ใกล้ที่สุด (รูแรก) เข้าไป ในชั้นวางก่อน ตรวจดูให้แน่ใจว่าหัวสกรูหันเข้าหาด้านในของชั้นวาง สล็อตเปิดของชุดรางอยู่ใกล้กับด้านหน้า ของชั้นวางมากที่สุด
   c. ที่ด้านซ้ายของชั้นวาง ให้ต่อหน้าแปลนที่ส่วนท้ายของรางเลื่อนเข้ากับ ขอบด้านหน้าของชั้นวางโดยใช้สกรู M5 สองตัวปล่อยให้รูตรงกลางเปิดอยู่ ตรวจดูให้แน่ใจว่าชุดรางถูกปล่อยให้หลวมเล็กน้อย ที่ด้านหน้าของชั้นวางเพื่อให้สามารถใส่ HMC ได้
8. ที่ด้านหลังของชั้นวาง ทางด้านขวา ให้ดึงปลายด้านที่ว่างของสไลด์ออก รางไปทางด้านหลังและยึดหน้าแปลนของรางสไลด์เข้ากับชั้นวางโดยใช้สกรู M5 สองตัว ปล่อยให้รูสกรูตรงกลางเปิด
9. ทำซ้ำขั้นตอน “7” ในหน้า 8 และขั้นตอน “8” ในหน้า 8 เพื่อติดตั้ง ชุดรางสไลด์ด้านขวาบนด้านขวาของชั้นวาง
10. ที่ด้านหน้าของชั้นวาง ให้ติดตั้งเวิร์กสเตชัน HMC ในชั้นวางโดยทำตามขั้นตอน ต่อไปนี้:
    a. ถือเวิร์กสเตชัน HMC ในแนวระนาบ เสียบตัวยึดสไลด์ลงในรางสไลด์ HMC ที่คุณติดตั้งในขั้นตอนก่อนหน้า ดัน HMC ไปข้างหน้าจนกระทั่งหน้าแปลนที่ด้านหน้าของ HMC อยู่ ตรงกับรูสกรูเปิดที่ด้านหน้าของชั้นวาง
    b. เชื่อมต่อ HMC กับด้านซ้ายของกรอบโดยใช้สกรู M5 หนึ่งตัว ทำซ้ำขั้นตอนนี้กับทางด้านขวา ของชั้นวาง
11. ดำเนินการต่อด้วย “การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ” ในหน้า 9

การยึดรางกับโครงเครื่องและยึดกับชั้นวาง

คุณต้องติดตั้งรางบนโครงเครื่องและยึดกับชั้นวาง ใช้วิธีการนี้ เพื่อดำเนินการกับภารกิจนี้

เกี่ยวกับภารกิจนี้

ข้อควรสนใจ: เพื่อหลีกเลี่ยงความล้มเหลวของรางและอันตรายที่อาจเกิดขึ้นต่อตัวคุณเอง และเครื่อง ตรวจสอบให้แน่ใจว่าคุณมีรางและอุปกรณ์ติดตั้งที่ถูกต้อง สำหรับชั้นวาง ถ้าชั้นวางมีช่องค้ำรูปสี่เหลี่ยม หรือช่องค้ำ screw-thread ตรวจสอบให้แน่ใจว่า รางและอุปกรณ์ติดตั้งตรงกับช่องค้ำที่ใช้บน ชั้นวาง อย่าติดตั้งฮาร์ดแวร์ที่ไม่ตรงกันโดยใช้แหวนรองหรือ ตัวรอง หากคุณไม่มีรางและอุปกรณ์ติดตั้ง ที่ถูกต้องสำหรับชั้นวางของคุณ ให้ติดต่อผู้ตัวแทนจำหน่าย IBM ของคุณ

หมายเหตุ: หน่วย 1 EIA หน่วยในชั้นวางวัดโดยเพิ่มขึ้นตามแนวตั้งที่ 44.45 มม. (1.75 นิ้ว) ต่อหน่วย การเพิ่มขึ้น แต่ละ 44.45 มม. (1.75 นิ้ว) เรียกว่า “EIA.” ในบางประเทศ การเพิ่มที่เท่ากัน สามารถเรียกว่า “U.”

หมายเหตุ: ระบบต้องการพื้นที่ว่างยูนิตชั้นวาง 1 EIA (1U)

ตรวจสอบว่า คุณมีชิ้นส่วนที่จำเป็นเพื่อติดตั้งราง ชิ้นส่วนต่อไปนี้ ถูกรวมกับชุดของราง:

- 4 - สกรูหัวแฉก 6.35 มม. (0.25 นิ้ว)
- 2 - รางด้านใน
- 2 - รางรองรับ HMC
- 2 - Nut clips สำหรับรูยึด EIA แบบสี่เหลี่ยม
- 2 - Nut clips สำหรับรูยึด EIA แบบวงกลม
- 8 - สกรูหน้าแปลนหกเหลี่ยม M5

กระบวนการ

1. ถอดส่วนของรางออกจากแพ็กเกจและวางลงบนพื้นที่งาน
2. ระบุช่องว่าง 1U ในชั้นวางของ HMC
3. เมื่อต้องการยึดรางด้านในกับ HMC ให้ดำเนินการภารกิจต่อไปนี้:
   a. ระบุรางด้านในทางขวา
   b. จัดแนวรูบนรางด้านในทางขวาให้ตรงกับหมุดรางด้านในอยู่ทางด้านขวา ของ HMC ตรวจสอบให้แน่ใจว่าหมุดทั้งหมดอยู่ในแนวเดียวกันกับรูรางด้านใน
   c. ดันรางด้านในของ HMC ไปทางด้านหน้าของ HMC จนกระทั่งล็อคเข้าที่ จนสุด
   d. ยึดรางด้านในด้านขวากับด้านขวาของเวิร์กสเตชัน HMC โดยติดตั้ง สกรูแฉก 6.35 มม. (0.25 นิ้ว) สองตัวเข้ากับรูสกรู
   e. ทำซ้ำขั้นตอน 3.a - "3.d" ในหน้า 9 เพื่อติดตั้งรางด้านในด้านซ้ายกับด้านซ้าย ของเวิร์กสเตชัน HMC
4. ย้ายไปยังด้านหน้าของชั้นวาง ทางด้านซ้าย ให้ติดตั้ง nut clip หนึ่งตัวลงใน รูที่ขอบด้านหน้าของชั้นวางในสล็อต 1U ที่กำหนดไว้สำหรับ HMC

   หมายเหตุ: ชุดรางประกอบด้วย nut clip สำหรับรูทั้งแบบเหลี่ยมและแบบกลมของชั้นวาง ตรวจสอบให้แน่ใจว่า คุณใช้ nut clip ที่เหมาะสมที่เข้ากับรูในชั้นวาง
5. ย้ายไปยังด้านหลังของชั้นวาง ทางด้านซ้าย ให้ติดตั้ง nut clip หนึ่งตัวลงในรูตรงกลาง ที่ขอบด้านหน้าของชั้นวางในสล็อต 1U ที่กำหนดไว้สำหรับ HMC
6. ที่ด้านหน้าของชั้นวาง ให้ติดตั้งรางรองรับ HMC ในชั้นวางโดย ทำตามขั้นตอนต่อไปนี้:
   a. จัดแนวหมุดของรางรองรับด้านบนและด้านล่างของ nut clip ที่คุณติดตั้งในขั้นตอน ก่อนหน้า..
   b. ที่ด้านขวาของชั้นวาง ให้เชื่อมต่อหน้าแปลนที่ส่วนท้ายของรางรองรับเข้ากับ ขอบด้านหน้าของชั้นวางโดยใช้สกรู M5 สองตัวเข้าที่รูสกรูบนและล่าง โดยปล่อยให้รูสกรูตรงกลาง เปิดอยู่ ตรวจสอบให้แน่ใจว่าชุดรางหลวมเล็กน้อยที่ด้านหน้าของชั้นวาง เพื่อให้สามารถใส่ HMC ได้
7. ที่ด้านหลังของชั้นวางทางด้านขวา ให้ดึงปลายด้านที่ว่างของรางรองรับ ไปทางด้านหลังและยึดหน้าแปลนของรางรองรับเข้ากับชั้นวางโดยใช้สกรู M5 สองตัว โดยปล่อยให้รูสกรูตรงกลางเปิดอยู่
8. ทำซ้ำขั้นตอน "6" ในหน้า 9 และขั้นตอน "7" ในหน้า 9 เพื่อติดตั้งชุดรางรองรับ ด้านซ้ายบนด้านซ้ายของชั้นวาง
9. ที่ด้านหน้าของชั้นวาง ให้ติดตั้งเวิร์กสเตชัน HMC ในชั้นวางโดยทำตามขั้นตอน ต่อไปนี้:
   a. ถือเวิร์กสเตชัน HMC ในแนวระนาบ ใส่รางด้านในเข้ากับรางรองรับ HMC ที่คุณติดตั้งในขั้นตอนก่อนหน้า ดัน HMC ไปข้างหน้าจนกระทั่งหน้าแปลนที่ด้านหน้าของ HMC อยู่ ตรงกับรูสกรูเปิดที่ด้านหน้าของชั้นวาง
   b. เชื่อมต่อ HMC กับด้านซ้ายของกรอบโดยใช้สกรู M5 หนึ่งตัว ทำซ้ำขั้นตอนนี้กับทางด้านขวา ของชั้นวาง

   หมายเหตุ: หากมี ให้ถอดขายึดสำหรับการขนส่งสีส้มที่ติดอยู่ที่ด้านหลังของระบบ และใส่สกรูกลับเข้าไปใหม่
10. ดำเนินการต่อด้วย "การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ" ในหน้า 9

การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ

ติดตั้งระบบบนรางและเชื่อมต่อและเดินสายไฟ

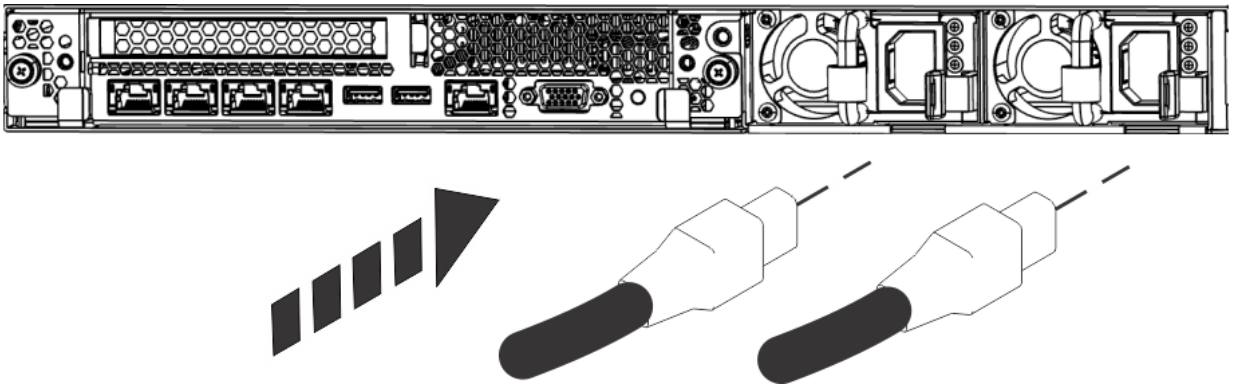
เกี่ยวกับภารกิจนี้

ข้อควรระวัง: ชิ้นส่วนหรือยูนิตนี้หนักมาก แต่มีน้ำหนักน้อยกว่า 18 กก. (39.7 ปอนด์) โปรดใช้ความระมัดระวังขณะยก, ถอด, หรือติดตั้งชิ้นส่วนหรือยูนิตนี้ (C008)

กระบวนการ

1. ถอดฟิลม์พลาสติกเคลือบออกจากด้านบนแชสซีระบบ
2. เสียบสายไฟเข้ากับแหล่งจ่ายไฟ

   หมายเหตุ: ห้ามเชื่อมต่อปลายอีกด้านของสายไฟเข้ากับแหล่งจ่ายไปในขณะนี้



รูปที่ 2. การเสียบสายไฟเข้ากับแหล่งจ่ายไฟ

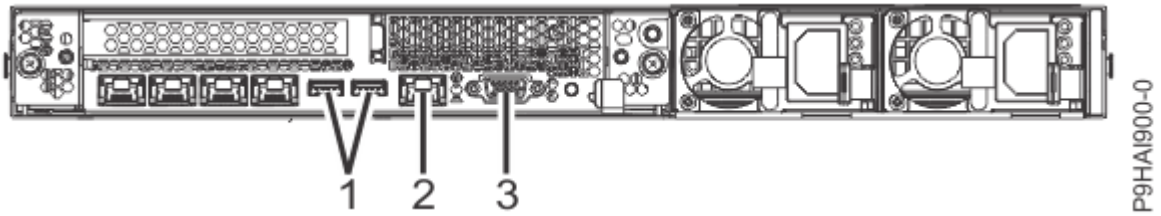
3. ขันตัวยึด hook-and-loop ให้แน่นเพื่อยึดสายไฟ
4. ดำเนินการต่อกับ “การเดินสายเคเบิล 7063-CR2 HMC ที่ติดตั้งในชั้นวาง” ในหน้า 10

การเดินสายเคเบิล 7063-CR2 HMC ที่ติดตั้งในชั้นวาง

ศึกษาเกี่ยวกับวิธีการติดตั้งHardware Management Console (HMC) ที่ประกอบเข้ากับชั้นวางของคุณ

กระบวนการ

1. ตรวจสอบว่า HMC ถูกติดตั้งในชั้นวางและสายไฟถูกเสียบใน ตัวจ่ายไฟ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ” ในหน้า 9 หลังจากคุณติดตั้ง HMC ในชั้นวาง ให้ดำเนินการขั้นตอนถัดไป
2. เชื่อมต่อคีย์บอร์ด มอนิเตอร์ และเมาส์



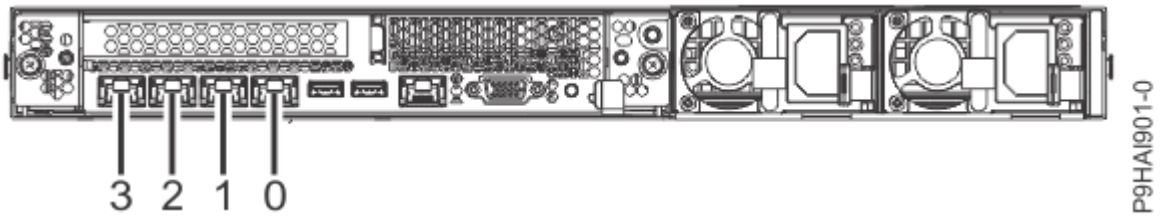
รูปที่ 3. พอร์ตด้านหลัง

ตารางที่ 4. พอร์ตอินพุตและเอาต์พุต

หมายเลข ID	รายละเอียด
1	USB 2.0 ใช้สำหรับคีย์บอร์ดและเมาส์
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Video Graphics Array (VGA) ที่ใช้สำหรับมอนิเตอร์ เฉพาะการตั้งค่า 1024 x 768 ที่ 60 Hz VGA เท่านั้นที่สนับสนุน สนับสนุนสายเคเบิลสูงสุดถึง 3 เมตรเท่านั้น

หมายเหตุ: ระบบมีพอร์ต USB ด้านหน้าสองพอร์ตที่คุณสามารถใช้

3. เชื่อมต่อพอร์ต Ethernet Intelligent Platform Management Interface (IPMI) กับเครือข่าย



รูปที่ 4. พอร์ตอีเทอร์เน็ต

ตารางที่ 5. พอร์ตอีเทอร์เน็ต	
หมายเลข ID	**รายละเอียด**
0	Intelligent Platform Management Interface (IPMI) ของอีเทอร์เน็ตแบบแบ่งใช้และการเชื่อมต่อ HMC Network
1, 2 และ 3	การเชื่อมต่อเครือข่าย HMC

หมายเหตุ: การเชื่อมต่อนี้ต้องการเข้าถึง baseboard management controller (BMC) บน HMC การเข้าถึง BMC จำเป็นสำหรับภารกิจบริการและเพื่อจัดการกับเฟิร์มแวร์ HMC สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 34

คำเตือน: ผลิตภัณฑ์นี้ อาจไม่ได้รับการรับรองในประเทศของคุณสำหรับการเชื่อมต่อด้วย สื่อใด ๆ ก็ตามไปยังอินเตอร์เฟสของเครือข่ายโทรคมนาคมแบบพับลิก การรับรองเพิ่มเติมอาจเป็นข้อบังคับตามกฎหมายก่อนทำการเชื่อมต่อ ดังกล่าว โปรดติดต่อ IBM สำหรับข้อมูลเพิ่มเติม

4. เชื่อมต่อสายอีเทอร์เน็ตที่ใช้สำหรับการเชื่อมต่อกับ ระบบที่ถูกจัดการ

   Notes:

   - หากคุณกำลังใช้การเชื่อมต่อแบบแบ่งใช้สำหรับ IPMI และ HMC สายเคเบิลเส้นเดียวไปยังพอร์ต 0 ในรูปที่ 2 สามารถตอบสนองข้อกำหนดทั้งสำหรับ IPMI และ HMC
   - เมื่อต้องการศึกษาเพิ่มเติมเกี่ยวกับการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 34
5. หากระบบที่ถูกจัดการได้รับการติดตั้งแล้ว คุณจะสามารถตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแอ็คทีฟอยู่หรือไม่ โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่ถูกจัดการในขณะที่ขั้นตอนติดตั้งกำลังดำเนินไป
6. เสียบสายไฟของระบบและสายไฟสำหรับอุปกรณ์พ่วงต่ออื่น ๆ เข้ากับแหล่งจ่ายไฟกระแสสลับ (AC)
7. ตรวจสอบสถานะกำลังไฟโดยใช้ LED แหล่งจ่ายไฟเป็นตัวบ่งชี้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ LED บนระบบ 7063-CR2 LED บนระบบ 7063-CR2
8. กดปุ่ม เปิด/ปิด เพื่อเริ่มระบบ ไฟเปิดเครื่องจะหยุดกะพริบ และยังคงติดอยู่เพื่อบ่งชี้ว่าระบบเปิดอยู่

ผลลัพธ์

ถัดไป คุณจำเป็นต้องติดตั้งและกำหนดคอนฟิกซอฟต์แวร์ HMC ของคุณ ดำเนินการต่อด้วย “การกำหนดคอนฟิก 7063-CR2 HMC” ในหน้า 11

การกำหนดคอนฟิก 7063-CR2 HMC

ศึกษาเกี่ยวกับวิธีการติดตั้งและกำหนดคอนฟิก Hardware Management Console (HMC)

ตรวจสอบเวอร์ชัน HMC ที่จัดส่งมาพร้อมกับ HMC ของคุณ หากต้องการทราบวิธีการดูเวอร์ชัน และรีลีสของรหัสเครื่อง HMC โปรดดูที่ ตรวจสอบเวอร์ชันของ HMC ที่เป็น ถูกส่งมาพร้อมกับ HMC ของคุณ คุณสามารถดาวน์โหลด HMC เวอร์ชันล่าสุดที่ พร้อมใช้งานจากเว็บไซต์ Fix Central ใช้สื่อบันทึกแบบถอดออกได้ (เช่น DVD หรือ USB) เพื่อสร้างไฟล์ ISO ที่สามารถบูตได้จากแพ็กเกจ HMC (อิมเมจ ISO)

หมายเหตุ: ตารางต่อไปนี้อธิบายข้อมูลการล็อกอินที่กำหนดไว้ล่วงหน้า (ดีฟอลต์) สำหรับอินเตอร์เฟส HMC และ BMC

ตารางที่ 6.			
คอนโซลหรืออินเตอร์เฟส	**ID ดีฟอลต์**	**รหัสผ่านดีฟอลต์**	**รายละเอียด**
BMC (OpenBMC)	`root`	`0penBmc`	ID ผู้ใช้รูทและรหัสผ่านใช้เพื่อล็อกอินเข้าสู่ BMC ในครั้งแรก
HMC	`hscroot`	`abc123`	ID ผู้ใช้ hscroot และรหัสผ่านจะถูกใช้เพื่อล็อกออนเข้าสู่ HMC ในครั้งแรก รหัสผ่านจะคำนึงถึงขนาดตัวพิมพ์และสามารถใช้โดยสมาชิกของบทบาทผู้ดูแลระดับสูง
HMC	`root`	`passw0rd`	ID ผู้ใช้รูทและรหัสผ่านจะถูกใช้โดยผู้ให้บริการ เพื่อดำเนินการกับขั้นตอนการดูแลรักษา ซึ่งไม่สามารถใช้เพื่อล็อกออนเข้าสู่ HMC ได้

หมายเหตุ: การติดตั้งต่อไปนี้ถูกแสดงไว้ตามตัวอย่าง

การติดตั้ง HMC โดยใช้แฟล็ชไดร์ฟ USB

เมื่อต้องการติดตั้ง HMC โดยใช้แฟล็ชไดร์ฟ USB ให้ทำตามขั้นตอนต่อไปนี้สำหรับระบบ Linux®:

หมายเหตุ: ตัวอย่างในระบบปฏิบัติการอื่น โปรดดูที่:

- Windows: สื่อบันทึกการติดตั้งแบบแฟลช USB (Windows)
- Mac: สื่อบันทึกการติดตั้งแบบแฟลช USB (macOS)

1. ดาวน์โหลด HMC เวอร์ชันที่คุณต้องการจากเว็บไซต์ Fix Central
2. รันคำสั่งต่อไปนี้: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (โดยที่ **sdx** เป็นชื่อของไดร์ฟ USB)

   หมายเหตุ: คุณสามารถรันคำสั่ง Linux `lsblk` เพื่อระบุชื่ออุปกรณ์ ของไดร์ฟ USB เมื่ออุปกรณ์ถูกเชื่อมต่อ
3. เสียบไดร์ฟ USB และเปิดระบบ

   หมายเหตุ: ไดร์ฟ USB ต้องมีพื้นที่อย่างน้อย 8 GB ไดร์ฟ USB บางไดร์ฟอาจไม่กว้างพอดีกับ พอร์ต USB ที่ด้านหลังของระบบ ทดสอบความพอดีของไดร์ฟ USB ก่อนที่คุณ จะดำเนินการต่อ
4. เมื่อเมนู Petitboot ถูกแสดง ให้เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **USB**

การติดตั้ง HMC โดยใช้สื่อบันทึกเสมือนจาก BMC

เมื่อต้องการติดตั้ง HMC โดยใช้สื่อบันทึกเสมือนจาก BMC ให้ทำตามขั้นตอนต่อไปนี้:

1. เปิดเว็บเบราว์เซอร์ที่สนับสนุน ในแถบแอดเดรส พิมพ์ IP แอดเดรสของ BMC ที่คุณต้องการ เชื่อมต่อ ตัวอย่างเช่น คุณสามารถใช้รูปแบบ `https://<BMC IP>` ใน แถบแอดเดรสของเว็บเบราว์เซอร์
2. จากหน้าต่าง **OpenBMC logon** พิมพ์แอดเดรส **Host** ของ BMC และ **Username** และ **Password** ที่ ถูกมอบหมายให้กับคุณ

   หมายเหตุ: ID ผู้ใช้ดีฟอลต์คือ `root` และรหัสผ่านดีฟอลต์คือ `0penBmc`

   หากคุณใช้เฟิร์มแวร์ระดับ OP940.01 หรือใหม่กว่า รหัสผ่าน root จะหมดอายุตามดีฟอลต์ คุณต้องเปลี่ยนรหัสผ่านดีฟอลต์ก่อนจึงจะสามารถเข้าถึง BMC ได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเปลี่ยนรหัสผ่านดีฟอลต์ที่หมดอายุ โปรดดูที่ การตั้งค่า รหัสผ่าน

   หากคุณลืมรหัสผ่าน คุณสามารถรีเซ็ตให้เป็นค่าจากโรงงานได้ ของระบบเพื่อกู้คืนรหัสผ่านดีฟอลต์ เมื่อต้องการรีเซ็ตระบบ โปรดดูที่ การดำเนินการรีเซ็ตให้เป็นค่าจากโรงงาน

3. คลิก **Log in**
4. เลือก **Server control**.
5. เลือก **Virtual Media**.
6. คลิก **Choose file**.
7. ค้นหา HMC Recovery media ISO และคลิก **Open**
8. คลิก **Start**
9. เปิด ระบบ
10. เมื่อเมนู Petitboot ถูกแสดง ให้เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **USB**

การติดตั้ง HMC โดยใช้ DVD ไดร์ฟภายนอกที่เชื่อมต่อกับ USB

เมื่อต้องการติดตั้ง HMC โดยใช้ไดร์ฟ DVD ภายนอกที่เชื่อมต่อกับ USB ให้ทำตามขั้นตอนต่อไปนี้:

1. ดาวน์โหลดเวอร์ชันการกู้คืนของ HMC ที่คุณต้องการจากเว็บไซต์ Fix Central
2. เขียนอิมเมจ HMC recovery DVD ลงในสื่อบันทึก DVD-R DL เป็นอิมเมจ
3. ปิดกำลังไฟ HMC
4. เชื่อมต่อไดร์ฟ USB DVD ภายนอกกับ HMC และใส่ DVD การกู้คืน HMC

   หมายเหตุ: คุณอาจต้องเชื่อมต่อ ไดร์ฟ USB DVD กับแหล่งจ่ายไฟภายนอกหรือใช้สายเคเบิล USB ตัว Y เพื่อเชื่อมต่อกับ พอร์ต USB เพื่อเติมเพื่อให้มีกำลังไฟเพียงพอสำหรับไดร์ฟ DVD
5. Power บน HMC

   หมายเหตุ: หน้าจอมอนิเตอร์อาจไม่แสดงสัญญาณระหว่างการเริ่มทำงาน กระบวนการอาจ ใช้เวลา 2 ถึง 3 นาทีก่อนที่หน้าจอมอนิเตอร์จะแสดงสถานะใด ๆ
6. เมื่อ Petitboot bootloader เริ่มทำงาน ให้หยุดการบู๊ตอัตโนมัติ

   หมายเหตุ: ซึ่งจะบังคับใช้ การหมดเวลา 10 วินาที หากไม่มีการดำเนินการใด ๆ ภายใน 10 วินาที ระบบจะพยายามบู๊ตจาก ฮาร์ดดิสก์ไดร์ฟ
7. รอจนกว่าอุปกรณ์ **CD/DVD** จะปรากฏในเมนู Petitboot

   หมายเหตุ: กระบวนการนี้ อาจใช้เวลาประมาณ 1นาที
8. เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **CD/DVD**

การติดตั้ง 7063-CR1 ในชั้นวาง

ศึกษาวิธีการติดตั้ง 7063-CR1 Hardware Management Console (HMC) ในชั้นวาง

คุณสามารถดูเอกสารคู่มือการติดตั้งแบบออนไลน์ หรือคุณสามารถพิมพ์ ข้อมูลเดียวกันในเวอร์ชัน PDF เมื่อต้องการดูหรือพิมพ์เวอร์ชัน PDF โปรดดูที่ การติดตั้งและ การกำหนดค่า Hardware Management Console

สิ่งที่จำเป็นต้องมีสำหรับการติดตั้งระบบ 7063-CR1 บนชั้นวาง

ใช้ข้อมูลเพื่อทำความเข้าใจกับสิ่งที่จำเป็นต้องมีที่จำเป็นสำหรับการติดตั้ง ระบบ

เกี่ยวกับภารกิจนี้

ข้อควรระวัง:

หรือ

หรือ

ชิ้นส่วนหรือยูนิตนี้มีน้ำหนักระหว่าง 18 ถึง 32 กก. (70.5 ถึง 121.2 ปอนด์) ควรใช้คนสองคนเพื่อยกชิ้นส่วนหรือยูนิตนี้อย่างปลอดภัย (C009)

คุณอาจต้องอ่าน เอกสารต่อไปนี้ก่อนที่คุณจะเริ่มต้นการติดตั้งเซิร์ฟเวอร์:

- เวอร์ชันล่าสุดของเอกสารนี้ถูกเก็บไว้แบบออนไลน์ โปรดดูที่ การติดตั้ง 7063-CR1 เข้ากับชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm)
- เมื่อต้องการวางแผนการติดตั้งเซิร์ฟเวอร์ของคุณ โปรดดูที่ การวางแผนไซต์และฮาร์ดแวร์

กระบวนการ

ตรวจสอบให้แน่ใจว่า คุณมีรายการต่อไปนี้ก่อนที่จะเริ่มต้นการติดตั้ง:

- ไขควงแฉกเบอร์ 2
- ไขควงหัวแบน
- ที่ตัดกล่อง
- สายรัดข้อมือป้องกันไฟฟ้าสถิต (ESD)
- ชั้นวางที่มีที่ว่างหนึ่งหน่วย Electronic Industries Association (EIA) (1U)

หมายเหตุ: หากคุณไม่ได้ติดตั้งชั้นวาง ให้ติดตั้งชั้นวาง สำหรับคำแนะนำ โปรดดูที่ ชั้นวางและคุณลักษณะชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm)

การจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ

ใช้ข้อมูลนี้เพื่อจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ

กระบวนการ

1. ตรวจสอบว่าคุณได้รับทุกกล่อง ที่คุณสั่งซื้อ
2. นำคอมโพเนนต์เซิร์ฟเวอร์ออกจากกล่องตามต้องการ
3. รายการชิ้นส่วนและตรวจสอบว่าคุณได้รับชิ้นส่วนทั้งหมดที่คุณสั่งซื้อ ก่อนที่คุณจะติดตั้งแต่ละคอมโพเนนต์ของเซิร์ฟเวอร์

   หมายเหตุ:

   ข้อมูลใบสั่งซื้อ รวมอยู่กับผลิตภัณฑ์ของคุณ คุณยังสามารถได้รับข้อมูลการสั่งซื้อจาก ตัวแทนด้านการตลาดของคุณ หรือ IBM Business Partner

   ถ้าชิ้นส่วนไม่ถูกต้อง หายไป หรือเสียหาย ให้ติดต่อรีซอร์สใด ๆ ต่อไปนี้:

   - ตัวแทนจำหน่าย IBM
   - สายข้อมูลอัตโนมัติเกี่ยวกับการผลิต IBM Rochester ที่ 1-800-300-8751 (สหรัฐอเมริกาเท่านั้น)
   - เว็บไซต์ ไดเร็กทอรีของ ผู้ติดต่อทั่วโลก (http://www.ibm.com/planetwide) เลือก ที่ตั้งของคุณเพื่อดูข้อมูลผู้ติดต่อฝ่ายสนับสนุนและบริการ

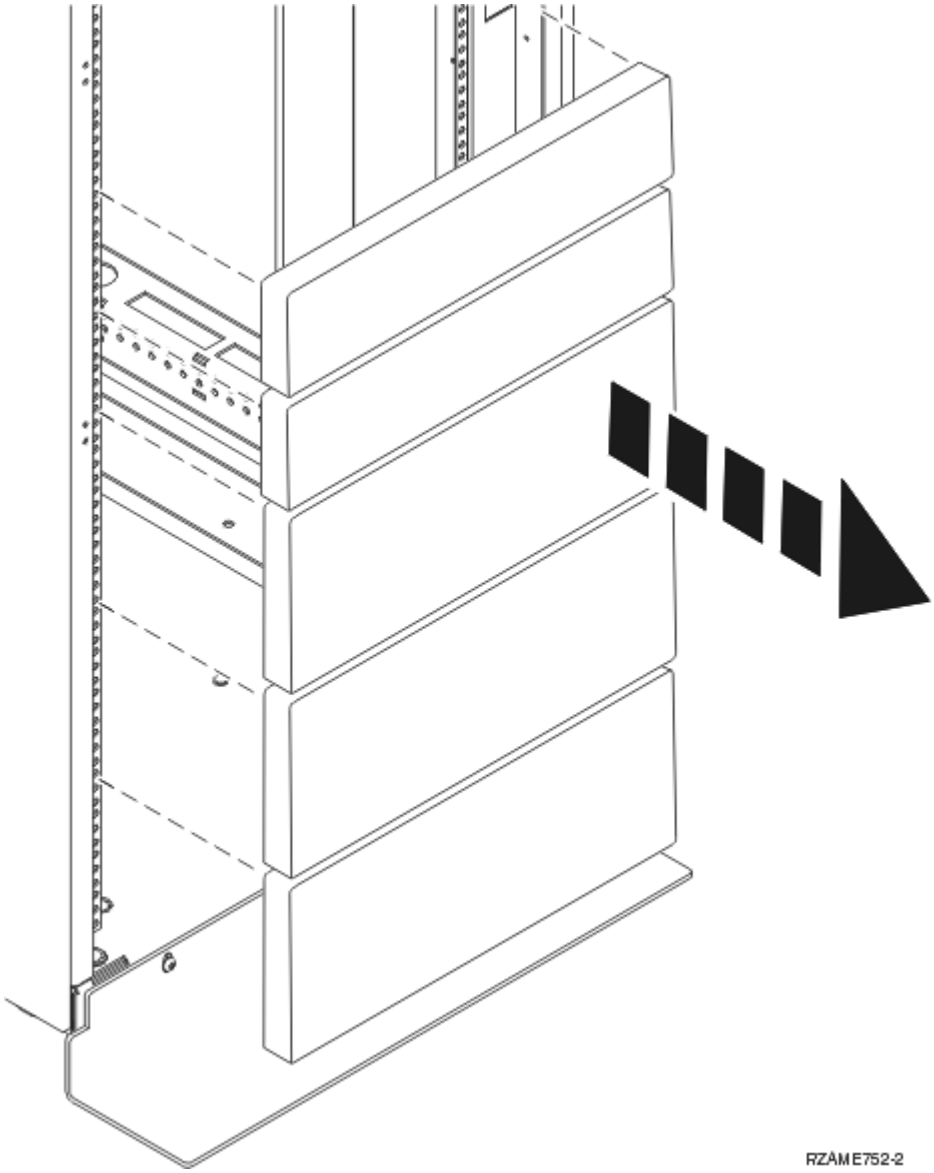
การกำหนดและทำเครื่องหมายตำแหน่งในชั้นวางสำหรับระบบ 7063-CR1

คุณอาจจำเป็นต้องกำหนดตำแหน่งที่ต้องติดตั้งยูนิตระบบลงในชั้นวาง

กระบวนการ

1. อ่าน หมายเหตุความปลอดภัยของชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm)
2. ระบุตำแหน่งที่จะวาง ยูนิตระบบในชั้นวาง เมื่อคุณวางแผนสำหรับการติดตั้งยูนิต ระบบในชั้นวาง ให้พิจารณาข้อมูลต่อไปนี้:
   - วางยูนิตที่ใหญ่กว่าและหนักกว่าใน ส่วนล่างของชั้นวาง
   - วางแผนติดตั้งยูนิตระบบในส่วนล่างของชั้นวางก่อน
   - บันทึกตำแหน่ง Electronic Industries Alliance (EIA) ในแผนของคุณ

3. ถ้าจำเป็น ให้ถอดพาเนลฟิลเลอร์ออก เพื่อให้สามารถเข้าถึงด้านในของส่วนแนบชั้นวางที่คุณวางแผนจะ วางยูนิต ดังแสดงใน รูปที่ 5 ในหน้า 15



รูปที่ 5. การถอดพาเนลฟิลเลอร์

4. กำหนดตำแหน่งที่จะวางระบบในชั้นวาง บันทึกตำแหน่ง EIA
5. หันหน้าเข้าหาชั้นวางและทำงานจากด้านขวา ใช้เทป ปากกาทำเครื่องหมาย หรือดินสอ เพื่อทำเครื่องหมายที่รูด้านล่างของยูนิต EIA แต่ละตัว
6. ทำซ้ำขั้นตอน “5” ในหน้า 15 สำหรับรูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
7. ไปที่ด้านหลังของชั้นวาง
8. ที่ด้านขวา, ให้หายูนิต EIA ที่ตรงกับยูนิต EIA ด้านล่างซึ่งทำเครื่องหมายอยู่บนด้านหน้าของชั้นวาง
9. ทำเครื่องหมายที่ยูนิต EIA ด้านล่าง
10. ทำเครื่องหมายรูที่ตรงกันทางด้านซ้ายของชั้นวาง

การยึดรางกับโครงเครื่องและยึดกับชั้นวาง

คุณต้องติดตั้งรางบนโครงเครื่องและยึดกับชั้นวาง ใช้วิธีการนี้ เพื่อดำเนินการกับภารกิจนี้

เกี่ยวกับภารกิจนี้

ข้อควรสนใจ: เพื่อหลีกเลี่ยงความล้มเหลวของรางและอันตรายที่อาจเกิดขึ้นต่อตัวคุณเอง และเครื่อง ตรวจสอบให้แน่ใจว่าคุณมีรางและอุปกรณ์ติดตั้งที่ถูกต้อง สำหรับชั้นวาง ถ้าชั้นวางมีช่องค้ำรูปสี่เหลี่ยม หรือช่องค้ำ screw-thread ตรวจสอบให้แน่ใจว่า รางและอุปกรณ์ติดตั้งตรงกับช่องค้ำที่ใช้บน ชั้นวาง อย่าติดตั้งฮาร์ดแวร์ที่ไม่ตรงกันโดยใช้แหวนรองหรือ ตัวรอง หากคุณไม่มีรางและอุปกรณ์ติดตั้ง ที่ถูกต้องสำหรับชั้นวางของคุณ ให้ติดต่อผู้ตัวแทนจำหน่าย IBM ของคุณ

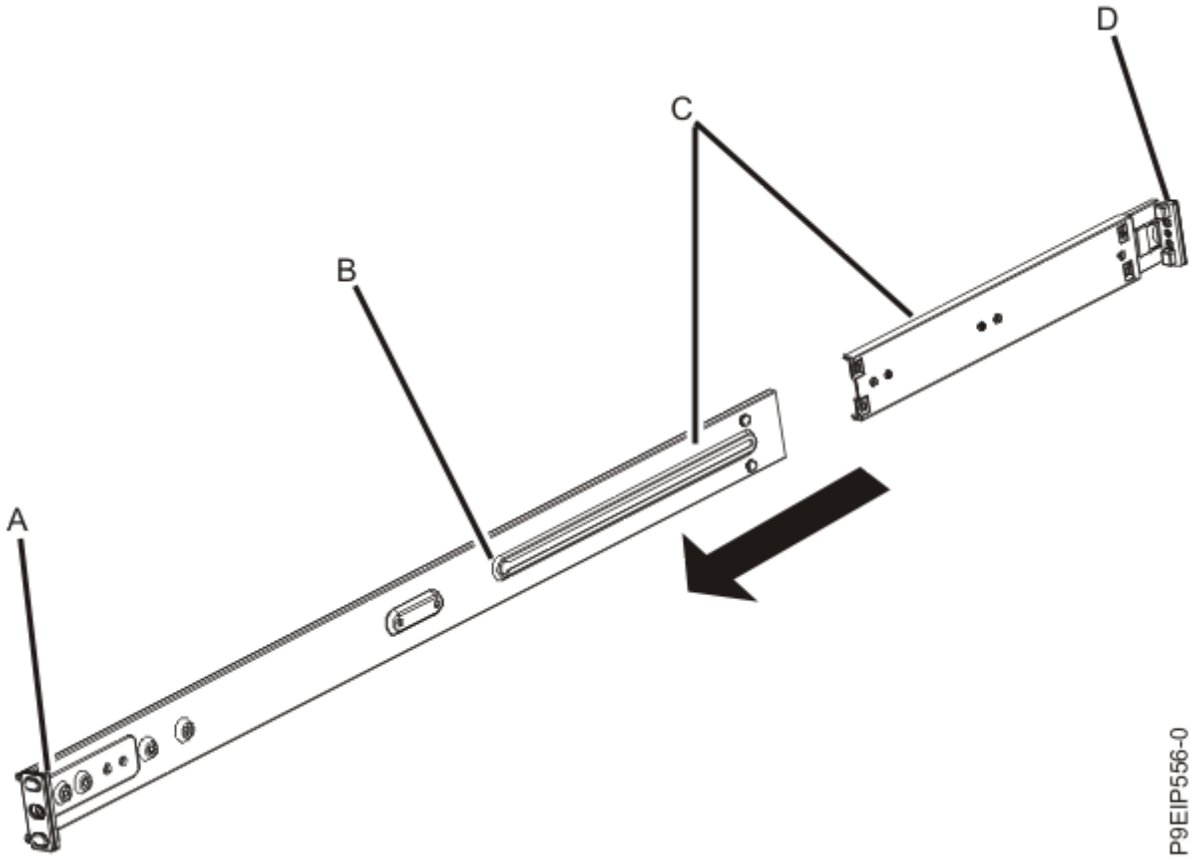
หมายเหตุ: ระบบต้องการพื้นที่ว่างยูนิตชั้นวาง 1 EIA (1U)

ตรวจสอบว่า คุณมีชิ้นส่วนที่จำเป็นเพื่อติดตั้งราง ชิ้นส่วนต่อไปนี้ ถูกรวมกับชุดของราง:

- สกรูสำหรับรางสไลด์ ใช้เพื่อยึดชิ้นส่วนสองชิ้นของรางสไลด์แต่ละชิ้น
- สกรูสำหรับชั้นวางรางสไลด์ ใช้เพื่อยึดรางกับชั้นวาง
- ราง
- สกรู 10 - 32 x 0.635 ซม. (0.25 นิ้ว) ใช้เพื่อยึดรางกับโครงเครื่อง

กระบวนการ

1. ถอดส่วนของรางออกจากแพ็กเกจและวางลงบนพื้นที่งาน
2. เปลี่ยนหมุนสี่เหลี่ยมของชั้นวางราง (**A**) และ (**D**) ด้วยหมุนกลมชั้นวางราง
3. เชื่อมต่อชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวางแต่ละชิ้น เมื่อต้องการเชื่อมต่อชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวาง ให้ดำเนินการดังต่อไปนี้:
   a. ระบุชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวางด้านซ้าย จัดตำแหน่งชิ้นส่วนที่สั้นและชิ้นส่วนที่ยาว (**C**) ตรวจสอบให้แน่ใจว่า หมุดสำหรับรางชั้นวางอยู่ในตำแหน่งเดียวกับ (**A**) และ (**D**)



   b. ชิ้นส่วนที่สั้นกว่าของรางสไลด์ชั้นวางจะมีหมุดโลหะอยู่ ใส่หมุดลงในช่องที่อยู่ในชิ้นส่วนที่ยาวกว่า ของรางสไลด์ชั้นวาง (**B**) เลื่อนชิ้นส่วนที่สั้นกว่าของรางชั้นวางเข้าไปในชิ้นส่วนที่ยาวกว่า ของรางชั้นวาง
   c. จัดตำแหน่งช่องให้ลงในชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวาง ใช้ไขควงแฉก เชื่อมต่อสองส่วนโดยคลายสกรูรางสองตัวผ่านช่องใน รางสไลด์ของชั้นวาง

หมายเหตุ: ห้ามขันสกรูรางสไลด์ชั้นวางให้แน่น

d. ทำซ้ำขั้นตอนเหล่านี้สำหรับรางสไลด์ด้านขวา

4. ติดตั้งรางสไลด์ชั้นวางลงในชั้นวาง

a. ย้ายไปยังด้านหน้าของชั้นวาง

b. เลือกรางสไลด์ชั้นวางด้านซ้าย และหายูนิต EIA ที่คุณได้ทำเครื่องหมายไว้ก่อนหน้านี้ รางสไลด์แต่ละด้าน ยังถูกทำเครื่องหมาย **Back** เพื่อกำหนดด้านหลังของชั้นวาง ตรวจสอบให้แน่ใจ คุณกำลังยึดจุดปลายด้านหน้าของ รางสไลด์ชั้นวาง

c. ขยายรางจากด้านหน้าของชั้นวางไปทางด้านหลังของชั้นวาง และจัดตำแหน่งหมุดรางสไลด์ชั้นวาง ให้ตรงกับช่องในหน้าแปลนชั้นวางที่คุณได้ทำเครื่องหมายไว้ก่อนหน้านี้

d. ดันหมุดรางชั้นวางลงในหน้าแปลนชั้นวางด้านหลังจนกว่าแลตช์รางชั้นวางด้านหลัง ล็อกอยู่ในตำแหน่ง

e. ดึงด้านหน้าของรางชั้นวางไปทางด้านหน้าของหน้าแปลนรางชั้นวาง จัดตำแหน่งหมุดรางสไลด์ ให้ตรงกับช่องในหน้าแปลนราง และดึงจนกว่าแลตช์รางสไลด์จะล็อกอยู่ในตำแหน่ง

f. ใช้ไขควรเพื่อขันสกรูรางที่คุณติดตั้งในขั้นตอนที่ 2 ให้แน่น

หมายเหตุ: คุณอาจต้องใช้ช่องว่าง 2U เพื่อเข้าถึงและขันสกรูรางให้แน่น

g. ทำซ้ำขั้นตอนที่ 4a - 4f สำหรับรางเลื่อนด้านขวา

การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ

ติดตั้งระบบบนรางและเชื่อมต่อและเดินสายไฟ

เกี่ยวกับภารกิจนี้

ข้อควรระวัง:

หรือ

หรือ

ชิ้นส่วนหรือยูนิตนี้มีน้ำหนักระหว่าง 18 ถึง 32 กก. (70.5 ถึง 121.2 ปอนด์) ควรใช้คนสองคนเพื่อยกชิ้นส่วนหรือยูนิตนี้อย่างปลอดภัย (C009)

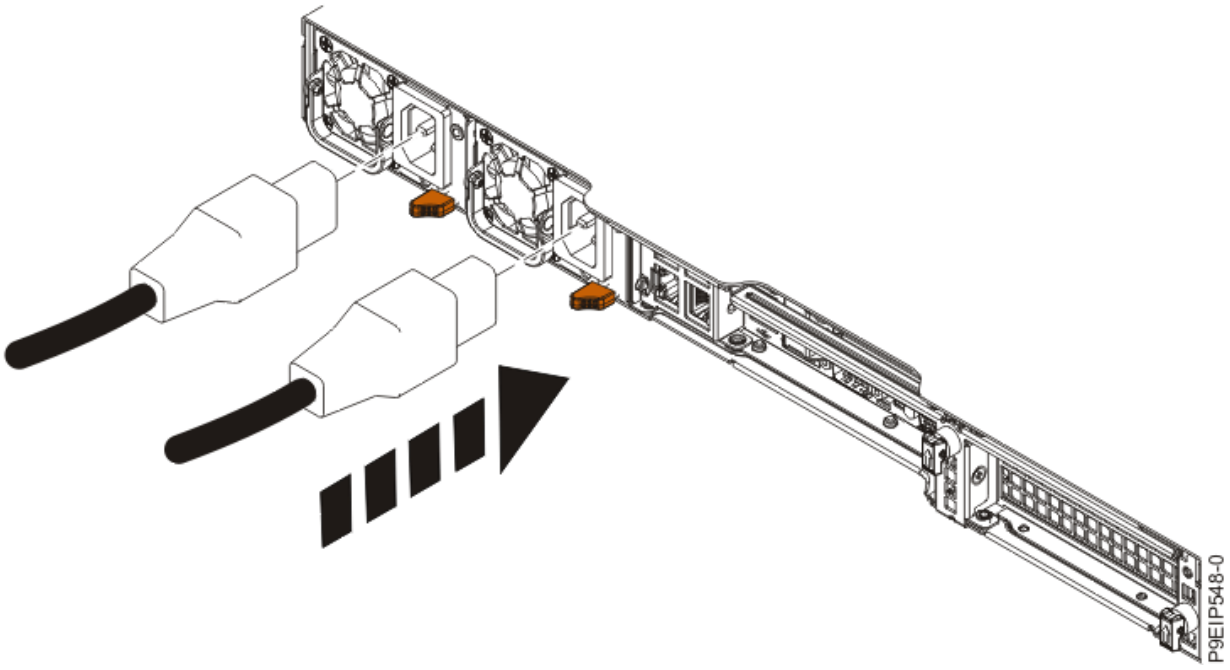
กระบวนการ

1. ถอดฟิลม์พลาสติกเคลือบออกจากด้านบนโครงเครื่องของระบบ
2. ย้ายไปยังด้านหน้าของชั้นวาง
3. ใช้ 2 คนแต่ละคนที่แต่ละด้านของระบบ ยกระบบและจัดตำแหน่งรางของโครงเครื่องของระบบ บนแต่ละด้านของโครงเครื่องกับรางเลื่อนของชั้นวาง
4. ค่อย ๆ ดันระบบเข้าไปทางด้านหลังของชั้นวาง
5. ยึดระบบกับชั้นวางโดยการหมุนสกรูผ่านที่จับบนแต่ละด้าน ของโครงเครื่อง

หมายเหตุ: คุณต้องใช้ washer ที่มีสกรู เลื่อน washer ลงบนสกรูยาวสองตัว (1.5 ซม. (0.59 นิ้ว)) ที่มาพร้อมกับชุดราง หมุนสกรูด้วย washer ทั้งด้านขวาและซ้าย ของระบบด้านหน้า

6. เสียบสายไฟเข้ากับแหล่งจ่ายไฟ

หมายเหตุ: ห้ามเชื่อมต่อปลายอีกด้านของสายไฟเข้ากับแหล่งจ่ายไปในขณะนี้



รูปที่ 6. การเสียบสายไฟเข้ากับแหล่งจ่ายไฟ

7. ดำเนินการต่อด้วย “การเดินสายเคเบิล 7063-CR1 HMC ที่ติดตั้งในชั้นวาง” ในหน้า 18

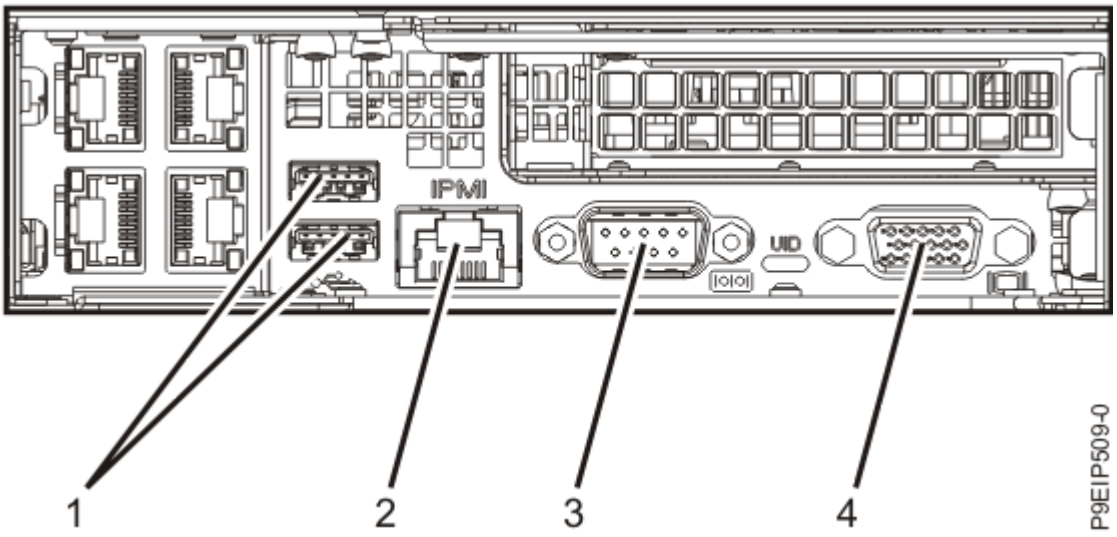
การเดินสายเคเบิล 7063-CR1 HMC ที่ติดตั้งในชั้นวาง

ศึกษาเกี่ยวกับวิธีการติดตั้งHardware Management Console (HMC) ที่ประกอบเข้ากับชั้นวางของคุณ

กระบวนการ

1. ตรวจสอบว่า HMC ถูกติดตั้งในชั้นวางและสายไฟถูกเสียบใน ตัวจ่ายไฟ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ” ในหน้า 17 หลังจากคุณติดตั้ง HMC ในชั้นวาง ให้ดำเนินการขั้นตอนถัดไป

   หมายเหตุ: หากมีปลั๊กอุดพอร์ตที่คุณจำเป็นต้องใช้ที่ด้านหลังของระบบ ให้ถอดและทิ้งไป ฝาครอบพอร์ตทำให้แน่ใจว่าคุณได้รับการเตือนว่าคุณต้องรีเซ็ตรหัสผ่าน ผู้ดูแลระบบ บนระบบที่ถูกจัดการของคุณเมื่อ IPL ระบบเริ่มต้น
2. เชื่อมต่อคีย์บอร์ด มอนิเตอร์ และเมาส์

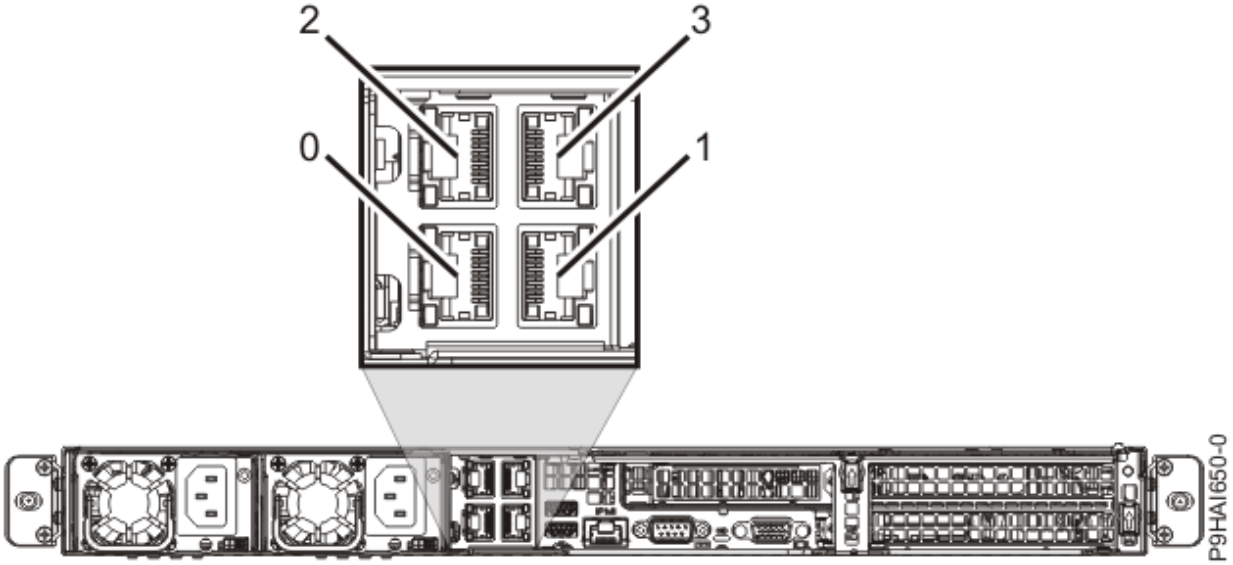


รูปที่ 7. พอร์ตด้านหลัง

ตารางที่ 7. พอร์ตอินพุตและเอาต์พุต	
หมายเลข ID	**รายละเอียด**
1	USB 2.0 ใช้สำหรับคีย์บอร์ดและเมาส์
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Serial IPMI
4	Video Graphics Array (VGA) ที่ใช้สำหรับมอนิเตอร์เฉพาะค่าติดตั้ง 1024 x 768 ที่ 60 Hz VGA เท่านั้นที่สนับสนุน สนับสนุนสายเคเบิลสูงสุดถึง 3 เมตรเท่านั้น

หมายเหตุ: ระบบมีพอร์ต USB ด้านหน้าสองพอร์ตที่คุณสามารถใช้ พอร์ตอนุกรมด้านหน้า จะใช้งานไม่ได้

3. เชื่อมต่อสายอีเทอร์เน็ตที่ใช้สำหรับการเชื่อมต่อกับ ระบบที่ถูกจัดการ



รูปที่ 8. พอร์ตอีเทอร์เน็ต

หมายเหตุ: เมื่อต้องการศึกษาเพิ่มเติมเกี่ยวกับการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 34

4. หากระบบที่ถูกจัดการได้รับการติดตั้งแล้ว คุณจะสามารถตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแอ็คทีฟอยู่หรือไม่ โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่ถูกจัดการในขณะที่ขั้นตอนติดตั้งกำลังดำเนินไป
5. เชื่อมต่อพอร์ต Ethernet Intelligent Platform Management Interface (IPMI) กับเครือข่าย

   หมายเหตุ: การเชื่อมต่อนี้ต้องการเข้าถึง baseboard management controller (BMC) บน HMC การเข้าถึง BMC จำเป็นสำหรับภารกิจบริการและเพื่อจัดการกับเฟิร์มแวร์ HMC สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 34

6. เสียบสายไฟของระบบและสายไฟสำหรับอุปกรณ์พ่วงต่ออื่น ๆ เข้ากับแหล่งจ่ายไฟกระแสสลับ (AC)
7. ตรวจสอบสถานะกำลังไฟโดยใช้ LED แหล่งจ่ายไฟเป็นตัวบ่งชี้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ LED บนระบบ 7063-CR1 LED บนระบบ 7063-CR1

ผลลัพธ์

ถัดไป คุณจำเป็นต้องติดตั้งและกำหนดคอนฟิกซอฟต์แวร์ HMC ของคุณ ดำเนินการต่อกับ “การกำหนดคอนฟิก 7063-CR1 HMC” ในหน้า 20

การกำหนดคอนฟิก 7063-CR1 HMC

ศึกษาเกี่ยวกับวิธีการติดตั้งและกำหนดคอนฟิก Hardware Management Console (HMC)

ตรวจสอบเวอร์ชัน HMC ที่จัดส่งมาพร้อมกับ HMC ของคุณ คุณสามารถดาวน์โหลด HMC เวอร์ชันล่าสุดที่ พร้อมใช้งานจากเว็บไซต์ Fix Central ใช้สื่อบันทึกแบบถอดออกได้ (เช่น DVD หรือ USB) เพื่อสร้างไฟล์ ISO ที่สามารถบูตได้จากแพ็กเกจ HMC (อิมเมจ ISO)

หมายเหตุ: ตารางต่อไปนี้อธิบายข้อมูลการล็อกอินที่กำหนดไว้ล่วงหน้า (ดีฟอลต์) สำหรับอินเตอร์เฟส HMC และ BMC

ตารางที่ 8.

คอนโซลหรืออินเตอร์เฟส	ID ดีฟอลต์	รหัสผ่านดีฟอลต์	คำอธิบาย
BMC	`ADMIN`	`ADMIN`	ID ผู้ใช้ ADMIN และรหัสผ่านใช้เพื่อล็อกอินเข้าสู่ BMC ในครั้งแรก
HMC	`hscroot`	`abc123`	ID ผู้ใช้ hscroot และรหัสผ่านจะถูกใช้เพื่อล็อกออนเข้าสู่ HMC ในครั้งแรก รหัสผ่านจะคำนึงถึงขนาดตัวพิมพ์และสามารถใช้โดยสมาชิกของบทบาทผู้ดูแลระดับสูง
HMC	`root`	`passw0rd`	ID ผู้ใช้รูทและรหัสผ่านจะถูกใช้โดยผู้ให้บริการ เพื่อดำเนินการกับขั้นตอนการดูแลรักษา ซึ่งไม่สามารถใช้เพื่อล็อกออนเข้าสู่ HMC ได้

หมายเหตุ: การติดตั้งต่อไปนี้ถูกแสดงไว้ตามตัวอย่าง

การติดตั้ง HMC โดยใช้แฟล็ชไดร์ฟ USB

เมื่อต้องการติดตั้ง HMC โดยใช้แฟล็ชไดร์ฟ USB ให้ทำตามขั้นตอนต่อไปนี้สำหรับระบบ Linux:

หมายเหตุ: ตัวอย่างในระบบปฏิบัติการอื่น ดูที่:

- Windows: สื่อบันทึกการติดตั้งแบบแฟลช USB (Windows)
- Mac: สื่อบันทึกการติดตั้งแบบแฟลช USB (macOS)

1. ดาวน์โหลด HMC เวอร์ชันที่คุณต้องการจากเว็บไซต์ Fix Central
2. รันคำสั่งต่อไปนี้: **`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`** (โดยที่ **`sdx`** เป็นชื่อของไดร์ฟ USB)

   หมายเหตุ: คุณสามารถรันคำสั่ง Linux `lsblk` เพื่อระบุชื่ออุปกรณ์ ของไดร์ฟ USB เมื่ออุปกรณ์ถูกเชื่อมต่อ
3. เสียบไดร์ฟ USB และเปิดระบบ

   หมายเหตุ: ไดร์ฟ USB ต้องมีพื้นที่อย่างน้อย 4 GB ไดร์ฟ USB บางไดร์ฟอาจไม่กว้างพอดีกับ พอร์ต USB ที่ด้านหลังของระบบ ทดสอบความพอดีของไดร์ฟ USB ก่อนที่คุณ จะดำเนินการต่อ
4. เมื่อเมนู Petitboot ถูกแสดง ให้เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **USB**

การติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตจากวิวเวอร์คอนโซล

เมื่อต้องการติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตจากวิวเวอร์คอนโซล ให้ทำตามขั้นตอน ต่อไปนี้:

1. ล็อกอินเข้าสู่เว็บอินเตอร์เฟส BMC (`http://<bmc-ip>`)
2. เลือก **ตัวควบคุมแบบรีโมต**
3. เลือก **เปลี่ยนทิศทางคอนโซล**

4. คลิก **เรียกใช้งานคอนโซล**.
5. ใน Java™ iKVM Viewer ให้เลือก **สื่อบันทึกเสมือน** > **หน่วยเก็บข้อมูลเสมือน**
6. ภายใต้ **ประเภทของโลจิคัลไดร์ฟ** ให้เลือก **ไฟล์ ISO**
7. คลิก **เปิดอิมเมจ** และหาตำแหน่งไฟล์ ISO บนระบบของคุณ
8. กด **Plugin** เพื่อเมาท์ไฟล์ ISO
9. เปิด ระบบ
10. เมื่อเมนู Petitboot ถูกแสดง ให้เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **CD/DVD**

การติดตั้ง HMC โดยใช้ DVD ไดร์ฟภายนอกที่เชื่อมต่อกับ USB

เมื่อต้องการติดตั้ง HMC โดยใช้ไดร์ฟ DVD ภายนอกที่เชื่อมต่อกับ USB ให้ทำตามขั้นตอนต่อไปนี้:

1. ดาวน์โหลดเวอร์ชันการกู้คืนของ HMC ที่คุณต้องการจากเว็บไซต์ Fix Central
2. เขียนอิมเมจ DVD การกู้คืน HMC ลงในสื่อบันทึก DVD-R เป็นอิมเมจ หรือ คุณสามารถสั่งซื้อ สื่อบันทึกการกู้คืนบน DVD
3. ปิดกำลังไฟ HMC
4. เชื่อมต่อไดร์ฟ USB DVD ภายนอกกับ HMC และใส่ DVD การกู้คืน HMC

   หมายเหตุ: คุณอาจต้องเชื่อมต่อ ไดร์ฟ USB DVD กับแหล่งจ่ายไฟภายนอกหรือใช้สายเคเบิล USB ตัว Y เพื่อเชื่อมต่อกับ พอร์ต USB เพื่อเติมเพื่อให้มีกำลังไฟเพียงพอสำหรับไดร์ฟ DVD
5. Power บน HMC

   หมายเหตุ: หน้าจอมอนิเตอร์อาจไม่แสดงสัญญาณระหว่างการเริ่มทำงาน กระบวนการอาจ ใช้เวลา 2 ถึง 3 นาทีก่อนที่หน้าจอมอนิเตอร์จะแสดงสถานะใด ๆ
6. เมื่อ Petitboot bootloader เริ่มทำงาน ให้หยุดการบู๊ตอัตโนมัติ

   หมายเหตุ: ซึ่งจะบังคับใช้ การหมดเวลา 10 วินาที หากไม่มีการดำเนินการใด ๆ ภายใน 10 วินาที ระบบจะพยายามบู๊ตจาก ฮาร์ดดิสก์ไดร์ฟ
7. รอจนกว่าอุปกรณ์ **CD/DVD** จะปรากฏในเมนู Petitboot

   หมายเหตุ: กระบวนการนี้ อาจใช้เวลาประมาณ 1นาที
8. เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **CD/DVD**

การติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตที่โฮสต์โดยไฟล์เซิร์ฟเวอร์ SMB

เมื่อต้องการติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตที่โฮสต์โดยไฟล์เซิร์ฟเวอร์ Server Message Block (SMB) ให้ทำตามขั้นตอนต่อไปนี้:

1. คัดลอกไฟล์ ISO การกู้คืนลงในโฮสต์แบบแบ่งใช้บนไฟล์เซิร์ฟเวอร์ที่เข้ากันได้กับ SMB ของคุณ

   หมายเหตุ: ไม่สนับสนุน Server Message Block เวอร์ชัน 3 (SMBv3)
2. ล็อกอินเข้าสู่เว็บอินเตอร์เฟส BMC (`http://<bmc-ip>`)
3. เลือก **สื่อบันทึกแบบเสมือน**
4. เลือก **อิมเมจ CD-ROM**
5. กรอกข้อมูลต่อไปนี้:

   แบ่งใช้โฮสต์

   IP ของโฮสต์ SMB หากคุณกำลังใช้ชื่อโฮสต์ ให้ตรวจสอบว่า domain name system (DNS) บน BMC ถูกกำหนดค่าอย่างถูกต้อง

   พาธไปยังอิมเมจ

   พาธ SMB ไปยังระบบ เช่น: `/<share name>/<rest of path>/<name of iso>.iso`

   ผู้ใช้ (ตัวเลือก)

   ชื่อผู้ใช้ที่ใช้เพื่อล็อกอินเข้าสู่โฮสต์ SMB

รหัสผ่าน (ตัวเลือก)

รหัสผ่านสำหรับผู้ใช้

6. คลิก **บันทึก**
7. คลิก **เมาท์**
8. ตอนนี้ อุปกรณ์ 1 แสดงข้อความต่อไป: **มีไฟล์ iso ที่เมาท์อยู่**

   หมายเหตุ: หากข้อความไม่ปรากฏขึ้น ให้ตรวจสอบข้อมูลอีกครั้งและทำซ้ำขั้นตอนที่ 6 - 8
9. เปิด ระบบ
10. เมื่อเมนู Petitboot ถูกแสดง ให้เลือกอ็อพชัน **ติดตั้ง Hardware Management Console** ที่อยู่ภายใต้ **CD/DVD**

ทางเลือก: อัพเดตระดับเฟิร์มแวร์ HMC โดยใช้คีย์กุญแจ USB ที่ให้มาด้วย

หมายเหตุ: ถ้าคอนฟิกูเรชันของคุณได้รวมการอัพเดตเฟิร์มแวร์ HMC บนคีย์หน่วยความจำ USB ให้ ดำเนินขั้นตอนต่อไปนี้เพื่ออัพเดตระดับเฟิร์มแวร์ HMC

เมื่อต้องการอัพเดตระดับเฟิร์มแวร์ HMC โดยใช้คีย์กุญแจ USB ที่ให้มาด้วยให้ทำตาม ขั้นตอนต่อไปนี้:

1. เสียบไดร์ฟคีย์หน่วยความจำ USB ในพอร์ต USB ที่ด้านหลังของระบบ
2. เปิดระบบและล็อกออนเข้าสู่ HMC
3. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
4. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console**
5. ปฏิบัติตามคำสั่งบนหน้าจอในวิซาร์ด Install HMC Corrective Service

ถัดไป คุณจำเป็นต้องกำหนดคอนฟิกซอฟต์แวร์ HMC ของคุณ สำหรับคำแนะนำ โปรดดูที่ “การกำหนดคอนฟิก HMC” ในหน้า 34

หลักการที่เกี่ยวข้อง

กำหนดค่าการเชื่อมต่อ BMC

คุณสามารถกำหนดค่าหรือดูค่าติดตั้งเครือข่ายบน BMC สำหรับคอนโซลการจัดการ

การติดตั้ง เครื่องมือเสมือน HMC

ศึกษาเกี่ยวกับวิธีติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC)

เครื่องมือเสมือน HMC สามารถติดตั้งในโครงสร้างพื้นฐานแบบเสมือน x86 หรือ POWER ที่มีอยู่ เครื่องมือเสมือน HMC สนับสนุนไฮเปอร์ไวเซอร์เสมือน x86 ต่อไปนี้:

- Kernel-based virtual machine (KVM)
- Xen
- VMware

เครื่องมือเสมือน HMC สนับสนุนเวอร์ชวลไลซ์ไฮเปอร์ไวเซอร์ POWER ต่อไปนี้:

- PowerVM

ข้อกำหนดต่ำสุดสำหรับการรัน เครื่องมือเสมือน HMC:

- หน่วยความจำ 16 GB
- 4 ตัวประมวลผลเสมือน
- 2 อินเตอร์เฟสเครือข่าย (สูงสุด 4 อินเตอร์เฟส)
- 1 ดิสก์ไดร์ฟที่มีพื้นที่ว่าง 500 GB

Notes:

- ตัวประมวลผลบนระบบที่โฮสต์ เครื่องมือเสมือน HMC ต้องเป็นตัวประมวลผลที่เปิดใช้งานฮาร์ดแวร์แบบเสมือน Intel VT-x หรือ AMD-V

- เครื่องมือเสมือน HMC DVD ที่คุณได้รับไม่สามารถบูตได้ คุณต้องเมาท์สื่อบันทึกก่อน จากนั้นคัดลอกไฟล์ `.tgz` จากสื่อบันทึก วิธีเมาท์ DVD อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ ที่คุณใช้
- ไวยากรณ์คำสั่งที่ใช้ในตัวอย่างต่อไปนี้ อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการที่คุณใช้
- PowerVM virtualization hypervisor ต้องการพื้นที่ดิสก์ 160 GB อย่างไรก็ตาม ขอแนะนำให้ใช้หน่วยยความจำ 500 GB
- ตัวประมวลผล PowerVM ต้องการหน่วยประมวลผลอย่างน้อย 1.0 หน่วย และตัวประมวลผลเสมือนที่แบ่งใช้สี่ตัวในโหมดการแบ่งใช้แบบ capped ไม่แนะนำให้ใช้ตัวประมวลผลเฉพาะ ตัวประมวลผล PowerVM ยังต้องการหน่วยความจำ 16 GB

ข้อมูลที่เกี่ยวข้อง
อิมเมจการติดตั้งเครือข่าย HMC V8 และวิธีการติดตั้ง

การติดตั้ง เครื่องมือเสมือน HMC บน x86

ศึกษาวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) ในสภาวะแวดล้อม x86

การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ KVM

ศึกษาเกี่ยวกับวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) โดยใช้ไฮเปอร์ไวเซอร์ kernel-based virtual machine (KVM)

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC บน KVM ให้ทำตามขั้นตอนต่อไปนี้:

หมายเหตุ: ใช้อินเตอร์เฟสบรรทัดรับคำสั่งต่อไปนี้และต้องการสิทธิ์ผู้ใช้รูท ไวยากรณ์คำสั่ง อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ

1. ตรวจสอบว่าติดตั้งแพ็กเกจเสมือนบนระบบที่มี Red Hat Enterprise Linux (RHEL) เวอร์ชัน 7.0 หรือใหม่กว่า
2. ดาวน์โหลดไฟล์ `<KVM vHMC installation filename>.tar.gz` ไปยังระบบโฮสต์
3. รันคำสั่งต่อไปนี้: `mkdir -p /var/lib/libvirt/images/vHMC`
4. รันคำสั่งต่อไปนี้: `cd /var/lib/libvirt/images/vHMC`
5. เมื่อต้องการแตกอิมเมจดิสก์เสมือน ให้รันคำสั่งต่อไปนี้: `tar -zxvf <KVM vHMC installation filename>.tgz`

   หมายเหตุ: ในคำสั่งนี้ ให้ระบุพาธเต็มของไฟล์ เครื่องมือเสมือน HMC .tar ของคุณ
6. ไฟล์**domain.xml** จะอยู่ในไฟล์ `<KVM vHMC installation filename>.tar.gz` ปฏิบัติตามขั้นตอนต่อไปนี้:
   a. แก้ไขไฟล์ **domain.xml** และตรวจสอบว่า พาธไปยังดิสก์ของคุณถูกต้อง ไฟล์นี้จะมีสตริง **DISK_PATH**
   b. ตรวจสอบให้แน่ใจว่าใช้ `virtio` ในค่าบัส สำหรับอุปกรณ์ดิสก์ของคุณ
   c. คุณสามารถเลือกชื่อที่แตกต่างกันสำหรับ VM ของคุณ ชื่อดีฟอลต์ ในไฟล์ **domain.xml** คือ **vHMC**
   d. ตรวจสอบว่าแอดเดรสการควบคุมการเข้าถึงสื่อ (MAC) ถูกกำหนดไว้ใน ไฟล์ **domain.xml** ไฟล์นี้จะมี สตริง **MAC_ADDRESS**

      หมายเหตุ: ลบบรรทัดนี้หาก คุณต้องการให้ MAC แอดเดรสถูกสร้างขึ้นโดยอัตโนมัติสำหรับคุณ
   e. ตรวจสอบว่าบริดจ์ของคุณตรงกับอุปกรณ์อีเทอร์เน็ตของคุณ ไฟล์ **domain.xml** ดีฟอลต์ จะระบุหนึ่งอิเทอร์เน็ต
   f. หากคุณกำลังใช้ Activation Engine ให้แทนที่ **AEDISK** ด้วยชื่อของอิมเมจดิสก์เสมือนของ Activation Engine ไม่เช่นนั้น ให้ลบอิลิเมนต์ดิสก์ออก
7. เมื่อต้องการกำหนด VM ให้รันคำสั่งต่อไปนี้: `virsh define <domain>.xml`
8. เมื่อต้องการตรวจสอบว่ามีการเพิ่ม HMC เสมือนเข้ากับรายการ VM ที่กำหนดไว้หรือไม่ ให้รันคำสั่งต่อไปนี้: `virsh list --all`
9. เมื่อต้องการเริ่มต้น VM ให้รันคำสั่งต่อไปนี้: `virsh start vHMC`
10. เมื่อต้องการกำหนดหมายเลขแสดง Virtual Network Computing (VNC) ของคอนโซลของคุณ ให้รันคำสั่งต่อไปนี้: `virsh vncdisplay vHMC`
11. เมื่อต้องการเชื่อมต่อกับคอนโซลของคุณด้วยวิวเวอร์ VNC ให้รันคำสั่ง ต่อไปนี้: `vncviewer HOSTNAME:ID`(โดยที่ ID คือ หมายเลขที่แสดง, ตัวอย่างเช่น 0)

หมายเหตุ: หาก คุณต้องการเข้าถึงจากระยะไกล คุณต้องลบ หรือกำหนดคอนฟิกไฟลวอลล์ของคุณ เพื่ออนุญาตให้เข้าถึงพอร์ต 5900

การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ Xen

ศึกษาเกี่ยวกับวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) โดยใช้ไฮเปอร์ไวเซอร์ Xen

เครื่องมือเสมือน HMC สนับสนุน Xen เวอร์ชัน 4.2 หรือสูงกว่า

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ Xen ให้ทำตามขั้นตอนต่อไปนี้:

หมายเหตุ: ขั้นตอนต่อไปนี้ใช้อินเตอร์เฟสบรรทัดรับคำสั่งและต้องการสิทธิ์ ผู้ใช้รูท ไวยากรณ์คำสั่ง อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ

1. ตรวจสอบว่าติดตั้งแพ็กเกจเสมือนบนระบบที่มี Red Hat Enterprise Linux (RHEL) เวอร์ชัน 6.4 หรือสูงกว่าหรือไม่
2. ดาวน์โหลดไฟล์ <XEN vHMC installation filename>.tar.gz ไปยังระบบโฮสต์
3. รันคำสั่งต่อไปนี้: `mkdir -p /var/lib/libvirt/images/vHMC`
4. รันคำสั่งต่อไปนี้: `cd /var/lib/libvirt/images/vHMC`
5. เมื่อต้องการแตกอิมเมจดิสก์เสมือน ให้รันคำสั่งต่อไปนี้: `tar -zxvf <XEN vHMC installation filename>.tgz`

   หมายเหตุ: ในคำสั่งนี้ ให้ระบุพาธเต็มของไฟล์ เครื่องมือเสมือน HMC .tar ของคุณ
6. ไฟล์ **vhmc.cfg** ถูกจัดเตรียมไว้ในไฟล์ <XEN vHMC installation filename>.tar.gz เปิดไฟล์ **vhmc.cfg** ในเท็กซ์เอดิเตอร์ และแก้ไขค่าต่อไปนี้:
   a. เปลี่ยนชื่อของ HMC เสมือน (ทางเลือก): แก้ไขไฟล์ **vhmc.cfg** และตรวจสอบว่า พาธไปยังดิสก์ของคุณนั้นถูกต้อง ไฟล์นี้จะมีสตริง **DISK_PATH**
   b. แทนที่ **DISK_PATH** ด้วยพาธสำหรับ `disk1.img`:

   ```
   disk = [ 'file:DISKPATH,hda,w' ]
   ```

   c. แทนที่ **ethernet adapter** และเพิ่ม MAC address (ทางเลือก):

   ```
   vif = [ 'type=virtio, model=e1000, bridge=eth0' ]
   ```

   MAC Address ทางเลือก:

   ```
   vif = [ 'type=virtio, mac=MACADDRESS, model=e1000, bridge=eth0' ]
   ```

   หมายเหตุ: เมื่อ Virtual HMC รีบูตแล้ว ไฮเปอร์ไวเซอร์ Xen จะสร้าง MAC address ขึ้นใหม่อีกครั้ง การเพิ่ม MAC Address เพิ่มเติมจะช่วยแก้ปัญหานี้

   d. แทนที่ **FLOPPYPATH** (หากคุณกำลังใช้ Activation Engine):

   ```
   device_model_args = [ "-fda", "FLOPPYPATH" ]
   ```
7. เมื่อต้องการสร้างและเริ่มต้น VM ให้รันคำสั่ง: `xl create vHMC.cfg`
8. เมื่อต้องการตรวจสอบว่า VM ถูกเพิ่มไปยังรายการของเครื่องเสมือนที่กำหนดไว้ ให้รันคำสั่งต่อไปนี้: `xl list`
9. เมื่อต้องการเพิ่มคอนโซลเสมือน VM ให้รันคำสั่งต่อไปนี้: `vncviewer localhost 0`

การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ VMware ESXi

ศึกษาเกี่ยวกับวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) โดยใช้ VMware ESXi

คุณสามารถติดตั้ง เครื่องมือเสมือน HMC บน VMware ESXi ได้โดยใช้ส่วนติดต่อผู้ใช้แบบกราฟิกบนไคลเอ็นต์ vSphere เพื่อปรับใช้เท็มเพลต Open Virtualization Format (OVF)

หมายเหตุ: คุณสามารถติดตั้ง เครื่องมือเสมือน HMC บน VMware ESXi เวอร์ชัน 6.0 หรือใหม่กว่า

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC บน VMware ESXi โดยใช้ไคลเอ็นต์ vSphere ให้ทำตามขั้นตอนต่อไปนี้:

หมายเหตุ: ไวยากรณ์คำสั่ง อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ

1. ขอรับไฟล์เก็บถาวร Tar : <VMware vHMC installation file name>.tgz

2. ใช้คำสั่ง `tar` เพื่อคลายไฟล์ OVA ออกจากไฟล์จัดเก็บถาวร Tar
3. สตาร์ทไคลเอ็นต์ vSphere และล็อกอินเข้าสู่โฮสต์ ESXi
4. จากเมนู **File** ให้เลือก **Deploy OVF template**
5. คลิก **Browse** และเลือกไฟล์ OVA
6. คลิก **ถัดไป**
7. หลังจากการปรับใช้เสร็จสิ้นแล้ว ให้คลิก **ปิด** และเลือกไอคอน เครื่องมือเสมือน HMC เพื่อเปิด เครื่องมือเสมือน HMC

การติดตั้ง เครื่องมือเสมือน HMC บน POWER

ศึกษาวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) บนสภาวะแวดล้อม POWER เสมือน

การติดตั้ง เครื่องมือเสมือน HMC บน PowerVM (โลจิคัลพาร์ติชัน)

เรียนรู้วิธีติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) ในสภาวะแวดล้อม PowerVM

เครื่องมือเสมือน HMC สนับสนุนเซิร์ฟเวอร์ POWER9 บนเฟิร์มแวร์ระดับ FW910 หรือใหม่กว่า สำหรับข้อมูลเพิ่มเติม โปรดดูที่ การกระจาย Linux ที่สนับสนุน สำหรับ POWER8 และ POWER9 Linux บนระบบ Power (https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm)

หมายเหตุ:

1. คุณสามารถจัดการเซิร์ฟเวอร์ที่โฮสต์ เครื่องมือเสมือน HMC
2. คุณไม่สามารถจัดการเซิร์ฟเวอร์ที่โฮสต์ เครื่องมือเสมือน HMC อื่นซึ่งกำลังจัดการเซิร์ฟเวอร์ซึ่งโฮสต์ เครื่องมือเสมือน HMC นี้

   ตัวอย่าง เครื่องมือเสมือน HMC A รันอยู่บน server A และ เครื่องมือเสมือน HMC B รันอยู่บน server B เครื่องมือเสมือน HMC A ไม่สามารถจัดการ server B และ เครื่องมือเสมือน HMC B ไม่สามารถจัดการ server A ในเวลาเดียวกัน หนึ่งใน เครื่องมือเสมือน HMC สามารถจัดการเซิร์ฟเวอร์อื่น แต่ทั้งสอง เครื่องมือเสมือน HMC ไม่สามารถจัดการแต่ละฝ่ายในเวลาเดียวกัน

.

สร้างอิมเมจการติดตั้ง HMC อัตโนมัติ (ทางเลือก)

คุณสามารถสร้างอิมเมจการติดตั้ง HMC อัตโนมัติที่ติดตั้ง เครื่องมือเสมือน HMC โดยอัตโนมัติโดยไม่พร้อมต์ให้ระบุวิซาร์ด **การติดตั้ง HMC**

หมายเหตุ: เครื่องมือเสมือน HMC บน PowerVM ไม่ได้จัดเตรียมการสนับสนุนกราฟิกอะแด็ปเตอร์สำหรับอะแด็ปเตอร์ที่กำหนดให้กับ พาร์ติชัน คุณสามารถใช้เว็บเบราว์เซอร์ที่สนับสนุนเพื่อเชื่อมต่อกับ HMC สำหรับการสนับสนุน ส่วนติดต่อผู้ใช้

เมื่อต้องการสร้างอิมเมจการติดตั้ง HMC อัตโนมัติ ให้ทำตามขั้นตอนต่อไปนี้:

1. สร้างสองไดเร็กทอรีโดยการรันคำสั่งต่อไปนี้ `mkdir -p oldiso` และ `mkdir -p newiso`
2. เมาท์อิมเมจการติดตั้ง HMC กับไดเร็กทอรี **oldiso** โดยการรัน คำสั่งต่อไปนี้: `sudo mount -o loop <image_path> oldiso`
3. คัดลอกเนื้อหาของไดเร็กทอรี **oldiso** ไปยังไดเร็กทอรี **newiso** โดยการรันคำสั่งต่อไปนี้: `cp -r oldiso/* newiso`
4. แก้ไขไฟล์ Grub สำหรับการติดตั้งอัตโนมัติโดยการรันคำสั่งต่อไปนี้: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`
5. ทำให้ไฟล์ Grub อ่านได้อย่างเดียวโดยการรันคำสั่งต่อไปนี้: `sudo chown 0444 newiso/boot/grub/grub.cfg`
6. สร้าง ISO การติดตั้ง HMC ใหม่โดยการรันคำสั่งต่อไปนี้: `mkisofs -o <new_iso_name> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso` (โดยที่ **ISO label** ต้องเป็น `HMC-<hmc version release number>` เช่น `HMC-8.0.870.0`)

หมายเหตุ: สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า Activation Engine และไฟล์คอนฟิกูเรชัน โปรดดูที่ “การใช้ Activation Engine สำหรับ เครื่องมือเสมือน HMC” ในหน้า 28

ตั้งค่าโลจิคัลวอลุ่ม

เมื่อต้องการตั้งค่าโลจิคัลวอลุ่ม ให้ทำตามขั้นตอนต่อไปนี้:

1. เลือกระบบที่ถูกจัดการ
2. จากพ็อดเมนู เลือก **System Actions** > **Power VM** > **Virtual Storage**
3. เลือก **Manage System VIOS** > **Action** > **Manage Virtual Storage**
4. เลือกแท็บ **Virtual Disks**
5. คลิก **Create virtual disk** และป้อนข้อมูลต่อไปนี้:
   - **Virtual disk name**: ชื่อของดิสก์เสมือน
   - **Storage pool name**: ชื่อของพูลหน่วยเก็บข้อมูล
   - **Virtual disk size**: ขนาดของดิสก์เสมือน
   - **Assigned partition**: ชื่อของโลจิคัลพาร์ติชัน

   หมายเหตุ: ต้องการพื้นที่ดิสก์อย่างน้อย 160 GB (แต่แนะนำให้มี 500 GB)

ตั้งค่าสื่อบันทึกการติดตั้ง - สร้างไลบรารีสื่อบันทึก

เมื่อต้องการสร้างไลบรารีสื่อบันทึก ให้ทำตามขั้นตอนต่อไปนี้:

1. เลือกระบบที่ถูกจัดการ
2. จากพ็อดเมนู เลือก **System Actions** > **Power VM** > **Virtual Storage**
3. เลือก **Manage System VIOS** > **Action** > **Manage Virtual Storage**
4. เลือกแท็บ **Optical Devices**
5. คลิก **Create Library** และป้อนข้อมูลต่อไปนี้:
   - **Storage pool**: ชือของพูลหน่วยเก็บข้อมูล
   - **Media library size**: ขนาดของไลบรารีสื่อบันทึก
6. คลิก **OK**

การตั้งค่าสื่อบันทึกการติดตั้ง - อัพโหลดสื่อบันทึกไปยัง VIOS

เมื่อต้องการอัพโหลดสื่อบันทึกไปยัง Virtual I/O Server (VIOS) ให้ทำตามขั้นตอนต่อไปนี้:

1. ล็อกอินเข้าสู่ VIOS
2. ในโหมดรูทของ VIOS ให้รันคำสั่งต่อไปนี้: `oem_setup_env`
3. เมื่อต้องการอนุญาตการเชื่อมต่อ NFS ให้รันคำสั่งต่อไปนี้: `nfso -o nfs_use_reserved_ports=1`
4. เมื่อต้องการเมาท์ NFS ลงในโฟลเดอร์ VIOS แบบโลคัล ให้รันคำสั่งต่อไปนี้: `mount <server_ip>:/ Mountpoint <local_folder>`
5. เมื่อต้องการตรวจสอบว่าเมาท์ NFS มี ISO การติดตั้ง HMC และอิมเมจคอนฟิกูเรชัน Activation Engine (ทางเลือก) หรือไม่ ให้รันคำสั่งต่อไปนี้: `ls`

การตั้งค่าสื่อบันทึกการติดตั้ง - ลิงก์สื่อบันทึกกับไลบรารีสื่อบันทึก

เมื่อต้องการลิงก์สื่อบันทึกกับไลบรารีสื่อบันทึก ให้ทำตามขั้นตอนต่อไปนี้:

1. กลับไปยัง **Manage System VIOS** > **Action** > **Manage Virtual Storage** และเลือกแท็บ **Optical Devices**
2. จากส่วน **Virtual Optical Media** ให้เลือก **Add Media** จากเมนู **Actions**
3. จากหน้าต่าง **Add Virtual Media** เลือก **Add existing file from VIOS** และป้อนข้อมูลต่อไปนี้:
   - **Media name**: ชื่อของสื่อบันทึก (เช่น `HMCInstall` หรือ `AEDrive`)
   - **Optical medai file name**: ชื่อไฟล์ของไฟล์ ISO การติดตั้ง (เช่น `01234567-ppc64ie.iso`)
4. คลิก **OK**

5. หากคุณสร้างอิมเมจคอนฟิกูเรชัน Activation Engine ให้ทำซ้ำขั้นตอนที่ 3 - 4 เพื่อเพิ่มอิมเมจคอนฟิกูเรชัน Activation Engine ไม่เช่นนั้น ให้ดำเนินการขั้นตอนที่ 6
6. ตรวจสอบว่าสื่อบันทึกออพติคัลถูกอัพโหลดไปบังไลบรารีสื่อบันทึกแล้วโดยตรวจสอบว่า ชื่อสื่อบันทึกแสดงในรายการ **สื่อบันทึกออพติคัลเสมือน** ที่พร้อมใช้งาน

ตั้งค่าโลจิคัลพาร์ติชัน

เมื่อต้องการตั้งค่าโลจิคัลพาร์ติชัน ให้ทำตามขั้นตอนต่อไปนี้:

1. เลือกระบบที่ถูกจัดการ
2. จากพ็อดเมนู ให้เลือก **System Actions** > **Partitions** > **Partitions**
3. คลิก **Create Partition** และป้อนข้อมูลต่อไปนี้:
   - **Partition name**: ชื่อของพาร์ติชัน
   - **Partition ID**: ID ของพาร์ติชัน
   - **Partition Type**: เลือกระบบปฏิบัติการ (**AIX/Linux** หรือ **IBM i**)
4. คลิก **OK**
5. จัดสรรจำนวนของตัวประมวลผลและจำนวนของหน่วยความจำให้กับพาร์ติชัน

   หมายเหตุ: คุณต้องระบุตัวประมวลผลเสมือนอย่างน้อย 4 ตัวและหน่วยความจำอย่างน้อย 8 GB
6. จากพ็อดเมนู เลือก **Partition Actions** > **Virtual I/O** > **Virtual Networks**
7. คลิก **Attach Virtual Network** และเลือกเช็กบ็อกซ์ **Show and attach new virtual ethernet adapters** จากตาราง เลือกอะแด็ปเตอร์เน็ตเวิร์ก เสมือนที่คุณต้องการเชื่อมต่อกับโลจิคัลพาร์ติชัน

   หมายเหตุ: คุณสามารถระบุอะแด็ปเตอร์เครือข่ายเสมือนได้สูงสุด 4 อะแด็ปเตอร์
8. จากพ็อดเมนู เลือก **Partition Actions** > **Virtual I/O** > **Virtual Storage**
9. จากแท็บ **Virtual Optical Device** ให้คลิก **Add Virtual Optical**
10. ป้อน **Device Name** (เช่น `HMCInstall` หรือ `AEDrive`) และเลือก Virtual I/O Server ที่ต้องการจากตาราง

    หมายเหตุ: การติดตั้ง `AEDrive` เป็นทางเลือก
11. คลิก **OK**
12. ตรวจสอบว่าอุปกรณ์ออพติคัลเสมือนที่คุณเพิ่มจากขั้นตอนที่ 10 แสดงในตารางแล้ว
13. จากเมนู **Action** คลิก **Load**
14. เลือกไฟล์สื่อบันทึกที่จะกำหนดให้กับโลจิคัลพาร์ติชันและคลิก **OK**
15. ตรวจสอบว่าอุปกรณ์ออพติคัลเสมือนที่คุณโหลดจากขั้นตอนที่ 13 แสดงในตารางแล้ว

การเริ่มต้น เครื่องมือเสมือน HMC

หมายเหตุ: เมื่อคุณติดตั้ง เครื่องมือเสมือน HMC นพาร์ติชันโดยใช้ ไฟล์อิมเมจ ISO สำหรับ HMC คุณจะไม่สามารถเข้าถึงคอนโซลแบบกราฟิกโลคัลเพื่อเข้าถึงส่วนติดต่อผู้ใช้แบบเว็บ

เมื่อต้องการเริ่มต้น เครื่องมือเสมือน HMC บน PowerVM ให้ทำตามขั้นตอนต่อไปนี้:

1. เลือกพาร์ติชันที่ถูกจัดการ
2. เปิดการเชื่อมต่อที่แอ็คทีฟกับโลจิคัลพาร์ติชันโดยการเลือก **Actions** > **Console** > **Open Terminal Window**
3. เปิดใช้งานโลจิคัลพาร์ติชันโดยการเลือก **Actions** > **Activate**
4. เลือก **Activate (Normal)** และ **Current Configuration**
5. คลิก **Finish**
6. สลับไปที่หน้าต่างเทอร์มินัล
7. จากเมนู **Boot** เลือก **1 = SMS Menu**
8. จากเมนู **Main** เลือก **5 = Select Boot Options**
9. จากเมนู **Multiboot** เลือก **1 = Select Install/Boot Device**

10. จากเมนู **Select Device Type** เลือก **5 = List all devices**
11. เลือกอุปกรณ์ `HMCInstall` ตามตำแหน่งของอุปกรณ์
12. เลือก **2. Normal Mode Boot**
13. เลือก **1. Yes** เพื่อยืนยัน
14. ทำตามคำแนะนำบนหน้าจอจากวิซาร์ด **Install HMC**

    หมายเหตุ: ข้าม ขั้นตอนนี้หากคุณใช้อิมเมจการติดตั้ง HMC อัตโนมัติ
15. หลังจากการติดตั้งเสร็จสมบูรณ์และระบบเริ่มทำงาน คุณต้องเลือกภาษาจากไดอะล็อกบ็อกซ์ **language selection**
16. ยอมรับข้อตกลงการอนุญาตให้ใช้งาน

    หมายเหตุ: ตรวจสอบให้แน่ใจว่าคอนโทรเลอร์คำสั่งพร้อมที่จะยอมรับคำสั่ง ก่อนที่คุณจะรันคำสั่งใด ๆ เช่น การรันคำสั่ง **`lshmc -V`** จะกว่าจะสำเร็จ
17. ล็อกอินในฐานะ `hscroot` และใช้คำสั่ง **chhmc** เพื่อกำหนดค่าเครือข่าย

    ตัวอย่างต่อไปนี้แสดงลำดับของคำสั่ง **chhmc** ที่สามารถใช้เพื่อกำหนดค่าเครือข่ายและเปิดใช้งาน Secure Shell (SSH) และการเข้าถึงแบบรีโมตผ่านเว็บ บน HMC

    ```
    chhmc -c network -s modify -i ethX -a <hmc ip address> -nm <hmc network mask> --lparcomm on
    chhmc -c network -s modify -h <hmc hostname> -d <hmc domain name> -g <gateway ip>
    chhmc -c network -s add -ns <name server> -ds <domain search>
    chhmc -c ssh -s enable
    chhmc -c ssh.name -s add -a <ip address>
    chhmc -c SecureRemoteAccess.name -s add -a <ip address>
    chhmc -c remotewebui -s enable -i ethX
    hmcshutdown -r -t now
    ```

    - **ethX** เป็นชื่ออินเตอร์เฟสเครือข่ายที่ต้องการกำหนดค่า
    - **hmc ip address** เป็น IP ของ HMC ของคุณ
    - **hmc network mask** เป็น network mask ของ HMC
    - **hmc hostname** เป็นชื่อโฮสต์ของ HMC
    - **hmc domain name** เป็นชื่อโดเมนของ HMC
    - **gateway ip** เป็น IP แอดเดรสของเกตเวย์บนเครือข่าย
    - **name server** เป็นแอดเดรสของเซิร์ฟเวอร์ชื่อของเครือข่าย
    - **domain search** เป็นชื่อของโดเมนที่คุณต้องการให้ HMC ค้นหา
    - เมื่อต้องการอนุญาตให้เข้าถึง IP แอดเดรสทั้งหมด ให้ใช้ **-a 0.0.0.0 -nm 0** แทน **ip address**

    หมายเหตุ: เมื่อคุณใช้อะแด็ปเตอร์อีเทอร์เน็ตเสมือนหลายอะแด็ปเตอร์ ให้รันคำสั่ง **`cat /etc/sysconfig/network-scripts/ifcfg-ethX`** บน เครื่องมือเสมือน HMC บนแต่ละอินเตอร์เฟส เปรียบเทียบ media access control (MAC) แอดเดรสกับค่าที่ HMC แสดงในมุมมองอะแด็ปเตอร์ของเครือข่ายเสมือนของพาร์ติชัน คุณสามารถคลิก **ดูค่าติดตั้งอะแด็ปเตอร์อีเทอร์เน็ตเสมือน** สำหรับข้อมูลเพิ่มเติมเกี่ยวกบ อะแด็ปเตอร์อีเทอร์เน็ตเสมือน ขั้นตอนนี้จะช่วยคุณกำหนดอินเตอร์เฟสที่ถูกต้องที่จะใช้
18. รีสตาร์ทระบบ

การใช้ Activation Engine สำหรับ เครื่องมือเสมือน HMC

ศึกษาเกี่ยวกับวิธีการใช้ Activation Engine สำหรับ เครื่องมือเสมือน Hardware Management Console (HMC)

Activation Engine เป็นเฟรมเวิร์กที่อนุญาตให้กำหนดค่าคอมโพเนนต์ต่าง ๆ ภายในเครื่องเสมือน ระหว่างการเริ่มต้นระบบ เมื่อต้องการใช้ Activation Engine คุณจำเป็นต้องตั้งค่าโปรไฟล์ คอนฟิกูเรชัน XML เพื่ออนุญาตให้ เครื่องมือเสมือน HMCอยู่ในสถานะพร้อมที่จะจัดการ ในการเริ่มต้นใช้งานในครั้งแรก สำหรับข้อมูลเพิ่มเติม เกี่ยวกับการกำหนดคอนฟิกโปรไฟล์คอนฟิกูเรชัน XML โปรดดูที่ “การตั้งค่าโปรไฟล์การกำหนดคอนฟิกสำหรับ Activation Engine” ในหน้า 29 สามารถใช้ไฟล์คอนฟิกูเรชัน เพื่อกำหนดคอนฟิกตัวเลือกต่าง ๆ ต่อไปนี้:

- ตั้งค่าคีย์บอร์ดดีฟอลต์ (US)
- ภาษาดีฟอลต์ (US)
- ปิดใช้งานการตั้งค่าคีย์บอร์ด
- ปิดใช้งานการตั้งค่าหน้าจอ

- ข้อตกลงสิทธิการใช้งาน และรหัสเครื่อง
- ปิดใช้งานวิซาร์ดการติดตั้ง
- ปิดใช้งานวิซาร์ด Call Home
- กำหนดค่าได้ถึง 4 การ์ดอินเตอร์เฟสเครือข่าย
- กำหนดการตั้งค่าไฟล์วอลล์สำหรับแต่ละอินเตอร์เฟส
- กำหนดค่าอินเตอร์เฟสเครือข่ายเป็นเซิร์ฟเวอร์ IPv4 DHCP
- กำหนดค่าอินเตอร์เฟสไพรเวตและอินเตอร์เฟสเปิด
- กำหนดค่าอุปกรณ์อินเตอร์เฟสดีฟอลต์เกตเวย์

หมายเหตุ: จำนวนของอะแด็ปเตอร์อีเทอร์เน็ตที่กำหนดไว้ในไฟล์คอนฟิกูเรชัน **vHMC-Conf.xml** ต้องสัมพันธ์กับอะแด็ปเตอร์อีเทอร์เน็ตที่กำหนดไว้ ในไฟล์คอนฟิกูเรชัน **domain.xml**, **vHMC.cfg** หรือ **VMWare**

Activation Engine ต้องการดิสก์เสมือนที่เก็บคอนฟิกูเรชัน XML คุณสามารถแก้ไขไฟล์ **user_data** โดยใช้เท็กซ์เอดิเตอร์และใช้คู่มือการกำหนดคอนฟิก XML ที่แสดงใน ตัวอย่างต่อไปนี้

เมื่อต้องการสร้างอิมเมจดิสก์ ISO เสมือนที่มีคอนฟิกูเรชัน Activation Engine ในสภาวะแวดล้อม Linux ให้ทำตามขั้นตอนต่อไปนี้:

1. สร้างไดเร็กทอรี:

   ```
   mkdir -p config-drive/openstack/latest
   ```

2. คัดลอกไฟล์ **user_data** ที่แก้ไขแล้วลงในไดเร็กทอรี:

   ```
   cp user_data config-drive/openstack/latest
   ```

3. สร้างอิมเมจดิสก์เสมือนที่มีคอนฟิกูเรชัน Activation Engine:

   ```
   mkisofs -R -V config-2 -o AEdrive.iso config-drive
   ```

การตั้งค่าโปรไฟล์การกำหนดคอนฟิกสำหรับ Activation Engine

ศึกษาวิธีการตั้งค่าไฟล์การกำหนดคอนฟิกของ Activation Engine โดยใช้แท็ก XML

ไฟล์การกำหนดคอนฟิก

ใช้ไฟล์การกำหนดคอนฟิกตัวอย่างต่อไปนี้เพื่อศึกษาเกี่ยวกับแท็ก XML

```
<vHMC-Configuration>
   <ConfigurationVersion>2.0</ConfigurationVersion>
   <LicenseAgreement></LicenseAgreement>
   <AcceptLicense>Yes</AcceptLicense>
   <Locale>en_US.UTF-8</Locale>
   <SetupWizard>No</SetupWizard>
   <SetupCallHomeWizard>No</SetupCallHomeWizard>
   <SetupKeyboard>No</SetupKeyboard>
   <SetupDisplay>No</SetupDisplay>
   <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
      <Hostname></Hostname>
      <Domain></Domain>
      <DNSServers></DNSServers>
      <IPV4Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Netmask></Netmask>
         <Gateway></Gateway>
      </IPV4Config>
      <IPV6Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Gateway></Gateway>
      <IPV6Config>
      <Firewall>
         <PEGASUS>Enabled</PEGASUS>
         <RPD>Enabled</RPD>
         <FCS>Enabled</FCS>
         <I5250>Enabled</I5250>
```

```
         <PING>Enabled</PING>
         <L2TP>Disabled</L2TP>
         <SLP>Enabled</SLP>
         <RSCT>Enabled</RSCT>
         <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
         <SSH>Enabled</SSH>
         <NTP>Disabled</NTP>
         <SNMPTraps>Disabled</SNMPTraps>
         <SNMPAgents>Disabled</SNMPAgents>
      </Firewall>
   </Ethernet>
   <NTPServers>
      <ntpparam ntpserver="" ntpversion=""/>
   </NTPServers>
</vHMC-Configuration>
```

แท็ก XML สำหรับไฟล์การกำหนดคอนฟิก

แท็ก XML จะถูกใช้ในไฟล์การกำหนดคอนฟิก Activation Engine เพื่อตั้งค่าเฉพาะ สำหรับแอ็ตทริบิวต์ต่าง ๆ คุณสามารถตั้งค่าเหล่านี้ด้วยตัวเองใน ไฟล์การกำหนดคอนฟิก Activation Engine ใช้ตารางต่อไปนี้ เพื่อดูรายละเอียดของแต่ละแท็กและค่าที่ใช้ได้:

ตารางที่ 9. แท็ก XML

แท็ก	คำอธิบาย	ค่าที่ยอมรับได้	หมายเหตุ
ConfigurationVersion	อิลิเมนต์ที่จำเป็นที่กำหนดเวอร์ชันของการกำหนดคอนฟิกที่ใช้	**2.0**	
LicenseAgreement	อิลิเมนต์ที่จำเป็นที่แสดงข้อตกลงการใช้ไลเซนส์ เครื่องมือเสมือน HMC		
AcceptLicense	อิลิเมนต์ที่จำเป็นเพื่อยอมรับข้อตกลงการใช้ไลเซนส์ เครื่องมือเสมือน HMC	• **Yes**: ยอมรับข้อตกลงการใช้ไลเซนส์ HMC • **No**: พร้อมต์ให้ผู้ใช้ยอมรับข้อตกลงการใช้ไลเซนส์ HMC	หากคุณป้อนค่าที่ไม่ถูกต้อง Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็น **No**
Locale	อิลิเมนต์ที่จำเป็นเพื่อกำหนดการตั้งค่าสำหรับโลแคล	**en_US.UTF-8**	หากคุณป้อนค่าที่ไม่ถูกต้อง Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็น **US**
SetupWizard	อิลิเมนต์ที่จำเป็นเพื่อเปิดใช้งานหรือปิดใช้งานวิซาร์ด **HMC Setup**	• **Yes**: แสดงวิซาร์ด **HMC Setup** • **No**: ปิดใช้งานการแสดงวิซาร์ด **HMC Setup**	หากคุณป้อนค่าที่ไม่ถูกต้อง Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็น **Yes**
SetupCallHomeWizard	อิลิเมนต์ที่จำเป็นเพื่อเปิดใช้งานหรือปิดใช้งานวิซาร์ด **HMC Call Home**	• **Yes**: แสดงวิซาร์ด **HMC Call Home** • **No**: ปิดใช้งานการแสดงวิซาร์ด **HMC Call Home**	หากคุณป้อนค่าที่ไม่ถูกต้อง Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็น **Yes**
SetupKeyboard	อิลิเมนต์ที่จำเป็นเพื่อกำหนดการกำหนดคอนฟิกของคีย์บอร์ด	• **Yes**: พร้อมต์ให้ผู้ใช้ระบุการกำหนดคอนฟิกของคีย์บอร์ด • **No**: ยอมรับการกำหนดคอนฟิกดีฟอลต์ของคีย์บอร์ด (US)	หากคุณป้อนค่าที่ไม่ถูกต้อง Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็น **Yes**
SetupDisplay	อิลิเมนต์ที่จำเป็นเพื่อเปิดใช้งานหรือปิดใช้งานคอนฟิกูเรชันของจอแสดงผล	• **Yes**: พร้อมต์ให้ผู้ใช้ระบุคอนฟิกูเรชันของจอแสดงผล • **No**: ยอมรับคอนฟิกูเรชันดีฟอลต์ของจอแสดงผล	หากคุณป้อนค่าที่ไม่ถูกต้อง Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็น **Yes**

ตารางที่ 9. แท็ก XML (ต่อ)

แท็ก	คำอธิบาย	ค่าที่ยอมรับได้	หมายเหตุ
Ethernet	อิลิเมนต์ที่จำเป็นที่เก็บค่าสำหรับคอนฟิกูเรชันของอะแด็ปเตอร์อีเทอร์เน็ต คุณสามารถกำหนดค่า อะแด็ปเตอร์อีเทอร์เน็ตได้สูงสุด 4 อะแด็ปเตอร์	**Enable**: • **Yes**: กำหนดค่าอะแด็ปเตอร์นี้ • **No**: ไม่กำนหดค่าอะแด็ปเตอร์นี้ **DefaultGatewayDevice**: • **Yes**: กำหนดค่าอะแด็ปเตอร์นี้เป็นอะแด็ปเตอร์เครือข่ายหลัก • **No**: ไม่กำหนดค่าอะแด็ปเตอร์นี้เป็นอะแด็ปเตอร์เครือข่ายหลัก **PrivateInterface**: • **Yes**: กำหนดค่าอะแด็ปเตอร์นี้เป็นอินเตอร์เฟสไพรเวต **Yes** จำเป็นเพื่อกำหนดค่าอินเตอร์เฟสเป็นเซิร์ฟเวอร์ IPv4 DHCP • **No**: ไม่กำหนดค่าอะแด็ปเตอร์นี้เป็นอินเตอร์เฟสไพรเวต **No** จำเป็นเพื่อกำหนดค่าอินเตอร์เฟสเป็นชนิด IPv4 แบบสแตติก	Activation Engine จะรันคอนฟิกูเรชันดีฟอลต์หากมีการป้อนค่าที่ไม่ถูกต้องภายในส่วนอะแด็ปเตอร์อีเทอร์เน็ตหรือหากมีการกำหนด **อุปกรณ์ดีฟอลต์เกตเวย์** หลายค่า คุณสามารถตัดอิลิเมนต์ที่เป็นทางเลือกออกจากคอนฟิกูเรชันได้ แต่ต้องมีคอนฟิกูเรชัน IPV4 หรือ IPV6 เป็นอย่างน้อย หากคุณไม่ได้ระบุคอนฟิกูเรชัน IP ดังนั้น Activation Engine จะใช้คอนฟิกูเรชันดีฟอลต์
HostName	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดชื่อโฮสต์ของเครือข่าย	สตริงชื่อโฮสต์ใด ๆ ที่ใช้ได้	หากไม่ได้กำหนดอิลิเมนต์ Activation Engine จะใช้ค่าโลคัลโฮสต์ดีฟอลต์ **HostName**
Domain	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดโดเมนของเครือข่าย	ค่าโดเมนใด ๆ ที่ใช้ได้ (เช่น **example.us.com**)	หากไม่ได้กำหนดอิลิเมนต์นี้ Activation Engine จะใช้ค่าว่างดีฟอลต์ คือ **Domain**
DNSServers	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดเซิร์ฟเวอร์ DNS บนเครือข่าย	คุณสามารถระบุค่า DNS Server หนึ่งถึงสามค่าที่มี IPv4 หรือ IPv6 แอดเดรสที่คั่นด้วย เครื่องหมานคอมม่า • ตัวอย่าง 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • ตัวอย่าง 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • ตัวอย่าง 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844, ::ffff:903:201	หากไม่ได้กำหนดอิลิเมนต์ Activation Engine จะใช้ค่าว่างดีฟอลต์ คือ **DNSServers**

ตารางที่ 9. แท็ก XML (ต่อ)

แท็ก	คำอธิบาย	ค่าที่ยอมรับได้	หมายเหตุ
IP4Config	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดค่าติดตั้งคอนฟิกูเรชัน IPv4	**IPType**: อิลิเมนต์ที่จำเป็นเพื่อกำหนดชนิดคอนฟิกูเรชัน IPv4 • **Static**: กำหนดค่าอะแด็ปเตอร์นี้โดยใช้คอนฟิกูเรชันแบบสแตติก • **DHCP**: กำหนดค่าอะแด็ปเตอร์นี้โดยใช้คอนฟิกูเรชัน DHCP • **DHCPServer**: กำหนดค่าอะแด็ปเตอร์นี้เป็นเซิร์ฟเวอร์ IPv4 DHCP (ต้องการให้ตั้งค่า **PrivateInterface** เป็น **Yes**) **IPAddress**: อิลิเมนต์ที่เป็นทางเลือกที่จำเป็นหากเลือกคอนฟิกูเรชัน **Static** หรือ **DHCPServer** เท่านั้น • **Static Configuration**: ค่า IPv4 แอดเดรสใด ๆ ที่ใช้ได้ • **DHCPServer Configuration**: IP ของเซิร์ฟเวอร์ DHCP ใด ๆ ภายในช่วง IP **Netmask**: อิลิเมนต์ที่เป็นทาวเลือกที่จำเป็นหากเลือกคอนฟิกูเรชัน **Static** เท่านั้น • ค่าเน็ตมาสก์ IPv4 ใด ๆ ที่ใช้ได้ **Gateway**: เกตเวย์ที่เป็นทางเลือกที่จำเป็นหากเลือกคอนฟิกูเรชัน **Static** เท่านั้น • ค่าเน็ตมาสก์ IPv4 ใด ๆ ที่ใช้ได้	
IP6Config	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดค่าติดตั้งคอนฟิกูเรชัน IPv6	**IPType**: อิลิเมนต์ที่จำเป็นเพื่อกำหนดชนิดคอนฟิกูเรชัน IPv6 • **Static**: กำหนดค่าอะแด็ปเตอร์นี้โดยใช้คอนฟิกูเรชันแบบสแตติก • **DHCP**: กำหนดค่าอะแด็ปเตอร์นี้โดยใช้คอนฟิกูเรชัน DHCP **IPAddress**: คุณสามารถกำหนดรูปแบบยาวหรือสั้นของรูปแบบ IPv6 และ รูปแบบยาวหรือสั้นของส่วนนำหน้า IPv6 • ตัวอย่าง 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888 • ตัวอย่าง 2: IPv6: 2001:4860:4860::8888 • ตัวอย่าง 3: IPv6: 2001:4860:4860::8888/128 หากไม่ได้ระบุส่วนนำหน้า Activation Engine จะใช้ค่าติดตั้งดีฟอลต์ที่เป็นส่วนนำหน้า /64 **Gateway**: • ค่าแอดเดรส IPv6 ใด ๆ ที่ใช้ได้	

ตารางที่ 9. แท็ก XML (ต่อ)

แท็ก	คำอธิบาย	ค่าที่ยอมรับได้	หมายเหตุ
Firewall	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดค่าติดตั้งไฟร์วอลล์	**PEGASUS**: • **Enabled**: อนุญาตให้เปิดพอร์ต PEGASUS • **Disabled**: ปิดใช้งานพอร์ต PEGASUS **RPD**: • **Enabled**: อนุญาตให้เปิดพอร์ต RMC • **Disabled**: ปิดใช้งานพอร์ต RMC **FCS**: • **Enabled**: อนุญาตให้เปิดพอร์ต FCS • **Disabled**: ปิดใช้งานพอร์ต FCS **I5250**: • **Enabled**: อนุญาตให้เปิดพอร์ต 5250 • **Disabled**: ปิดใช้งานพอร์ต 5250 **PING**: • **Enabled**: อนุญาตให้เปิดพอร์ต Ping • **Disabled**: ปิดใช้งานพอร์ต Ping **L2TP**: • **Enabled**: อนุญาตให้เปิดพอร์ต L2TP • **Disabled**: ปิดใช้งานพอร์ต L2TP **SLP**: • **Enabled**: อนุญาตให้เปิดพอร์ต SLP • **Disabled**: ปิดใช้งานพอร์ต SLP **RSCT**: • **Enabled**: อนุญาตให้เปิดพอร์ต RSCT • **Disabled**: ปิดใช้งานพอร์ต RSCT **SECUREREMOTEACCESS**: • **Enabled**: อนุญาตให้เปิดพอร์ต secure remote access • **Disabled**: ปิดใช้งานพอร์ต secure remote access **SSH**: • **Enabled**: อนุญาตให้เปิดพอร์ต SSH • **Disabled**: ปิดใช้งานพอร์ต SSH	
Firewall	อิลิเมนต์ที่เป็นทางเลือกเพื่อกำหนดค่าติดตั้งไฟร์วอลล์	**NTP**: • **Enabled**: อนุญาตให้เปิดพอร์ต NTP • **Disabled**: ปิดใช้งานพอร์ต NTP **SMNPTraps**: • **Enabled**: อนุญาตให้เปิดพอร์ต SMNP trap • **Disabled**: ปิดใช้งานพอร์ต SMNP trap **SMNPAgents**: • **Enabled**: อนุญาตให้เปิดพอร์ต SMNP agent • **Disabled**: ปิดใช้งานพอร์ต SMNP agent	

ตารางที่ 9. แท็ก XML (ต่อ)

แท็ก	คำอธิบาย	ค่าที่ยอมรับได้	หมายเหตุ

NTPServers	จำเป็นต้องระบุแท็ก **NTPServers** หากคุณต้องการกำหนดค่าเซิร์ฟเวอร์ NTP มากถึง 5 เซิร์ฟเวอร์ภายใน เครื่องมือเสมือน HMC	**NTPServers**: ยอมรับ `<ntpparam ntpserver="server" ntpversion="version"/>`
		ntpparam:
		• **ntpserver**: ยอมรับค่า IPv4 หรือ IPv6 ใด ๆ ที่ใช้ได้และ ชื่อโฮสต์ที่ถูกต้อง
		• **ntpversion**: ยอมรับค่าตัวเลข 1-4
		ตัวอย่าง:
		`<NTPServers> <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/> <ntpparam ntpserver="192.168.34.1" ntpversion="4"/> <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>`
		`</NTPServers>`	

การกำหนดคอนฟิก HMC

ศึกษาวิธีการตั้งค่าการเชื่อมต่อเครือข่าย การกำหนดคอนฟิก HMC ของคุณ ดำเนินการขั้นตอนหลังการกำหนดคอนฟิก และอัพเกรดและอัพเดต HMC ของคุณ

การเลือกการตั้งค่าเครือข่ายบน HMC

ศึกษาเกี่ยวกับการตั้งค่าเครือข่ายที่คุณสามารถใช้บน Hardware Management Console (HMC)

การเชื่อมต่อเน็ตเวิร์ก HMC

ศึกษาวิธีที่ Hardware Management Console HMC สามารถใช้ในเครือข่าย

คุณสามารถใช้การเชื่อมต่อเน็ตเวิร์กประเภทต่าง ๆ เพื่อเชื่อมต่อ HMC ของคุณกับระบบที่ถูกจัดการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีตั้งค่า HMC เพื่อเชื่อมต่อกับเน็ตเวิร์ก โปรดดูที่ “การกำหนดคอนฟิก HMC” ในหน้า 49 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ HMC บนเครือข่าย โปรดดูที่ข้อมูลต่อไปนี้:

ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC

ศึกษาวิธีใช้ฟังก์ชันการจัดการและการให้บริการแบบรีโมต HMC โดยใช้เครือข่ายของคุณ

HMC สนับสนุนการสื่อสารโลจิคัลในประเภทดังต่อไปนี้:

HMC ไปยังระบบที่ถูกจัดการ
ใช้เพื่อดำเนินฟังก์ชันการจัดการฮาร์ดแวร์โดยส่วนใหญ่ ซึ่ง HMC ออกคำขอฟังก์ชันควบคุมผ่านทางตัวประมวลผลเซอร์วิสของระบบที่ถูกจัดการ บางครั้ง การเชื่อมต่อระหว่าง HMC และตัวประมวลผลเซอร์วิสเรียกว่าเป็น *เน็ตเวิร์กบริการ* การเชื่อมต่อนี้ต้องใช้สำหรับการจัดการระบบที่ถูกจัดการ

HMC to logical partition
ใช้เพื่อรวบรวมข้อมูลที่เกี่ยวข้องกับแพล็ตฟอร์ม (เหตุการณ์ข้อผิดพลาดแพล็ตฟอร์ม การทำรายการฮาร์ดแวร์) จากระบบปฏิบัติการที่รันอยู่บนโลจิคัลพาร์ติชัน และเพื่อประสานกิจกรรมบางอย่างของแพล็ตฟอร์ม (LPAR แบบไดนามิก, การซ่อมพร้อมกัน) กับระบบปฏิบัติการเหล่านั้น หากคุณต้องการใช้บริการและคุณลักษณะการแจ้งข้อผิดพลาด คุณต้องสร้างการเชื่อมต่อนี้

HMC กับ BMC

หมายเหตุ: การเชื่อมต่อ baseboard management controller (BMC) ใช้ได้เฉพาะกับรุ่น HMC 7063-CR1

ใช้เพื่อดำเนินการงานการให้บริการและซ่อมบำรุง การเชื่อมต่อ BMC ใช้เพื่อโหลดและดูแลรักษาเฟิร์มแวร์ HMC บนระบบ การเชื่อมต่อนี้จำเป็นสำหรับการเข้าถึง BMC บน HMC

HMC to remote users
ช่วยให้ผู้ใช้รีโมตสามารถเข้าถึงฟังก์ชัน HMC ผู้ใช้รีโมตสามารถ เข้าถึง HMC โดยวิธีดังต่อไปนี้:

- โดยการใช้เว็บเบราว์เซอร์เพื่อเข้าถึงฟังก์ชัน HMC GUI ทั้งหมดแบบรีโมต
- โดยการใช้ Secure Socket Shell (SSH) เพื่อเข้าถึงฟังก์ชันบรรทัดรับคำสั่ง HMC แบบรีโมต
- โดยใช้เทอร์มินัลเซิร์ฟเวอร์เสมือนสำหรับการเข้าถึงคอนโซลของโลจิคัลพาร์ติชัน แบบรีโมต

HMC เพื่อให้บริการ และสนับสนุน
ใช้เพื่อส่งข้อมูล เช่น รายงานความผิดพลาดฮาร์ดแวร์ ข้อมูลคลัง และการอัพเดตไมโครโค้ด ไปยังและจากผู้ให้บริการของคุณ คุณสามารถใช้พาธการสื่อสารนี้เพื่อเรียกการให้บริการโดยอัตโนมัติ

HMC ของคุณสามารถสนับสนุนฟิสิคัลอีเทอร์เน็ตอินเตอร์เฟสได้มากถึงสี่อินเตอร์เฟส ขึ้นอยู่กับแต่ละรุ่น เวอร์ชันสแตนด์อะโลนของ HMC สนับสนุนอินเตอร์เฟส HMC สามอินเตอร์เฟสเท่านั้น โดยใช้อีเทอร์เน็ตอะแด็ปเตอร์รวมหนึ่งอะแด็ปเตอร์ และจนถึงสองอะแด็ปเตอร์ปลั๊กอิน ใช้อินเตอร์เฟส แต่ละตัวเหล่านี้ในวิธีดังต่อไปนี้:

- เน็ตเวิร์กอินเตอร์เฟสหนึ่งสามารถใช้เฉพาะกับการสื่อสารแบบ HMC-ไปที่-ระบบที่ถูกจัดการเท่านั้น ซึ่งหมายความว่า เฉพาะ HMC และตัวประมวลผลเซอร์วิสของระบบที่ถูกจัดการเท่านั้นที่จะอยู่บนเน็ตเวิร์กนั้น เน็ตเวิร์กอินเตอร์เฟสตั้งแต่หนึ่งขึ้นไปสามารถใช้เฉพาะสำหรับการสื่อสารแบบ HMC-ไปที่-ระบบที่ถูกจัดการเท่านั้น ซึ่งหมายความว่า เฉพาะ HMC และตัวประมวลผลเซอร์วิสของระบบที่ถูกจัดการเท่านั้นที่จะอยู่บนเน็ตเวิร์กนั้น แม้ว่าอินเตอร์เฟส เครือข่ายที่อยู่ในตัวประมวลผลเซอร์วิสมีการเข้ารหัสโปรโตคอล Secure Sockets Layer (SSL) และมีการป้องกันด้วยรหัสผ่าน การมีเครือข่าย เฉพาะงานที่แยกต่างหากสามารถช่วยให้อินเตอร์เฟสเหล่านี้มีระดับความปลอดภัย สูงขึ้น
- โดยทั่วไปแล้ว อินเตอร์เฟสเน็ตเวิร์กแบบเปิดใช้กับการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC และโลจิคัลพาร์ติชันบนระบบที่ถูกจัดการ สำหรับการสื่อสารแบบ HMC-ไปที่-โลจิคัลพาร์ติชัน คุณยังสามารถใช้เน็ตเวิร์กอินเตอร์เฟสแบบเปิดนี้เพื่อจัดการกับ HMC จากระยะไกล
- หรือคุณอาจใช้อินเตอร์เฟสอื่นเพื่อเชื่อมต่อกับโลจิคัลพาร์ติชัน และจัดการ HMC จากระยะไกล อินเตอร์เฟสนี้ยังสามารถใช้เป็นการเชื่อมต่อ HMC แยกต่างหากไปยังกลุ่มโลจิคัลพาร์ติชันอื่น ตัวอย่างเช่น คุณอาจต้องการให้มี LAN การจัดการที่แยกต่างหากจาก LAN ซึ่งธุรกรรมทางธุรกิจปกติทั้งหมดกำลัง รันอยู่ ผู้ดูแลระบบจากระยะไกลสามารถเข้าถึง HMC และ หน่วยที่ได้รับการจัดการอื่น ๆโดยใช้วิธีนี้ ในบางครั้งโลจิคัลพาร์ติชันจะอยู่ใน โดเมนความปลอดภัยเครือข่ายอื่น อาจจะเป็นด้านหลังไฟร์วอลล์ และคุณอาจต้องการมี การเชื่อมต่อเครือข่าย HMC ที่แตกต่างกันสำหรับสองโดเมนเหล่านั้น

ข้อกำหนดเว็บเบราว์เซอร์สำหรับ HMC

Hardware Management Console (HMC) เวอร์ชัน 9.1.0 สนับสนุนโดย Google Chrome เวอร์ชัน 57, Microsoft Internet Explorer (IE) เวอร์ชัน 11.0, Mozilla Firefox เวอร์ชัน 45 และ 52 Extended Support Release (ESR) และ Safari เวอร์ชัน 10.1

ถ้า เบราว์เซอร์ของคุณมีการกำหนดคอนฟิกเพื่อใช้อินเทอร์เน็ตพร็อกซี โลคัล IP แอดเดรส ควรมีการรวมไว้ในรายการข้อยกเว้น โปรดปรึกษาผู้ดูแลระบบเครือข่าย ของคุณสำหรับข้อมูลเพิ่มเติมเกี่ยวกับรายการข้อยกเว้น ถ้าคุณยังคง จำเป็นต้องใช้พร็อกซีเพื่อเรียกใช้ HMC ให้เปิดใช้งาน การใช้ HTTP 1.1 ผ่านทาง การเชื่อมต่อพร็อกซี ภายใต้แท็บขั้นสูง ในหน้าต่าง อ็อพชันอินเทอร์เน็ต

ต้องเปิดใช้งานเซสชันคุกกี้เพื่อ ให้ ASMI สามารถทำงานได้เมื่อเชื่อมต่อกับ HMC แบบรีโมต รหัสพร็อกซี asm บันทึก และใช้ข้อมูลเซสชัน ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อเปิดใช้งาน เซสชันคุกกี้

การเปิดใช้งานเซสชันคุกกี้ใน Internet Explorer

1. เลือก เครื่องมือ และคลิก อ็อพชันอินเทอร์เน็ต
2. เลือก ความเป็นส่วนตัว และคลิก ขั้นสูง
3. ตรวจสอบให้แน่ใจว่าได้เลือก อนุญาตเซสชันคุกกี้เสมอ ถ้ายังไม่ได้เลือก ให้เลือก ยกเลิกการจัดการคุกกี้อัตโนมัติ และเลือก อนุญาต เซสชันคุกกี้เสมอ
4. เลือก พร้อมต์ภายใต้คุกกี้ของบุคคลที่หนึ่งและคุกกี้ของบุคคลที่สาม
5. คลิก ตกลง

การเปิดใช้งานเซสชันคุกกี้ใน Firefox

1. เลือก เครื่องมือ และคลิก อ็อพชัน

2. คลิก คุกกี้
3. เลือก อนุญาตให้ไซต์ตั้งค่าคุกกี้
4. เลือก ข้อยกเว้น และเพิ่ม HMC
5. คลิก ตกลง

เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC
Hardware Management Console (HMC) สามารถกำหนดค่าเพื่อให้เครือข่ายเปิดและเครือข่ายไพรเวต เครือข่ายไพรเวตอนุญาตให้ใช้ช่วงของ IP แอดเดรสที่ไม่สามารถกำหนดเส้นทางได้ที่เลือก เน็ตเวิร์กแบบ *พับลิก* หรือแบบ "เปิด" หมายถึงการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC กับโลจิคัลพาร์ติชันและ ระบบอื่น ๆ บนเน็ตเวิร์กปกติของคุณ

เน็ตเวิร์กส่วนตัว

เน็ตเวิร์กส่วนตัวของ HMC มีเพียงอุปกรณ์เดียว นั่นคือ HMC และระบบที่ถูกจัดการแต่ละระบบที่ HMC เชื่อมต่ออยู่ HMC ถูกเชื่อมต่อกับ Flexible Service Processor (FSP) ของระบบที่ถูกจัดการแต่ละระบบ

ในระบบส่วนใหญ่ FSP จะมีพอร์ตอีเทอร์เน็ตสองพอร์ตที่ใช้เลเบล **HMC1** และ **HMC2** คุณสามารถเชื่อมต่อไปถึงสอง HMC

บางระบบมี อ็อพชัน dual-FSP ในสถานการณ์นี้ FSP ที่สองทำหน้าที่เป็น อุปกรณ์สำรอง ข้อกำหนดการตั้งค่าพื้นฐานสำหรับระบบที่มีสอง FSP จำเป็นต้องเหมือนกับระบบ ที่ไม่มี FSP สำรอง HMC ต้องเชื่อมต่อกับแต่ละ FSP ดังนั้น จึงต้องการฮาร์ดแวร์เครือข่ายมากขึ้น (เช่น สวิทช์ LAN หรือฮับ) เมื่อมีมากกว่าหนึ่ง FSP หรือมีระบบที่ถูกจัดการหลายระบบ

หมายเหตุ: พอร์ต FSP แต่ละพอร์ตบนระบบที่ถูกจัดการจะต้องเชื่อมต่อกับ HMC เพียงเครื่องเดียวเท่านั้น

พับลิกเน็ตเวิร์ก

เครือข่ายเปิดสามารถเชื่อมต่อกับไฟร์วอลล์หรือเราเตอร์สำหรับการเชื่อมต่อกับอินเทอร์เน็ต การเชื่อมต่อกับอินเทอร์เน็ตอนุญาตให้ HMC สามารถ call home ได้เมื่อมีข้อผิดพลาดเกี่ยวกับฮาร์ดแวร์ที่ต้อง รายงาน

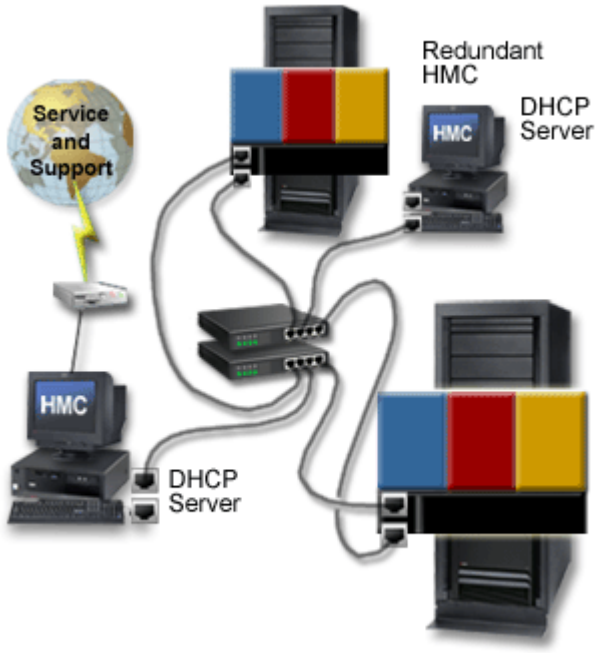
HMC ประกอบด้วยไฟร์วอลล์บนแต่ละ เน็ตเวิร์กอินเตอร์เฟส ไฟร์วอลล์ระดับต้นจะถูกตั้งค่าโดยอัตโนมัติเมื่อคุณรันวิซาร์ด HMC Guided Setup แต่คุณควรปรับการตั้งค่าไฟร์วอลล์หลังจากการติดตั้งและการคอนฟิก HMC เบื้องต้น

HMC เป็นเซิร์ฟเวอร์ DHCP
คุณสามารถใช้ Hardware Management Console (HMC) เป็นเซิร์ฟเวอร์ Dynamic Host Configuration Protocol (DHCP)

ถ้าคุณต้องการตั้งค่าเน็ตเวิร์กอินเตอร์เฟสแรกเป็นเน็ตเวิร์กส่วนตัว คุณสามารถเลือกได้จากช่วงของ IP แอดเดรสสำหรับเซิร์ฟเวอร์ DHCP เพื่อกำหนดให้กับไคลเอ็นต์ ช่วงแอดเดรสที่เลือกได้ประกอบไปด้วย เซ็กเมนต์จากช่วง IP แอดเดรสมาตรฐานที่ไม่สามารถเราต์ได้

นอกจากช่วงมาตรฐานเหล่านี้ ยังมีช่วงพิเศษของ IP แอดเดรส ที่สำรองไว้สำหรับ IP แอดเดรส คุณสามารถใช้ช่วงพิเศษนเพื่อหลีกเลี่ยงการขัดแย้งในกรณีที่เครือข่ายเปิดที่เชื่อมต่อกับ HMC กำลังใช้ช่วงแอดเดรส ที่ไม่สามารถกำหนดเส้นทางได้ ขึ้นอยู่กับช่วงที่เลือก อินเตอร์เฟสเครือข่าย HMC บนเครือข่ายส่วนตัวจะได้รับการกำหนด IP แอดเดรสแรกของช่วงดังกล่าวโดยอัตโนมัติ และจากนั้นตัวประมวลผลเซอร์วิสจะได้รับการกำหนดแอดเดรส จากช่วงที่เหลือ

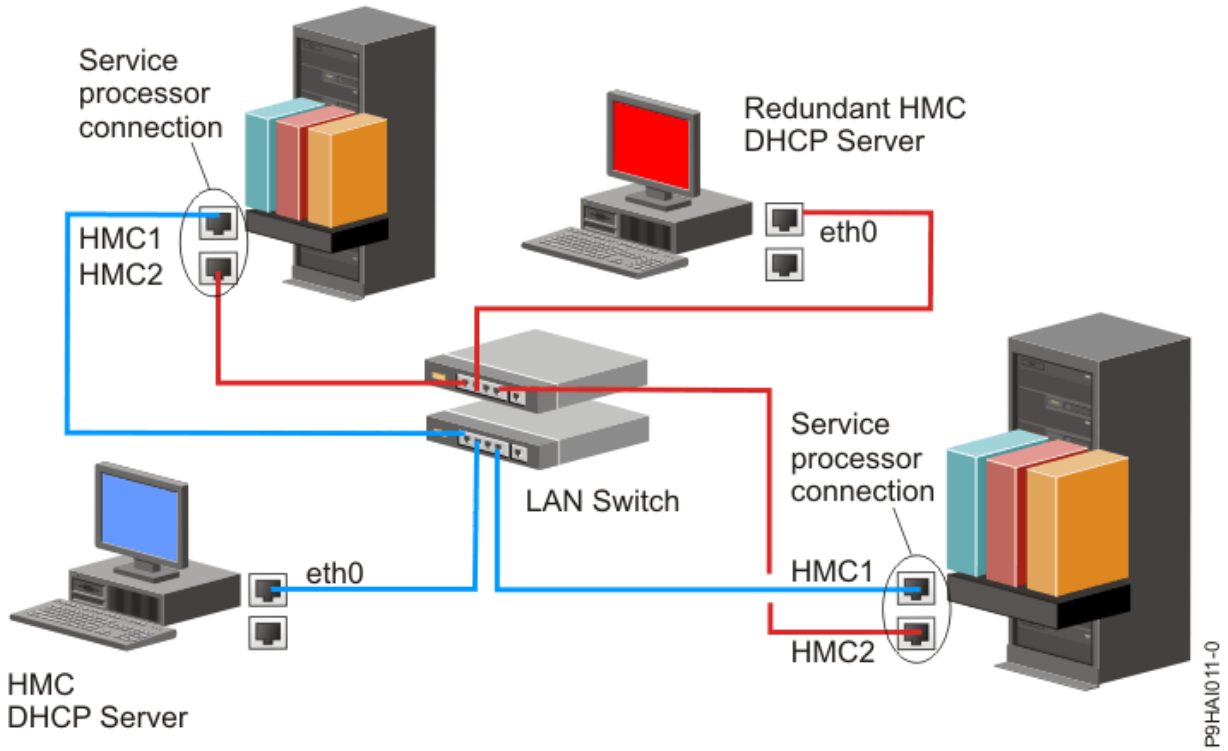
เซิร์ฟเวอร์ DHCP ใน HMC ใช้ การจัดสรรโดยอัตโนมัติ ซึ่งหมายความว่าแต่ละอินเตอร์เฟสอีเทอร์เน็ตของตัวประมวลผลเซอร์วิสเฉพาะ จะได้รับการกำหนด IP แอดเดรสเดียวกันอีกครั้งในแต่ละครั้งที่อินเตอร์เฟสเริ่มทำงาน แต่ละอินเตอร์เฟสอีเทอร์เน็ตจะมีตัวบ่งชี้เฉพาะ ที่อิงตามแอดเดรส Media Access Control (MAC) ในตัว ซึ่งทำให้เซิร์ฟเวอร์ DHCP สามารถกำหนดพารามิเตอร์ IP เดิมได้อีกครั้ง คุณสามารถตั้งค่าพอร์ต HMC ได้ทั้ง **eth0** และ **eth1** เพื่อใช้แอดเดรส DHCPคุณสามารถตั้งค่าพอร์ต HMC ได้ทั้ง **eth0** และ **eth1** เพื่อใช้แอดเดรส DHCP



รูปที่ 9. เน็ตเวิร์กส่วนตัวที่มีหนึ่ง HMC เป็นเซิร์ฟเวอร์ DHCP

หมายเหตุ: ถ้าคุณกำลังใช้ IPv6 กระบวนการค้นหาต้องทำด้วยตนเอง สำหรับ IPv6 การค้นหาโดยอัตโนมัติ จะไม่พร้อมใช้งาน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ “การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 56



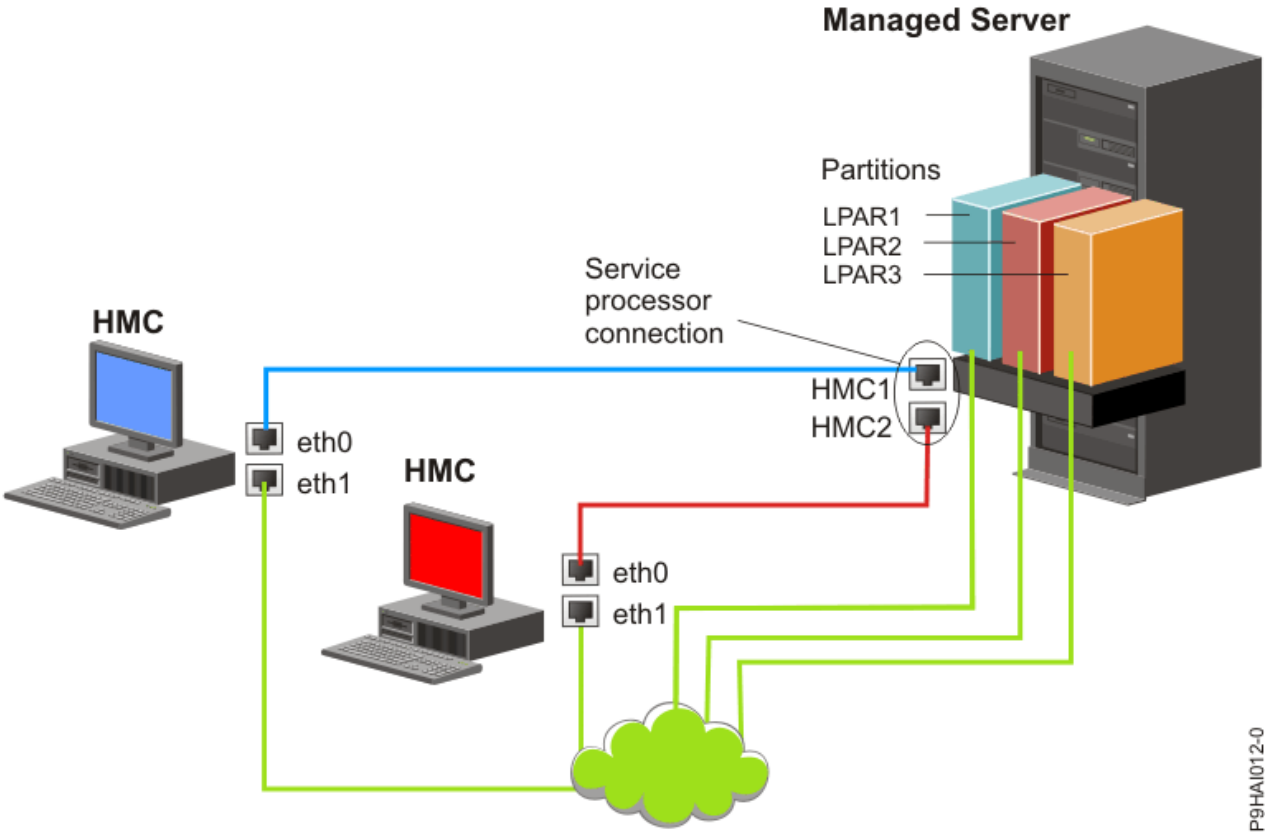
รูปภาพนี้แสดงสภาวะแวดล้อม HMC สำรอง พร้อมด้วย ระบบที่ถูกจัดการ 2 ระบบ HMC เครื่องแรกเชื่อมต่อกับพอร์ตแรกบนแต่ละ FSP และ HMC สำรองเชื่อมต่อกับพอร์ตที่สองบน HMC แต่ละเครื่อง แต่ละ HMC ถูกกำหนดค่าเป็นเซิร์ฟเวอร์

DHCP โดยใช้ช่วงของ IP แอดเดรสที่แตกต่างกัน การเชื่อมต่ออยู่บนเน็ตเวิร์กส่วนตัวที่แยกต่างหาก ด้วยเหตุนี้ จึงจำเป็นอย่างยิ่ง ที่จะต้องตรวจสอบให้แน่ใจว่าพอร์ต FSP ไม่ได้เชื่อมต่อกับ HMC มากกว่าหนึ่งเครื่อง

พอร์ต FSP ของระบบที่ถูกจัดการแต่ละระบบ ที่เชื่อมต่อกับ HMC ต้องมี IP แอดเดรสที่ไม่ซ้ำกัน เพื่อให้แน่ใจว่าแต่ละ FSP มี IP แอดเดรสที่ไม่ซ้ำกัน ให้ใช้ความสามารถเซิร์ฟเวอร์ DHCP แบบในตัวของ HMC เมื่อ FSP ตรวจพบ เน็ตเวิร์กลิงก์ที่แอ็คทีฟ ก็จะกระจายคำร้องขอเพื่อหาตำแหน่งของเซิร์ฟเวอร์ DHCP เมื่อตั้งค่าอย่างเหมาะสม HMC จะตอบสนองต่อคำร้องขอนั้น โดยจัดสรรหนึ่งในช่วงแอดเดรสที่เลือก

หากคุณมีหลาย FSP คุณต้องมีสวิตช์หรือฮับ LAN ส่วนตัวสำหรับ HMC ไปยังเน็ตเวิร์กส่วนตัว FSP อีกทางหนึ่งคือ เซ็กเมนต์ ส่วนตัวนี้สามารถมีอยู่ในรูปแบบหลายพอร์ตใน *virtual LAN* (VLAN) แบบไพรเวต บนสวิตช์ขนาดใหญ่ที่ถูกจัดการ หากคุณมี VLAN ไพรเวตจำนวนมาก คุณต้องตรวจสอบให้แน่ใจว่า แต่ละ VLAN แยกจากกัน และไม่มีทราฟฟิกข้ามระหว่างกัน

ถ้าคุณมี HMC มากกว่าหนึ่งเครื่อง คุณจะต้องเชื่อมต่อ HMC แต่ละเครื่องเข้ากับโลจิคัลพาร์ติชัน และเชื่อมต่อ HMC เข้าด้วยกัน บนเน็ตเวิร์กแบบเปิดเดียวกัน



รูปนี้แสดง HMC สองเครื่องที่เชื่อมต่อกับเซิร์ฟเวอร์ที่ถูกจัดการเดียวบนเน็ตเวิร์กส่วนตัว และกับโลจิคัลพาร์ติชัน 3 พาร์ติชันบนเน็ตเวิร์กสาธารณะ คุณสามารถมีอะแด็ปเตอร์อีเทอร์เน็ตเพิ่มเติม เพื่อให้ HMC สามารถมีอินเตอร์เฟสเครือข่ายสามอินเตอร์เฟส คุณสามารถใช้เน็ตเวิร์กที่สามนี้เป็นเน็ตเวิร์กการจัดการ หรือเชื่อมต่อกับ CSM (Cluster Systems Manager) Management Server

การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home

ศึกษาเพิ่มเติมเกี่ยวกับอ็อพชันของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

คุณสามารถกำหนดค่า Hardware Management Console (HMC) เพื่อส่งข้อมูลที่เกี่ยวข้องกับเซอร์วิสของฮาร์ดแวร์ ให้กับ IBM โดยใช้การเชื่อมต่ออินเทอร์เน็ตผ่าน LAN หรือการเชื่อมต่อผ่านโมเด็ม

คุณมีตัวเลือกด้านการสื่อสารสองตัวเลือกเมื่อกำหนดค่าการเชื่อมต่ออินเทอร์เน็ตผ่าน LAN ทางเลือกแรกคือใช้ Secure Sockets Layer (SSL) มาตรฐาน คุณสามารถเปิดใช้งานการสื่อสาร SSL เพื่อ เชื่อมต่อกับอินเทอร์เน็ตผ่านพร็อกซีเซิร์ฟเวอร์ การเชื่อมต่อ SSL มีแนวโน้มว่า จะสอดคล้องกับแนวทางความปลอดภัยขององค์กร

หมายเหตุ: หากการเชื่อมต่ออินเตอร์เฟสเครือข่ายเปิดของคุณใช้เฉพาะ Internet Protocol Version 6 (IPv6) คุณจะไม่สามารถใช้ VPN อินเทอร์เน็ตเพื่อเชื่อมต่อกับฝ่ายสนับสนุน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรโตคอล ที่ใช้ โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 40

ข้อดีของการใช้การเชื่อมต่ออินเทอร์เน็ตอาจได้แก่:

- ความเร็วในการรับส่งข้อมูลที่เร็วกว่า
- ลดค่าใช้จ่ายสำหรับลูกค้า (เช่น ค่าสายโทรศัพท์อนาล็อก ที่จัดเตรียมไว้โดยเฉพาะ)
- ความเชื่อถือได้สูงกว่า

ลักษณะความปลอดภัยต่อไปนี้มีผลบังคับใช้ ไม่ว่าคุณจะเลือกใช้ วิธีการเชื่อมต่อแบบใดก็ตาม:

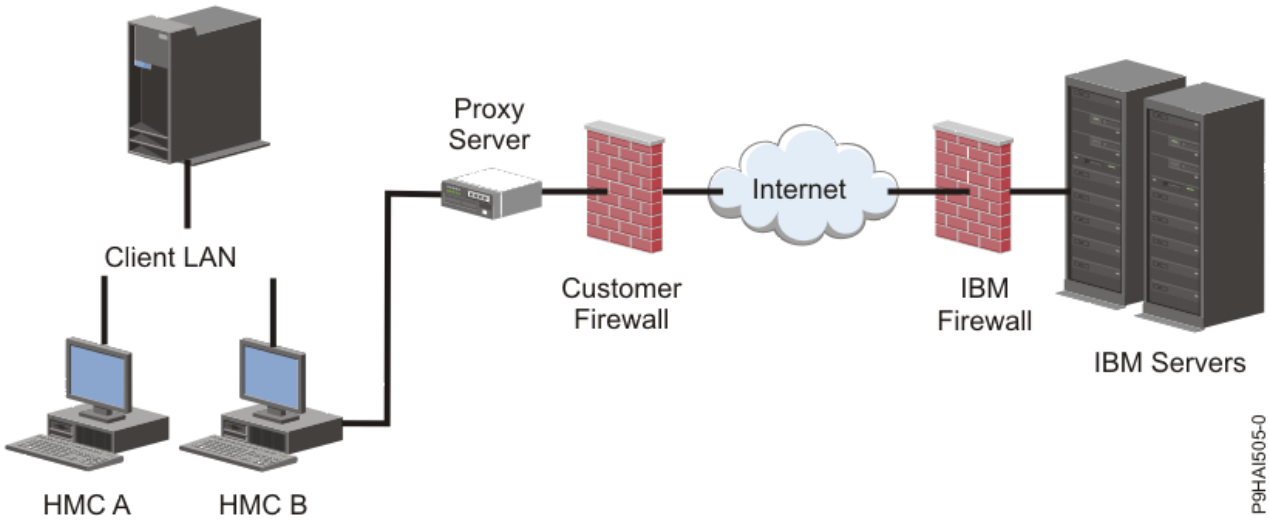
- คำร้องขอของระบบสนับสนุนแบบรีโมตเริ่มต้นจาก HMC ไปยัง IBM การเชื่อมต่อขาเข้าไม่ได้เริ่มจาก IBM Service Support System
- ข้อมูลทั้งหมดที่โอนระหว่าง HMC และ IBM Service Support System จะถูกเข้ารหัสโดยใช้การเข้ารหัส ระดับสูง ขึ้นอยู่กับเมธอดของภาวะเชื่อมต่อที่เลือก ซึ่งจะเข้ารหัสโดยใช้ SSL หรือ IPSec Encapsulating Security Payload (ESP)
- เมื่อคุณกำหนดค่าเริ่มต้นสำหรับการเชื่อมต่อที่เข้ารหัส HMC จะพิสูจน์ตัวตนปลายทางเป้าหมายเป็น IBM Service Support System

ข้อมูลที่ส่งไปยัง IBM Service Support System ประกอบด้วยข้อมูลเกี่ยวกับปัญหาของฮาร์ดแวร์ และคอนฟิกูเรชัน ไม่มีแอ็พพลิเคชันหรือข้อมูลลูกค้าถูกส่งไปยัง IBM

การใช้การเชื่อมต่ออินเทอร์เน็ตทางอ้อมด้วยพร็อกซีเซิร์ฟเวอร์

หากการติดตั้งของคุณต้องการให้ HMC อยู่ในเครือข่ายส่วนตัว คุณอาจสามารถเชื่อมต่อ ทางอ้อมกับอินเทอร์เน็ตโดยใช้พร็อกซี SSL ซึ่งสามารถส่งต่อคำร้องขอไปยังอินเทอร์เน็ต หนึ่งในข้อดี อีกประการหนึ่งของการใช้พร็อกซี SSL คือ พร็อกซีสามารถสนับสนุนการจัดทำบันทึกและอำนวยความสะดวกด้านการตรวจสอบ

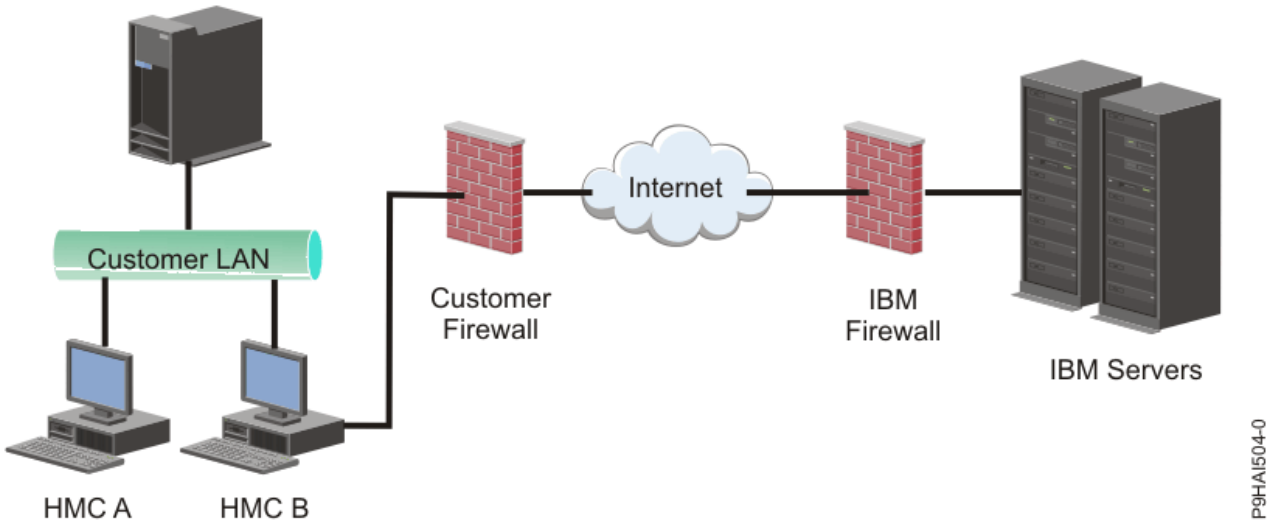
เมื่อต้องการส่งต่อ ซ็อกเก็ต SSL พร็อกซีเซิร์ฟเวอร์จะต้องสนับสนุนฟังก์ชันส่วนหัวพร็อกซีระดับต้น (ตามที่ระบุไว้ใน RFC 2616) และเมธอด CONNECT หรือ คุณสามารถเลือกกำหนดค่าการพิสูจน์ตัวตนพร็อกซีพื้นฐาน (RFC 2617) เพื่อให้ HMC พิสูจน์ตัวตนก่อนที่คุณจะพยายามส่งต่อซ็อกเก็ตผ่าน พร็อกซีเซิร์ฟเวอร์



เพื่อให้ HMC สื่อสารได้สำเร็จ พร็อกซีเซิร์ฟเวอร์ของลูกค้าจะต้องอนุญาตให้เชื่อมต่อ กับพอร์ต 443 คุณสามารถกำหนดคอนฟิกพร็อกซีเซิร์ฟเวอร์ของคุณเพื่อจำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 40 สำหรับ รายการ IP แอดเดรส

การใช้การเชื่อมต่อ SSL อินเทอร์เน็ตโดยตรง

หาก HMC ของคุณสามารถเชื่อมต่อกับอินเทอร์เน็ต และสามารถตั้งค่าไฟร์วอลล์ภายนอกเพื่ออนุญาตให้ แพ็กเก็ต TCP ที่สร้างขึ้นส่งไปยังปลายทางได้ดังอธิบายใน “รายการแอดเดรส Internet SSL” ในหน้า 40 คุณสามารถใช้การเชื่อมต่ออินเทอร์เน็ตโดยตรง



การใช้ SSL อินเทอร์เน็ตเพื่อเชื่อมต่อกับฝ่ายสนับสนุนแบบรีโมต

การสื่อสารทั้งหมดได้รับการจัดการผ่านซ็อกเก็ต TCP ที่เริ่มต้นโดย Hardware Management Console (HMC) และใช้ SSL ระดับสูงเพื่อเข้ารหัสข้อมูลที่ถูกส่ง แอดเดรส TCP/IP ปลายทางถูกเผยแพร่ (โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 40) เพื่อที่ว่าไฟร์วอลล์ภายนอก จะสามารถตั้งค่าเพื่ออนุญาตการเชื่อมต่อเหล่านี้

หมายเหตุ: พอร์ต HTTPS มาตรฐาน 443 ใช้สำหรับการสื่อสารทั้งหมด

HMC สามารถเปิดใช้งานเพื่อเชื่อมต่อโดยตรงกับอินเทอร์เน็ตหรือเพื่อเชื่อมต่อทางอ้อมจาก พร็อกซีเซิร์ฟเวอร์ที่ลูกค้าเป็นผู้จัดเตรียม การตัดสินใจเกี่ยวกับวิธีที่ดีที่สุดสำหรับการติดตั้ง ขึ้นอยู่กับการข้อกำหนดด้านความปลอดภัยและเครือข่ายขององค์กรของคุณ HMC (โดยตรงหรือผ่านพร็อกซี SSL) ใช้แอดเดรสต่อไปนี้เมื่อถูกกำหนดค่าเพื่อใช้ การเชื่อมต่อ SSL อินเทอร์เน็ต

การเลือก อินเทอร์เน็ตโปรโตคอล

ระบุเวอร์ชันของ IP แอดเดรสที่ใช้เมื่อ Hardware Management Console (HMC) เชื่อมต่อกับผู้ให้บริการ

ผู้ใช้ส่วนมากจะใช้ Internet Protocol Version 4 (IPv4) เพื่อเชื่อมต่อไปยังผู้ให้บริการ IPv4 แอดเดรส จะปรากฏในรูปแบบที่แสดง 4 ไบต์ของ IPv4 แอดเดรส ซึ่งคั่นด้วย จุด (เช่น 9.60.12.123) เพื่อเข้าถึงอินเทอร์เน็ต คุณยังสามารถใช้ Internet Protocol Version 6 (IPv6) เพื่อเชื่อมต่อไปยังผู้ให้บริการได้เช่นกัน ทั้งนี้ IPv6 มักถูกใช้งานโดยผู้บริหารเน็ตเวิร์ก เพื่อให้แน่ใจว่ามีพื้นที่ที่อยู่จะที่ไม่ซ้ำกัน ถ้าคุณ ไม่แน่ใจเกี่ยวกับอินเทอร์เน็ตโปรโตคอลที่ใช้ในการติดตั้งของคุณ โปรดติดต่อ ผู้ดูแลระบบเครือข่ายของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เวอร์ชันแต่ละเวอร์ชัน โปรดดูที่ “การตั้งค่า IPv4 address” ในหน้า 57 และ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 58

รายการแอดเดรส Internet SSL

ศึกษาเกี่ยวกับแอดเดรสที่ Hardware Management Console (HMC) ใช้เมื่อ HMC ใช้การเชื่อมต่อ SSL กับอินเทอร์เน็ต

HMC ใช้ IPv4 แอดเดรสต่อไปนี้เพื่อติดต่อฝ่ายบริการและสนับสนุนของ IBM เมื่อกำหนดคอนฟิกไว้เพื่อใช้การเชื่อมต่อ SSL กับอินเทอร์เน็ต

แอดเดรส IPv4 ต่อไปนี้ สำหรับทุกสถานที่:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216
- 170.225.15.41

แอดเดรส IPv4 ต่อไปนี้สำหรับทวีปอเมริกา:

- 129.42.160.48
- 129.42.160.49

- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

แอดเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่ที่ไม่ใช่อเมริกา:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

หมายเหตุ: เมื่อคุณกำหนดคอนฟิกไฟร์วอลล์เพื่ออนุญาตให้ HMC เชื่อมต่อกับเซิร์ฟเวอร์เหล่านี้ ต้องใช้ IP แอดเดรสเฉพาะภูมิภาคดังกล่าวเท่านั้น

HMC ใช้ IPv6 แอดเดรสต่อไปนี้เพื่อติดต่อฝ่ายบริการและสนับสนุนของ IBM เมื่อกำหนดคอนฟิกไว้เพื่อใช้การเชื่อมต่อ SSL กับอินเทอร์เน็ต:

- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์

ศึกษาเกี่ยวกับสิ่งที่คุณต้องทราบเมื่อคุณตัดสินใจที่จะใช้เซิร์ฟเวอร์ call-home มากกว่าหนึ่งเซิร์ฟเวอร์

เพื่อหลีกเลี่ยงไม่ให้มีความล้มเหลวจากจุดเดียว ให้กำหนดค่า Hardware Management Console (HMC) เพื่อใช้เซิร์ฟเวอร์ call-home หลายเซิร์ฟเวอร์ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานเซิร์ฟเวอร์แรก จะพยายามจัดการเหตุการณ์เซอร์วิสแต่ละเหตุการณ์ หากการเชื่อมต่อหรือการส่งข้อมูลล้มเหลวกับเซอร์วิส call-home นี้ จะมีการพยายามคำร้องขอเซอร์วิส โดยใช้เซอร์วิส call-home อื่นที่พร้อมใช้งานจนกว่าจะสำเร็จ หรือ ได้พยายามกับเซอร์วิสทั้งหมดแล้ว

HMC ที่เชื่อมต่อที่ได้รับการระบุแล้วจากการวิเคราะห์ปัญหาให้เป็นคอนโซล,การวิเคราะห์หลัก สำหรับระบบที่ถูกจัดการที่กำหนดที่รายงานปัญหา คอนโซลหลักนี้ยังเรพลิเคท รายงานปัญหาไปยัง HMC สำรองใด ๆ ด้วย HMC หลักจะต้องจดจำ HMC รองบนเน็ตเวิร์กได้ด้วย HMC หลัก จะรู้จัก HMC สำรองเป็นเซิร์ฟเวอร์ call-home เพิ่มเติมเมื่อ:

- HMC หลักถูกกำหนดค่าเพื่อใช้เซิร์ฟเวอร์ call-home "ที่ค้นพบ" และเซิร์ฟเวอร์ call-home บนซับเน็ตเดียวกันกับ HMC หลัก หรือจัดการระบบเดียวกัน
- เซิร์ฟเวอร์ call-home จะถูกเพิ่มเข้ากับรายการของคอนโซลเซิร์ฟเวอร์ call-home ที่พร้อมใช้งานสำหรับ การเชื่อมต่อขาแบบแมนนวล

การจัดเตรียมสำหรับการตั้งค่าของ HMC

ศึกษาเกี่ยวกับการตั้งค่าการกำหนดคอนฟิกที่คุณต้องทราบก่อนที่จะเริ่มต้น ขั้นตอนการกำหนดคอนฟิก

เมื่อต้องการกำหนดคอนฟิก HMC คุณต้องเข้าใจแนวคิดที่เกี่ยวข้อง ทำการตัดสินใจและ เตรียมข้อมูล

ศึกษาเกี่ยวกับข้อมูลที่คุณต้องการเพื่อเชื่อมต่อ HMC ของคุณกับตำแหน่งต่อไปนี้:

- ตัวประมวลผลเซอร์วิสในระบบที่ถูกจัดการของคุณ
- โลจิคัลพาร์ติชันในระบบที่ถูกจัดการเหล่านั้น
- รีโมตเวิร์กสเตชัน
- IBM Service เพื่อใช้ฟังก์ชัน “call-home”

เมื่อต้องการจัดเตรียมสำหรับการตั้งค่า HMC ให้ดำเนินการขั้นตอน ต่อไปนี้:

1. ขอรับและติดตั้งระดับท้ายสุดของโค้ด HMC ในเวอร์ชันที่คุณต้องการติดตั้ง
2. กำหนดสถานที่ติดตั้ง HMC ที่สัมพันธ์กับเซิร์ฟเวอร์ที่จะจัดการ หาก HMC อยู่ห่างจากระบบที่ถูกจัดการมากกว่า 25 ฟุต คุณต้องเตรียมการเข้าถึงเว็บเบราว์เซอร์ไปยัง HMC จากที่ตั้งของระบบที่ถูกจัดการนั้น เพื่อให้พนักงานฝ่ายบริการสามารถเข้าถึง HMC ได้
3. ระบุเซิร์ฟเวอร์ที่ HMC จัดการ

4. กำหนดว่าคุณจะใช้เครือข่ายไพรเวตหรือเครือข่ายเปิดเพื่อจัดการเซิร์ฟเวอร์ หากคุณเลือกใช้ เน็ตเวิร์กส่วนตัว ให้ใช้ DHCP เว้นแต่คุณกำลังใช้การตั้งค่า Cluster Systems Management (CSM) CSM ไม่ได้รับการสนับสนุน IPv6 เมื่อต้องการเข้าถึง CSM คุณต้องมีเน็ตเวิร์กสองวง สำหรับข้อมูลเพิ่มเติม เกี่ยวกับ CSM โปรดดูเอกสารคู่มือที่ให้พร้อมกับคุณลักษณะนั้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเน็ตเวิร์กแบบเปิดและเน็ตเวิร์กส่วนตัว โปรดดูที่ “การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 56
5. หากคุณใช้เครือข่ายเปิดเพื่อจัดการ FSP คุณต้องตั้งค่าแอดเดรสของ FSP ด้วยตัวเองผ่านเมนู Advanced System Management Interface ขอแนะนำให้ใช้เน็ตเวิร์กส่วนตัวที่ไม่สามารถกำหนดเราต์ได้
6. หากคุณมีสอง HMC ให้กำหนด HMC หลักและรอง HMC ต้องอยู่ใกล้กับระบบ และต้องเป็น HMC ที่กำหนดค่าเพื่อ call home
7. กำหนดค่าติดตั้งเครือข่ายที่คุณต้องการเพื่อเชื่อมต่อ HMC กับรีโมตเวิร์กสเตชัน โลจิคัลพาร์ติชัน และอุปกรณ์เครือข่าย
8. กำหนดวิธีที่ HMC จะ call home อ็อพชัน Call home รวมถึงการเชื่อมต่ออินเทอร์เน็ตแบบ Secure Socket Layer (SSL) ขาออกเท่านั้น โมเด็ม หรือการเชื่อมต่อ Virtual Private Network (VPN)
9. กำหนดผู้ใช้ HMC ที่คุณสร้างและรหัสผ่าน รวมทั้งบทบาทที่ผู้ใช้ได้รับ คุณต้องกำหนดรหัสผ่านให้กับผู้ใช้ **hscroot** และ **hscpe**
10. จัดทำเอกสารข้อมูลติดต่อบริษัทต่อไปนี้ที่ต้องใช้เมื่อคุณกำหนดค่า call home:
    - ชื่อบริษัท
    - การติดต่อผู้ดูแลระบบ
    - อีเมลแอดเดรส
    - หมายเลขโทรศัพท์
    - หมายเลขแฟ็กซ์
    - แอดเดรสของที่ตั้งทางกายภาพของ HMC
11. หากคุณวางแผนที่จะใช้อีเมลเพื่อแจ้งโอเปอร์เรเตอร์หรือผู้ดูแลระบบเมื่อข้อมูลถูกส่งไปยัง IBM Service ผ่าน call-home ให้ระบุเซิร์ฟเวอร์ Simple Mail Transfer Protocol (SMTP) และอีเมลแอดเดรสที่คุณใช้
12. คุณต้องกำหนดรหัสผ่านต่อไปนี้:
    - รหัสผ่านการเข้าถึงที่ใช้เพื่อพิสูจน์ตัวตน HMC กับ FSP
    - รหัสผ่าน ASMI ที่ใช้สำหรับผู้ใช้ **admin**
    - รหัสผ่าน ASMI ที่ใช้สำหรับผู้ใช้ **general**

    สร้างรหัสผ่านเมื่อคุณเชื่อมต่อจาก HMC ไปยังเซิร์ฟเวอร์ใหม่ เป็นครั้งแรก หาก HMC เป็น HMC สำรองหรือเครื่องที่สอง ให้ขอรับรหัสผ่านผู้ใช้ HMC และเตรียมป้อนค่าเมื่อ คุณเชื่อมต่อกับ FSP ของเซิร์ฟเวอร์ที่ถูกจัดการเป็นครั้งแรก

เมื่อคุณเสร็จสิ้นขั้นตอนการเตรียมเหล่านี้แล้ว ให้ดำเนินการ “เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 42

เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC

ใช้เวิร์กชีตนี้เพื่อดูข้อมูลการติดตั้งที่คุณต้องเตรียมพร้อมสำหรับการติดตั้ง

นโยบายรหัสผ่านที่ปรับปรุงสำหรับ HMC

คุณต้องตั้งรหัสผ่านใหม่ในการใช้งานครั้งแรกสำหรับระบบที่ผลิตขึ้นใหม่ที่มี HMC เวอร์ชัน 9.940.0 หรือใหม่กว่า และหลังจากที่ดำเนินการรีเซ็ตระบบกลับเป็นค่าจากโรงงาน การเปลี่ยนแปลงนโยบายนี้ ช่วยบังคับไม่ให้ HMC อยู่ในสถานะที่ใช้รหัสผ่านที่รู้จักกันดี

ด้วย HMC เวอร์ชัน 9.940.0 และใหม่กว่า รหัสผ่าน `hscroot` จะหมดอายุ และต้องเปลี่ยนก่อนที่คุณจะสามารถเข้าถึงฟังก์ชันของ HMC ได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการ เปลี่ยนรหัสผ่าน โปรดดูที่ https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm อย่างไรก็ตาม หากคุณกำลังอัพเกรดจากระดับ HMC ก่อนหน้า หรือการติดตั้งปฏิบัติการ คุณยังไม่จำเป็นต้องเปลี่ยนรหัสผ่าน

การตั้งค่าเน็ตเวิร์ก

อินเตอร์เฟส LAN: เลือกอะแด็ปเตอร์ที่มี (เช่น eth0, eth1) ที่ใช้โดย HMC นี้เพื่อ เชื่อมต่อกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน บริการและการสนับสนุน และผู้ใช้รีโมต สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 34 การเชื่อมต่อ จาก HMC สามารถอยู่บนเน็ตเวิร์กส่วนตัวหรือเน็ตเวิร์กแบบเปิด

ความเร็วของอีเทอร์เน็ตอะแด็ปเตอร์และ Duplex

ป้อนความเร็วและโหมด duplex ของอะแด็ปเตอร์อีเทอร์เน็ตที่ต้องการ อ็อพชัน autodetection จะระบุว่าอ็อพชันใดเหมาะสมที่สุด ถ้าคุณไม่แน่ใจว่าความเร็ว และ duplex ใดจะก่อให้เกิดผลลัพธ์ที่ดีที่สุดสำหรับฮาร์ดแวร์ของคุณ ดีฟอลต์ = Autodetection ความเร็วของสื่อบันทึกระบุความเร็วในโหมด duplex ของอีเทอร์เน็ตอะแด็ปเตอร์ เลือก Autodetection ยกเว้นคุณต้องการระบุความเร็วของสื่อที่แน่นอน อุปกรณ์ใด ๆ ที่เชื่อมต่อกับ FSP (สวิทช์/HMC) ต้องตั้งค่าเป็น Auto (ความเร็ว) / โหมด Auto (Duplex) เนื่องจากเป็น ค่าติดตั้ง FSP ดีฟอลต์และไม่สามารถเปลี่ยนได้

ตารางที่ 10. ความเร็วของอีเทอร์เน็ตอะแด็ปเตอร์และ Duplex

ลักษณะเฉพาะ	**eth0**	**eth1**	**eth2**	**eth3**
เลือกความเร็วและโหมด duplex				
ความเร็วของสื่อบันทึก (Autodetection, 10/100/1000 Full/Half Duplex)				

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเน็ตเวิร์กแบบเปิดและเน็ตเวิร์กส่วนตัว โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 36

ตารางที่ 11. เครือข่ายไพรเวตหรือแบบเปิด

ลักษณะเฉพาะ	**eth0**	**eth1**	**eth2**	**eth3**
ระบุเครือข่าย **ไพรเวต** หรือ **เปิด** สำหรับแต่ละอะแด็ปเตอร์				

Dynamic Host Configuration Protocol (DHCP) มีวิธีอัตโนมัติสำหรับการตั้งค่าคอนฟิกไคลเอ็นต์แบบไดนามิก คุณสามารถระบุ HMC นี้เป็นเซิร์ฟเวอร์ DHCP ถ้าเป็น HMC เครื่องแรกหรือเครื่องเดียวบนเน็ตเวิร์กส่วนตัว ให้เปิดใช้งาน HMC เป็น เซิร์ฟเวอร์ DHCP เมื่อคุณเปิดใช้งาน HMC เป็นเซิร์ฟเวอร์ DHCP ระบบที่ถูกจัดการบนเครือข่ายจะถูกตั้งค่าและค้นพบโดย HMC โดยอัตโนมัติ

สำหรับอีเทอร์เน็ตอะแด็ปเตอร์ที่ระบุ เป็นเน็ตเวิร์กส่วนตัว ให้ดำเนินการตามตารางต่อไปนี้:

ตารางที่ 12. เซิร์ฟเวอร์ DHCP

ลักษณะเฉพาะ	**eth0**	**eth1**
คุณต้องการระบุ HMC นี้เป็นเซิร์ฟเวอร์ DHCP หรือไม่? (ใช่/ไม่ใช่)		
หากใช่ ให้บันทึกช่วงของ IP ที่คุณต้องการใช้		

หากคุณกำลังใช้ 7063-CR1 HMC คุณ ต้องเชื่อมต่อพอร์ต Ethernet **IPMI** กับเครือข่ายเพื่อเข้าถึง baseboard management controller (BMC) บน HMC สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “กำหนดค่าการเชื่อมต่อ BMC” ในหน้า 57 กรอกข้อมูลในตารางต่อไปนี้สำหรับการเชื่อมต่อ BMC ของคุณ

ตารางที่ 13. การเชื่อมต่อ BMC	
ลักษณะเฉพาะ	**IPMI**
คุณต้องการกำหนดค่าการเชื่อมต่อนี้โดยใช้โหมด DHCP หรือไม่ (ใช่/ไม่ใช่)	
หากไม่ แสดงรายการสแตติกแอดเดรสที่ระบุด้านล่าง:	
IP แอดเดรส:	
Subnet mask:	
เกตเวย์:	

สำหรับอีเทอร์เน็ตอะแด็ปเตอร์ที่ระบุเป็นเน็ตเวิร์ก *เปิด* ให้ดำเนินการตามตารางต่อไปนี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอินเทอร์เน็ตโปรโตคอลเวอร์ชันอื่น โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 52

การใช้ IPv6

หากคุณกำลังใช้ IPv6 ให้ปรึกษากับผู้บริหารเน็ตเวิร์กของคุณ แล้วเลือกวิธีที่คุณต้องการใช้รับ IP แอดเดรส หลังจากนั้น ให้ดำเนินการตาม ตารางต่อไปนี้:

ตารางที่ 14. IPv6 (static)				
ลักษณะเฉพาะ	**eth0**	**eth1**	**eth2**	**eth3**
คุณกำลังใช้ IP แอดเดรสที่กำหนดแบบสแตติกหรือไม่? หากใช่ ให้บันทึกแอดเดรสนั้นไว้ที่นี่				

ตารางที่ 15. IPv6 (เซิร์ฟเวอร์ DHCP)				
ลักษณะเฉพาะ	**eth0**	**eth1**	**eth2**	**eth3**
คุณกำลังรับ IP แอดเดรสจากเซิร์ฟเวอร์ DHCP ใช่หรือไม่? (ใช่/ไม่ใช่)				

ตารางที่ 16. IPv6 (เราเตอร์ IPv6)				
ลักษณะเฉพาะ	**eth0**	**eth1**	**eth2**	**eth3**
คุณกำลังรับ IP แอดเดรสจากเราเตอร์ IPv6 ใช่หรือไม่?				

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า IPv6 address โปรดดูที่ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 58 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ IPv6 แอดเดรสเท่านั้น โปรดดูที่ “การใช้ IPv6 แอดเดรสเท่านั้น” ในหน้า 58

การใช้ IPv4

กรอกข้อมูลในตารางต่อไปนี้สำหรับอะแด็ปเตอร์อีเทอร์เน็ตที่ระบุเป็นเครือข่ายเปิดโดยใช้ IPv4

ตารางที่ 17. IPv4				
ลักษณะเฉพาะ	**eth0**	**eth1**	**eth2**	**eth3**
คุณต้องการรับ IP แอดเดรสโดยอัตโนมัติหรือไม่? (ใช่/ไม่ใช่)				
ถ้า ไม่ แสดงรายการแอดเดรสที่ระบุ ด้านล่าง:				
TCP/IP Interface Address:				
TCP/IP Interface Network Mask:				
ค่าติดตั้งไฟร์วอลล์:				
คุณต้องการกำหนดคอนฟิกไฟร์วอลล์ HMC หรือไม่? (ใช่/ไม่ใช่)				
หากใช่ ให้แสดงรายการแอ็พพลิเคชันและ IP แอดเดรสที่ต้องได้รับอนุญาต ผ่านไฟร์วอลล์:				

ข้อมูลTCP/IP

ต้องใช้แอดเดรส TCP/IP ที่ไม่ซ้ำกันสำหรับแต่ละโหนด ทั้งสำหรับ Support Element (SE) และ Hardware Management Console (HMC) โดย network mask ที่กำหนด จะถูกใช้ ในการสร้างแอดเดรสที่ไม่ซ้ำกัน ตามค่าดีฟอลต์ สำหรับ LAN ส่วนตัวแบบโลคัล หากโหนดเชื่อมต่อกับเครือข่ายขนสดใหญ่ที่มี TCP/IP แอดเดรสที่มีการจัดการ คุณสามารถระบุ TCP/IP แอดเดรสที่จะใช้ ระบบจะสร้าง ค่าดีฟอลต์

การตั้งค่าไฟร์วอลล์

ค่าติดตั้งไฟร์วอลล์ HMC จะสร้างเครื่องกีดกั้นด้านความปลอดภัยที่อนุญาตหรือปฏิเสธ การเข้าถึงเน็ตเวิร์กแอ็พพลิเคชันที่เฉพาะเจาะจงบน HMC คุณสามารถระบุค่าติดตั้งการควบคุมเหล่านี้แต่ละค่าสำหรับแต่ละอินเตอร์เฟสเครือข่ายฟิสิคัล ซึ่งช่วยให้คุณสามารถควบคุมว่าแอ็พพลิเคชันเครือข่าย HMC ใดที่สามารถเข้าถึงได้ บนแต่ละเครือข่าย

หากคุณกำหนดค่าอะแด็ปเตอร์อย่างน้อยหนึ่งอะแด็ปเตอร์เป็นอะแด็ปเตอร์เครือข่ายเปิด คุณต้องระบุ ข้อมูลเพิ่มเติมเพื่อให้ HMC ของคุณสามารถเข้าถึง LAN ได้:

ตารางที่ 18. อะแด็ปเตอร์เน็ตเวิร์กแบบเปิด	
ข้อมูลโฮสต์แบบโลคัล	
ชื่อโฮสต์ HMC:	
โดเมนเนม:	
รายละเอียดของ HMC:	
ข้อมูลเกตเวย์	
แอดเดรสเกตเวย์: (nnn.nnn.nnn.nnn)	
อุปกรณ์เกตเวย์:	
การเปิดใช้ DNS	
คุณต้องการใช้ DNS หรือไม่? (ใช่/ไม่ใช่)	

ตารางที่ 18. อะแด็ปเตอร์เน็ตเวิร์กแบบเปิด (ต่อ)	
ข้อมูลโฮสต์แบบโลคัล	
หากตอบ “ใช่” ให้ระบุลำดับการค้นหาเซิร์ฟเวอร์ DNS ที่ด้านล่างนี้:	
1.	
2.	
ลำดับการค้นหาโดเมนซัฟฟิกซ์:	
1.	
2.	

ข้อมูลโลคัลโฮสต์
เมื่อต้องการระบุ Hardware Management Console (HMC) ให้กับเน็ตเวิร์ก ให้ป้อน ชื่อโฮสต์และโดเมนเนมของ HMC นอกจากว่าคุณใช้เฉพาะชื่อโฮสต์แบบย่อ บนเน็ตเวิร์กของคุณเท่านั้น ให้ป้อนชื่อโฮสต์แบบเต็ม ตัวอย่างโดเมนเนม: name.yourcompany.com

ข้อมูลเกตเวย์
เมื่อต้องการกำหนดเกตเวย์ดีฟอลต์ ให้ระบุ TCP/IP แอดเดรสที่จะใช้สำหรับการกำหนดเส้นทางแพ็กเก็ต IP เกตเวย์แอดเดรส จะแจ้งให้คอมพิวเตอร์แต่ละเครื่องหรืออุปกรณ์เครือข่ายว่าจะส่งข้อมูลเมื่อใด หากสถานีเป้าหมาย ไม่อยู่บนซับเน็ตเดียวกับต้นทาง

การเปิดใช้ DNS
Domain Name System (DNS) ใช้ในการจัดหาหลักการตั้งชื่อมาตรฐาน สำหรับการระบุตำแหน่งคอมพิวเตอร์บนมาตรฐาน IP ด้วยการกำหนดเซิร์ฟเวอร์ DNS คุณสามารถใช้ ชื่อโฮสต์เพื่อระบุเซิร์ฟเวอร์และ Hardware Management Consoles (HMCs) แทนที่จะใช้ IP แอดเดรส

ลำดับการค้นหาเซิร์ฟเวอร์ DNS
ป้อน IP แอดเดรสของเซิร์ฟเวอร์ DNS ที่จะถูกค้นหา สำหรับการแม็พชื่อโฮสต์ และ IP แอดเดรส ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

ลำดับการค้นหาโดเมนซัฟฟิกซ์
ป้อนโดเมนซัฟฟิกซ์ที่คุณกำลังใช้ HMC จะใช้โดเมนซัฟฟิกซ์ เพื่อผนวกเข้ากับชื่อที่ไม่ถูกต้องสำหรับการค้นหา DNS ซัฟฟิกซ์จะถูกค้นหา ตามลำดับที่แสดงอยู่ในรายการ ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

การแจ้งเตือนทางอีเมล

แสดงรายการข้อมูลติดต่อทางอีเมล หากคุณต้องการได้รับแจ้งทางอีเมลเมื่อเกิดปัญหาเกี่ยวกับฮาร์ดแวร์ บนระบบ

ตารางที่ 19. การแจ้งเตือนทางอีเมล	
ลักษณะเฉพาะ	**ฟิลด์รายการ**
อีเมลแอดเดรส:	
เซิร์ฟเวอร์ SMTP:	
พอร์ต:	
ข้อผิดพลาดที่จะแจ้ง:	
เฉพาะปัญหา call-home เท่านั้น	
ปัญหาทั้งหมด	

เซิร์ฟเวอร์ SMTP
พิมพ์แอดเดรส simple mail transfer Protocol (SMTP) ของเซิร์ฟเวอร์ ที่จะได้รับแจ้งเกี่ยวกับเหตุการณ์ของระบบ ตัวอย่างของชื่อเซิร์ฟเวอร์ SMTP คือ `relay.us.ibm.com`

SMTP เป็นโปรโตคอล ที่ใช้เพื่อส่งอีเมล เมื่อคุณใช้ SMTP ไคลเอ็นต์จะส่งข้อความและสื่อสาร กับเซิร์ฟเวอร์ SMTP โดใช้โปรโตคอล SMTP

ถ้า คุณไม่ทราบแอดเดรส SMTP ของเซิร์ฟเวอร์ของคุณ หรือไม่แน่ใจ ให้ติดต่อ ผู้บริหารเน็ตเวิร์กของคุณ

พอร์ต
พิมพ์หมายเลขพอร์ตของเซิร์ฟเวอร์ที่จะรับแจ้งเกี่ยวกับเหตุการณ์ของระบบ หรือ ใช้พอร์ตดีฟอลต์

อีเมลแอดเดรสที่จะรับแจ้ง
ป้อนอีเมลแอดเดรสที่ตั้งค่าให้รับข้อความแจ้งเตือน เมื่อเกิดเหตุการณ์ของระบบ

- เลือก **เหตุการณ์ปัญหา call-home เท่านั้น** เพื่อรับการแจ้งเตือนเมื่อ เกิดเหตุการณ์ที่สร้างฟังก์ชัน call-home เท่านั้น
- เลือก **All problem events** เพื่อรับการแจ้งเตือน เมื่อเกิดเหตุการณ์ใด ๆ

ข้อมูลติดต่อฝ่ายบริการ

ตารางที่ 20. ข้อมูลติดต่อฝ่ายบริการ

ลักษณะเฉพาะ	**ฟิลด์รายการ**
ชื่อบริษัท	
ชื่อผู้ดูแล	
อีเมลแอดเดรส	
หมายเลขโทรศัพท์	
หมายเลขโทรศัพท์อื่น	
หมายเลขโทรสาร	
หมายเลขโทรศัพท์อื่น	
ที่อยู่	
ที่อยู่ 2	
เมืองหรือเขต	
สถานะ	
รหัสไปรษณีย์	
ประเทศหรือภูมิภาค	
ตำแหน่งของ HMC (ถ้าเหมือนกับที่อยู่ของผู้ดูแลระบบข้างต้น ให้ระบุ “same”):	
ที่อยู่	
ที่อยู่ 2	
เมืองหรือเขต	
สถานะ	
รหัสไปรษณีย์	
ประเทศหรือภูมิภาค	

การให้สิทธิและการเชื่อมต่อส่วนบริการ

เลือก ประเภทของการเชื่อมต่อเพื่อติดต่อผู้ให้บริการของคุณ สำหรับรายละเอียดของวิธีเหล่านี้ ที่รวมคุณสมบัติด้านความปลอดภัยและข้อกำหนดการกำหนดคอนฟิก โปรดดูที่ “การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้” ในหน้า 64

ตารางที่ 21. การให้สิทธิและการเชื่อมต่อส่วนบริการ	
ลักษณะเฉพาะ	**ฟิลด์รายการ**
Secure Sockets Layer (SSL) ผ่านอินเทอร์เน็ต	_____
Virtual private network (VPN) ผ่าน อินเทอร์เน็ต	_____

Secure Sockets Layer (SSL) ผ่านอินเทอร์เน็ต:

หากคุณมีการเชื่อมต่ออินเทอร์เน็ตจาก HMC ของคุณอยู่แล้ว คุณสามารถใช้การเชื่อมต่อนี้เพื่อติดต่อ ผู้ให้บริการของคุณ คุณสามารถเชื่อมต่อกับผู้ให้บริการของคุณโดยตรงโดยใช้ Secure Sockets Layer (SSL) ที่เข้ารหัสโดยใช้การเชื่อมต่ออินเทอร์เน็ตที่มีอยู่ เลือก **ใช้พร็อกซี SSL** หากคุณ ต้องการกำหนดค่าการใช้ SSL ที่เข้ารหัสโดยใช้การเชื่อมต่อทางอ้อมที่ใช้พร็อกซี SSL

ตารางที่ 22. SSL	
ลักษณะเฉพาะ	**ฟิลด์รายการ**
ใช้พร็อกซี SSL? (ใช่/ไม่ใช่)	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
แอดเดรส:	
พอร์ต:	
พิสูจน์ตัวตนด้วยพร็อกซี SSL?	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
ผู้ใช้:	
รหัสผ่าน:	

โปรโตคอลการเชื่อมต่ออินเทอร์เน็ตที่ใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรโตคอลอินเทอร์เน็ตที่แตกต่างกัน โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 52

___ IPv4

___ IPv6

___ IPv4 และ IPv6

Virtual Private Network (VPN)

หากคุณมีการเชื่อมต่ออินเทอร์เน็ตจาก HMC ของคุณอยู่แล้ว คุณสามารถใช้การเชื่อมต่อนี้เพื่อติดต่อ ผู้ให้บริการของคุณ คุณสามารถเชื่อมต่อกับผู้ให้บริการของคุณโดยตรงโดยใช้ virtual private network (VPN) โดยใช้การเชื่อมต่ออินเทอร์เน็ตที่มีอยู่

หมายเหตุ: หากคุณเลือก Virtual Private Network (VPN) ผ่านอินเทอร์เน็ต คุณจะไม่สามารถเลือกอ็อพชันอื่น

เซิร์ฟเวอร์ Call-home

กำหนดว่า HMC ใดที่ คุณต้องการคอนฟิกเพื่อให้เชื่อมต่อกับฝ่ายสนับสนุนและบริการเป็นเซิร์ฟเวอร์ Call-Home สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เซิร์ฟเวอร์ Call-Home หลาย ๆ เซิร์ฟเวอร์ โปรดดูที่ “การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์” ในหน้า 41

___ HMC นี้

___ HMC อื่น

หากคุณเลือก **HMC อื่น** จะแสดงรายการ HMC อื่นที่กำหนดค่าเป็น เซิร์ฟเวอร์ call-home ที่นี่:

ตารางที่ 23. HMC อื่นที่กำหนดค่าเป็นเซิร์ฟเวอร์ call-home
แสดงรายการของชื่อโฮสต์ HMC หรือ IP แอดเดรสที่กำหนดค่าเป็นเซิร์ฟเวอร์ call-home

ประโยชน์เพิ่มเติมสำหรับการสนับสนุน

My Systems และ Premium Search

ตารางที่ 24. My Systems และ Premium Search	
ลักษณะเฉพาะ	**ฟิลด์รายการ**
แสดงรายการ IBM ID ของคุณ	_____
แสดง IBM ID เพิ่มเติม	_____

เมื่อต้องการเข้าถึงข้อมูลสนับสนุนที่มีค่าที่กำหนดเองในส่วน My Systems และ Premium Search ของเว็บไซต์ Electronic Services ลูกค้าต้องลงทะเบียน IBM ID ของตนกับระบบนี้ ถ้าคุณยังไม่มี คุณสามารถลงทะเบียนสำหรับ IBM ID ได้ที่: www.ibm.com/account/profile

หมายเหตุ: IBM จัดเตรียมฟังก์ชันบนเว็บที่กำหนดในแบบของคุณที่ใช้ข้อมูลที่ แอ็พพลิเคชัน IBM Electronic Service Agent รวบรวมไว้ เพื่อใช้ฟังก์ชันเหล่านี้ คุณต้องลงทะเบียนบนเว็บไซต์ IBM Registration ก่อนที่ http://www.ibm.com/account/profile

เมื่อต้องการอนุญาตให้ผู้ใช้ใช้ข้อมูล Electronic Service Agent เพื่อกำหนดฟังก์ชันบนเว็บในแบบของตน ให้ป้อน IBM ID ที่คุณลงทะเบียนไว้บนเว็บไซต์ IBM Registration ไปที่ http://www.ibm.com/support/electronic the valuable เพื่อดูข้อมูลการสนับสนุนที่มีประโยชน์ ซึ่งพร้อมใช้งานสำหรับลูกค้าที่ลงทะเบียน IBM ID ไว้กับระบบ

การกำหนดคอนฟิก HMC

กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก ความปลอดภัย เซอร์วิสแอ็พพลิเคชัน และความต้องการส่วนตัวบางอย่างของผู้ใช้

ขึ้นอยู่กับระดับของการปรับแต่งค่าเองที่คุณต้องการกำหนดให้กับคอนฟิกูเรชัน HMC ของคุณ คุณมีอ็อพชันหลายอ็อพชันสำหรับการตั้งค่า HMC เพื่อให้เหมาะสมกับความต้องการของคุณ วิซาร์ดการติดตั้งที่แนะนำ คือเครื่องมือใน HMC ซึ่งได้รับการออกแบบมาเพื่อช่วยให้การตั้งค่า HMC เป็นไปอย่างง่ายดาย คุณสามารถเลือกใช้วิธีลัดผ่านทางวิซาร์ดเพื่อสร้างสภาวะแวดล้อมของ HMC ตามที่แนะนำได้อย่างรวดเร็ว หรือคุณสามารถเลือกที่จะสำรวจการกำหนดค่าทั้งหมดที่วิซาร์ดแนะนำ คุณยังสามารถดำเนินการขั้นตอนการกำหนดคอนฟิกโดยไม่ต้องใช้วิซาร์ดโดย การกำหนดค่า HMC โดยใช้เมนูของ HMC

ก่อนที่คุณจะเริ่มต้น ให้รวบรวมข้อมูลการตั้งค่าที่ต้องการ ซึ่งคุณจำเป็นต้องปฏิบัติตามขั้นตอนต่าง ๆ ให้เสร็จสิ้นอย่างสมบูรณ์ โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 41 สำหรับรายการของข้อมูลที่ต้องการ เมื่อคุณเตรียมการเสร็จสิ้น ตรวจดูให้แน่ใจว่าคุณเสร็จสิ้น “เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 42 และกลับไปสู่ส่วนนี้

การกำหนดคอนฟิก HMC โดย ใช้พาธด่วนผ่านทางวิซาร์ดเซ็ตอัพที่แนะนำ

ในหลาย ๆ กรณี HMC สามารถตั้งค่าเพื่อ ให้ทำงานได้อย่างมีประสิทธิภาพโดยใช้ค่าติดตั้งดีฟอลต์หลาย ๆ ค่า ใช้รายการตรวจสอบวิธีลัดนี้เพื่อเตรียม HMC สำหรับการให้บริการ เมื่อคุณดำเนินการขั้นตอนเหล่านี้ HMC จะถูกกำหนดค่าเป็นเซิร์ฟเวอร์ Dynamic Host Configuration Protocol (DHCP) ในเครือข่ายส่วนตัว (เชื่อมต่อโดยตรง)

การกำหนดค่า HMC โดยใช้เมนู

ส่วนนี้มีรายการที่ครบถ้วนของงานคอนฟิกูเรชัน HMC ทั้งหมด ซึ่งช่วยแนะแนวทางตลอดกระบวนการกำหนดคอนฟิก HMC ของคุณ เลือก อ็อพชันนี้ถ้าคุณไม่ต้องการใช้ วิซาร์ดการติดตั้งที่แนะนำ

คุณต้องรีสตาร์ท HMC เพื่อให้ค่าติดตั้งคอนฟิกูเรชันมีผลใช้งาน ดังนั้น คุณอาจต้องการพิมพ์รายการตรวจสอบนี้ และเก็บไว้กับคุณเมื่อทำการกำหนดคอนฟิก HMC

ข้อมูลนี้ประกอบด้วยการอ้างอิงถึง งานที่ไม่รวมอยู่ในเอกสารนี้ คุณสามารถเข้าสู่ ข้อมูลฮาร์ดแวร์ของ IBM Power Systems บน HMC หรือบนเว็บได้ บน HMC, IBM Knowledge Center สามารถถูกเข้าถึงจากมุมบนขวา ของแถบงาน บนเว็บ IBM Knowledge Center สามารถเข้าถึงได้ที่ https://www.ibm.com/support/knowledgecenter

ข้อมูลนี้ประกอบด้วยการอ้างอิงถึงงานที่ไม่รวมอยู่ใน PDF นี้ คุณสามารถเข้าถึงสื่อประกอบเพิ่มเติม ที่สนับสนุนได้โดยอ้างถึงส่วนของ **Additional Resources** บนหน้า HMC Welcome

สิ่งที่ต้องการก่อน

ก่อนที่คุณจะเริ่มกำหนดคอนฟิก HMC โดยใช้เมนู HMC ตรวจดู ให้แน่ใจว่าได้ทำงานจัดเตรียมคอนฟิกูเรชัน ตามที่อธิบายใน “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 41 แล้ว

ตารางที่ 25. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่ที่สามารถหาข้อมูลที่เกี่ยวข้องได้

ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. สตาร์ท HMC	“การเริ่มต้น HMC” ในหน้า 51
2. ตั้งค่าวันที่และเวลา	
3. เปลี่ยนรหัสผ่านที่กำหนดไว้ล่วงหน้า	
4. สร้างผู้ใช้เพิ่มเติม และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
5. กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก	“การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 52
6. สำหรับ HMC โมเดล 7063-CR1 คุณต้อง กำหนดค่า IP แอดเดรสของ baseboard management controller (BMC)	“กำหนดค่าการเชื่อมต่อ BMC” ในหน้า 57
7. หากคุณกำลังใช้เครือข่ายเปิดและ IP แอดเดรสแบบคงที่ ให้ตั้งค่า ข้อมูลการระบุ	
8. หากคุณกำลังใช้เครือข่ายเปิดและ IP แอดเดรสแบบคงที่ ให้กำหนดค่า รายการการกำหนดเส้นทางเป็นดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” ในหน้า 59
9. หากคุณกำลังใช้เครือข่ายเปิดและ IP แบบคงที่ ให้กำหนดค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 60
10. ถ้าคุณกำลังใช้ IP แอดเดรส แบบคงที่ และเปิดใช้งาน DNS ให้กำหนดคอนฟิกโดเมนซัฟฟิกซ์	“การตั้งค่าคอนฟิกโดเมนซัฟฟิกส์” ในหน้า 60
11. กำหนดคอนฟิกเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการและสนับสนุน IBM และส่งคืนรายการตรวจสอบนี้เมื่อคุณได้ทำขั้นตอนนี้เสร็จสิ้นแล้ว	“การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน” ในหน้า 62
12. ตั้งค่าฐานข้อมูล Events สำหรับการจัดทำเวอร์ชัน	“การกำหนดคอนฟิก Events Manager for Call Home” ในหน้า 65
13. เชื่อมต่อระบบที่ถูกจัดการเข้ากับแหล่งจ่ายไฟ	
14. ตั้งค่ารหัสผ่านให้กับระบบที่ถูกจัดการ และรหัสผ่านของ ASMI แต่ละรายการ (general และ admin)	“การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ” ในหน้า 66
15. เข้าใช้ ASMI เพื่อตั้งวันที่และเวลาบนระบบที่ถูกจัดการ	
16. สตาร์ทระบบที่ถูกจัดการ และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
17. ตรวจสอบว่า คุณมีหนึ่งโลจิคัลพาร์ติชันบนระบบที่ถูกจัดการ	
18. ทางเลือก: เพิ่มระบบที่ถูกจัดการอีก และกลับไปสู่รายการตรวจสอบเมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	

ตารางที่ 25. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่ที่สามารถหาข้อมูลที่เกี่ยวข้องได้ (ต่อ)	
ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
19. ทางเลือก: หากคุณกำลังติดตั้งเซิร์ฟเวอร์ใหม่ด้วย HMC ของคุณ ให้ตั้งค่าโลจิคัลพาร์ติชันและติดตั้งระบบปฏิบัติการ	
20. หากคุณไม่ได้กำลังติดตั้งเซิร์ฟเวอร์ใหม่ในเวลานี้ ให้ทำงาน postconfiguration ซึ่งเลือกดำเนินการได้ เพื่อปรับค่าคอนฟิกูเรชัน ของคุณต่อไปอีก	“ขั้นตอน Postconfiguration” ในหน้า 68

การเริ่มต้น HMC

คุณสามารถล็อกอินเข้าสู่ HMC และเลือกภาษาที่คุณต้องการจะแสดงในอินเตอร์เฟส ใช้ User ID `hscroot` ที่เป็นค่าดีฟอลต์และรหัสผ่าน `abc123` เพื่อล็อกอินเข้าสู่ HMC ในครั้งแรก

เกี่ยวกับภารกิจนี้

เมื่อต้องการเริ่มต้น HMC ให้ทำโพรซีเดอร์ต่อไปนี้:

กระบวนการ

1. เปิด HMC โดยกดปุ่มเปิด/ปิด
2. หากภาษาอังกฤษเป็นการกำหนดค่าตามความชอบของภาษาของคุณ โปรดดำเนินขั้นตอนที่ 4

   ถ้าคุณต้องการใช้ภาษาอื่นที่นอกเหนือจากภาษาอังกฤษ ให้พิมพ์หมายเลข **2** เมื่อคุณได้รับข้อความเตือนให้เปลี่ยนโลแคล

   หมายเหตุ: ข้อความแจ้งเตือนนี้จะปรากฏอยู่เป็นเวลา 30 นาทีหากคุณไม่ดำเนินการใด ๆ
3. เลือกโลแคลที่คุณต้องการแสดงจากรายการ ในหน้าต่าง **การเลือกโลแคล** และคลิก **ตกลง** โลแคลจะระบุภาษาที่อินเตอร์เฟส HMC ใช้
4. คลิก **ล็อคออนและเรียกใช้เว็บแอ็พพลิเคชัน Hardware Management Console**
5. ล็อกอินเข้าสู่ HMC โดยใช้ ID ผู้ใช้และรหัสผ่านดีฟอลต์ต่อไปนี้:

   ID: `hscroot`
   รหัสผ่าน: `abc123`

   HMC Enhanced
   แสดง GUI ที่ปรับปรุงใหม่ซึ่งมีคุณลักษณะ PowerVM ที่ปรับปรุง

   HMC Classic
   แสดง GUI มาตรฐานซึ่งไม่มีคุณลักษณะ PowerVM ที่ปรับปรุง

   หมายเหตุ: เมื่อ HMC ทำงานเป็นเซิร์ฟเวอร์ DHCP, HMC จะใช้รหัสผ่านดีฟอลต์ เมื่อเชื่อมต่อกับตัวประมวลผลเซอร์วิสในครั้งแรก
6. กด Enter

การเปลี่ยนวันที่และเวลา

นาฬิกาแบบใช้แบตเตอรี่จะบันทึกวันที่และเวลาสำหรับ Hardware Management Console (HMC) คุณอาจต้องรีเซ็ตวันที่ และเวลาของคอนโซลหากเปลี่ยนแบตเตอรี่ หรือย้ายระบบของคุณไปยังเขตเวลาที่แตกต่าง ศึกษาเกี่ยวกับวิธีการเปลี่ยนวันที่และเวลาสำหรับ HMC

เกี่ยวกับภารกิจนี้

หากคุณเปลี่ยนข้อมูลของวันที่ และเวลา, การเปลี่ยนแปลงนั้นจะไม่ส่งผลต่อระบบ และโลจิคัลพาร์ติชันที่ HMC จัดการอยู่

เมื่อต้องการเปลี่ยน วันที่และเวลาสำหรับ HMC ให้ดำเนินการ ตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ตรวจสอบให้แน่ใจว่าคุณมีหนึ่งในบทบาทต่อไปนี้ :

- ผู้ดูแลระบบพิเศษ
- ตัวแทนการบริการ
- ตัวดำเนินการ
- ผู้ดู

2. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การตั้งค่าคอนโซล**
3. ในหน้าต่างย่อยเนื้อหา ให้คลิก **เปลี่ยน วันที่และเวลา**
4. หากคุณเลือก **UTC** ในฟิลด์ **Clock** การตั้งค่าเวลา จะปรับ Daylight Saving Time โดยอัตโนมัติในเขตเวลาที่คุณเลือก ใส่วันที่ เวลา และเขตเวลา แล้วคลิก **OK**

ผลลัพธ์

การตั้งค่าชนิดเน็ตเวิร์ก HMC
ตั้งค่า HMC ของคุณ เพื่อให้สามารถสื่อสารกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน ผู้ใช้ระยะไกล และบริการและการสนับสนุนได้

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ
ตั้งค่า HMC เพื่อให้สามารถเชื่อมต่อกับและจัดการระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิด

Before you begin

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อ กับระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิด ให้ทำต่อไปนี้:

Table 26. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. กำหนดอินเตอร์เฟสที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ ขอแนะนำให้ใช้ **eth0**	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42
2. ระบุอีเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุพอร์ตอีเทอร์เน็ตที่กำหนดเป็น eth0” on page 55
3. กำหนดคอนฟิกอีเทอร์เน็ตอะแด็ปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสื่อบันทึก	“การตั้งค่าความเร็วของสื่อบันทึก” on page 56
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” on page 56
c. ตั้งสแตติกแอดเดรส	“การตั้งค่า IPv6 แอดเดรส” on page 58
d. ตั้งค่าไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” on page 58
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” on page 59
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” on page 60
4. ตั้งค่าอะแด็ปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” on page 67

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ
กำหนดคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับ และจัดการระบบที่ถูกจัดการ ได้โดยใช้เน็ตเวิร์กส่วนตัว

Before you begin

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อ กับระบบที่ถูกจัดการโดยใช้เน็ตเวิร์กส่วนตัว ให้ทำต่อไปนี้:

Table 27. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ	
ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. กำหนดอินเตอร์เฟสที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42
2. ระบุอีเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุพอร์ตอีเทอร์เน็ตที่กำหนดเป็น eth0” on page 55
3. กำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP	“การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” on page 56
4. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” on page 67

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน

Before you begin

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ โลจิคัลพาร์ติชันได้โดยใช้เน็ตเวิร์กแบบเปิด ให้ทำต่อไปนี้:

Table 28. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน	
ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. กำหนดอินเตอร์เฟสที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42
2. ระบุอีเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุพอร์ตอีเทอร์เน็ตที่กำหนดเป็น eth0” on page 55
3. กำหนดคอนฟิกอีเทอร์เน็ตอะแด็ปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสื่อบันทึก	“การตั้งค่าความเร็วของสื่อบันทึก” on page 56
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” on page 56
c. ตั้งสแตติกแอดเดรส	“การตั้งค่า IPv6 แอดเดรส” on page 58
d. ตั้งค่าไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” on page 58
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” on page 59
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” on page 60
4. ตั้งค่าอะแด็ปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” on page 67

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล

Before you begin

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ ผู้ใช้ระยะไกลได้โดยใช้เน็ตเวิร์กแบบเปิด ให้ทำต่อไปนี้:

Table 29. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล

ภารกิจ	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. กำหนดอินเตอร์เฟสที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42
2. ระบุอีเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุพอร์ตอีเทอร์เน็ตที่กำหนดเป็น eth0” on page 55
3. กำหนดคอนฟิกอีเทอร์เน็ตอะแด็ปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสื่อบันทึก	“การตั้งค่าความเร็วของสื่อบันทึก” on page 56
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” on page 56
c. ตั้งสแตติกแอดเดรส	“การตั้งค่า IPv6 แอดเดรส” on page 58
d. ตั้งค่าไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” on page 58
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” on page 59
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” on page 60
g. ตั้งค่าซัฟฟิกส์	“การตั้งค่าคอนฟิกโดเมนซัฟฟิกส์” on page 60
4. ตั้งค่าอะแด็ปเตอร์เพิ่มเติม หากมี	

การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC

Before you begin

เมื่อต้องการคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC เพื่อให้สามารถ รายงานปัญหาได้ ให้ปฏิบัติดังต่อไปนี้:

Table 30. การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC

งาน	**ตำแหน่งค้นหาข้อมูลที่เกี่ยวข้อง**
1. ตรวจสอบให้แน่ใจว่าคุณมีข้อมูลลูกค้าที่จำเป็นทั้งหมด	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” on page 42
2. กำหนดคอนฟิก HMC นี้เพื่อรายงานข้อผิดพลาด หรือเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่เพื่อรายงานความผิดพลาด	“การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน” on page 62 “การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้” on page 64
3. ตรวจสอบว่าคอนฟิกูเรชัน Call-Home ของคุณใช้การได้	“การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่” on page 64
4. ให้สิทธิผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม	“การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” on page 64
5. จัดกำหนดการการส่งข้อมูลของข้อมูลระบบ	“ข้อมูลการบริการส่งข้อมูล” on page 65

การระบุพอร์ตอีเทอร์เน็ตที่กำหนดเป็น eth0
การเชื่อมต่ออีเทอร์เน็ตของคุณกับเซิร์ฟเวอร์ที่ถูกจัดการต้องทำโดยใช้พอร์ตอีเทอร์เน็ต ที่กำหนดเป็น `eth0` บน HMC ของคุณ

หากคุณไม่ได้ติดตั้งอะแด็ปเตอร์อีเทอร์เน็ตเพิ่มเติมในสล็อต PCI บน HMC ของคุณ ดังนั้น พอร์ตอะแด็ปเตอร์หลักแบบรวมจะถูกกำหนดเป็น `eth0` หรือ `eth1` เสมอบน HMC ของคุณ หากคุณตั้งใจที่จะใช้ HMC เป็น เซิร์ฟเวอร์ DHCP สำหรับระบบที่ถูกจัดการของคุณ

หากคุณติดตั้งอะแด็ปเตอร์อีเทอร์เน็ตเพิ่มเติมในสล็อต PCI ดังนั้นพอร์ตที่ถูกกำหนดเป็น `eth0` จะขึ้นอยู่กับตำแหน่งและชนิดของอะแด็ปเตอร์อีเทอร์เน็ตที่ติดตั้งอยู่

หมายเหตุ: กฎทั่วไปต่อไปนี้อาจไม่ได้ใช้กับคอนฟิกูเรชันทั้งหมด

ตารางต่อไปนี้แสดงกฎของการติดตั้งอีเทอร์เน็ตตามประเภท HMC

ตารางที่ 31. ประเภท HMC และกฎที่เกี่ยวข้องสำหรับการติดตั้งอีเทอร์เน็ต

ประเภท HMC	**กฎสำหรับการติดตั้งอีเทอร์เน็ต**
HMC แบบติดตั้งในชั้นวางที่มีพอร์ตอีเทอร์เน็ตรวมสองพอร์ต	HMC สนับสนุนอะแด็ปเตอร์อีเทอร์เน็ต เพิ่มเติมเพียงอะแด็ปเตอร์เดียว • หากคุณติดตั้งอะแด็ปเตอร์อีเทอร์เน็ตเพิ่มเติม ดังนั้น พอร์ตดังกล่าวจะถูกกำหนดเป็น `eth0` ในกรณีนี้ พอร์ตอีเทอร์เน็ตรวมหลักจะถูกกำหนดเป็น `eth1` และ พอร์ตอีเทอร์เน็ตรวมสำรองจะถูกกำหนดเป็น `eth2` • หากอะแด็ปเตอร์อีเทอร์เน็ตเป็นอะแด็ปเตอร์อีเทอร์เน็ตพอร์ตคู่ ดังนั้น พอร์ตที่ติดเลเบล Act/Link A คือ `eth0` พอร์ตที่ติดเลเบล `Act/link B` คือ `eth1` ในกรณีนี้ พอร์ตอีเทอร์เน็ตรวมหลักจะถูกกำหนดเป็น `eth2` และพอร์ตอีเทอร์เน็ตรวมสำรองจะถูกกำหนดเป็น `eth3` • หากไม่มีอะแด็ปเตอร์ติดตั้งอยู่ ดังนั้น พอร์ตอีเทอร์เน็ตรวมหลักจะถูกกำหนดเป็น `eth0`
รุ่นสแตนด์อะโลนที่มีพอร์ตอีเทอร์เน็ตรวม พอร์ตเดียว	นิยามขึ้นอยู่กับชนิดของอะแด็ปเตอร์อีเทอร์เน็ตที่ติดตั้งอยู่: • หากติดตั้งอะแด็ปเตอร์อีเทอร์เน็ตเพียงอะแด็ปเตอร์เดียว ดังนั้น อะแด็ปเตอร์ดังกล่าวจะถูกกำหนดเป็น `eth0` • หากอะแด็ปเตอร์อีเทอร์เน็ตเป็นอะแด็ปเตอร์อีเทอร์เน็ตพอร์ตคู่ ดังนั้น พอร์ตที่ติดเลเบล `Act/link A` คือ `eth0` พอร์ตที่ติดเลเบล `Act/link B` จะเป็น `eth1` ในกรณีนี้ พอร์ตอีเทอร์เน็ตรวมหลักจะถูกกำหนดเป็น `eth2` • หากไม่มีอะแด็ปเตอร์ติดตั้งอยู่ ดังนั้น พอร์ตอีเทอร์เน็ตรวมจะถูกกำหนดเป็น `eth0` • หากมีอะแด็ปเตอร์อีเทอร์เน็ตหลายอะแด็ปเตอร์ติดตั้งอยู่ โปรดดูที่ “การพิจารณาชื่ออินเตอร์เฟสของอีเทอร์เน็ตอะแด็ปเตอร์” ในหน้า 55

การพิจารณาชื่ออินเตอร์เฟสของอีเทอร์เน็ตอะแด็ปเตอร์
ถ้าคุณกำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP เซิร์ฟเวอร์นั้นสามารถดำเนินงาน ได้เฉพาะในตัวเชื่อมต่อ network interface card (NIC) ที่ HMC ระบุเป็น `eth0` และ `eth1` เท่านั้น คุณยังอาจต้องพิจารณาว่า ตัวเชื่อมต่อ NIC ใดที่คุณต้องการต่อเข้าสายเคเบิลอีเทอร์เน็ตด้วย ศึกษา เพิ่มเติมเกี่ยวกับการพิจารณาว่าตัวเชื่อมต่อ NIC ใดที่ HMC ระบุเป็น `eth0` และ `eth1`

เกี่ยวกับภารกิจนี้
เมื่อต้องการตรวจสอบชื่อที่ HMC กำหนดให้กับอะแด็ปเตอร์อีเทอร์เน็ต ให้ทำตามขั้นตอน ต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง คลิกไอคอน **HMC Management**  จากนั้นเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา ให้คลิก **Change Network Settings**
3. จากหน้าต่าง **Change Network Settings** ให้คลิกแท็บ **LAN adapters** รายการตัวอย่างต่อไปนี้แสดงว่าพอร์ตอีเทอร์เน็ตนี้ถูกระบุเป็น `eth0`: `Ethernet eth0 52:54:00:fa:b6:8e (<IP address of HMC>)`
4. บันทึกผลลัพธ์ของคุณ หากคุณต้องการดูหรือเปลี่ยนค่าติดตั้งอะแด็ปเตอร์ LAN ให้คลิก **Details**
5. คลิก **OK**

การตั้งค่าความเร็วของสื่อบันทึก
ศึกษาวิธีการระบุความเร็วของสื่อที่รวมถึงความเร็วและโหมด duplex ของ อะแด็ปเตอร์อีเทอร์เน็ต

ก่อนเริ่มต้นภารกิจ
ดีฟอลต์สำหรับค่าติดตั้งอะแด็ปเตอร์ HMC คือ **Autodetection** ถ้าอะแด็ปเตอร์นี้ถูกเชื่อมต่อ กับสวิตช์ LAN คุณต้องจับคู่ค่าติดตั้งพอร์ตของสวิตช์ เมื่อต้องการตั้งค่า ความเร็วสื่อบันทึกและดูเฟล็กซ์ ให้ดำเนินการตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. ในส่วนข้อมูล local area network (LAN) ให้เลือก **Autodetection** หรือความเร็วสื่อและ duplex ที่เหมาะสมรวมกัน
6. คลิก **OK**

การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด
private service network ประกอบด้วย Hardware Management Console (HMC) และระบบที่ถูกจัดการ เน็ตเวิร์กส่วนบุคคลจะถูกจำกัดอยู่แค่คอนโซลและระบบที่ถูกจัดการ และจะแยกต่างหากจากเน็ตเวิร์กภายในบริษัท *เน็ตเวิร์กแบบเปิด* ประกอบด้วยเน็ตเวิร์กส่วนบุคคล และเน็ตเวิร์กภายในบริษัท เน็ตเวิร์กแบบเปิดอาจประกอบด้วยจุดสิ้นสุดเน็ตเวิร์กนอกเหนือจากคอนโซล และระบบที่ถูกจัดการ และยังครอบคลุมถึงอุปกรณ์เน็ตเวิร์กย่อย และเน็ตเวิร์ก

เกี่ยวกับภารกิจนี้
เมื่อต้องการเลือกเครือข่ายไพรเวตหรือพับลิก ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **LAN Adapter**
6. ในเพจ local area network information ให้เลือก **Private** หรือ **Open**
7. คลิก **OK**

การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP
Dynamic Host Configuration Protocol (DHCP) มีวิธีอัตโนมัติสำหรับการตั้งค่าคอนฟิกไคลเอ็นต์แบบไดนามิก

เมื่อต้องการกำหนดค่า Hardware Management Console (HMC) เป็นเซิร์ฟเวอร์ DHCP ให้ทำตาม ขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings** หน้าต่าง Customize Network Settings จะเปิด
3. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
4. เลือก **Private** จากนั้นเลือก ชนิดของเน็ตเวิร์ก
5. ในส่วนเซิร์ฟเวอร์ DHCP เลือก **Enable DHCP Server** เพื่อ เปิดใช้งาน HMC เป็น เซิร์ฟเวอร์ DHCP

   หมายเหตุ: คุณสามารถตั้งค่า HMC ที่จะเป็นเซิร์ฟเวอร์ DHCP บนเน็ตเวิร์กส่วนตัวเท่านั้น หากคุณใช้เครือข่ายเปิด อ็อพชันเพื่อเลือก **Enable DHCP** จะไม่พร้อมใช้งาน
6. เลือกช่วงแอดเดรสของเซิร์ฟเวอร์ DHCP
7. คลิก **OK**

ถ้าคุณได้ตั้งค่า HMC ของคุณไปเป็นเซิร์ฟเวอร์ DHCP บนเน็ตเวิร์กส่วนตัวแล้ว คุณต้องตรวจสอบว่า คุณได้ตั้งค่าเน็ตเวิร์กส่วนตัว HMC DHCP อย่างถูกต้อง สำหรับข้อมูลเกี่ยวกับการเชื่อมต่อ HMC เข้ากับเน็ตเวิร์กส่วนตัว, โปรดดูที่ “การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 56

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “ HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 36

กำหนดค่าการเชื่อมต่อ BMC
คุณสามารถกำหนดค่าหรือดูค่าติดตั้งเครือข่ายบน BMC สำหรับคอนโซลการจัดการ

หมายเหตุ: งานนี้ใช้กับ 7063-CR1 เท่านั้น การเชื่อมต่อนี้ต้องการเข้าถึง baseboard management controller (BMC) บน HMC

เมื่อต้องการกำหนดค่าการเชื่อมต่อ BMC ให้ทำตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change BMC/IPMI network settings**
3. เลือกโหมดการเชื่อมต่อ (**DHCP** หรือ **Static**)

   หาก คุณเลือกโหมด **Static** ให้ระบุแอดเดรสต่อไปนี้:

   - **IP address**
   - **Subnet mask**
   - **Gateway**
4. คลิก **OK**

คุณยังสามารถกำหนดค่าการเชื่อมต่อเครือข่าย BMC ได้โดยใช้อินเตอร์เฟส Petitboot bootloader สำหรับข้อมูลเพิ่มเติม โปรดดูที่ การกำหนดค่า IP แอดเดรสเฟิร์มแวร์

การตั้งค่า IPv4 address
ศึกษาถึงวิธีการตั้งค่า IPv4 address ของคุณบน HMC

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **Basic Settings**
6. เลือก IPv4 แอดเดรส

7. หากคุณเลือกระบุ IP แอดเดรส ให้ใส่ TCP/IP interface address และ TCP/IP interface network mask
8. คลิก **OK**

การตั้งค่า IPv6 แอดเดรส
ศึกษาวิธีการเซ็ตอัพ IPv6 address บน HMC

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **IPv6 Settings**
6. เลือกอ็อพชัน **Autoconfig** หรือเพิ่ม IP แอดเดรสแบบสแตติก
7. ถ้าคุณได้เพิ่ม IP แอดเดรสแล้ว ให้ป้อน IPv6 แอดเดรสและความยาวของคำนำหน้า และคลิก **OK**
8. คลิก **OK**

การใช้ IPv6 แอดเดรสเท่านั้น
ศึกษาเกี่ยวกับวิธีการตั้งค่า HMC เพื่อให้ใช้ IPv6 แอดเดรสเท่านั้น

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การตั้งค่าคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **เปลี่ยนค่าติดตั้งเครือข่าย**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. เลือก **ไม่มีแอดเดรส IPv4**
6. คลิกแท็บ **IPv6 Settings**
7. เลือก **ใช้ DHCPv6 เพื่อกำหนดค่าค่าติดตั้ง IP** หรือเพิ่ม IP แอดเดรสแบบสแตติก จากนั้นคลิก **ตกลง**

สิ่งที่ต้องทำต่อไป
หลังจากที่คุณคลิก **ตกลง** คุณต้องรีสตาร์ท HMC ของคุณเพื่อให้การเปลี่ยนแปลงเหล่านี้ มีผล

การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC
ในเน็ตเวิร์กแบบเปิด ไฟร์วอลล์จะถูกใช้เพื่อควบคุมการเข้าสู่เน็ตเวิร์กภายในบริษัทจากภายนอก HMC ก็มีไฟร์วอลล์ในอะแด็ปเตอร์อีเทอร์เน็ตแต่ละตัว เมื่อต้องการควบคุม HMC จากระยะไกล หรือให้รีโมตแอ็คเซสแก่บุคคลอื่น แก้ไขการตั้งค่าคอนฟิกไฟร์วอลล์ของอีเทอร์เน็ตอะแด็ปเตอร์บน HMC ซึ่งเชื่อมต่อกับเน็ตเวิร์กแบบเปิด

เกี่ยวกับภารกิจนี้

เมื่อต้องการกำหนดคอนฟิกไฟร์วอลล์, ให้ใช้ขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**

4. เลือกอะแด็ปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **Firewall**
6. การใช้หนึ่งในวิธีต่อไปนี้ คุณสามารถอนุญาต IP แอดเดรสใด ๆ โดยใช้แอ็พพลิเคชันเฉพาะเจาะจง ผ่านไฟร์วอลล์ หรือคุณสามารถระบุหนึ่งหรือหลาย IP แอดเดรส
   - อนุญาต IP แอดเดรสใด ๆ โดยใช้แอ็พพลิเคชันเฉพาะเจาะจงผ่านไฟร์วอลล์:
     a. จากช่องด้านบน, ให้เลือกแอ็พพลิเคชัน
     b. คลิก **Allow Incoming** แอ็พพลิเคชันจะแสดงช่องด้านล่าง เพื่อแสดงว่าถูกเลือกแล้ว
   - ระบุ IP แอดเดรสเพื่ออนุญาตให้ผ่านไฟร์วอลล์ได้:
     a. จากช่องด้านบน ให้เลือกแอ็พพลิเคชัน
     b. คลิก **Allow Incoming by IP Address**
     c. ในหน้าต่าง Hosts Allowed, ป้อน IP แอดเดรสและ network mask
     d. คลิก **Add** และคลิก **OK**
7. คลิก **OK**

การเปิดใช้การเข้าถึงเชลล์ที่จำกัดแบบรีโมต
คุณสามารถเปิดใช้งานการเข้าถึงเชลล์ที่จำกัดแบบรีโมตเมื่อคุณกำหนดคอนฟิกไฟร์วอลล์

เกี่ยวกับภารกิจนี้
เมื่อต้องการเปิดใช้งานการเข้าถึงเชลล์ที่จำกัดแบบรีโมต ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ
1. ในพื้นที่การนำทาง ให้คลิก **การจัดการ HMC**
2. คลิก **Remote Command Execution**
3. เลือก **เปิดใช้งานการเรียกใช้งานคำสั่งรีโมต โดยใช้ ssh** จากนั้นคลิก **OK**

สิ่งที่ต้องทำต่อไป
ถึงตอนนี้ การเข้าถึงเชลล์ที่จำกัดแบบรีโมตถูกเปิดใช้งานแล้ว

การเปิดใช้งาน การเข้าถึงเว็บแบบรีโมต
คุณสามารถเปิดใช้งานการเข้าถึงเว็บแบบรีโมตสำหรับ Hardware Management Console (HMC) ของคุณ

เกี่ยวกับภารกิจนี้
เมื่อต้องการเปิดใช้งานการเข้าถึงเว็บแบบรีโมต ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ
1. ในพื้นที่การนำทาง ให้คลิก **การจัดการ HMC**
2. คลิก **การดำเนินการแบบรีโมต**
3. เลือก **เปิดใช้งาน** จากนั้นคลิก **ตกลง**

สิ่งที่ต้องทำต่อไป
ถึงตอนนี้ การเข้าถึงเว็บแบบรีโมตถูกเปิดใช้งานแล้ว

การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์
ศึกษาเกี่ยวกับวิธีการตั้งค่าการเราต์ entry ตามดีฟอลต์เกตเวย์ งานนี้พร้อมใช้งาน เมื่อคุณใช้เครือข่ายเปิด

ก่อนเริ่มต้นภารกิจ
เมื่อต้องการกำหนดค่ารายการการกำหนดเส้นทางเป็นดีฟอลต์เกตเวย์ ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings** หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ **Routing**
4. ในส่วนข้อมูลดีฟอลต์เกตเวย์ ป้อนเกตเวย์แอดเดรสและอุปกรณ์เกตเวย์ของ entry การเราต์ที่คุณต้องการกำหนดเป็นดีฟอลต์เกตเวย์
5. คลิก **OK**

การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส

ถ้าคุณวางแผนที่จะติดตั้งเน็ตเวิร์กแบบเปิด ให้ตั้งค่าโดเมนเนมเซอร์วิส

เกี่ยวกับภารกิจนี้

ถ้าคุณวางแผนที่จะติดตั้งเน็ตเวิร์กแบบเปิด ให้ตั้งค่าโดเมนเนมเซอร์วิส Domain Name System (DNS) is a เป็นระบบฐานข้อมูลแบบกระจายสำหรับการจัดการชื่อของโฮสต์ และ Internet Protocol (IP) แอดเดรสที่เชื่อมโยงกัน การตั้งค่าคอนฟิกโดเมน เนมเซอร์วิสประกอบด้วยการเปิดใช้งาน DNS และการระบุโดเมนซัฟฟิกซ์ค้นหา

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Change network settings** หน้าต่าง Change Network Settings จะเปิด
3. คลิกแท็บ **Name Services**
4. เลือก **DNS enables** เพื่อเปิดใช้งาน DNS
5. ระบุเซิร์ฟเวอร์ DNS และโดเมนซัฟฟิกซ์ค้นหา แล้วคลิก **Add**
6. คลิก **OK**

การตั้งค่าคอนฟิกโดเมนซัฟฟิกส์

รายการของส่วนต่อท้ายโดเมนจะใช้เพื่อแปลง IP แอดเดรสที่ขึ้นต้นด้วยรายการแรก ในรายการ

เกี่ยวกับภารกิจนี้

ส่วนต่อท้ายโดเมนเป็นสตริงที่ผนวกเข้ากับชื่อโฮสต์ที่ใช้เพื่อช่วยแปลง IP แอดเดรส ตัวอย่างเช่น ชื่อโฮสต์ของ `myname` อาจแปลงไม่ได้ อย่างไรก็ตาม หากสตริง `myloc.mycompany.com` เป็นอิลิเมนต์ในตารางส่วนต่อท้ายของโดเมน ดังนั้น จะมีการพยายามแปลง `myname.mloc.mycompany.com`

เมื่อต้องการกำหนดค่ารายการส่วนต่อท้ายโดเมน ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การตั้งค่าคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **เปลี่ยนค่าติดตั้งเครือข่าย** หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ **Name Services**
4. ป้อนสตริงที่จะใช้เป็น entry ของโดเมนซัฟฟิกส์
5. คลิก **Add** เพื่อเพิ่ม entry นั้นลงในรายการ

การคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP

คุณสามารถกำหนดค่า Hardware Management Console (HMC) ของคุณ เพื่อให้ใช้การพิสูจน์ตัวตนรีโมต LDAP (Lightweight Directory Access Protocol)

ก่อนเริ่มต้นภารกิจ

เมื่อผู้ใช้ลงชื่อเข้าใช้ HMC ระบบจะดำเนินการพิสูจน์ตัวตน ของไฟล์รหัสผ่านภายในก่อน หากไม่พบไฟล์รหัสผ่านภายใน HMC สามารถติดต่อเซิร์ฟเวอร์ LDAP ระยะไกลสำหรับการพิสูจน์ตัวตนได้ คุณต้องคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP

หมายเหตุ: ก่อนที่คุณกำหนดคอนฟิก HMC เพื่อใช้การพิสูจน์ตัวตน LDAP คุณต้องตรวจสอบให้แน่ใจว่า การเชื่อมต่อเน็ตเวิร์กที่มีอยู่ระหว่างเซิร์ฟเวอร์ HMC และ LDAP ยังคงทำงานอยู่ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ การกำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 52

เกี่ยวกับภารกิจนี้

เมื่อต้องการกำหนดค่า HMC เพื่อให้ใช้การพิสูจน์ตัวตน LDAP ให้ดำเนินการตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **Users and Security**  จากนั้นเลือก **Systems and Console Security**
2. ในบานหน้าต่างเนื้อหา เลือก **Manage LDAP** หน้าต่าง LDAP Server Definition แสดงขึ้น
3. เลือก **Enable LDAP**
4. กำหนดเซิร์ฟเวอร์ LDAP ที่ต้องการใช้เพื่อพิสูจน์ตัวตน
5. กำหนดแอ็ตทริบิวต์ LDAP ที่ใช้เพื่อระบุผู้ใช้ที่กำลังได้รับการพิสูจน์ตัวตน ค่าดีฟอลต์คือ **uid** แต่คุณสามารถ ใช้แอ็ตทริบิวต์ของคุณเองได้
6. กำหนดแผนผังชื่อจำเพาะ รู้จักกันในชื่อของฐานการค้นหา สำหรับเซิร์ฟเวอร์ LDAP
7. คลิก **OK**
8. หากผู้ใช้ต้องการใช้การพิสูจน์ตัวตน LDAP ผู้ใช้ต้อง กำหนดค่าโปรไฟล์เพื่อให้ใช้การพิสูจน์ตัวตน LDAP จากระยะไกล แทนการพิสูจน์ตัวตนแบบโลคัล

การกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos

คุณสามารถกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center (KDC) สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberoos ได้

ก่อนเริ่มต้นภารกิจ

เมื่อผู้ใช้ล็อกอินเข้าสู่ HMC การพิสูจน์ตัวตนจะตรวจสอบกับไฟล์รหัสผ่านในเครื่องก่อน หากไม่พบไฟล์รหัสผ่านภายใน HMC สามารถติดต่อเซิร์ฟเวอร์ Kerberos ระยะไกลสำหรับการพิสูจน์ตัวตนได้ คุณต้องกำหนดคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย Kerberos

หมายเหตุ: ก่อนที่ คุณจะกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos คุณต้องตรวจสอบให้แน่ใจว่ามีการเชื่อมต่อเน็ตเวิร์กการทำงาน ระหว่าง HMC และเซิร์ฟเวอร์ KDC สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ การกำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 52

เกี่ยวกับภารกิจนี้

เมื่อต้องการกำหนดค่า HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตน Kerberos แบบรีโมต ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. เปิดใช้งานเซอร์วิส Network Time Protocol (NTP) บน HMC และตั้งค่าเซิร์ฟเวอร์ HMC และ KDC ให้ซิงโครไนซ์โดยใช้เซิร์ฟเวอร์ NTP เดียวกัน เมื่อต้องการเปิดใช้งานเซอร์วิส NTP บน HMC ให้ทำตาม ขั้นตอนต่อไปนี้:

   a) ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings**

b) ในบานหน้าต่างเนื้อหา เลือก **Change Date and Time**

c) เลือกแท็บ **NTP Configuration**

d) เลือก **Enable NTP service on this HMC**

e) คลิก **OK**

2. คอนฟิกแต่ละโปรไฟล์ผู้ใช้ของ HMC ระยะไกลเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย Kerberos แทนที่จะใช้การพิสูจน์ตัวตนภายใน
3. หรือ คุณสามารถเลือกอิมพอร์ตไฟล์คีย์เซอร์วิสลงใน HMC นี้ ไฟล์คีย์เซอร์วิสจะมีบัญชีโฮสต์ที่ระบุ HMC ให้แก่เซิร์ฟเวอร์ ไฟล์คีย์เซอร์วิสรู้จักกันในชื่อของ *คีย์แท็บ* เมื่อต้องการอิมพอร์ตไฟล์คีย์เซอร์วิสลงใน HMC นี้ ให้ทำตามขั้นตอนต่อไปนี้:

a) ในพื้นที่การนำทาง ให้คลิกไอคอน **Users and Security**  จากนั้นเลือก **Systems and Console Security**

b) ในบานหน้าต่างเนื้อหา เลือก **Mange KDC**

c) เลือก **Actions > Import Service Key** หน้าต่าง Import Service Key จะปรากฏขึ้น

d) พิมพ์ตำแหน่งของไฟล์คีย์เซอร์วิส

e) คลิก **OK**

4. เพิ่มเซิร์ฟเวอร์ KDC ใหม่ลงใน HMC นี้ เมื่อต้องการเพิ่มเซิร์ฟเวอร์ KDC ใหม่เข้ากับ HMC นี้ ให้ทำตาม ขั้นตอนต่อไปนี้:

a) ในพื้นที่การนำทาง ให้คลิกไอคอน **Users and Security**  จากนั้นเลือก **Systems and Console Security**

b) ในบานหน้าต่างเนื้อหา เลือก **Manage KDC**

c) เลือก **Actions > Add KDC Server** หน้าต่าง Import Service Key จะปรากฏขึ้น

d) พิมพ์ชื่อกลุ่มระบบเครือข่ายและชื่อโฮสต์ หรือ IP แอดเดรส ของเซิร์ฟเวอร์ KDC

e) คลิก **OK**

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน

คอนฟิก HMC นี้เพื่อให้สามารถติดต่อผู้ให้บริการเกี่ยวกับความผิดพลาดได้โดยใช้การเชื่อมต่อทาง LAN โทรศัพท์หรือโมเด็ม หรือ VPN

การกำหนดค่า HMC เพื่อให้สามารถเชื่อมต่อกับฝ่ายบริการและสนับสนุนโดยใช้วิซาร์ดการตั้งค่า call-home
กำหนดค่า HMC เพื่อให้เป็นเซิร์ฟเวอร์ call-home โดยใช้วิซาร์ด call-home

ก่อนเริ่มต้นภารกิจ

โพรซีเดอร์นี้อธิบายวิธีกำหนดค่า HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้การเชื่อมต่อโดยตรง (ผ่าน LAN) และการเชื่อมต่อทางอ้อม (SSL) กับอินเทอร์เน็ต

ก่อนที่จะ เริ่มงานนี้ ให้ตรวจสอบให้แน่ใจว่า:

- ผู้ดูแลระบบเครือข่ายตรวจสอบว่าอนุญาตให้เชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 41
- หากคุณกำลังกำหนดค่าการสนับสนุนอินเทอร์เน็ตผ่านพร็อกซีเซิร์ฟเวอร์ คุณต้องมี ข้อมูลต่อไปนี้ด้วย:
  - IP แอดเดรสและพอร์ตของพร็อกซีเซิร์ฟเวอร์
  - ข้อมูลการพิสูจน์ตัวตนสำหรับพร็อกซี
- มีการใช้อะแด็ปเตอร์ที่กำหนดเป็น **eth1** (อะแด็ปเตอร์ที่กำหนดเป็น เครือข่ายเปิด) สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเลือกการตั้งค่าเครือข่ายบน HMC” ในหน้า 34
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

เมื่อต้องการกำหนดค่า HMC เพื่อให้เป็นเซิร์ฟเวอร์ call-home โดยใช้วิซาร์ด call-home ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **สามารถให้บริการได้**  จากนั้นเลือก **การจัดการเซอร์วิส**
2. ในบานหน้าต่างเนื้อหา คลิก **วิซาร์ดการตั้งค่า Call-Home** วิซาร์ดภาวะการเชื่อมต่อและเซิร์ฟเวอร์ Call-Home จะเปิดขึ้น ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อกำหนดคอนฟิก Call-Home

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน
คอนฟิก HMC นี้เพื่อให้สามารถติดต่อผู้ให้บริการเกี่ยวกับความผิดพลาดได้โดยใช้การเชื่อมต่อทาง LAN โทรศัพท์หรือโมเด็ม หรือ VPN

การกำหนดค่า HMC เพื่อติดต่อฝ่ายบริการและสนับสนุนโดยใช้อินเทอร์เน็ตผ่าน LAN และ SSL
อธิบายวิธีกำหนดค่า HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้การเชื่อมต่อกับอินเทอร์เน็ตโดยตรง (ผ่าน LAN) และ ทางอ้อม (SSL)

ก่อนเริ่มต้นภารกิจ

ก่อนที่จะ เริ่มงานนี้ ให้ตรวจสอบให้แน่ใจว่า:

- ผู้ดูแลระบบเครือข่ายตรวจสอบว่าอนุญาตให้เชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 41
- มีการกำหนดค่าข้อมูลที่ติดต่อของลูกค้าไว้ ตรวจสอบข้อมูลผู้ติดต่อโดยไปที่อินเตอร์เฟส HMC และคลิก **ความสามารถในการให้บริการ>การจัดการเซอร์วิส>จัดการ ข้อมูลลูกค้า**
- หากคุณกำลังกำหนดค่าการสนับสนุนอินเทอร์เน็ตผ่านพร็อกซีเซิร์ฟเวอร์ คุณต้องมี ข้อมูลต่อไปนี้ด้วย:
  - IP แอดเดรสและพอร์ตของพร็อกซีเซิร์ฟเวอร์
  - ข้อมูลการพิสูจน์ตัวตนสำหรับพร็อกซี
- คุณจำเป็นต้องคอนฟิกอย่างน้อยหนึ่งเน็ตเวิร์กอินเตอร์เฟสที่เปิดอยู่ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 36
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

เกี่ยวกับภารกิจนี้

เมื่อต้องการกำหนดค่า HMC เป็นเซิร์ฟเวอร์ Call Home โดยใช้อินเทอร์เน็ตผ่าน LAN และ SSL ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **สามารถให้บริการได้**  จากนั้นเลือก **การจัดการเซอร์วิส**
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity** หน้าต่างคอนโซลเซิร์ฟเวอร์ Call-Home จะปรากฏขึ้น
3. คลิก **Configure.**
4. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออก ให้เลือก **เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ Call-Home**
5. ยอมรับข้อตกลง
6. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออก ให้เลือกเพจ **Internet**
7. ทำเครื่องหมายในกล่อง **Allow an existing internet connections for service**
8. ถ้าคุณกำลังใช้พร็อกซี SSL ให้เลือก **Use SSL proxy**
9. หากคุณกำลังใช้พร็อกซี SSL ให้ระบุข้อมูลแอดเดรสและพอร์ตของพร็อกซี ขอรับข้อมูลนี้ได้จากผู้บริหารเน็ตเวิร์ก
10. ถ้าคุณเลือก **Use SSL proxy** และพร็อกซีต้องใช้การพิสูจน์ตัวตนด้วย user ID และรหัสผ่าน ให้เลือก **Authenticate with the SSL proxy** พิมพ์ ID ผู้ใช้ และรหัสผ่าน ขอรับข้อมูล user ID และรหัสผ่านได้จากผู้บริหารเน็ตเวิร์ก
11. เลือก **โปรโตคอลของอินเตอร์เน็ต** ที่คุณต้องการใช้

12. บนเพจ **อินเตอร์เน็ต** ให้คลิก **ทดสอบ**
13. ในหน้าต่างทดสอบอินเทอร์เน็ต คลิก **เริ่มต้น**
14. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์
15. ในหน้าต่างทดสอบอินเทอร์เน็ต คลิก **ยกเลิก**
16. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออก ให้คลิก **ตกลง**

การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อ ไปยังบริการและการสนับสนุนสำหรับ HMC นี้
เลือกเซิร์ฟเวอร์ call-home ที่มีอยู่ของ Hardware Management Console (HMC) ที่ HMC รู้จัก และพบเพื่อรายงานข้อผิดพลาด

ก่อนเริ่มต้นภารกิจ

HMC ที่ค้นพบเป็น HMC ที่เปิดใช้งานเป็นเซิร์ฟเวอร์ Call-Home และอยู่บนซับเน็ตเดียวกัน หรือจัดการระบบที่ถูกจัดการเดียวกันกับ HMC นี้

เมื่อต้องการเลือก HMC ที่พบเพื่อ call home เมื่อ HMC รายงานข้อผิดพลาด ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **Serviceability**  จากนั้นเลือก **Service Management**
2. ในบานหน้าต่างเนื้อหา คลิก **Manage Outbound Connectivity** หน้าต่าง Call-Home Server Consoles จะปรากฏขึ้น
3. คลิก **Use discovered call-home server consoles** HMC จะแสดง IP แอดเดรสหรือชื่อโฮสต์ของ HMC ที่คอนฟิกสำหรับ Call-Home
4. คลิก **OK**

ผลลัพธ์

คุณยังสามารถเพิ่มเซิร์ฟเวอร์ Call-Home ของ HMC ที่มีอยู่ซึ่งอยู่บนซับเน็ตอื่นได้เอง เลือก IP แอดเดรสหรือชื่อโฮสต์ของ HMC ที่กำหนดค่าสำหรับ call home และคลิก **Add** จากนั้นคลิก **OK**

การตรวจสอบว่าการเชื่อมต่อของคุณ ไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่
ทดสอบการรายงานปัญหา เพื่อตรวจสอบให้แน่ใจว่า การเชื่อมต่อไปยังส่วนบริการ และสนับสนุนกำลังทำงานอยู่

เกี่ยวกับภารกิจนี้

เมื่อต้องการตรวจสอบว่าคอนฟิกูเรชัน call-home ของคุณใช้งานได้ ให้ทำตาม ขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **สามารถให้บริการได้**  จากนั้นเลือก **การจัดการเซอร์วิส**
2. ในบานหน้าต่างเนื้อหา คลิก **สร้างเหตุการณ์**
3. เลือก **ทดสอบการรายงานปัญหาโดยอัตโนมัติ** และ พิมพ์ข้อคิดเห็น
4. คลิก **Request Service** รอ 2-3 นาที เพื่อให้คำร้องขอถูกส่ง
5. ในหน้าต่าง Service Management ให้เลือก **Manage Events**
6. เลือก **All open problems**
7. ตรวจสอบว่ามีการกำหนดเหตุการณ์และตัวเลข PMH ให้กับหมายเลขปัญหาที่คุณเปิด
8. เลือกเหตุการณ์ดังกล่าว และคลิก **ปิด**
9. ในหน้าต่าง **ปิด** ให้พิมพ์ชื่อและความคิดเห็นสั้น ๆ

การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม
คุณต้องให้สิทธิ์แก่ผู้ใช้ในการดูข้อมูลเกี่ยวกับระบบของคุณ

ก่อนเริ่มต้นภารกิจ

ก่อนที่คุณจะให้สิทธิ์ผู้ใช้เพื่อดูข้อมูลระบบที่เก็บรวบรวมมา คุณต้องขอรับ IBM ID ก่อน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการขอรับ IBM ID โปรดดูที่ “เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 42

เกี่ยวกับภารกิจนี้

เมื่อต้องการให้สิทธิ์ผู้ใช้เพื่อดูข้อมูลระบบที่รวบรวมไว้ ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **Serviceability**  จากนั้นเลือก **Service Management**
2. ในบานหน้าต่างเนื้อหา เลือก **Authorize User**
3. ป้อน IBM ID ของคุณ
4. คลิก **OK**

ข้อมูลการบริการส่งข้อมูล

คุณสามารถส่งข้อมูลให้กับผู้ให้บริการทันที หรือคุณสามารถกำหนดเวลาให้ส่ง ข้อมูลเป็นประจำ

ก่อนเริ่มต้นภารกิจ

IBM จัดเตรียมฟังก์ชันบนเว็บในแบบของคุณ ที่ใช้ข้อมูลที่ IBM Electronic Service Agent รวบรวมไว้ เพื่อใช้ฟังก์ชันเหล่านี้ คุณต้องลงทะเบียนบนเว็บไซต์ IBM Registration ก่อนที่ http://www.ibm.com/account/profile เมื่อต้องการอนุญาตให้ผู้ใช้ใช้ข้อมูล Electronic Service Agent เพื่อทำให้ฟังก์ชันบนเว็บเป็นแบบของตัวเอง โปรดดูที่ “การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” ในหน้า 64 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ข้อดีของการลงทะเบียน IBM ID กับ ระบบของคุณ ดูที่ http://www.ibm.com/support/electronic

หมายเหตุ: คุณต้องส่งข้อมูลให้ผู้ให้บริการทันทีที่ HMC ถูกติดตั้งและกำหนดค่า เพื่อใช้งาน

เกี่ยวกับภารกิจนี้

เมื่อต้องการส่งข้อมูลการบริการ ให้ทำดังนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **สามารถให้บริการได้**  จากนั้นเลือก **การจัดการเซอร์วิส**
2. ในบานหน้าต่างเนื้อหา คลิก **ข้อมูล เซอร์วิสการส่งข้อมูล**
3. ดำเนินการงานในหน้าต่าง **ส่งข้อมูลเซอร์วิส** และคลิก **ตกลง**

การกำหนดคอนฟิก Events Manager for Call Home

ศึกษาวิธีการกำหนดคอนฟิกภารกิจ Events Manager for Call Home คุณสามารถมอนิเตอร์และอนุมัติข้อมูลใด ๆ ที่กำลังส่งผ่าน จาก HMC ไปยัง IBM ผ่าน ภารกิจนี้

โหมด Events Manager for Call Home (เปิดใช้งานหรือปิดใช้งาน) ถูกตั้งค่าโดยใช้อินเตอร์เฟสบรรทัดรับคำสั่งของ HMC การเปิดใช้งานภารกิจ Events Manager for Call Home จะบล็อค HMC ไม่ให้เรียกเหตุการณ์โฮมโดยอัตโนมัติเมื่อเกิดขึ้น เพื่อป้องกันการเรียกเหตุการณ์โฮมโดยไม่มี การอนุมัติ, HMCs ทั้งหมดที่รันอยู่ในสภาวะแวดล้อมนี้ต้องมีการเปิดใช้งาน Events Manager for Call Home

เมื่อต้องการเปิดใช้งาน หรือปิดใช้งานภารกิจ Events Manager for Call Home ให้รัน คำสั่งต่อไปนี้:

```
chhmc -c emch
-s {enable | disable}
[--callhome {enable | disable}]
[--help]
```

หมายเหตุ: การเปิดใช้งานงาน Events Manager for Call Home จะพักเหตุการณ์ call home ไว้จนกว่าจะได้รับการอนุมัติ สำหรับงาน call home หากคุณปิดใช้งานงาน Events Manager for Call Home จะไม่เปิดใช้งานคุณลักษณะ call home โดยอัตโนมัติ เซ็ตอัพนี้ ป้องกันการเรียกโฮมโดยไม่ได้ตั้งใจของข้อมูลกลับ ไปยัง IBM เลือกจากอ็อพชันคำสั่งต่อไปนี้ เพื่อตั้งค่าคอนฟิกูเรชันที่ต้องการ:

- เมื่อต้องการเปิดใช้งานงาน Events Manager for Call Home: **chhmc -c emch -s enable**
- เมื่อต้องการปิดใช้งานงาน Events Manager for Call Home และเปิดใช้งาน call home อีกครั้งโดยอัตโนมัติ: **chhmc -c emch -s disable --callhome enable**
- เมื่อต้องการปิดใช้งานงาน Events Manager for Call Home และไม่เปิดใช้งาน call home โดยอัตโนมัติ: **chhmc -c emch -s disable --callhome disable**

ตรวจสอบให้แน่ใจว่า HMC สามารถสื่อสารกับ HMCs อื่นที่ปรับใช้ใน สภาวะแวดล้อมนี้ Events Manager for Call Home มีฟังก์ชันทดสอบการเชื่อมต่อ เมื่อลงทะเบียน HMC

คุณสามารถลงทะเบียน HMC กับ Events Manager for Call Home หลังจากคุณลงทะเบียน HMC, events manager จะเคียวรี HMC ที่ ลงทะเบียนสำหรับเหตุการณ์ใด ๆ ซึ่งกำลังรอถูกเรียกโฮมไปยัง IBM Events Manager แสดงข้อมูลที่กำลังถูกส่งกลับไปยัง IBM และอนุมัติเหตุการณ์เหล่านี้ หลังจากอนุมัติแล้ว Event Manager จะแจ้ง HMC ที่ลงทะเบียนว่าสามารถดำเนินการเรียกโฮมต่อไปได้

ภารกิจ Events Manager for Call Home สามารถรันจาก HMC ใด ๆ หรือ จากหลาย HMCs เมื่อต้องการลงทะเบียนคอนโซลการจัดการที่มีภารกิจ Events Manager for Call Home ให้ทำขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **สามารถให้บริการได้**  และจากนั้นเลือก **Events Manager for Call Home**
2. จากบานหน้าต่าง **Events Manager for Call Home** คลิก **จัดการคอนโซล**
3. จากหน้าต่าง **จัดการคอนโซลที่ลงทะเบียน** คลิก **เพิ่มคอนโซล** เพื่อป้อนข้อมูลเพื่อลงทะเบียน คอนโซลการจัดการที่มีภารกิจ Events Manager for Call Home
4. คลิก **ตกลง** เพื่อ commit การเปลี่ยนแปลงในรายการ ของคอนโซลการจัดการที่ลงทะเบียน

หมายเหตุ: Events Manager for Call Home สามารถใช้ได้โดยที่โหมด event manager ปิดใช้งาน คุณยังคงสามารถลงทะเบียน HMC และดูเหตุการณ์ ใน events manager แต่ Events Manager ไม่ควบคุมเมื่อ เรียกโฮมสำหรับเหตุการณ์

การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ

คุณต้องตั้งรหัสผ่านสำหรับเซิร์ฟเวอร์และ Advanced System Management (ASM) ของคุณ อ่านเพิ่มเติมเกี่ยวกับวิธีการใช้อินเตอร์เฟส HMC เพื่อตั้งรหัสผ่านเหล่านี้

ก่อนเริ่มต้นภารกิจ

หากคุณได้รับข้อความ `Authentication Pending` HMC จะเตือนให้คุณตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ

เกี่ยวกับภารกิจนี้

หากคุณไม่ได้รับข้อความ Authentication Pending ให้ทำ ขั้นตอนต่อไปนี้ให้เสร็จสิ้น เพื่อตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ

การอัพเดตรหัสผ่านเซิร์ฟเวอร์ของคุณ

Before you begin

เมื่อต้องการอัพเดตรหัสผ่านของเซิร์ฟเวอร์ ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้เลือกระบบที่ถูกจัดการและคลิกไอคอน **ผู้ใช้และ การรักษาความปลอดภัย**  จากนั้นเลือก **ผู้ใช้และบทบาท**
2. คลิก **เปลี่ยนรหัสผ่าน** หน้าต่าง อัพเดตรหัสผ่าน จะเปิด

3. พิมพ์ข้อมูลที่จำเป็น และคลิก **OK**

การอัพเดตรหัสผ่านทั่วไปสำหรับ Advanced System Management (ASM)

Before you begin

Note : ค่าดีฟอลต์ของรหัสผ่านสำหรับ ID ผู้ใช้ทั่วไปคือ `general` และค่าดีฟอลต์ของรหัสผ่านสำหรับ ID ผู้ดูแลระบบ คือ `admin`

เมื่อต้องการอัพเดตรหัสผ่านทั่วไปของ ASM ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทางของ HMC ให้เลือกระบบที่ถูกจัดการ
2. ในพื้นที่งาน ให้คลิก **การดำเนินการ**
3. คลิก **Advanced System Management (ASM)** หน้าต่าง Launch ASM Interface จะเปิด
4. เลือก Service Processor IP Address และคลิก **OK** อินเตอร์เฟส ASM จะเปิด
5. บนบานหน้าต่าง ASMI Welcome ให้ระบุ User ID และรหัสผ่าน และ คลิก **Log In**
6. ในพื้นที่การนำทาง ให้ขยาย **ล็อกอินโปรไฟล์**
7. เลือก **Change Password**
8. ระบุข้อมูลที่จำเป็น และคลิก **Continue**

การรีเซ็ตรหัสผ่านผู้ดูแลระบบ Advanced System Management (ASM)

Before you begin

เมื่อต้องการรีเซ็ตรหัสผ่านของผู้ดูแลระบบ ให้ติดต่อผู้ให้บริการ ที่ได้รับสิทธิ

การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ

ศึกษาเกี่ยวกับวิธีตรวจสอบว่าคุณเชื่อมต่อกับเครือข่ายอย่างถูกต้อง

เกี่ยวกับภารกิจนี้

เมื่อต้องการทดสอบการเชื่อมต่อเครือข่าย คุณต้องเป็นสมาชิกหนึ่งในบทบาทต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ตัวแทนการบริการ

เมื่อต้องการทดสอบการเชื่อมต่อระหว่าง HMC และระบบที่ถูกจัดการ ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **Console Settings**
2. ในบานหน้าต่างเนื้อหา คลิก **Test Network Connectivity**
3. ในแท็บ Ping ให้พิมพ์ชื่อโฮสต์หรือ IP แอดเดรสของระบบใด ๆ ซึ่งคุณต้องการเชื่อมต่อ เมื่อต้องการทดสอบเน็ตเวิร์กแบบเปิด ให้พิมพ์เกตเวย์ คลิก **Ping**

ผลลัพธ์

หากคุณยังไม่ได้สร้างโลจิคัลพาร์ติชันใด ๆ คุณจะไม่สามารถ ping แอดเดรสได้ คุณสามารถใช้ HMC เพื่อสร้าง โลจิคัลพาร์ติชันบนเซิร์ฟเวอร์ของคุณ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ การแบ่งโลจิคัลพาร์ติชัน

เมื่อต้องการทำความเข้าใจกับวิธีการใช้ HMC ในเน็ตเวิร์ก โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 34

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดคอนฟิก HMC เพื่อเชื่อมต่อกับ เครือข่าย โปรดดูที่ “การกำหนดค่า HMC โดยใช้เมนู ” ในหน้า 49

ขั้นตอน Postconfiguration

หลังจากที่คุณติดตั้งและกำหนดค่า HMC ให้สำรองข้อมูล HMC ตามที่จำเป็น

การสำรองข้อมูลคอนโซลการจัดการ

งานนี้จะสำรอง (หรือจัดเก็บ) ข้อมูลที่ถูกเก็บอยู่บนฮาร์ดดิสก์ HMC ของคุณซึ่งต้องใช้ความระมัดระวังในการสนับสนุนการดำเนินการของ HMC

ก่อนเริ่มต้นภารกิจ

ระบบรีโมตของคุณต้องมี Network File System (NFS) หรือ Secure Shell (ssh) ที่ถูกกำหนดคอนฟิกไว้ และเน็ตเวิร์กนี้ต้องสามารถเข้าถึงได้ จาก HMC เมื่อต้องการทำงานนี้ให้เสร็จสิ้น คุณต้องปิดและรีบูต HMC ใช้เฉพาะ HMC เพื่อดำเนินงานนี้

เกี่ยวกับภารกิจนี้

เมื่อต้องการสำรองข้อมูลของฮาร์ดดิสก์ไดร์ฟ HMC ไว้บนระบบรีโมต คุณต้องเป็นสมาชิกของบทบาทอย่างใดอย่างหนึ่งต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ตัวดำเนินการ
- ตัวแทนการบริการ

การสำรองข้อมูล HMC หลังจากทำการเปลี่ยนแปลงใน HMC หรือข้อมูลที่เชื่อมโยงกับโลจิคัลพาร์ติชัน

ข้อมูล HMC ที่เก็บไว้บนฮาร์ดไดร์ฟของ HMC สามารถบันทึกลงใน DVD-RAM บนระบบโลคัล ระบบรีโมตที่เทาท์ กับระบบไฟล์ HMC (เช่น NFS) หรือส่งไปยังรีโมตไซต์โดยใช้ File Transfer Protocol (FTP)

หมายเหตุ: สำหรับ HMC โมเดล 7063-CR1 คุณสามารถ เชื่อมต่อไดร์ฟ USB DVD ภายนอก

การใช้ HMC คุณสามารถสำรองข้อมูลที่มีความสำคัญทั้งหมดได้ เช่นข้อมูลดังต่อไปนี้:

- ไฟล์ค่า Preference ผู้ใช้
- รายละเอียดผู้ใช้
- ไฟล์แพล็ตฟอร์มคอนฟิกูเรชัน HMC
- ไฟล์บันทึกการทำงาน HMC
- HMC อัพเดตผ่าน Install Corrective Service

เมื่อต้องการสำรองข้อมูลฮาร์ดไดร์ฟ HMC ไปยังระบบรีโมต ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **สำรองข้อมูล คอนโซลการจัดการ**
3. จากหน้าต่าง **สำรองข้อมูลคอนโซลการจัดการ** เลือกอ็อพชันการเก็บถาวรที่คุณต้องการ ดำเนินการ
4. คลิก **ถัดไป** แล้วทำตามคำสั่งตามความเหมาะสม ซึ่งขึ้นอยู่กับอ็อพชันที่คุณเลือก
5. คลิก **ตกลง** เพื่อดำเนินการกับกระบวนการสำรองข้อมูล

การอัพเดต การอัพเกรด และการโอนย้ายรหัสเครื่อง HMC ของคุณ

การอัพเดตและอัพเกรดควรดำเนินการเป็นระยะ ๆ เพื่อให้ HMC สามารถเพิ่มคุณสมบัติการทำงานใหม่ ๆ และปรับปรุงคุณลักษณะที่มีอยู่ ศึกษาเพิ่มเติมเกี่ยวกับความแตกต่างระหว่างการอัพเดต การอัพเกรด และการโอนย้ายรหัสเครื่อง HMC ของคุณ รวมทั้งศึกษาวิธีดำเนินการอัพเดต อัพเกรด หรือโอนย้ายรหัสเครื่อง HMC

เมื่อคุณทำงานแต่ละงานเหล่านี้เสร็จสิ้น HMC จะรีบูต แต่พาร์ติชันไม่รีบูต

การอัพเดตรหัส HMC
ใช้การบำรุงรักษากับระดับ HMC ที่มีอยู่

คุณไม่จำเป็นต้องทำงาน **Save upgrade data**

การอัพเกรดรหัส HMC
แทนที่ซอฟต์แวร์ HMC ด้วยรีลีสใหม่หรือระดับโปรแกรมฟิกซ์ของโปรแกรมเดียวกัน

คุณต้องบูตจากสื่อบันทึกที่กู้คืน

การโอนย้ายรหัส HMC
ย้ายข้อมูล HMC จาก HMC เวอร์ชันหนึ่งเป็นเวอร์ชันอื่น

การโอนย้ายระบบเป็นการอัพเกรดชนิดหนึ่ง

หมายเหตุ: สำหรับ HMC โมเดล 7063-CR1 คุณสามารถเชื่อมต่อไดร์ฟ USB DVD ภายนอกได้

การกำหนดเวอร์ชันและรีลีสของรหัสเครื่อง HMC ของคุณ

ศึกษาวิธีการดูเวอร์ชันและรีลีสของรหัสเครื่อง HMC

เกี่ยวกับภารกิจนี้
ระดับของโค้ดเครื่องบน HMC จะกำหนดคุณลักษณะที่พร้อมใช้งาน รวมถึง การบำรุงรักษาและการปรับปรุงเฟิร์มแวร์เซิร์ฟเวอร์ในเวลาเดียวกันเพื่ออัพเกรดเป็นรีลีสใหม่

เมื่อต้องการดู เวอร์ชันและรีลีสของโค้ดเครื่อง HMC ให้ทำตามขั้นตอนต่อไปนี้:

กระบวนการ

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **Console Management**
2. ในบานหน้าต่างเนื้อหา คลิก **Update the Hardware Management Console**
3. ในหน้าต่างใหม่ ให้ดูและบันทึกข้อมูลที่ปรากฏภายใต้หัวข้อ **Current HMC Driver Information** รวมถึง เวอร์ชันของ HMC รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน

การขอรับและการใช้การอัพเดตรหัสเครื่องสำหรับ HMC เมื่อมี การเชื่อมต่ออินเตอร์เน็ต

ศึกษาวิธีขอรับอัพเดตรหัสเครื่องสำหรับ HMC เมื่อ HMC มีการเชื่อมต่ออินเตอร์เน็ต

เกี่ยวกับภารกิจนี้
เมื่อต้องการขอรับการอัพเดตโค้ดเครื่องสำหรับ HMC ให้ดำเนินการขั้นตอนทั้งหมด

ขั้นตอนที่ 1. ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเตอร์เน็ต

About this task

เมื่อต้องการดาวน์โหลดอัพเดตจากระบบหรือเว็บไซต์บริการและสนับสนุนลงใน HMC หรือเซิร์ฟเวอร์ของคุณ คุณต้องมีหนึ่งในการเชื่อมต่อต่อไปนี้:

- การเชื่อมต่อ SSL โดยมีหรือไม่มีพร็อกซี SSL
- อินเตอร์เน็ตผ่าน VPN

เพื่อให้แน่ใจว่าคุณมีการเชื่อมต่ออินเตอร์เน็ต ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **สามารถให้บริการได้**  จากนั้นเลือก **การจัดการเซอร์วิส**
2. ในบานหน้าต่างเนื้อหา **จัดการการเชื่อมต่อขาออก**

3. เลือกแท็บสำหรับชนิดของการเชื่อมต่อขาออก ที่คุณเลือกใช้สำหรับ HMC ของคุณ (VPN อินเตอร์เน็ต หรือ SSL)

   Note : ถ้าไม่มีการเชื่อมต่อกับส่วนบริการและสนับสนุน ให้ตั้งค่าการเชื่อมต่อบริการ ก่อนที่จะดำเนินการต่อสำหรับขั้นตอนนี้ สำหรับคำแนะนำเกี่ยวกับวิธีการตั้งค่าการเชื่อมต่อกับส่วนบริการและสนับสนุน โปรดดูที่ การตั้งค่าเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการและสนับสนุน IBM
4. คลิก **Test**
5. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์

   ถ้าการทดสอบไม่เสร็จสมบูรณ์ ให้แก้ปัญหาการเชื่อมต่อและแก้ไข ปัญหา ก่อนที่จะดำเนินการต่อตามขั้นตอนนี้ อีกทางหนึ่ง คุณสามารถ ขอรับอัพเดตบนดีวีดี

   Note : สำหรับ HMC โมเดล 7063-CR1 คุณสามารถ เชื่อมต่อไดร์ฟ USB DVD ภายนอก
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่” on page 70

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

About this task

เมื่อต้องการดูระดับโค้ดเครื่องของ HMC ที่มีอยู่ ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน ของ HMC
4. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่” on page 70

ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

About this task

เมื่อต้องการดูระดับโค้ดเครื่องของ HMC ที่มี ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเตอร์เน็ต ให้ไปที่ http://www.ibm.com/eserver/support/fixes
2. เลือกตระกูลที่เหมาะสมในรายการตระกูล ผลิตภัณฑ์
3. เลือก **Hardware Management Console** ใน รายการชนิดผลิตภัณฑ์หรือโปรแกรมฟิกซ์
4. คลิก **ทำต่อไป**

   ไซต์ Hardware Management Console จะปรากฏขึ้น
5. เลื่อนลงไปยังระดับเวอร์ชัน HMC ของคุณ เพื่อ ดูระดับ HMC ที่มีอยู่

   Note : ถ้าคุณต้องการ คุณสามารถติดต่อ ส่วนบริการและสนับสนุน
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 4. ใช้อัพเดตรหัสเครื่อง HMC” on page 70

ขั้นตอนที่ 4. ใช้อัพเดตรหัสเครื่อง HMC

About this task

เมื่อต้องการใช้การอัพเดตโค้ดเครื่องของ HMC ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ก่อนที่คุณจะติดตั้งอัพเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูลคอนโซลที่สำคัญบน HMC ของคุณ

สำหรับข้อแนะนำ โปรดดูที่ “การสำรองข้อมูลคอนโซลการจัดการ” on page 68 จากนั้น ให้ดำเนินการขั้นตอนถัดไป

2. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
3. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console** วิซาร์ด Install Corrective Service จะเปิดขึ้น
4. ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อติดตั้งอัพเดต
5. ปิดเครื่อง แล้วรีสตาร์ท HMC เพื่อให้ อัพเดตมีผล
6. คลิก **ล็อคออนและเรียกใช้เว็บแอ็พพลิเคชัน Hardware Management Console**
7. ล็อกอินเข้าสู่อินเตอร์เฟส HMC

ขั้นตอนที่ 5. ตรวจสอบว่าอัพเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

About this task

เมื่อต้องการตรวจสอบว่าการอัพเดตโค้ดเครื่องของ HMC ติดตั้งอย่างถูกต้อง ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน ของ HMC
4. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัพเดตที่คุณติดตั้ง
5. หากระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:
   a. เลือกการเชื่อมต่อเครือข่ายบน HMC
   b. ลองทำการอัพเดตเฟิร์มแวร์อีกครั้ง โดยใช้ที่เก็บอื่น
   c. ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การขอรับอัพเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP

ศึกษาวิธีการขอรับการอัพเดตโค้ดเครื่องสำหรับ Hardware Management Console (HMC) โดย ใช้ DVD หรือเซิร์ฟเวอร์ FTP

เกี่ยวกับภารกิจนี้

เมื่อต้องการขอรับการอัพเดตโค้ดเครื่องของ HMC ให้ดำเนินการขั้นตอนทั้งหมด

หมายเหตุ: สำหรับ HMC โมเดล 7063-CR1 คุณสามารถเชื่อมต่อไดร์ฟ USB DVD ภายนอกได้

ขั้นตอนที่ 1. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

Before you begin

เมื่อต้องการดูระดับโค้ดเครื่องของ HMC ที่มีอยู่ ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console**

3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน ของ HMC
4. ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่” on page 72

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

Before you begin

เมื่อต้องการดูระดับโค้ดเครื่องของ HMC ที่มี ให้ทำตามขั้นตอนต่อไปนี้:

About this task

Procedure

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ไปที่เว็บไซต์ Fix Central
2. เลื่อนลงไปยังระดับเวอร์ชัน HMC ของคุณ เพื่อ ดูระดับ HMC ที่มีอยู่

   Note : ถ้าคุณต้องการ คุณสามารถติดต่อส่วนบริการและสนับสนุน IBM
3. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. ขอรับอัพเดตรหัสเครื่อง HMC” on page 72

ขั้นตอนที่ 3. ขอรับอัพเดตรหัสเครื่อง HMC

Before you begin

เมื่อต้องการขอรับการอัพเดตโค้ดเครื่องของ HMC ให้ทำตามขั้นตอนต่อไปนี้:

About this task

คุณสามารถสั่งซื้ออัพเกรดรหัสเครื่อง HMC ผ่านทางเว็บไซต์ Fix Central โดยติดต่อส่วนบริการและสนับสนุน หรือดาวน์โหลด ไปยังเซิร์ฟเวอร์ FTP

สั่งซื้อการอัพเดตโค้ดเครื่อง HMC ผ่านเว็บไซต์ Fix Central

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ไปที่เว็บไซต์ Fix Central
2. ภายใต้ Supported HMC products ให้เลือกระดับ HMC ล่าสุด
3. เลื่อนลงไปยังชื่อไฟล์ / พื้นที่แพ็กเกจ และหาอัพเดตที่คุณต้องการสั่งซื้อ
4. ในคอลัมน์ Order ให้เลือก **Go**
5. คลิก **Continue** เพื่อลงชื่อเข้าใช้ด้วย IBM ID ของคุณ
6. ปฏิบัติตามพร้อมต์บนหน้าจอเพื่อทำการสั่งซื้อ

การดาวน์โหลดอัพเดตรหัสเครื่อง HMC ลงในสื่อบันทึกแบบถอดออกได้

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ไปที่เว็บไซต์ Fix Central
2. ภายใต้ Supported HMC products ให้เลือกระดับ HMC ล่าสุด
3. เลื่อนลงมายังชื่อไฟล์ / พื้นที่แพ็กเกจ และหาอัพเดตที่คุณต้องการ ดาวน์โหลด
4. ตรวจสอบอัพเดตที่คุณต้องการดาวน์โหลด
5. ยอมรับข้อตกลงไลเซนส์ และบันทึกอัพเดตลงในสื่อบันทึกแบบถอดออกได้

What to do next

เมื่อเสร็จเรียบร้อย ให้ดำเนินการต่อด้วย “ขั้นตอนที่ 4. ใช้อัพเดตรหัสเครื่อง HMC” on page 72

ขั้นตอนที่ 4. ใช้อัพเดตรหัสเครื่อง HMC

Before you begin

เมื่อต้องการใช้การอัพเดตโค้ดเครื่องของ HMC ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ก่อนที่คุณจะติดตั้งอัพเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูล HMC ของคุณ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การสำรองข้อมูลคอนโซลการจัดการ” on page 68
2. ถ้าคุณได้รับหรือสร้างอัพเดตบนดีวีดีแรม ให้ใส่แผ่นดิสก์ดังกล่าวในไดร์ฟดีวีดีบน HMC ถ้าคุณได้รับหรือสร้างอัพเดตบนอุปกรณ์หน่วยความจำแบบ USB ให้เสียบอุปกรณ์หน่วยความจำนั้น
3. ก่อนที่คุณจะติดตั้งอัพเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูลคอนโซลที่สำคัญบน HMC ของคุณ สำหรับข้อแนะนำ โปรดดูที่ “การสำรองข้อมูลคอนโซลการจัดการ” on page 68 จากนั้น ให้ดำเนินการขั้นตอนถัดไป
4. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
5. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console** วิซาร์ด Install Corrective Service จะเปิดขึ้น
6. ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อติดตั้งอัพเดต
7. ปิดเครื่อง รีสตาร์ท และกลับเข้าสู่ระบบ HMC เพื่อให้การอัพเดตมีผล
8. ดำเนินการต่อด้วย “ขั้นตอนที่ 5. ตรวจสอบว่าอัพเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์” on page 73

ขั้นตอนที่ 5. ตรวจสอบว่าอัพเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

Before you begin

เมื่อต้องการตรวจสอบว่าการอัพเดตโค้ดเครื่องของ HMC ติดตั้งสำเร็จ ให้ทำตามขั้นตอน ต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC การจัดการ**  แล้วเลือก **การจัดการคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **อัพเดต Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน ของ HMC
4. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัพเดตที่คุณติดตั้ง
5. หากระดับของโค้ดที่แสดงไม่ใช่ระดับที่คุณติดตั้ง ให้ดำเนินการ ขั้นตอนต่อไปนี้:
   a. ลองอัพเดตรหัสเครื่องอีกครั้ง ถ้าคุณสร้างดีวีดีในขั้นตอนนี้ ให้ใช้สื่อบันทึกใหม่
   b. ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การอัพเกรดซอฟต์แวร์ HMC ของคุณ

ศึกษาวิธีการอัพเกรดซอฟต์แวร์บน HMC จากรีลีสหนึ่งเป็นรีลีสถัดไปขณะที่คุณ เก็บรักษาข้อมูลกำหนดคอนฟิก HMC ของคุณไว้

เกี่ยวกับภารกิจนี้

เมื่อต้องการอัพเกรดโค้ดเครื่องบน HMC ให้ดำเนินการขั้นตอนทั้งหมด

หมายเหตุ: สำหรับโมเดล HMC 7063-CR1 และ 7063-CR2, คุณสามารถเชื่อมต่อไดร์ฟ USB DVD ภายนอก

ขั้นตอนที่ 1. ขอรับอัพเกรด

About this task

คุณสามารถสั่งซื้อการอัพเกรดโค้ดเครื่องของ HMC ผ่านเว็บไซต์ Fix Central

เมื่อต้องการขอรับการอัพเกรดผ่านเว็บไซต์ Fix Central ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่เว็บไซต์ Hardware Management Console ที่ http://www-933.ibm.com/support/fixcentral/
2. คลิก **Continue**

   ไซต์ Hardware Management Console จะปรากฏขึ้น
3. นำทางไปยังเวอร์ชัน HMC ที่คุณต้องการอัพเกรด
4. ค้นหาตำแหน่งส่วนดาวน์โหลดและสั่งซื้อ

   Note : หากคุณไม่สามารถเข้าถึงอินเทอร์เน็ต โปรดติดต่อฝ่ายบริการและสนับสนุนของ IBM เพื่อสั่งซื้อการอัพเกรดบน DVD
5. ปฏิบัติตามพร้อมต์บนหน้าจอเพื่อทำการสั่งซื้อ
6. หลังจากที่เสร็จเรียบร้อย ให้ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่” on page 74

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

About this task

เมื่อต้องการกำหนดระดับรหัสเครื่องที่มีอยู่บน HMC ให้ปฏิบัติตาม ขั้นตอนเหล่านี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Settings** ในพื้นที่ การนำทาง ให้คลิก **Updates**
2. ในบานหน้าต่างเนื้อหา คลิก **Update the Hardware Management Console**
3. ในหน้าต่างใหม่ ให้ดูและบันทึกข้อมูลที่ปรากฏภายใต้หัวข้อข้อมูล Current HMC Driver รวมถึง เวอร์ชันของ HMC รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน
4. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ” on page 74

ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ

About this task

เมื่อต้องการสำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. เลือกระบบที่คุณต้องการบันทึกข้อมูลโปรไฟล์
2. คลิก **Actions** > **View All Actions** > **Legacy** > **Manage Partition Data** > **Backup**
3. พิมพ์ชื่อไฟล์สำรองและบันทึกข้อมูลนี้
4. คลิก **OK**
5. ทำซ้ำขั้นตอนเหล่านี้สำหรับแต่ละระบบ
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 4. สำรองข้อมูล HMC” on page 74

ขั้นตอนที่ 4. สำรองข้อมูล HMC

About this task

สำรองข้อมูล HMC ก่อนที่คุณจะติดตั้งซอฟต์แวร์ HMC เวอร์ชันใหม่เพื่อให้ระดับก่อนหน้า สามารถเรียกคืนได้ในกรณีที่เกิดปัญหาขณะคุณอัพเกรดซอฟต์แวร์ ห้ามใช้ข้อมูลคอนโซลที่สำคัญนี้หลังจากที่อัพเกรดเป็น ซอฟต์แวร์ HMC เวอร์ชันใหม่ได้สำเร็จ

Note : เมื่อต้องการสำรองข้อมูลลงใน สื่อบันทึกที่สามารถถอดออกได้ คุณต้องมีสื่อบันทึกดังกล่าว

เมื่อต้องการสำรองข้อมูล HMC ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ถ้าคุณวางแผนที่จะสำรองข้อมูลไปยังสื่อบันทึก ให้ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อจัดรูปแบบ สื่อบันทึก:
   a. ใส่สื่อบันทึกลงในไดร์ฟ
   b. ในพื้นที่การนำทาง ให้คลิกไอคอน **Serviceability**  จากนั้นเลือก **Service Management**
   c. ในบานหน้าต่างเนื้อหา คลิก **Format Media**
   d. เลือกชนิดของสื่อบันทึก
   e. เลือกชนิดการจัดรูปแบบ
   f. คลิก **OK**
2. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Management**
3. ในบานหน้าต่างเนื้อหา คลิก **Backup Management Console Data**
   หน้าต่าง **Backup Management Console Data** จะปรากฏขึ้น
4. เลือกอ็อพชันการเก็บถาวร
   คุณสามารถสำรองข้อมูลลงในสื่อบันทึกบนระบบโลคัล ระบบรีโมตที่เมาส์กับระบบไฟล์ HMC (เช่น NFS) หรือส่งการสำรองข้อมูลไปยังรีโมตไซต์โดยใช้ File Transfer Protocol (FTP)
   - เมื่อต้องการสำรองข้อมูลลงในระบบภายในเครื่อง ให้เลือก **Back up to media on local system** และปฏิบัติตามคำแนะนำ
   - เมื่อต้องการสำรองข้อมูลไปยังระบบระยะไกลที่เชื่อมต่อ ให้เลือก **Back up to mounted remote system** และปฏิบัติตามคำแนะนำ
   - เมื่อต้องการสำรองข้อมูลไปยังไซต์ FTP ระยะไกล ให้เลือก **Send back up critical data to remote site** และปฏิบัติตามคำแนะนำ
5. ดำเนินการต่อด้วย “ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน” on page 75

ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน

About this task

ก่อนที่คุณจะอัพเกรดเป็นซอฟต์แวร์ HMC เวอร์ชันใหม่ ให้บันทึกข้อมูลคอนฟิกูเรชัน HMC เพื่อเป็นการป้องกัน

เมื่อต้องการบันทึกคอนฟิกูเรชัน HMC ปัจจุบัน ให้ทำตาม ขั้นตอนต่อไปนี้:

Procedure

1. เลือกระบบที่ถูกจัดการหรือพาร์ติชันที่คุณต้องการบันทึกข้อมูลคอนฟิกูเรชัน HMC
2. จากพ็อดเมนู ให้เลือก **Actions** > **Schedule Operations**
   การดำเนินการที่กำหนดเวลาไว้ทั้งหมดสำหรับเป้าหมายที่คุณเลือกจะถูกแสดง
3. เลือก **Sort** > **By Object**
4. เลือกแต่ละอ็อบเจ็กต์ และบันทึกรายละเอียดต่อไปนี้:
   - ชื่ออ็อบเจ็กต์
   - วันที่กำหนดการ
   - เวลาดำเนินการ (ในรูปแบบ 24 ชั่วโมง)
   - ทำซ้ำ (หากเลือก Yes ให้ทำตามขั้นตอนต่อไปนี้):
     a. เลือก **View** > **Schedule Details**
     b. บันทึกข้อมูลช่วงเวลา
     c. ปิดหน้าต่างการดำเนินการตามกำหนดการ
     d. ทำซ้ำสำหรับการดำเนินการตามกำหนดการแต่ละอย่าง

5. ปิดหน้าต่าง **Customize Scheduled Operations**
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล” on page 76

ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล

About this task

เมื่อต้องการบันทึกสถานะคำสั่งแบบรีโมต ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **Users and Security**  จากนั้นเลือก **Sysytems and Console Security**
2. ในบานหน้าต่างเนื้อหา ให้คลิก **Enable Remote Command Execution**
3. บันทึกว่าเช็กบ็อกซ์ **Enable remote command execution using the ssh facility** ถูกเลือกหรือไม่
4. คลิก **Cancel**
5. ดำเนินการต่อด้วย “ขั้นตอนที่ 7. บันทึกข้อมูลอัพเกรด” on page 76

ขั้นตอนที่ 7. บันทึกข้อมูลอัพเกรด

About this task

คุณสามารถบันทึกคอนฟิกูเรชัน HMC ปัจจุบันลงในพาร์ติชันของดิสก์ ที่กำหนดบน HMC หรือในสื่อบันทึกภายในเครื่องก็ได้ บันทึกข้อมูลการอัพเกรดทันทีหลังจากคุณอัพเกรดซอฟต์แวร์ HMC ของคุณเป็น รีลีสใหม่เท่านั้น คุณสามารถเรียกคืนค่าติดตั้งคอนฟิกูเรชัน HMC หลังจากที่คุณอัพเกรด

Note : อนุญาตให้มีข้อมูลสำรองได้เพียงระดับเดียวเท่านั้น แต่ละครั้งที่คุณบันทึกข้อมูลการอัพเกรด ระดับก่อนหน้านี้จะถูกเขียนทับ

เมื่อต้องการบันทึกข้อมูลการอัพเกรด ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Management**
2. ในบานหน้าต่างเนื้อหา คลิก **Save Upgrade Data** วิซาร์ด **Save Upgrade Data** จะเปิดขึ้น
3. เลือกสื่อบันทึกที่คุณต้องการบันทึกข้อมูล อัพเกรด ถ้าคุณเลือกที่จะบันทึกสื่อบันทึกแบบถอดได้ ให้ใส่สื่อบันทึกในตอนนี้ คลิก **Next**
4. คลิก **Finish**
5. รอให้งานเสร็จสมบูรณ์

   ถ้างาน Save Upgrade Data ล้มเหลว ให้ติดต่อระดับของการสนับสนุนถัดไปก่อนที่จะดำเนินการ

   Note : ถ้างานบันทึกข้อมูลอัพเกรดล้มเหลว ห้ามดำเนินกระบวนการอัพเกรด
6. คลิก **OK**
7. ดำเนินการต่อด้วย “ขั้นตอนที่ 8. อัพเกรดซอฟต์แวร์ HMC” on page 76

ขั้นตอนที่ 8. อัพเกรดซอฟต์แวร์ HMC

About this task

เมื่อต้องการอัพเกรดซอฟต์แวร์ HMC ให้รีสตาร์ทระบบโดยใช้ สื่อบันทึกแบบถอดออกได้ในไดร์ฟ DVD

Procedure

1. ใส่สื่อบันทึกสำหรับการติดตั้งผลิตภัณฑ์ HMC ลงในไดร์ฟดีวีดี
2. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Management**
3. ในพื้นที่การนำทาง เลือก **Shutdown or Restart the Management Console**
4. ตรวจสอบว่า **Restart the HMC** ถูกเลือกไว้
5. คลิก **OK**
   HMC จะเริ่มทำงานอีกครั้ง และ ข้อมูลระบบจะเลื่อนอยู่บนหน้าต่าง
6. เลือก **Upgrade** และคลิก **Next**
7. เลือกจากอ็อพชันต่อไปนี้:
   - หากคุณบันทึกข้อมูลการอัพเกรดระหว่างงานก่อนหน้านี้ ให้ดำเนินการขั้นตอนถัดไป
   - หากคุณไม่ได้บันทึกข้อมูลการอัพเกรดก่อนหน้านี้ในโพรซีเดอร์นี้ คุณต้องบันทึกข้อมูลการอัพเกรดเดี๋ยวนี้ ก่อนที่จะดำเนินการต่อ
8. เลือก **Upgrade from media** และคลิก **Next**
9. ยืนยันค่าติดตั้ง และคลิก **Finish**
10. ปฏิบัติตามพร้อมต์

    Note :

    - ถ้าหน้าจอว่างเปล่า ให้กด space bar เพื่อดูข้อมูล
    - ดีวีดีแผ่นแรกอาจใช้เวลาประมาณ 20 ในการติดตั้ง
11. ที่พร้อมต์ล็อกอิน ให้ล็อกอินโดยใช้ user ID และรหัสผ่านของคุณ
    การติดตั้งรหัส HMC เสร็จสมบูรณ์
12. ดำเนินการต่อด้วย “ขั้นตอนที่ 9. ตรวจสอบว่าอัพเกรดสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์” on page 77

ขั้นตอนที่ 9. ตรวจสอบว่าอัพเกรดสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

About this task

เมื่อต้องการตรวจสอบว่าการอัพเกรด HMC ติดตั้งสำเร็จ ให้ทำตามขั้นตอนต่อไปนี้:

Procedure

1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management**  แล้วเลือก **Console Management**
2. ในบานหน้าต่างเนื้อหา คลิก **Update the Hardware Management Console**
3. ในหน้าต่างใหม่ ให้ดูและบันทึกข้อมูลที่ปรากฏภายใต้หัวข้อข้อมูล Current HMC Driver รวมถึง เวอร์ชันของ HMC รีลีส ระดับการซ่อมบำรุง ระดับบิวด์ และเวอร์ชันฐาน
4. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัพเดตที่คุณติดตั้ง
5. หากระดับของโค้ดที่แสดงไม่ใช่ระดับที่คุณติดตั้ง ให้ลองทำดำเนินการอัพเกรดอีกครั้ง โดยใช้ DVD ใหม่ ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การอัพเกรด HMC จากตำแหน่งรีโมตโดยใช้อิมเมจการอัพเกรดบนเครือข่าย

ศึกษาวิธีการอัพเกรดซอฟต์แวร์บน HMC จากตำแหน่งรีโมตโดยใช้ อิมเมจการอัพเกรดบนเครือข่าย

เกี่ยวกับภารกิจนี้

ศึกษาวิธีการอัพเกรดซอฟต์แวร์บน HMC จากตำแหน่งรีโมตโดยใช้ อิมเมจการอัพเกรดบนเครือข่าย

กระบวนการ

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่ เว็บไซต์ Hardware Management Console Support and downloads (http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html)
2. ดาวน์โหลดอิมเมจเครือข่าย HMC V9 ที่เหมาะสมและบันทึกลงบนเซิร์ฟเวอร์ FTP
   คุณไม่สามารถดาวน์โหลดไฟล์เหล่านี้ โดยตรงไปยัง HMC คุณต้องดาวน์โหลดไฟล์อิมเมจไปยังเซิร์ฟเวอร์ ที่ยอมรับคำร้องขอ FTP
3. ตรวจสอบให้แน่ใจว่าคุณดาวน์โหลดไฟล์ต่อไปนี้:
   - img2a
   - img3a
   - base.img
   - disk1.img
   - hmcnetworkfiles.sum
4. บันทึกข้อมูลการอัพเกรดบน HMC รันคำสั่งต่อไปนี้เพื่อบันทึกข้อมูลการอัพเกรด:
   - เมื่อต้องการบันทึกข้อมูลบนทั้ง DVD และ HDD ให้รันคำสั่งต่อไปนี้:

     mount /media/cdrom

     saveupgdata -r diskdvd
   - เมื่อต้องการบันทึกบน HDD ให้รันคำสั่งต่อไปนี้:

     saveupgdata -r disk
5. คัดลอกไฟล์การอัพเกรดไปยังพาร์ติชันดิสก์ที่สามารถบูตได้ บน HMC รันคำสั่ง **getupgfiles** เพื่อคัดลอก ไฟล์

   ตัวอย่าง: **getupgfiles -h <ftp server> -u <user id> -d <remote directory>**

   โดย
   - **ftp server** เป็นชื่อโฮสต์หรือ IP ของเซิร์ฟเวอร์ FTP ที่คุณดาวน์โหลด อิมเมจเครือข่าย HMC
   - **user id** เป็ร ID ผู้ใช้บนเซิร์ฟเวอร์ FTP หากคุณไม่ได้ระบุรหัสผ่าน ด้วยอาร์กิวเมนต์ `--passwd` คุณจะได้รับพร้อมต์ให้ป้อนรหัสผ่าน
   - **remote directory** คือไดเร็กทอรีบนเซิร์ฟเวอร์ FTP ของคุณที่บันทึกอิมเมจเครือข่าย HMC ไว้
6. รีสตาร์ท HMC เพื่ออัพเกรดโค้ดที่คัดลอกลงในพาร์ติชันดิสก์ที่สามารถบู๊ตได้ รัน **chhmc -c altdiskboot -s enable --mode upgrade** เพื่อรีสตาร์ท HMC
7. รีสตาร์ท HMC และเริ่มต้นการอัพเกรด รันคำสั่ง **hmcshutdown -r -t now** เพื่อเริ่มต้นการอัพเกรด

การรักษาความปลอดภัย HMC

ศึกษาวิธีการปรับปรุงความปลอดภัย Hardware Management Console (HMC) ของคุณที่ใช้ ตามมาตรฐานความปลอดภัยขององค์กรของคุณ Hardware Management Console (HMC)

การกำหนดคอนฟิกดีฟอลต์ของ HMC ให้ความปลอดภัยที่เพียงพอสำหรับผู้ใช้ระดับองค์กรส่วนใหญ่ ด้วย Hardware Management Console (HMC) เวอร์ชัน 8.4.0 หรือใหม่กว่าคุณสามารถปรับปรุงการรักษาความปลอดภัย HMC เพิ่มเติมตามมาตรฐานความปลอดภัยขององค์กรของคุณ เมื่อต้องการปรับปรุงความปลอดภัยสำหรับ HMC คุณต้องเซ็ต HMC เป็นความปลอดภัยขั้นต่ำ Level 1 คุณ สามารถเลือกความปลอดภัย Level 2 และ Level 3 ขึ้นกับสภาวะแวดล้อมและข้อกำหนดความปลอดภัย ขององค์กร

หมายเหตุ: ก่อนที่จะเปลี่ยนระดับความปลอดภัยตรวจสอบกับทีมข้อกำหนดความปลอดภัยของ องค์กรของคุณ

ความปลอดภัย Level 1

เมื่อต้องการรักษาความปลอดภัย HMC (ความปลอดภัยระดับ 1) ดำเนินขั้นตอนต่อไปนี้:

1. เปลี่ยนรหัสผ่านดีฟอลต์สำหรับผู้ใช้ `hscroot` สำหรับข้อมูลเพิ่มเติม เกี่ยวกับนโยบายรหัสผ่าน โปรดดูที่ “นโยบายรหัสผ่านที่ได้รับการพัฒนา” ในหน้า 80
2. หาก HMC ไม่ได้อยู่ในสภาพแวดล้อมที่ปลอดภัยทางกายภาพ ให้เซ็ตรหัสผ่าน `grub` โดยรันคำสั่งต่อไปนี้: `chhmc -c grubpasswd -s enable --passwd <new grub password>`

3. ถ้าคุณตั้งค่า Integrated Management Module (IMM) บน HMC ให้กำหนดรหัสผ่าน IMM ที่รัดกุม
4. กำหนดรหัสผ่านที่รัดกุมสำหรับผู้ใช้ *admin* และผู้ใช้ทั่วไปบนเซิร์ฟเวอร์ทั้งหมด
5. อัพเดต HMC ด้วยโปรแกรมฟิกซ์ความปลอดภัยที่รีลีสล่าสุด สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรแกรมฟิกซ์ ความปลอดภัย โปรดดูที่ IBM Fix Central

ความปลอดภัย Level 2

หากคุณมีผู้ใช้หลายคนให้ทำตามขั้นตอนต่อไปนี้เพื่อเพิ่มความปลอดภัยให้กับ HMC:

1. สร้างแอคเคาต์สำหรับแต่ละผู้ใช้บน HMC และกำหนดบทบาทและรีซอร์สให้กับผู้ใช้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบทบาทต่างๆ ใน HMC โปรดดูที่ HMC ภารกิจ, บทบาทผู้ใช้, ID และคำสั่ง ที่เกี่ยวข้อง

   หมายเหตุ: ตรวจสอบให้แน่ใจว่าคุณกำหนดเฉพาะทรัพยากรและบทบาทที่จำเป็นสำหรับผู้ใช้นั้น ถูกสร้างขึ้นบน HMC หากจำเป็นคุณสามารถสร้างบทบาทที่กำหนดเองได้
2. เปิดใช้งานเรพลิเคชันข้อมูลผู้ใช้ระหว่าง Hardware Management Consoles ที่ต่างกัน เรพลิเคชันข้อมูลผู้ใช้สามารถทำได้ในโหมด Master-slave หรือโหมด Peer-Peer สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเรพลิเคชัน ข้อมูลผู้ใช้ โปรดดูที่ จัดการเรพลิเคชันข้อมูล
3. อิมพอร์ตใบรับรองที่ลงนามโดย Certificate Authority

ความปลอดภัย Level 3

ถ้าคุณมี Hardware Management Consoles หลายชุดและผู้ดูแลระบบหลายคน ให้ทำตามขั้นตอนต่อไปนี้เพื่อเพิ่มความปลอดภัยให้กับ HMC:

1. ใช้การพิสูจน์ตัวตนรวมศูนย์เช่น Lightweight Directory Access Protocol (LDAP) หรือ Kerberos สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดคอนฟิก LDAP โปรดดูที่ วิธีกำหนดคอนฟิก LDAP บน HMC
2. เปิดใช้งานเรพลิเคชันข้อมูลผู้ใช้ระหว่าง Hardware Management Consoles ที่ต่างกัน
3. ตรวจสอบให้แน่ใจว่า HMC อยู่ใน NIST SP 800-131A mode เพื่อที่ HMC ใช้เฉพาะรหัสที่รัดกุม
4. บล็อกพอร์ตที่ไม่จำเป็นในไฟร์วอลล์ สำหรับข้อมูลเกี่ยวกับพอร์ต HMC ที่สามารถ ใช้ได้ให้ดูที่ตารางต่อไปนี้:

ตารางที่ 32. พอร์ตที่ใช้โดยผู้ใช้สำหรับการโต้ตอบกับ HMC

พอร์ต	คำอธิบาย	ชนิด	เวอร์ชันโปรโตคอล (โหมดดีฟอลต์)	เวอร์ชันโปรโตคอล (โหมด NIST)
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	SNMP Agent	UDP	SNMP v3	SNMP v3
162	SNMP Trap	UDP	SNMP v3	SNMP v3
427	SLP	UDP	ไม่มีข้อมูล	ไม่มีข้อมูล
443	HMC GUI และ REST API	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (ข้อความธรรมดา + แฮชและเครื่องหมาย)	RSCT (ข้อความธรรมดา + แฮชและเครื่องหมาย)
2300	5250 เทอร์มินัลสำหรับ IBM i	TCP	ข้อความธรรมดา	ข้อความธรรมดา
2301	5250 เทอร์มินัลที่มีการรักษาความปลอดภัยสำหรับ IBM i	TCP	TLS 1.2	TLS 1.2

ตารางที่ 32. พอร์ตที่ใช้โดยผู้ใช้สำหรับการโต้ตอบกับ HMC (ต่อ)				
พอร์ต	**คำอธิบาย**	**ชนิด**	**เวอร์ชันโปรโตคอล (โหมดดีฟอลต์)**	**เวอร์ชันโปรโตคอล (โหมด NIST)**
5989	CIM (พอร์ตเดิม, ไม่ทำงาน)	TCP	ไม่ทำงาน	ไม่ทำงาน
9900	FCS: HMC-HMC discovery	UDP	FCS	FCS
9920	FCS: HMC-HMC communication	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	VTerm แอ็พเพล็ตใน GUI	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	HMC REST API (legacy port)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	RSCT เพียร์โดเมน	UDP	RSCT (ข้อความธรรมดา + แฮชและเครื่องหมาย)	RSCT (ข้อความธรรมดา + แฮชและเครื่องหมาย)
12348	RSCT เพียร์โดเมน	UDP	RSCT (ข้อความธรรมดา + แฮชและเครื่องหมาย)	RSCT (ข้อความธรรมดา + แฮชและเครื่องหมาย)

Notes:

- คุณต้องใช้เพียง SSH (พอร์ต 22), HTTPS (พอร์ต 443 และพอร์ต 12443), 5250 เทอร์มินัลที่รักษาความปลอดภัยสำหรับ IBM i (พอร์ต 2301) และ VTerm (พอร์ต 9960) ที่ถูกเผย กับอินทราเน็ต พอร์ตอื่น ๆ ทั้งหมดจะต้องถูกใช้ในเครือข่ายส่วนตัวหรือแยกตัว คุณสามารถ ใช้พอร์ต Ethernet และ VLAN สำหรับ Resource Monitoring and Control (RMC) (พอร์ต 657), FCS (พอร์ต 9900 และพอร์ต 9920) และ RSCT Peer Domain (พอร์ต 12347 และพอร์ต 12348)
- พอร์ตที่แสดงในคำสั่ง **netstat** และใช้สำหรับกระบวนการภายใน เท่านั้น

นโยบายรหัสผ่านที่ได้รับการพัฒนา

คุณสามารถบังคับใช้ข้อกำหนดรหัสผ่านสำหรับผู้ใช้ที่ผ่านการพิสูจน์ตัวตนแบบโลคัลโดยใช้ คอนโซลการจัดการฮาร์ดแวร์ (HMC) ฟังก์ชั่นนโยบายรหัสผ่านที่ปรับปรุงช่วยให้ผู้ดูแลระบบสามารถกำหนดข้อจำกัดของรหัสผ่านได้ นโยบายรหัสผ่านที่ปรับปรุงนั้นใช้กับระบบที่ HMC ถูกติดตั้งอยู่

ผู้ดูแลระบบสามารถใช้นโยบายรหัสที่ปรับปรุงเพื่อกำหนดนโยบายรหัสผ่านเดียวสำหรับ ผู้ใช้ทั้งหมด HMC จัดเตรียมนโยบายรหัสผ่านความปลอดภัยระดับกลางซึ่ง ผู้ดูแลระบบสามารถเปิดใช้งานเพื่อตั้งค่าข้อ จำกัด รหัสผ่าน ผู้ดูแลระบบยังสามารถเลือกเปิดใช้งานนโยบาย ความปลอดภัยระดับกลางหรือนโยบายที่ผู้ใช้กำหนดเองใหม่ได้ นโยบายรหัสผ่านความปลอดภัยปานกลาง HMC ไม่สามารถลบออก จากระบบได้ ตารางต่อไปนี้แสดงรายการของชุดข้อมูลนโยบายความปลอดภัยขนาดกลางและ ค่าดีฟอลต์

ตารางที่ 33. แอ็ตทริบิวต์รหัสผ่านสำหรับนโยบายรหัสผ่านความปลอดภัย ระดับกลาง HMC		
แอ็ตทริบิวต์	**คำอธิบาย**	**ค่าดีฟอลต์**
`min_pwage`	จำนวนวันน้อยที่สุดที่รหัสผ่านจะต้องยังคงใช้งานอยู่	1
`pwage`	จำนวนวันสูงสุดที่รหัสผ่านอาจยังคงใช้งานอยู่	180
`min_length`	ความยาวต่ำสุดของรหัสผ่าน	8
`hist_size`	จำนวนรหัสผ่านที่บันทึกไว้ก่อนหน้าซึ่งไม่สามารถนำกลับมาใช้ใหม่ได้	10
`warn_pwage`	เมื่อรหัสผ่านใกล้จะหมดอายุจำนวนวันก่อนที่ผู้ใช้ จะได้รับการเตือนว่ารหัสผ่านกำลังจะหมดอายุ	7

ตารางที่ 33. แอ็ตทริบิวต์รหัสผ่านสำหรับนโยบายรหัสผ่านความปลอดภัย ระดับกลาง HMC (ต่อ)		
แอ็ตทริบิวต์	**คำอธิบาย**	**ค่าดีฟอล์ต**
`min_digits`	จำนวนตัวเลขขั้นต่ำที่จำเป็นต้องใช้ในการ รหัสผ่าน	ไม่มี
`min_uppercase`	จำนวนอักขระตัวพิมพ์ใหญ่ขั้นต่ำ	1
`min_lowercase`	จำนวนอักขระตัวพิมพ์เล็กขั้นต่ำ	6
`min_special_chars`	จำนวนอักขระพิเศษขั้นต่ำที่ต้องใช้ใน รหัสผ่าน	ไม่มี

พิจารณารายการต่อไปนี้เกี่ยวกับนโยบายรหัสผ่านความปลอดภัยระดับกลาง HMC:

- นโยบายไม่ใช้กับ ID ผู้ใช้ **hscroot**, **hscpe** และ **root**
- นโยบายนี้มีผลเฉพาะกับผู้ใช้ที่ผ่านการพิสูจน์ตัวตนแบบโลคัลซึ่งจัดการโดย HMC และนโยบายไม่สามารถบังคับใช้กับผู้ใช้ LDAP หรือ Kerberos
- นโยบายรหัสผ่านความปลอดภัยระดับกลาง HMC หรือ นโยบายที่ผู้ใช้กำหนดอนุญาตให้ผู้ดูแลระบบตั้งข้อจำกัดการนำรหัสผ่านกลับมาใช้ใหม่
- นโยบายรหัสผ่านความปลอดภัยระดับกลาง HMC เป็นแบบอ่านอย่างเดียว และแอ็ตทริบิวต์ของรหัสผ่านความปลอดภัยระดับกลาง HMC ไม่สามารถ ถูกเปลี่ยนแปลงได้ คุณสามารถสร้างรหัสผ่านที่ผู้ใช้กำหนดเองใหม่เพื่อตั้งค่าการจำกัดรหัสผ่าน

คุณสามารถใช้คำสั่งต่อไปนี้เพื่อตั้งค่านโยบายรหัสผ่านความปลอดภัยระดับกลาง HMC:

mkpwdpolicy
อิมพอร์ตนโยบายรหัสผ่านจากไฟล์ ซึ่งมีพารามิเตอร์ทั้งหมด หรือสร้าง นโยบายรหัสผ่าน

lspwdpolicy
แสดงโปรไฟล์นโยบายรหัสผ่านที่มีอยู่ทั้งหมดและค้นหาพารามิเตอร์เฉพาะ คุณสามารถ ดูนโยบายรหัสผ่านที่ใช้งานอยู่ในปัจจุบัน

rmpwdpolicy
ลบนโยบายรหัสผ่านที่ไม่ได้ใช้งานที่มีอยู่

หมายเหตุ: คุณไม่สามารถลบนโยบายความปลอดภัยระดับกลางที่ใช้งาน อยู่และนโยบายรหัสผ่านแบบอ่านอย่างเดียวที่เป็นค่าดีฟอลต์

chpwdpolicy
เปลี่ยนพารามิเตอร์ของนโยบายรหัสผ่านที่ไม่ใช้งาน

โปรไฟล์ความปลอดภัย: Global Data Protection Regulation (GDPR) และ Payment Card Industry Data Security Standard (PCI-DSS)

ศึกษาเกี่ยวกับ Hardware Management Console (HMC) ว่าจัดการข้อมูลความเป็นส่วนตัวของ ผู้ใช้อย่างไร

Hardware Management Console (HMC) เป็นเครื่องมือแบบปิดที่ไม่ได้จัดเก็บข้อมูลผู้ถือ บัตร ดังนั้นจึงเป็นเพียงส่วนย่อยของข้อกำหนดและขั้นตอนการประเมินความปลอดภัยของความปลอดภัย IT ซึ่ง ถูกกำหนดโดย PCI-DSS ใช้งานได้กับ HMC เฉพาะโค้ดที่ไว้วางใจเท่านั้นที่ถูกแจกจ่ายโดย IBM เท่านั้นที่สามารถถูกติดตั้งบน HMC เมื่อช่องโหว่ใดๆ ถูกรับรู้ ผ่าน IBM PSIRT process โปรแกรมฟิกซ์เฉพาะกิจ จะถูกเผยแพร่ ข้อกำหนดและคำแนะนำประกอบด้วยรายการต่อไปนี้:

เคียวรี GDPR

ตารางที่ 34. เคียวรี GDPR . ตารางแสดงข้อมูลเกี่ยวกับคำถามที่เกี่ยวข้องกับ GDPR	
คำถาม	**คำตอบ**
ข้อมูลประเภทใดที่ถูกเก็บไว้ใน HMC?	HMC เก็บ ข้อมูลคอนฟิกูเรชันฮาร์ดแวร์ Power เทคโนโลยีเสมือน PowerVM และข้อมูลเมทริกประสิทธิภาพ

ตารางที่ 34. เคียวรี GDPR . ตารางแสดงข้อมูลเกี่ยวกับคำถามที่เกี่ยวข้องกับ GDPR *(ต่อ)*	
คำถาม	**คำตอบ**
HMC ประมวลผลข้อมูลส่วนบุคคลหรือไม่?	คุณสามารถให้ข้อมูลติดต่อสำหรับฟังก์ชั่นการโทรกลับบ้าน การให้ข้อมูลติดต่อสำหรับ ฟังก์ชันการโทรกลับบ้านเป็นทางเลือก
บัญชีที่กำหนดไว้ล่วงหน้าใดที่จะใช้สำหรับการควบคุมดูแลของ HMC?	ผู้ใช้ผู้ดูแลระบบใช้ชื่อผู้ใช้ *hscroot*
แอคเคาต์ใน HMC เกี่ยวข้องกับบุคคลที่เจาะจงหรือไม่?	ไม่
จำเป็นหรือไม่ที่จะต้องให้ข้อมูลส่วนบุคคลใน HMC?	ไม่ คุณไม่จำเป็นต้องให้ข้อมูลส่วนบุคคล อย่างไรก็ตาม การให้ข้อมูลนี้ เป็นทางเลือก
ไฟล์บันทึก HMC มีข้อมูลส่วนบุคคลหรือไม่?	ไม่
เป็นไปได้หรือไม่ที่จะลบข้อมูลส่วนบุคคลอย่างสมบูรณ์และถาวร?	ใช่ ยกเลิกการตั้งค่าฟังก์ชันโทรกลับบ้าน

เคียวรี PCI-DSS

ตารางที่ 35. เคียวรี PCI-DSS . ตารางแสดงข้อมูลเกี่ยวกับคำถามที่เกี่ยวข้องกับ PCI-DSS	
คำถาม	**คำตอบ**
จะติดตั้งและบำรุงรักษาการกำหนดค่าไฟร์วอลล์เพื่อปกป้องข้อมูลของ ผู้ถือบัตรอย่างไร?	HMC ไม่ได้จัดเก็บหรือเข้าถึงข้อมูลผู้ถือบัตรใด ๆ อย่างไรก็ตาม HMC มีคอนฟิกูเรชันไฟร์วอลล์ และผู้ใช้สามารถควบคุมและเปิดใช้งานพอร์ตเฉพาะ
ฉันสามารถใช้ค่าเริ่มต้นที่ผู้จำหน่ายจัดให้ สำหรับรหัสผ่านระบบและพารามิเตอร์ความปลอดภัยอื่น ๆ ได้หรือไม่?	ก่อนที่คุณจะติดตั้งระบบบนเครือข่ายให้เปลี่ยนรหัสผ่านที่กำหนดไว้ล่วงหน้าทั้งหมดของผู้ใช้ *hscroot*
HMC ปกป้องข้อมูลที่เก็บไว้ของผู้ถือบัตรอย่างไร?	HMC ไม่ได้จัดเก็บหรือเข้าถึงข้อมูลผู้ถือบัตรใด ๆ
HMC เข้ารหัสข้อมูลของผู้ถือบัตรอย่างไรเมื่อข้อมูลถูกส่งผ่านเครือข่ายสาธารณะ แบบเปิด?	HMC ไม่ได้จัดเก็บหรือเข้าถึงข้อมูลผู้ถือบัตรใด ๆ
จะใช้และอัพเดตโปรแกรมซอฟต์แวร์ป้องกันไวรัสเป็นประจำอย่างไร?	HMC เป็นโปรแกรมแบบปิด ดังนั้นมัลแวร์ไม่สามารถติด HMC ได้
จะพัฒนาและรักษาระบบและแอพพลิเคชั่นที่ปลอดภัยได้อย่างไร?	คุณต้องติดตั้งแพตช์ที่จำเป็นกับระบบของคุณด้วยตนเองจากเว็บไซต์ IBM Fix Central เฉพาะโค้ดที่ไว้วางใจเท่านั้นที่ถูกแจกจ่ายโดย IBM เท่านั้นที่สามารถถูกติดตั้งบน HMC
HMC จำกัดการเข้าถึงข้อมูลผู้ถือบัตรหรือไม่?	HMC ไม่ได้จัดเก็บหรือเข้าถึงข้อมูลผู้ถือบัตรใด ๆ
จะกำหนด ID เฉพาะให้กับแต่ละคนที่สามารถเข้าถึงคอมพิวเตอร์ได้อย่างไร?	คุณสามารถใช้ข้อกำหนดนี้ได้โดยตรวจสอบให้แน่ใจว่าไม่มี ID ที่แชร์และทำตามนโยบาย รหัสผ่าน
จะจำกัดการเข้าถึงทางกายภาพกับข้อมูลผู้ถือบัตรได้อย่างไร?	HMC ไม่ได้จัดเก็บหรือเข้าถึงข้อมูลผู้ถือบัตรใดๆ
จะติดตามและตรวจสอบการเข้าถึงทรัพยากรเครือข่ายและข้อมูลผู้ถือบัตรได้อย่างไร?	HMC ไม่ได้จัดเก็บหรือเข้าถึงข้อมูลผู้ถือบัตรใด ๆ
HMC ทดสอบความปลอดภัยของระบบและโปรเซสอย่างไร?	เครื่องมือสแกนถูกใช้เพื่อเรียกใช้การสแกนเพื่อความปลอดภัยใน HMC เวอร์ชันที่รีลีสทั้งหมด เครื่องมือ สแกนประกอบด้วย: *Qualys*, *Nessus*, *testssl*, *sslscan* และ *ASoC*

ตารางที่ 35. เคียวรี PCI-DSS . ตารางแสดงข้อมูลเกี่ยวกับคำถามที่เกี่ยวข้องกับ PCI-DSS *(ต่อ)*	
คำถาม	**คำตอบ**
จะดูแลนโยบายความปลอดภัยที่มีการรักษาความปลอดภัยข้อมูลสำหรับพนักงานและ ผู้รับเหมาอย่างไร?	ผู้ดูแลระบบปิดใช้งานการเข้าสู่ระบบของผู้ใช้ระยะไกล เปิดใช้งานการเข้าสู่ระบบ ของผู้ใช้ตามความต้องการและปิดการใช้งานเข้าสู่ระบบของผู้ใช้เมื่อไม่จำเป็นต้องเข้าถึงอีกต่อไป

การแก้ไขปัญหาทั่วไปขณะรักษาความปลอดภัย HMC

ศึกษาวิธีการแก้ไขปัญหาที่คุณอาจพบเมื่อคุณรักษาความปลอดภัย HMC

จะรักษาความปลอดภัยการเชื่อมต่อระหว่าง Hardware Management Console (HMC) และระบบอย่างไร?

HMC เชื่อมต่อกับระบบผ่าน Flexible Service Processor (FSP) โปรโตคอล proprietary binary ชื่อโปรโตคอล Network Client (NETC) ถูกใช้สำหรับการจัดการทั้ง FSP และ Power ไฮเปอร์ไวเซอร์ ตารางต่อไปนี้แสดงพอร์ตที่ใช้โดย HMC:

ตารางที่ 36. พอร์ตบน FSP ที่ใช้เพื่อโต้ตอบกับ HMC			
พอร์ตบน FSP	**คำอธิบาย**	**เวอร์ชันโปรโตคอล (โหมดดีฟอลต์)**	**เวอร์ชันโปรโตคอล (โหมด NIST)**
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). ย้อนกลับไปเป็น SSLv3 เพื่อสนับสนุนเฟิร์มแวร์รุ่นเก่า	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). ย้อนกลับไปเป็น SSLv3 เพื่อสนับสนุนเฟิร์มแวร์รุ่นเก่า	NETC (TLS 1.2)

จะล็อก HMC ได้อย่างไร?

ถ้าคุณต้องการปรับปรุงการรักษาความปลอดภัยสำหรับโครงสร้างพื้นฐานของคุณ คุณสามารถใช้อุปกรณ์ Intrusion Prevention System (IPS) หรือเพิ่ม Hardware Management Consoles และเซิร์ฟเวอร์ IBM Power Systems ทั้งหมดให้อยู่หลังไฟร์วอลล์ นอกจากนี้คุณสามารถปิดการใช้งาน เซอร์วิสเครือข่ายบน HMC หากคุณไม่ได้ใช้งานจากระยะไกลหรือหากคุณต้องการล็อก HMC เมื่อต้องการ ปิดใช้งานบริการเครือข่ายบน HMC ให้ทำตามขั้นตอนต่อไปนี้:

1. ปิดใช้งาน การเรียกใช้คำสั่งระยะไกล โดยใช้พอร์ต SSH
2. ปิดใช้งาน เทอร์มินัลเสมือนระยะไกล (พอร์ต VTerm)
3. ปิดใช้งาน การเข้าถึงเว็บระยะไกล (อินเทอร์เฟสผู้ใช้แบบกราฟิก HMC และ REST API)
4. บล็อกพอร์ตในไฟร์วอลล์โดยใช้การตั้งค่าเครือข่าย HMC สำหรับแต่ละพอร์ต Ethernet ที่กำหนดค่าไว้

วิธีเซ็ต HMC ในโหมดทำงานร่วมกันได้ NIST SP 800-131A

ใน HMC เวอร์ชัน 8.1.0 หรือใหม่กว่าเมื่อคุณเซ็ต HMC ในโหมดทำงานร่วมกันได้ มีเพียงการเข้ารหัส ที่แข็งแกร่งที่แสดงรายการโดย NIST SP 800-131A ที่ได้รับการสนับสนุน คุณอาจไม่สามารถเชื่อมต่อกับเซิร์ฟเวอร์ ระบบพลังงานรุ่นเก่าเช่นเซิร์ฟเวอร์ POWER5 ที่ไม่ สนับสนุน Transport Layer Security (TLS 1.2) สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเปลี่ยนโหมด ความปลอดภัยดูที่ โหมด HMC V8R8 NIST

วิธีดูและเปลี่ยนรหัสที่ใช้โดย HMC

ใน HMC เวอร์ชัน 8.1.0 หรือใหม่กว่า HMC สนับสนุนชุดรหัสที่ปลอดภัยมากขึ้นตามที่กำหนดไว้ใน NIST 800-131A รหัสที่ถูกใช้ในโหมดดีฟอลต์คือ strong สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ รหัสการเข้ารหัสที่ถูกใช้โดย HMC ให้รันคำสั่ง

lshmcencr ถ้ามาตรฐานองค์กร ของคุณต้องการใช้ชุดรหัสที่ต่างไป ให้รันคำสั่ง **chhmcencr** เพื่อแก้ไขรัหสการเข้ารหัส

เมื่อต้องการแสดงรหัสการเข้ารหัสที่ถูกใช้โดย HMC เพื่อเข้ารหัสรหัสผ่านผู้ใช้ ให้รัน คำสั่งต่อไปนี้:

```
lshmcencr -c passwd -t c
```

เมื่อต้องการแสดงรหัสการเข้ารหัสที่สามารถใช้ได้ขณะนี้ โดยส่วนติดต่อผู้ใช้เว็บ HMC และ REST API ให้รันคำสั่งต่อไปนี้:

```
lshmcencr -c webui -t c
```

เมื่อต้องการแสดงรหัสการเข้ารหัสและอัลกอริทึม MAC ที่สามารถใช้ได้ขณะนี้ โดยส่วนติดต่อผู้ใช้ HMC SSH ให้รันคำสั่งต่อไปนี้:

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

วิธีตรวจสอบความแข็งแกร่งของใบรับรองบน HMC

ใบรับรองแบบลงนามเองบน HMC ใช้ SHA256 กับการเข้ารหัส 2048-bit RSA ซึ่งแข็งแกร่ง ถ้าคุณใช้ใบรับรองที่ลงนามโดย CA ตรวจสอบให้แน่ใจว่าคุณไม่ได้กำลังใช้การเข้ารหัส 1024-bit ซึ่งอ่อนแอ ใบรับรองต่อไปนี้สามารถถูกใช้สำหรับ HMC:

- ใบรับรองที่ลงนามโดย CA สามารถถูกใช้สำหรับส่วนติดต่อผู้ใช้แบบกราฟิก HMC และ REST API (พอร์ต 443 และ 12443)
- พอร์ต 9920 ใช้สำหรับการสื่อสาร HMC กับ HMC คุณไม่สามารถเปลี่ยนใบรับรองนี้ด้วย ใบรับรองของคุณเอง

วิธีเลือกระหว่างใบรับรองที่ลงนามด้วยตัวเอง (ดีฟอลต์) หรือใบรับรองที่ลงนามโดย CA

HMC สร้างใบรับรองโดยอัตโนมัติระหว่างการติดตั้ง แต่คุณสามารถสร้าง Certificate Signing Request (CSR) จาก HMC และรับใบรับรองใหม่ที่ถูกออกโดย Certificate Authority คุณสามารถอิมพอร์ตใบรับรองนี้เข้าสู่ HMC ตรวจสอบให้แน่ใจว่าคุณได้รับชื่อโดเมนสำหรับ HMC สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการใบรับรองใน HMC ดูที่ จัดการใบรับรอง

วิธีตรวจสอบ HMC

การตรวจสอบบน Hardware Management Consoles มุ่งเน้นที่รหัสที่ตั้งค่าไว้และกิจกรรม การใช้งานของผู้ใช้ HMC ต่างๆ ใช้คำสั่งต่อไปนี้เพื่อดูกิจกรรมการใช้งานของผู้ใช้ HMC ต่างๆ:

ตารางที่ 37. รหัสที่ถูกใช้โดย HMC

วัตถุประสงค์	**คำสั่ง**
การเข้ารหัสรหัสผ่าน (การตั้งค่าโกลบอล)	`lshmcencr -c passwd -t c`
การเข้ารหัสรหัสผ่านสำหรับแต่ละผู้ใช้	`lshmcusr -Fname:password_encryption`
SSH ciphers	`lshmcencr -c ssh -t c`
SSH MAC	`lshmcencr -c sshmac -t c`
Cipher ที่ใช้สำหรับส่วนติดต่อผู้ใช้แบบกราฟิก HMC และ REST API	`lshmcencr -c webui -t c`

ใช้คำสั่งต่อไปนี้เพื่อมอนิเตอร์ข้อมูลคอนโซลและเหตุการณ์ที่บริการได้สำหรับใช้ใน HMC:

ตารางที่ 38. คำสั่งเพื่อดูผู้ใช้ที่ล็อกออนหรือข้อมูลเหตุการณ์ที่บริการได้ใน HMC	
ข้อมูล	**คำสั่ง**
GUI users	`lslogon -r webui -u`
GUI tasks	`lslogon -r webui -t`
CLI users	`lslogon -r ssh -u`
CLI tasks	`lslogon -r ssh -t`
การดำเนินการบน HMC	`lssvcevents -t console -d <number of days>`
การดำเนินการบนระบบ	`lssvcevents -t hardware -m <managed system> -d <number of days>`

การมอนิเตอร์เหตุการณ์จากศูนย์กลางสำหรับ HMC: ถ้าคุณมี Hardware Management Consoles จำนวนมาก ให้เซ็ตไฟล์ `rsyslog` เพื่อรวบรวมข้อมูลการใช้งานทั้งหมด

วิธีที่ IBM แก้ไขช่องโหว่ด้านความปลอดภัยของ HMC

IBM มีโปรเซสตอบสนองเหตุการณ์เกี่ยวกับความปลอดภัยชื่อ IBM Product Security Incident Response Team (PSIRT) IBM Product Security Incident Response Team (PSIRT) เป็นทีมโกลบอล ที่จัดการใบรับ การตรวจสอบ และการร่วมมือภายในของ ข้อมูลช่องโหว่ด้านความปลอดภัยที่เกี่ยวข้องกับ IBM offerings คอมโพเนนต์ Open Source และ IBM ที่ถูกจัดส่งมาพร้อมกับ HMC จะถูกมอนิเตอร์และวิเคราะห์ โปรแกรมฟิกซ์เฉพาะกิจและการแก้ไขด้านความปลอดภัยถูกจัดเตรียมโดย IBM สำหรับ รีลีสที่สนับสนุนทั้งหมดของ HMC

วิธีติดตามโปรแกรมฟิกซ์เฉพาะกิจใหม่บน HMC

กระดานข่าวความปลอดภัยมีข้อมูลเกี่ยวกับช่องโหว่และโปรแกรมฟิกซ์เฉพาะกิจสำหรับ เวอร์ชัน HMC เมื่อต้องการติดตามโปรแกรมฟิกซ์เฉพาะกิจบน HMC คุณสามารถ:

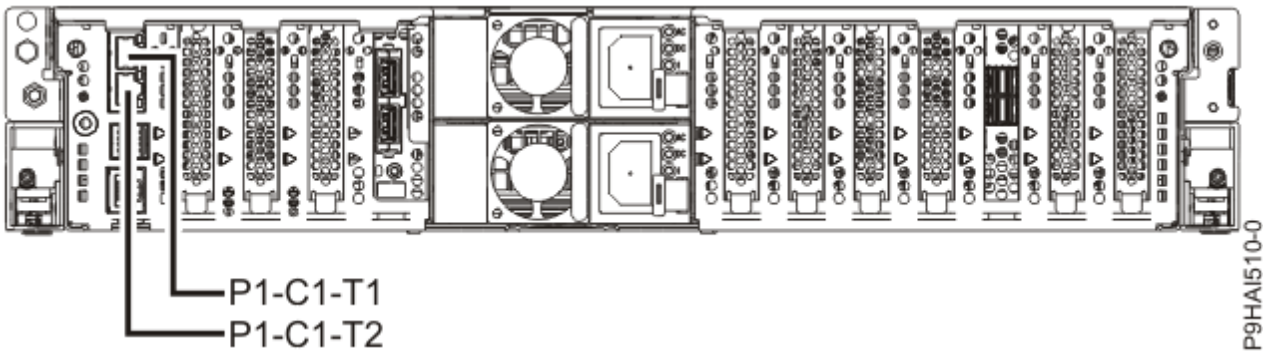
- ค้นหากระดานข่าวความปลอดภัยล่าสุดที่ IBM Security Bulletin
- ติดตาม @IBMPowereSupp บน Twitter สำหรับการแจ้งเตือน
- สมัครการแจ้งเตือนทางสนับสนุนที่ IBM Support

ตำแหน่งพอร์ตของ HMC

คุณสามารถค้นหาตำแหน่งพอร์ตได้โดยใช้โค้ดตำแหน่ง ใช้ภาพประกอบ ตำแหน่งพอร์ตของ HMC เพื่อแม็พโค้ดตำแหน่งกับ ตำแหน่งพอร์ตของ HMC บนเซิร์ฟเวอร์

ตำแหน่งพอร์ตของโมเดล 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H และ 9223-22S HMC

ใช้ไดอะแกรมและตารางนี้ เพื่อแม็พพอร์ต HMC บน 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H และ 9223-22S

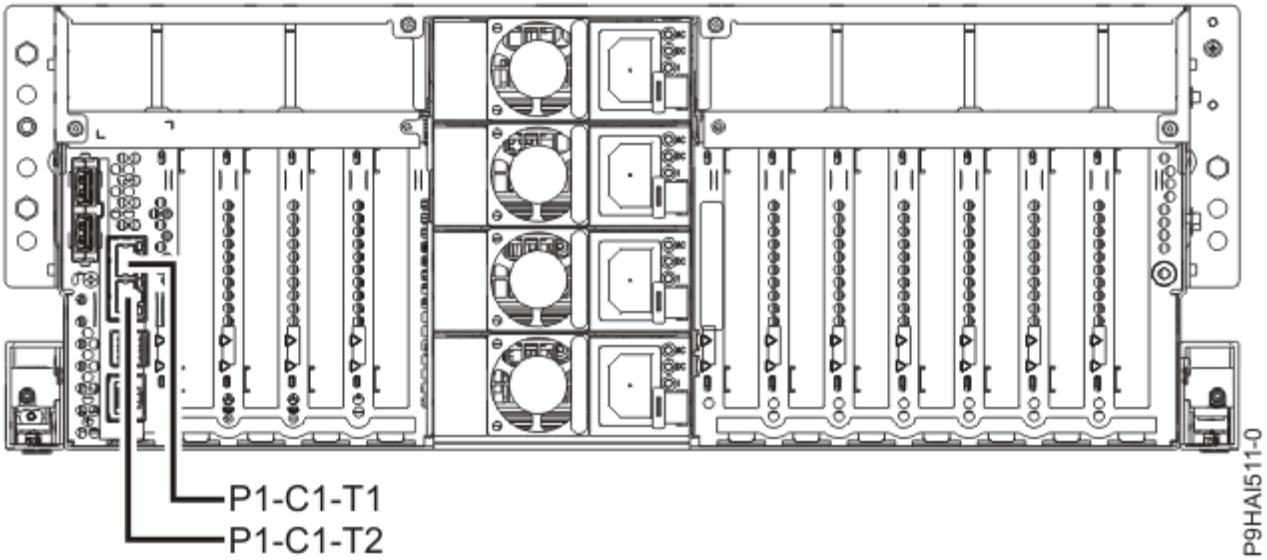


รูปที่ 10. 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H และ 9223-22S ตำแหน่งพอร์ตของ HMC

ตารางที่ 39. 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H และ 9223-22S ตำแหน่งพอร์ตของ HMC		
พอร์ต	**โค้ดตำแหน่งฟิสิคัล**	**ระบุไฟสัญญาณ LED**
พอร์ต HMC 1	Un-P1-C1-T1	ไม่มี
พอร์ต HMC 2	Un-P1-C1-T2	ไม่ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ตของ HMC บน 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H หรือ 9223-22S โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 9008-22L, 9009-22A, 9009-22G, 9223-22H หรือ 9223-22S		

ตำแหน่งพอร์ตของโมเดล 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H และ 9223-42S HMC

ใช้ไดอะแกรมและตารางนี้ เพื่อแม็พพอร์ต HMC บน 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H และ 9223-42S



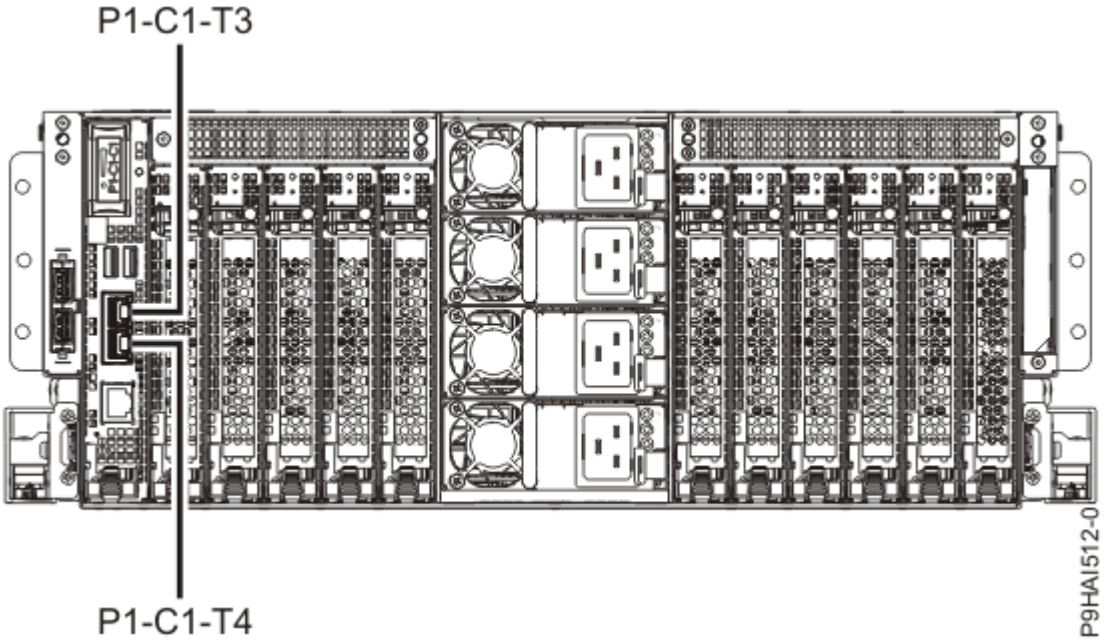
รูปที่ 11. 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H และ 9223-42S ตำแหน่งพอร์ตของ HMC

ตารางที่ 40. 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H และ 9223-42S ตำแหน่งพอร์ตของ HMC		
พอร์ต	**โค้ดตำแหน่งฟิสิคัล**	**ระบุไฟสัญญาณ LED**
พอร์ต HMC 1	Un-P1-C1-T1	ไม่มี

ตารางที่ 40. 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H และ 9223-42S ตำแหน่งพอร์ตของ HMC (ต่อ)		
พอร์ต	**โค้ดตำแหน่งฟิสิคัล**	**ระบุไฟสัญญาณ LED**
พอร์ต HMC 2	Un-P1-C1-T2	ไม่ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ตของ HMC บน 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H หรือ 9223-42S โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H หรือ 9223-42S		

ตำแหน่งพอร์ตของโมเดล 9040-MR9 HMC

ใช้ แผนภาพนี้และตารางเพื่อแม็พพอร์ต HMC บน 9040-MR9

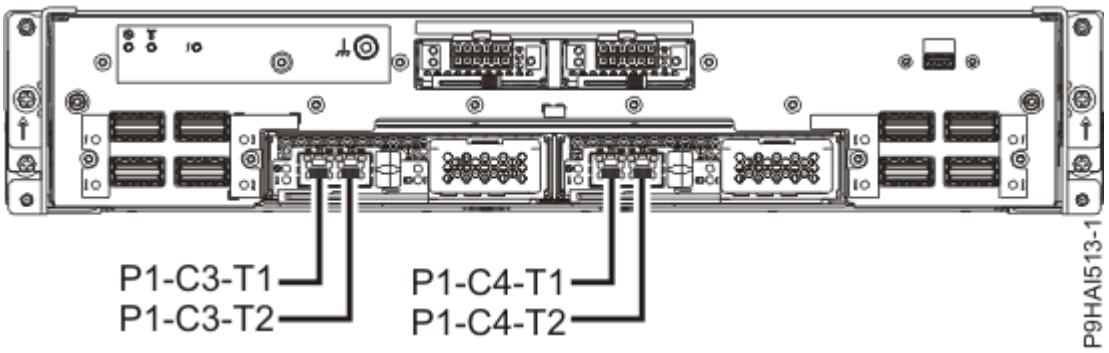


รูปที่ 12. ตำแหน่งพอร์ต HMC 9040-MR9

ตารางที่ 41. ตำแหน่งพอร์ต HMC 9040-MR9		
พอร์ต	**โค้ดตำแหน่งฟิสิคัล**	**ระบุไฟสัญญาณ LED**
พอร์ต HMC 1	Un-P1-C1-T3	ไม่มี
พอร์ต HMC 2	Un-P1-C1-T4	ไม่ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ตของ HMC บน 9040-MR9 โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่ง		

ตำแหน่งพอร์ตของโมเดล 9080-M9S HMC

ใช้ แผนภาพนี้และตารางเพื่อแม็พพอร์ต HMC บน 9080-M9S



รูปที่ 13. ตำแหน่งพอร์ต HMC 9080-M9S

ตารางที่ 42. ตำแหน่งพอร์ต HMC 9080-M9S		
พอร์ต	**ตำแหน่งพอร์ตฟิสิคัล**	**ระบุไฟสัญญาณ LED**
การ์ดตัวประมวลผลเซอร์วิส 1 - พอร์ต HMC 1	Un-P1-C3-T1	ไม่ใช่
การ์ดตัวประมวลผลเซอร์วิส 1 - พอร์ต HMC 2	Un-P1-C3-T2	ไม่ใช่
การ์ดตัวประมวลผลเซอร์วิส 2 - พอร์ต HMC 1	Un-P1-C4-T1	ไม่ใช่
การ์ดตัวประมวลผลเซอร์วิส 2 - พอร์ต HMC 2	Un-P1-C4-T2	ไม่ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ตของ HMC บน 9080-M9S โปรดดูที่ ตำแหน่งชิ้นส่วน และโค้ดตำแหน่ง		

หมายเหตุ

ข้อมูลนี้พัฒนาขึ้นสำหรับผลิตภัณฑ์ และบริการที่มีในประเทศสหรัฐอเมริกา

IBM อาจไม่นำเสนอผลิตภัณฑ์ การบริการ หรือคุณลักษณะที่กล่าวถึงใน เอกสารนี้ในประเทศอื่น โปรดปรึกษาตัวแทน IBM ในท้องถิ่น ของคุณสำหรับข้อมูลเกี่ยวกับผลิตภัณฑ์และการบริการที่มีอยู่ใน พื้นที่ของคุณขณะนี้ การอ้างอิงใด ๆ ถึงผลิตภัณฑ์ โปรแกรม หรือการบริการของ IBM ไม่ได้มีวัตถุประสงค์ที่จะระบุหรือตีความว่าสามารถใช้ได้เฉพาะผลิตภัณฑ์ โปรแกรม หรือการบริการของ IBM เพียงอย่างเดียวเท่านั้น ผลิตภัณฑ์ โปรแกรม หรือบริการที่ทำงานได้เท่าเทียมกัน ซึ่งไม่ละเมิดทรัพย์สินทางปัญญาของ IBM อาจสามารถใช้แทนกันได้ อย่างไรก็ตาม เป็นความรับผิดชอบของผู้ใช้ ในการประเมิน และตรวจสอบการทำงานของผลิตภัณฑ์ โปรแกรม หรือเซอร์วิส ที่ไม่ใช่ของ IBM

IBM อาจมีสิทธิบัตรหรือเอกสารซึ่งอยู่ระหว่างดำเนินการขอสิทธิบัตร ที่ครอบคลุมถึงหัวข้อที่ได้กล่าวไว้ในเอกสารนี้ การตกแต่งเอกสารนี้ไม่ได้ทำให้คุณได้รับใบอนุญาตสำหรับ สิทธิบัตรนี้ คุณสามารถสอบถามเกี่ยวกับไลเซนส์, โดยเขียนและส่งไปที่:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION นำเสนอสิ่งพิมพ์นี้ "ตามสภาพ" โดยไม่มี การรับประกันประเภทใด ๆ ไม่ว่าโดยชัดแจ้งหรือโดยนัย รวมถึงแต่ไม่จำกัดเฉพาะ การรับประกัน โดยนัยถึงการไม่ละเมิดสิทธิ การขายได้ หรือความเหมาะสมสำหรับวัตถุประสงค์เฉพาะ บางขอบเขตอำนาจไม่อนุญาตให้ปฏิเสธการรับประกันโดยชัดเจนหรือโดยนัยในบางกรณี ดังนั้นข้อความนี้อาจไม่บังคับใช้ในกรณีของคุณ

ข้อมูลนี้อาจเกิดความผิดพลาดทางเทคนิค หรือการพิมพ์ ซึ่งจะมีการแก้ไขข้อมูลเหล่านั้นเป็นระยะ ๆ ซึ่งข้อมูลที่ถูกแก้ไขนี้จะอยู่ในเอกสารฉบับ ถัดไป IBM อาจปรับปรุงและ/หรือเปลี่ยนแปลงในผลิตภัณฑ์ และ/หรือโปรแกรมที่อธิบายในสิ่งพิมพ์นี้ได้ตลอดเวลา โดยไม่ต้องแจ้ง ให้ทราบ

การอ้างอิงใด ๆ ในข้อมูลนี้โดยอ้างอิงเว็บไซต์ที่ไม่ใช่ของ IBM ระบุไว้เพื่อความสะดวกเท่านั้น และ ไม่ได้เป็นการสนับสนุน เว็บไซต์ดังกล่าวในลักษณะใด ๆ เอกสารประกอบที่อยู่ในเว็บไซต์เหล่านั้น ไม่ได้เป็นส่วนหนึ่งของเอกสารประกอบสำหรับผลิตภัณฑ์ IBM นี้ และการใช้งานเว็บไซต์เหล่านั้น ถือเป็นความเสี่ยงของคุณเอง

IBM อาจใช้หรือแจกจ่ายข้อมูลใด ๆ ที่คุณได้ให้ไว้ด้วยวิธีใด ๆ ที่เชื่อว่ามีความเหมาะสมโดยไม่มีข้อผูกมัดใด ๆ กับคุณ

ข้อมูลประสิทธิภาพ และตัวอย่างลูกค้าที่ระบุมีการนำเสนอสำหรับวัตถุประสงค์การสาธิตเท่านั้น ผลลัพธ์ของประสิทธิภาพการทำงานจริงอาจขึ้นอยู่กับคอนฟิกูเรชันและเกณฑ์การทำงานที่ ระบุเฉพาะ

ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ได้จัดทำโดย IBM เป็นข้อมูลที่ได้รับมาจาก ผู้จำหน่ายของผลิตภัณฑ์เหล่านั้น จากการประกาศที่มีการเผยแพร่ หรือจากแหล่งข้อมูลที่มีอยู่ในสาธารณะอื่น ๆ IBM ไม่ได้ทดสอบผลิตภัณฑ์ดังกล่าว และไม่สามารถยืนยัน ความถูกต้องของประสิทธิภาพ ความเข้ากันได้ หรือการเรียกร้องอื่นใดที่เกี่ยวข้องกับ ผลิตภัณฑ์ที่ไม่ใช่ของ IBM คำถาม เกี่ยวกับความสามารถในการทำงานของผลิตภัณฑ์ที่มิใช่ของ IBM ควรส่งไปที่ ซัพพลายเออร์ของผลิตภัณฑ์เหล่านั้น

ข้อความใด ๆ ที่เกี่ยวข้องกับทิศทางในอนาคตและเจตจำนงค์ของ IBM อาจมีการเปลี่ยนแปลง หรือเพิกถอนได้โดยไม่ต้องแจ้งล่วงหน้า และ นำเสนอเฉพาะเป้าหมาย และวัตถุประสงค์เท่านั้น

ราคาของ IBM ทั้งหมดที่แสดงเป็นราคาจำหน่ายปลีกที่แนะนำของ IBM เป็นราคาปัจจุบัน และอาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ ราคาของผู้แทนจำหน่ายอาจแตกต่างกันออกไป

โดยข้อมูลนี้มีวัตถุประสงค์เพื่อใช้ในการวางแผนเท่านั้น ข้อมูล เหล่านี้อาจมีการเปลี่ยนแปลงก่อนที่จะมีคำอธิบาย ของผลิตภัณฑ์ออกมา

ข้อมูลนี้จะประกอบด้วยตัวอย่างของข้อมูล และรายงาน ที่ใช้ในการดำเนินธุรกิจในแต่ละวัน เพื่อให้การยกตัวอย่างสมบูรณ์ ที่สุดเท่าที่จะทำได้ อาจมีการยกตัวอย่างชื่อบุคคล บริษัท ยี่ห้อ หรือผลิตภัณฑ์ ชื่อทั้งหมดเหล่านี้เป็นชื่อสมมุติ และหากชื่อ และที่อยู่ที่ใช้มีความคล้ายคลึง หรือใกล้เคียง กับองค์กรธุรกิจที่มีอยู่จริงถือเป็นเหตุบังเอิญ

ถ้าคุณดูเอกสารฉบับนี้โดยใช้สำเนาชั่วคราว รูปและสีของรูปประกอบอาจไม่แสดงให้เห็น

ห้ามทำซ้ำภาพวาดและข้อมูลจำเพาะที่อยู่ในเอกสารนี้ทั้งหมด หรือบางส่วนโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจาก IBM

IBM ได้จัดทำข้อมูลนี้เพื่อใช้กับเครื่องที่ระบุเฉพาะ IBM ไม่ได้แสดงว่าข้อมูลนี้เหมาะสมสำหรับวัตถุประสงค์อื่น

ระบบคอมพิวเตอร์ของ IBM มีกลไกที่ออกแบบมา เพื่อลดความเป็นไปได้ที่จะเกิดความเสียหาย หรือการสูญหายของข้อมูลที่ไม่สามารถตรวจพบ อย่างไรก็ตามความเสี่ยงเหล่านี้ยังไม่สามารถจำกัดให้หมดไปได้ ผู้ใช้ที่ประสบการณ์เกี่ยวกับสัญญาณขาดหายที่ไม่ได้วางแผนไว้ล่วงหน้า ระบบขัดข้อง ระบบกำลังไฟฟ้าที่ไม่แน่นอนหรือขาดหาย หรือส่วนประกอบขัดข้อง ควรจะทำการตรวจสอบความถูกต้องของการดำเนินการ และข้อมูลที่ถูกบันทึกหรือส่งโดยระบบ ในช่วงเวลาหรือเวลาใกล้เคียงกับที่ สัญญาณขาดหายหรือขัดข้อง นอกจากนั้น ในการดำเนินงานที่มีความอ่อนไหว หรือสำคัญมาก ผู้ใช้ควรมีขั้นตอน เพื่อให้มั่นใจว่ามีการตรวจสอบข้อมูลอย่างเป็นอิสระก่อนที่จะเชื่อถือ ข้อมูลเหล่านั้น ผู้ใช้ควรทำการตรวจสอบ เว็บไซต์การสนับสนุนของ IBM เป็นระยะ ๆ สำหรับข้อมูลล่าสุด และโปรแกรมฟิกซ์สำหรับ ระบบ และซอฟต์แวร์ที่เกี่ยวข้อง

ข้อความการให้สัตยาบัน

ผลิตภัณฑ์นี้ อาจไม่ได้รับการรับรองในประเทศของคุณสำหรับการเชื่อมต่อด้วย สื่อใด ๆ ก็ตามไปยังอินเตอร์เฟสของเครือข่ายโทรคมนาคมแบบพับลิก การรับรองเพิ่มเติมอาจเป็นข้อบังคับตามกฎหมายก่อนทำการเชื่อมต่อ ดังกล่าว โปรดติดต่อตัวแทนหรือผู้ค้าปลีกของ IBM ถ้ามีคำถามใด ๆ

คุณลักษณะความสามารถเข้าถึงได้สำหรับเซิร์ฟเวอร์ IBM Power Systems

คุณลักษณะความสามารถเข้าถึงได้ช่วยให้ผู้ใช้ที่ทุพพลภาพ เช่น มีเคลื่อนไหวได้จำกัด หรือมีการมองเห็นที่จำกัด สามารถใช้เนื้อหาทางด้าน เทคโนโลยีสารสนเทศได้เป็นผลสำเร็จ

ภาพรวม

เซิร์ฟเวอร์ IBM Power Systems มีคุณลักษณะความสามารถเข้าถึงได้ที่สำคัญต่อไปนี้:

- การดำเนินการคีย์บอร์ดอย่างเดียว
- การดำเนินการที่ใช้โปรแกรมอ่านหน้าจอ

เซิร์ฟเวอร์ IBM Power Systems ใช้มาตรฐาน W3C ล่าสุด, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) เพื่อให้แน่ใจว่าเป็นไปตาม US ส่วน 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) และ แนวทางความสามารถเข้าถึงได้ ในเนื้อหาเว็บ (WCAG) 2.0 (www.w3.org/TR/WCAG20/) เพื่อให้ได้รับ ประโยชน์จากคุณลักษณะความสามารถเข้าถึงได้ ให้ใช้รีลีสล่าสุดของโปรแกรมอ่านหน้าจอ และ เว็บเบราว์เซอร์ล่าสุดที่เซิร์ฟเวอร์ IBM Power Systems สนับสนุน

เอกสารคู่มือผลิตภัณฑ์ทางออนไลน์ของเซิร์ฟเวอร์ IBM Power Systems ใน IBM Knowledge Center เปิดใช้งานสำหรับความสามารถเข้าถึงได้ คุณลักษณะความสามารถเข้าถึงได้ของ IBM Knowledge Center มีการอธิบายไว้ในส่วน ความสามารถเข้าถึงได้ ของวิธีใช้ IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility)

การนำทางของคีย์บอร์ด

ผลิตภัณฑ์นี้ใช้คีย์การนำทางมาตรฐาน

ข้อมูลอินเตอร์เฟส

ส่วนติดต่อผู้ใช้ของเซิร์ฟเวอร์ IBM Power Systems ไม่มีเนื้อหาที่กะพริบ 2 - 55 ครั้งต่อ วินาที

ส่วนติดต่อผู้ใช้ของเว็บเซิร์ฟเวอร์ IBM Power Systems อาศัยสไตล์ชีตแบบต่อเรียงเพื่อจัดแสดง เนื้อหาอย่างสมบูรณ์และเพื่อให้สามารถใช้งานได้ง่าย แอ็พพลิเคชันจัดเตรียมวิธีที่เทียบเท่าสำหรับ ผู้ใช้ที่มีการมองเห็นจำกัดเพื่อใช้ค่าติดตั้งหน้าจอของระบบ รวมถึง โหมดความเปรียบต่างสูง คุณสามารถควบคุมขนาดฟอนต์ โดยใช้ค่าติดตั้งอุปกรณ์ หรือเว็บเบราว์เซอร์

ส่วนติดต่อผู้ใช้ของเว็บเซิร์ฟเวอร์ IBM Power Systems มีแลนด์มาร์กการนำทาง WAI-ARIA ที่ คุณสามารถใช้เพื่อนำทางไปยังพื้นที่นำทางในแอ็พพลิเคชันอย่างรวดเร็ว

ซอฟต์แวร์ของผู้จำหน่าย

เซิร์ฟเวอร์ IBM Power Systems มีซอฟต์แวร์ของผู้จำหน่ายบางรายการที่ไม่ได้ครอบคลุมภายใต้ ข้อตกลงไลเซนส์ของ IBM IBM ไม่มีส่วนรับรองเกี่ยวกับคุณลักษณะความสามารถเข้าถึงได้ของผลิตภัณฑ์เหล่านี้ โปรดติดต่อผู้จำหน่ายสำหรับข้อมูลความสามารถเข้าถึงได้เกี่ยวกับผลิตภัณฑ์เหล่านี้

ข้อมูลความสามารถเข้าถึงได้ที่เกี่ยวข้อง

นอกเหนือจาก IBM help desk และเว็บไซต์สนับสนุนมาตรฐานแล้ว IBM มีบริการโทรศัพท์ TTY สำหรับ ใช้โดยลูกค้าที่หูหนวก หรือมีปัญหาการได้ยินเพื่อติดต่อฝ่ายขายและฝ่ายสนับสนุน:

TTY เซอร์วิส
800-IBM-3383 (800-426-3383)
(ภายในอเมริกาเหนือ)

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความรับผิดชอบที่ IBM มีต่อความสามารถเข้าถึงได้ โปรดดูที่ IBM Accessibility (www.ibm.com/able)

ข้อควรพิจารณานโยบายความเป็นส่วนตัว

ผลิตภัณฑ์ซอฟต์แวร์ของ IBM ซึ่งรวมถึงซอฟต์แวร์เป็นเซอร์วิส โซลูชัน (“ข้อเสนอซอฟต์แวร์”) อาจใช้คุกกี้ หรือเทคโนโลยีอื่น เพื่อรวบรวมข้อมูลการใช้งานผลิตภัณฑ์ เพื่อช่วยปรับปรุงประสบการณ์ของ ผู้ใช้ขั้นปลาย และปรับแต่งการโต้ตอบให้เหมาะกับผู้ใช้ขั้นปลายแต่ละราย หรือสำหรับ วัตถุประสงค์อื่น ในหลายกรณี ไม่มีข้อมูลที่สามารถระบุตัวบุคคล ได้ที่รวบรวมโดยข้อเสนอซอฟต์แวร์ Software Offering ของเราบางตัว สามารถใช้คุณเก็บรวบรวข้อมูลที่ระบุเฉพาะบุคคลได้ ถ้าข้อเสนอซอฟต์แวร์นี้ใช้คุกกี้เพื่อรวบรวมข้อมูลที่สามารถระบุ เฉพาะบุคคลข้อมูลเฉพาะเกี่ยวกับการใช้คุกกี้ของข้อเสนอนี้มีการระบุไว้ ด้านล่าง

ขึ้นอยู่กับกำหนดคอนฟิกที่ปรับใช้ Software Offering นี้อาจใช้คุ๊กกี้เซสชันที่รวบรวม ชื่อผู้ใช้ของกำหนดคอนฟิกแต่ละรายและ IP แอดเดรสสำหรับการจัดการเซสชัน คุ๊กกี้เหล่านี้สามารถปิดใช้งาน แต่การปิดใช้งานคุ๊กกี้เหล่านี้ยังจะ ยกเลิกฟังก์ชันที่คุ๊กกี้เปิดใช้งานด้วย

หากกำหนดคอนฟิกที่ปรับใช้สำหรับ Software Offering มีให้คุณในฐานะลูกค้า ความสามารถในการรวบรวม ข้อมูลการระบุตัวบุคคลจากผู้ใช้ผ่านคุ๊กกี้และเทคโนโลยีอื่น คุณควรค้นหาคำแนะนำด้านกฎหมายเกี่ยวกับ กฎหมายใด ๆ ที่มีผลบังคับใช้กับการรวมรวมข้อมูลดังกล่าว รวมถึงข้อกำหนด สำหรับการแจ้งให้ทราบและยอมรับ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เทคโนโลยีต่าง ๆ รวมถึงคุ๊กกี้ เพื่อวัตถุประสงค์ เหล่านี้ โปรดดูที่ นโยบายความเป็นส่วนตัว ของ IBM ที่ http://www.ibm.com/privacy และ คำแถลงเกี่ยวกับความเป็นส่วนตัวแบบออนไลน์ ของ IBM ที่ http://www.ibm.com/privacy/details/us/en/ ใน ส่วนที่ชื่อ “Cookies, Web Beacons and Other Technologies”

เครื่องหมายการค้าและเครื่องหมายบริการ

IBM, ตราสัญลักษณ์ IBM และ ibm.com เป็นเครื่องหมายการค้าหรือเครื่องหมายการค้าจดทะเบียน ของ International Business Machines Corp., ซึ่งจดทะเบียนในหลายเขตอำนาจศาลทั่วโลก ชื่อผลิตภัณฑ์และบริการอื่น ๆ อาจเป็นเครื่องหมายการค้าของ IBM หรือ บริษัทอื่น ๆ รายการปัจจุบันของเครื่องหมายการค้าของ IBM มีอยู่ บนเว็บที่ ข้อมูลลิขสิทธิ์และเครื่องหมายการค้า

เครื่องหมายการค้าจดทะเบียน Linux ถูกใช้ ตามไลเซนส์ย่อยจาก Linux Foundation ซึ่ง เป็นผู้ได้รับอนุญาตแต่เพียงผู้เดียวจาก Linus Torvalds เจ้าของเครื่องหมายดังกล่าวทั่วโลก

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph และ Gluster เป็นเครื่องหมายการค้าหรือเครื่องหมายการค้าจดทะเบียนของ Red Hat, Inc. หรือ สาขาในสหรัฐอเมริกาและประเทศอื่น ๆ

Microsoft และ Windows คือเครื่องหมายการค้าของ Microsoft Corporation ในสหรัฐอเมริกา ประเทศอื่น ๆ หรือทั้งสองกรณี

Java และเครื่องหมายการค้าและตราสัญลักษณ์ที่อิงตาม Java ทั้งหมดหรือเครื่องหมายการค้าจดทะเบียนของ Oracle และ/หรือ บริษัทในเครือ

ประกาศเกี่ยวกับการปล่อยกำลังไฟฟ้า

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A ต่อไปนี้ใช้กับเซิร์ฟเวอร์ IBM ที่มีตัวประมวลผล POWER9 และคุณลักษณะ ยกเว้นกำหนดให้เป็น ความเข้ากันได้ทางแม่เหล็กไฟฟ้า (EMC) คลาส B ในข้อมูลคุณสมบัติ

เมื่อแนบมอนิเตอร์กับอุปกรณ์ คุณต้องใช้สายมอนิเตอร์ที่กำหนดให้ และอุปกรณ์ยับยั้งการแทรกแซงใด ๆ ที่ให้มากับมอนิเตอร์

คำประกาศของแคนาดา

CAN ICES-3 (A)/NMB-3(A)

คำประกาศของประชาคมยุโรปและโมร็อกโก

ผลิตภัณฑ์นี้เป็นไปตามข้อกำหนดการป้องกันของคำสั่ง 2014/30/EU ของรัฐสภายุโรปและของสภาว่าด้วยการประสานกันของกฎหมายของประเทศสมาชิกที่เกี่ยวข้อง กับความเข้ากันได้ทางแม่เหล็กไฟฟ้า IBM ไม่สามารถรับผิดชอบต่อความผิดพลาดเสียหายใดๆ เพื่อให้เป็นไปตามข้อกำหนดในการป้องกันอันเกิดจากการดัดแปลงผลิตภัณฑ์โดยไม่ได้รับการแนะนำ รวมถึง การใช้การ์ดต่างๆ ที่ไม่ใช่ตัวเลือกของ IBM

ผลิตภัณฑ์นี้อาจก่อให้เกิดสัญญาณรบกวนหากใช้ในบริเวณที่อยู่อาศัย ต้องหลีกเลี่ยงการใช้งานดังกล่าว เว้นแต่ผู้ใช้จะใช้มาตรการพิเศษเพื่อลดการปล่อยคลื่นแม่เหล็กไฟฟ้า เพื่อป้องกันการรบกวนการรับสัญญาณวิทยุและโทรทัศน์

คำเตือน: อุปกรณ์นี้เป็นไปตาม Class A ของ CISPR 32 ในสภาพแวดล้อมที่อยู่อาศัย อุปกรณ์นี้ อาจทำให้เกิดสัญญาณรบกวนทางวิทยุ

คำประกาศของเยอรมนี

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaatenund hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) “. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504

โทรศัพท์: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

ข้อมูล ทั่วไป:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

คำประกาศของมาคมอุตสาหกรรมเครื่องใช้ไฟฟ้าญี่ปุ่นและเทคโนโลยีสารสนเทศ (JEITA)

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

คำแถลงนี้ใช้กับผลิตภัณฑ์ที่มีกำลังไฟน้อยกว่าหรือเท่ากับ 20 A ต่อเฟส

高調波電流規格　JIS C 61000-3-2 適合品

คำแถลงนี้ใช้กับผลิตภัณฑ์ที่มีกำลังไฟมากกว่าหรือเท่ากับ 20 A ต่อเฟส

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類　：6（単相、ＰＦＣ回路付）
• 換算係数　：0

คำแถลงนี้ใช้กับผลิตภัณฑ์ที่มีกำลังไฟน้อยกว่าหรือเท่ากับ 20 A ต่อเฟส, สามเฟส

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類　：5（3相、ＰＦＣ回路付）
• 換算係数　：0

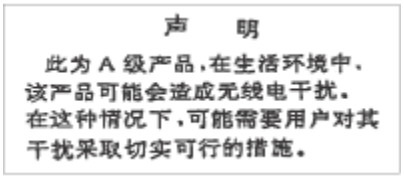
คำประกาศของคณะกรรมการควบคุมความสมัครใจสำหรับสัญญาณรบกวนแห่งประเทศญี่ปุ่น (VCCI)

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

คำประกาศของเกาหลี

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

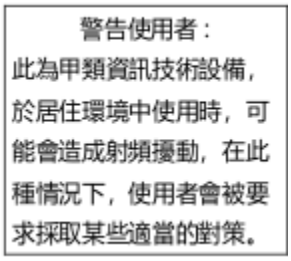
คำประกาศของสาธารณรัฐประชาชนจีน



คำประกาศของรัสเซีย

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

คำประกาศของไต้หวัน



IBM ข้อมูลการติดต่อของประเทศไต้หวัน:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

คำประกาศของคณะกรรมการกลางกำกับดูแลการสื่อสารของสหรัฐอเมริกา (FCC)

เครื่องมือนี้ได้รับการทดสอบ และพบว่าเป็นไปตามข้อจำกัดของอุปกรณ์ดิจิทัลคลาส A ตามหมวด 15 ของกฎ FCC ข้อจำกัดเหล่านี้ถูกออกแบบมา เพื่อให้มีการป้องกันในระดับที่สมเหตุสมผลต่อการรบกวนที่เป็นอันตรายเมื่อเครื่องมือถูกใช้งานในสภาพการใช้งานเชิงพาณิชย์ อุปกรณ์นี้สามารถจะสร้าง ใช้งาน และสามารถแผ่คลื่นความถี่วิทยุ และหากไม่ได้ติดตั้งและใช้งานตามคู่มือการใช้งาน อาจเป็นเหตุให้เกิดการรบกวนที่สร้างความเสียหายต่อการสื่อสารทางวิทยุ การทำงานของอุปกรณ์นี้ในบริเวณที่พักอาศัยอาจก่อให้เกิดการรบกวนที่เป็นอันตราย ในกรณีนี้ ผู้ใช้งานจำเป็นที่จะต้องแก้ไขสัญญาณรบกวนโดยที่ต้องรับผิดชอบค่าใช้จ่ายด้วยตนเอง

สายเคเบิลและตัวเชื่อมต่อที่ได้รับการหุ้มฉนวน และมีการเดินสายดินเอาไว้เรียบร้อยแล้ว จะต้องถูกนำมาใช้งาน เพื่อให้เป็นไปตามข้อจำกัดต่าง ๆ ในเรื่องการแผ่สัญญาณของ FCC สายเคเบิลและตัวเชื่อมต่อที่เหมาะสมสามารถหาซื้อได้จากตัวแทนจำหน่ายที่ได้รับอนุญาตของ IBM IBM ไม่รับผิดชอบ การเกิดสัญญาณรบกวนคลื่นวิทยุหรือโทรทัศน์ที่เกิดขึ้นเนื่องจากการใช้สายเคเบิลและตัวเชื่อมต่อที่นอกเหนือไปจากที่ แนะนำหรือโดยการเปลี่ยนแปลงหรือปรับแต่งอุปกรณ์นี้

โดยไม่ได้รับอนุญาต การเปลี่ยนแปลงหรือปรับแต่งโดยไม่ได้รับอนุญาต อาจทำให้สิทธิในการใช้งานอุปกรณ์นี้ของผู้ใช้เป็นโมฆะ

อุปกรณ์นี้สอดคล้องกับหมวดที่ 15 ของกฎ FCC การใช้งานต้องอยู่ภายใต้เงื่อนไขสองประการต่อไปนี้: (1) อุปกรณ์นี้ไม่ควรก่อให้เกิดการรบกวนที่เป็นอันตราย และ (2) อุปกรณ์นี้ต้องยอมรับการรบกวนในลักษณะใดก็ตามที่ได้รับมา ซึ่งรวมถึงการรบกวนที่อาจก่อให้เกิดการทำงานที่ไม่พึงประสงค์

ฝ่ายที่รับผิดชอบ:International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
ติดต่อสำหรับข้อมูลการปฏิบัติตามข้อกำหนดของ FCC เท่านั้น: fccinfo@us.ibm.com

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส B

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส B ต่อไปนี้นำไปใช้กับคุณลักษณะที่ถูกกำหนดให้เป็น ความเข้ากันได้ทางแม่เหล็กไฟฟ้า (EMC) คลาส B ในข้อมูลการติดตั้งคุณสมบัติ

เมื่อแนบมอนิเตอร์กับอุปกรณ์ คุณต้องใช้สายมอนิเตอร์ที่กำหนดให้ และอุปกรณ์ยับยั้งการแทรกแซงใด ๆ ที่ให้มากับมอนิเตอร์

คำประกาศของแคนาดา

CAN ICES-3 (B)/NMB-3(B)

คำประกาศของประชาคมยุโรปและโมร็อกโก

ผลิตภัณฑ์นี้เป็นไปตามข้อกำหนดการป้องกันของคำสั่ง 2014/30/EU ของรัฐสภายุโรปและของสภาว่าด้วยการประสานกันของกฎหมายของประเทศสมาชิกที่เกี่ยวข้อง กับความเข้ากันได้ทางแม่เหล็กไฟฟ้า IBM ไม่สามารถรับผิดชอบต่อความผิดพลาดเสียหายใดๆ เพื่อให้เป็นไปตามข้อกำหนดในการป้องกันอันเกิดจากการดัดแปลงผลิตภัณฑ์โดยไม่ได้รับการแนะนำ รวมถึง การใช้การ์ดต่างๆ ที่ไม่ใช่ตัวเลือกของ IBM

คำประกาศของเยอรมนี

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaatenund hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) “. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
โทรศัพท์: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B

คำประกาศของมาคมอุตสาหกรรมเครื่องใช้ไฟฟ้าญี่ปุ่นและเทคโนโลยีสารสนเทศ (JEITA)

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

คำแถลงนี้ใช้กับผลิตภัณฑ์ที่มีกำลังไฟน้อยกว่าหรือเท่ากับ 20 A ต่อเฟส

高調波電流規格　JIS C 61000-3-2 適合品

คำแถลงนี้ใช้กับผลิตภัณฑ์ที่มีกำลังไฟมากกว่าหรือเท่ากับ 20 A ต่อเฟส

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類　：6（単相、ＰＦＣ回路付）
• 換算係数　：0

คำแถลงนี้ใช้กับผลิตภัณฑ์ที่มีกำลังไฟน้อยกว่าหรือเท่ากับ 20 A ต่อเฟส, สามเฟส

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類　：5（3相、ＰＦＣ回路付）
• 換算係数　：0

คำประกาศของคณะกรรมการควบคุมความสมัครใจสำหรับสัญญาณรบกวนแห่งประเทศญี่ปุ่น (VCCI)

この装置は，クラスＢ情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　　ＶＣＣＩ－Ｂ

คำประกาศของไต้หวัน

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

คำประกาศของคณะกรรมการกลางกำกับดูแลการสื่อสารของสหรัฐอเมริกา (FCC)

อุปกรณ์นี้ได้รับการทดสอบ และพบว่าเป็นไปตามข้อจำกัดของอุปกรณ์ดิจิทัลคลาส B ตามหมวดที่ 15 ของ กฎ FCC ข้อจำกัดเหล่านี้ถูกออกแบบมาเพื่อให้มีการป้องกันในระดับที่สมเหตุสมผลต่อการรบกวนที่เป็นอันตราย เมื่ออุปกรณ์ถูกใช้งานในสภาพการใช้งานเชิงพาณิชย์ อุปกรณ์นี้สามารถที่จะก่อให้เกิด ใช้งาน และแผ่คลื่นความถี่วิทยุ และถ้าหากไม่ได้ติดตั้งและใช้งานตามคู่มือการใช้งาน อาจเป็นเหตุให้เกิดการรบกวนที่สร้างความเสียหายต่อการสื่อสารทางวิทยุ อย่างไรก็ตาม ไม่สามารถรับรองได้ว่าการรบกวนจะไม่เกิดขึ้นใน การติดตั้ง หากอุปกรณ์นี้ ทำให้เกิดการรบกวนที่สร้างความเสียหายต่อการรับสัญญาณวิทยุ หรือโทรทัศน์ ซึ่งสามารถตรวจสอบโดยการปิดและเปิดอุปกรณ์ ผู้ใช้ จะได้รับการแนะนำให้พยายามแก้ไขการรบกวนโดยใช้หนึ่งในมาตรการต่อไปนี้:

- การปรับเปลี่ยน หรือย้ายเสาอากาศ
- เพิ่มระยะห่างระหว่างอุปกรณ์กับตัวรับสัญญาณ
- เชื่อมอุปกรณ์ไปยังปลั๊กบนวงจรที่ต่างจากวงจรที่ตัวรับเชื่อมต่ออยู่
- ปรึกษาตัวแทนจำหน่ายที่ได้รับอนุญาตของ IBM หรือตัวแทนบริการเพื่อขอความช่วยเหลือ

สายเคเบิลและตัวเชื่อมต่อที่ได้รับการหุ้มฉนวน และมีการเดินสายดินเอาไว้เรียบร้อยแล้ว จะต้องถูกนำมาใช้งาน เพื่อให้เป็นไปตามข้อจำกัดต่าง ๆ ในเรื่องการแผ่สัญญาณของ FCC สายเคเบิลและตัวเชื่อมต่อที่เหมาะสมสามารถหาซื้อได้จากตัวแทนจำหน่ายที่ได้รับอนุญาตของ IBM IBM ไม่รับผิดชอบ การเกิดสัญญาณรบกวนคลื่นวิทยุหรือโทรทัศน์ที่เกิดขึ้นเนื่องจากการใช้สายเคเบิลและตัวเชื่อมต่อที่นอกเหนือไปจากที่ แนะนำหรือโดยการเปลี่ยนแปลงหรือปรับแต่งอุปกรณ์นี้โดยไม่ได้รับอนุญาต การเปลี่ยนแปลงหรือปรับแต่งโดยไม่ได้รับอนุญาต อาจทำให้สิทธิในการใช้งานอุปกรณ์นี้ของผู้ใช้เป็นโมฆะ

อุปกรณ์นี้สอดคล้องกับหมวดที่ 15 ของกฎ FCC โดยการทำงานอยู่ภายใต้เงื่อนไขสองประการ ต่อไปนี้:

(1) อุปกรณ์นี้ต้องไม่ก่อให้เกิดการรบกวนที่เป็นอันตราย และ (2) อุปกรณ์นี้ต้องยอมรับการรบกวนใด ๆ ที่ได้รับรวมถึงสัญญาณรบกวนที่อาจทำให้เกิดการทำงานที่ไม่ต้องการ

ฝ่ายที่รับผิดชอบ:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
ติดต่อสำหรับข้อมูลการปฏิบัติตามข้อกำหนดของ FCC เท่านั้น: fccinfo@us.ibm.com

ข้อตกลงและเงื่อนไข

ค่าอนุญาตในการใช้เอกสารเหล่านี้เป็นไปตามข้อกำหนด และเงื่อนไขต่อไปนี้

ความสามารถในการใช้งาน: ข้อกำหนดและเงื่อนไขเหล่านี้ เป็นข้อกำหนดและเงื่อนไขเพิ่มเติมในเรื่องของเงื่อนไขการใช้งานสำหรับเว็บไซต์ผู้ผลิต IBM IBM

การใช้งานส่วนบุคคล: คุณสามารถจัดทำสำเนาของเอกสารเหล่านี้เพื่อใช้เป็นการส่วนตัว มิใช่เพื่อการพาณิชย์ โดยมีเงื่อนไขว่าจะต้องคงข้อความประกาศความเป็นเจ้าของไว้โดยครบถ้วน คุณไม่สามารถแจกจ่าย แสดง หรือสร้างงาน ที่สืบเนื่องจากเอกสารเหล่านี้ หรือมาจากบางส่วนของเอกสารเหล่านี้ โดยไม่ได้รับความยินยอมอย่างชัดแจ้งจากผู้ผลิต IBM IBM

การใช้งานในเชิงพาณิชย์: คุณสามารถจัดทำสำเนา, แจกจ่าย, และแสดงเอกสารนี้ได้เฉพาะภายในองค์กรของคุณ โดยมีเงื่อนไขว่าจะต้องคงข้อความประกาศความเป็นเจ้าของไว้โดยครบถ้วน คุณไม่สามารถสร้างงานที่สืบเนื่องจากเอกสารเหล่านี้ หรือนำมาสร้างใหม่ แจกจ่าย หรือแสดงเอกสารเหล่านี้ หรือบางส่วนของเอกสารเหล่านี้ภายนอกองค์กรของคุณ โดยไม่ได้รับความยินยอมอย่างชัดแจ้งจากผู้ผลิต IBM IBM

สิทธิ์: นอกเหนือจากคำอนุญาตที่ได้แสดงไว้ในที่นี้ ไม่มีคำอนุญาต ไลเซนส์ หรือสิทธิ์อื่นใด ที่ได้ให้สิทธิ์ไว้ ทั้งโดยแจ้งหรือโดยนัย กับเอกสารหรือข้อมูลใด ๆ เนื้อหา ซอฟต์แวร์ หรือทรัพย์สินทางปัญญาที่มีอยู่ในที่นี้

ผู้ผลิต ขอสงวนสิทธิ์ในการเพิกถอนคำอนุญาตที่ให้ไว้ในที่นี้เมื่อใดก็ตามที่พิจารณาแล้วว่าการใช้เอกสารเหล่านี้ก่อนให้เกิดความเสียหาย ต่อผลประโยชน์ของบริษัท หรือเมื่อ IBM ได้พิจารณาแล้วว่าไม่มีการปฏิบัติตามข้อกำหนด ข้างต้นไว้อย่างเหมาะสม

คุณไม่สามารถดาวน์โหลด ส่งออก หรือทำการส่งออกข้อมูลนี้ซ้ำได้ ยกเว้นได้ปฏิบัติตามกฎหมายและข้อบังคับที่กำหนดไว้ รวมถึงกฎหมายและข้อบังคับในการส่งออกทั้งหมดของสหรัฐอเมริกา

ผู้ผลิตไม่ขอรับประกันเกี่ยวกับเนื้อหาของเอกสารเหล่านี้ เอกสารเหล่านี้จัดเตรียมไว้ "ตามสภาพที่เป็น" โดยไม่มีการรับประกันใด ๆ ไม่ว่าจะโดยเปิดเผยหรือโดยนัย รวมถึงแต่ไม่จำกัดเพียงการรับประกันโดยนัย ของการขายสินค้า การไม่ละเมิด และความเหมาะสม สำหรับวัตถุประสงค์เฉพาะทาง