

ระบบพลังงาน

การติดตั้งและตั้งค่า Hardware Management Console



ระบบพลังงาน

การติดตั้งและตั้งค่า Hardware
Management Console



หมายเหตุ

ก่อนการใช้ข้อมูลนี้และผลิตภัณฑ์ที่ข้อมูลนี้ สันับสนุน โปรดอ่านข้อมูลใน “ประกาศด้านความปลอดภัย” ในหน้า vii, “คำประกาศ” ในหน้า 103, คู่มือ *IBM Systems Safety Notices*, G229-9054 และ *IBM Environmental Notices and User Guide*, Z125-5823

เอ็ดจันนี้ประยุกต์ใช้กับ IBM Hardware Management Console เวอร์ชัน 7 รีลีส 7.7.0 ระดับการดูแลรักษา 0 และใช้กับรีลีส และโมดิฟิเคชัน ลำดับต่อมาทั้งหมด จนกว่าจะมีการระบุเป็นอย่างอื่นในเอ็ดจันใหม่

© ลิขสิทธิ์ของ IBM Corporation 2010, 2013.

© Copyright IBM Corporation 2010, 2013.

สารบัญ

ประกาศด้านความปลอดภัย	vii
---------------------------------	-----

การติดตั้งและตั้งค่า Hardware Management Console	1
---	----------

มีอะไรใหม่สำหรับการติดตั้งและการกำหนดคอนฟิก HMC	1
ภารกิจการติดตั้งและคอนฟิกูเรชัน	1
การติดตั้งและการกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่	2
การอัปเดตและอัปเดตรหัส HMC ของคุณ	2
การโอนย้ายระบบ HMC โค้ดเวอร์ชัน 6 ไปเป็นโค้ดเวอร์ชัน HMC	3
การเพิ่ม HMC ตัวที่สองในการติดตั้งที่มีอยู่	3
การเชื่อมต่อเน็ตเวิร์ก HMC	4
ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC	4
เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC	6
HMC เป็นเซิร์ฟเวอร์ DHCP	7
การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home	8
การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต	10
การเลือก อินเทอร์เน็ตโปรโตคอล	10
รายการแอตเตส Internet SSL	11
การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล	11
รายการแอตเตสเซิร์ฟเวอร์ VPN	12
การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต	12
การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์	13
การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC	13
การเชื่อมต่อเน็ตเวิร์ก HMC	13
ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC	14
เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC	15
HMC เป็นเซิร์ฟเวอร์ DHCP	16
การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home	18
การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต	20
การเลือก อินเทอร์เน็ตโปรโตคอล	20
รายการแอตเตส Internet SSL	20
การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล	21
รายการแอตเตสเซิร์ฟเวอร์ VPN	22
การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต	22
การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์	23
การจัดเตรียมสำหรับการตั้งค่าของ HMC	23
เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC	25
การตั้งค่า HMC	32
การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อโลน	32
การติดตั้ง 7310-CR4 HMC ลงในชั้นวาง	34
การทำให้รายการชิ้นส่วนให้เสร็จสิ้น	36
การกำหนดตำแหน่ง	36
การทำเครื่องหมายตำแหน่งโดยไม่ใช่แท็บเล็ตประกอบเข้ากับชั้นวาง	37

การติดตั้งรางแบบสไลด์ในชั้นวาง	38
การติดตั้ง HMC บนรางแบบสไลด์	41
การติดตั้งแขนยึดสายเคเบิล	44
การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง	44
การติดตั้ง 7042-CR5, 7042-CR6 และ 7042-CR7 เข้ากับชั้นวาง	45
การติดตั้งหน้าจอและคีย์บอร์ด	52
การทำให้รายการชิ้นส่วนให้เสร็จสิ้น	54
การทำเครื่องหมายตำแหน่งโดยไม่ใช่แท็บเล็ตประกอบเข้ากับชั้นวาง	54
การติดตั้งหน้าจอและคีย์บอร์ดเข้ากับชั้นวาง	54
การติดตั้งสวิตช์คอนโซล (ตัวเลือก)	59
การกำหนดคอนฟิก HMC	61
การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ผ่านทางวิซาร์ดเซตอัพที่แนะนำ	61
เริ่มต้น HMC และปฏิบัติตามขั้นตอนในวิซาร์ดเซตอัพที่แนะนำ	62
ตรวจทานคอนฟิกูเรชันของคุณ	62
การกำหนดคอนฟิก HMC โดยใช้เมนู HMC	62
การเริ่มต้น HMC	64
การเปลี่ยนวันที่และเวลา	64
การตั้งค่าชนิดเน็ตเวิร์ก HMC	65
การตั้งค่า HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ	65
การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ	65
การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับ โลจิสติกส์พาร์ติชัน	66
การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับ ผู้ใช้ระยะไกล	66
การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC	67
การระบุไอพีแอดเดรสที่จะถูกกำหนดเป็น eth0	67
การพิจารณาชื่ออินเทอร์เน็ตของไอพีแอดเดรสแต่ละแอดเดรส	68
การตั้งค่าความเร็วของสวิตช์	69
การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด	69
การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP	70
การตั้งค่า IPv4 address	70
การตั้งค่า IPv6 แอดเดรส	70
การใช้ IPv6 แอดเดรสเท่านั้น	71
การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC	71
การเปิดใช้การเข้าถึงเซลล์ที่จำกัดแบบรีโมต	72
การเปิดใช้งาน การเข้าถึงเว็บแบบรีโมต	72
การกำหนดคอนฟิก entry การเรตเป็นดีฟอลต์เกตเวย์	72
การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส	72
การตั้งค่าคอนฟิกโดเมนซัพพลิ	73
การคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP	73
การกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos	74
การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้	75
การคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับฝ่ายบริการและสนับสนุนได้โดยใช้วิซาร์ดการติดตั้ง Call-Home	75
การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน	75
การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้	78
การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่	79
การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม	79
ข้อมูลการบริการส่งข้อมูล	79
การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ	80

การอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณ	80
การอัปเดตรหัสผ่านทั่วไปสำหรับ Advanced System Management (ASM)	80
การรีเซ็ตรหัสผ่านผู้ดูแลระบบ Advanced System Management (ASM)	80
การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ	80
ขั้นตอน Postconfiguration	81
การสำรองข้อมูล HMC ที่สำคัญ	81
การสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ทั้งหมดไว้บนระบบรีโมต	82
การอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ	83
การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ	84
การขอรับและการใช้การอัปเดตรหัสเครื่องสำหรับ HMC เมื่อมีการเชื่อมต่ออินเทอร์เน็ต	84
ขั้นตอนที่ 1. ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต	84
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	84
ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	85
ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC	85
ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	85
การขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP	86
ขั้นตอนที่ 1. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	86
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	86
ขั้นตอนที่ 3. ขอรับอัปเดตรหัสเครื่อง HMC	86
ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC	87
ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	87
การอัปเดตซอฟต์แวร์ HMC ของคุณ	87
ขั้นตอนที่ 1. ขอรับอัปเดต	87
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	88
ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ	88
ขั้นตอนที่ 4. สำรองข้อมูล HMC	88
ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน	89
ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล	90
ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต	90
ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC	90
ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	91
การโอนย้ายรหัสเครื่องบน HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7	91
ตรวจสอบให้แน่ใจว่าสอดคล้องตามข้อกำหนดขั้นต่ำ	91
ขั้นตอนที่ 1. ขอรับอัปเดต	91
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	92
ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ	92
ขั้นตอนที่ 4. สำรองข้อมูลคอนโซลที่สำคัญ	92
ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน	93
ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล	94
ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต	94
ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7	94
ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	95
ขั้นตอนที่ 10. ขอรับแพ็คเกจอัปเดต	95
ขั้นตอนที่ 11. เปลี่ยนกำหนดการของการดำเนินการสำหรับ HMC	96
การอัปเดต HMC จากตำแหน่งรีโมตโดยใช้อิมเมจการอัปเดตบนเครือข่าย	96
ตำแหน่งพอร์ตของ HMC	97

คำประกาศ	103
เครื่องหมายการค้า	104
ประกาศเกี่ยวกับการปล่อยกำลังไฟฟ้า	105
คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A.	105
คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส B.	109
ข้อตกลงและเงื่อนไข.	113

ประกาศด้านความปลอดภัย

ประกาศด้านความปลอดภัยอาจพิมพ์อยู่ในคำแนะนำนี้โดยตลอด:

- ประกาศอันตราย เป็นการแจ้งถึงสถานการณ์ที่อาจเกิดอันตรายร้ายแรงถึงชีวิตหรืออันตรายร้ายแรงต่อผู้คน
- ประกาศข้อควรระวัง เป็นการแจ้งถึงสถานการณ์ที่อาจเกิดอันตรายกับคน เนื่องจากสภาวะที่เป็นอยู่บางอย่าง
- ประกาศข้อควรพิจารณา เป็นการแจ้งถึงความเป็นไปได้ของความเสียหายที่เกิดกับโปรแกรม อุปกรณ์ ระบบ หรือข้อมูล

ข้อมูลด้านความปลอดภัยเกี่ยวกับการค้าระดับโลก

หลายประเทศต้องการข้อมูลด้านความปลอดภัยที่มีอยู่ในเอกสารผลิตภัณฑ์ในภาษาประจำชาติของตนเอง หากประเทศของคุณมีความต้องการตามนี้ หนังสือข้อมูลด้านความปลอดภัยจะถูกบรรจุอยู่ในหีบห่อเอกสารที่จัดส่งพร้อมกับผลิตภัณฑ์ (เช่น ในหนังสือข้อมูลที่ตีพิมพ์ใน DVD หรือเป็นส่วนหนึ่งของผลิตภัณฑ์) หนังสือนี้จะประกอบด้วยข้อมูลด้านความปลอดภัยในภาษาประจำชาติของคุณพร้อมกับการอ้างอิงกับต้นฉบับภาษาอังกฤษ ก่อนใช้เอกสารภาษาอังกฤษในการติดตั้ง ปฏิบัติงาน หรือให้บริการผลิตภัณฑ์นี้ คุณต้องทำความเข้าใจกับข้อมูลด้านความปลอดภัยที่เกี่ยวข้องที่มีอยู่ในหนังสือ 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

เมื่อทำงานเกี่ยวกับระบบหรือแวลลุ่มไปด้วยระบบให้สังเกตข้อควรระวังต่อไปนี้:

กำลังไฟและกระแสไฟที่มาจากสายไฟ, สายโทรศัพท์, และสายสื่อสารเป็นอันตรายเพื่อหลีกเลี่ยงอันตรายที่เกิดจากไฟฟ้าช็อต:

- ให้เชื่อมต่อกำลังไฟเข้ากับยูนิิตด้วยสายไฟของ IBM เท่านั้น ห้ามใช้สายไฟของ IBM สำหรับผลิตภัณฑ์อื่นใด
- ห้ามเปิดหรือให้บริการตัวจ่ายไฟ
- ห้ามเชื่อมต่อ หรือปลดการเชื่อมต่อสายเคเบิลใดๆ หรือทำการติดตั้ง, บำรุงรักษา, หรือตั้งค่าคอนฟิกูเรชันผลิตภัณฑ์ใหม่ในระหว่างที่มีพายุฟ้าคะนอง
- ผลิตภัณฑ์นี้อาจประกอบด้วยสายไฟหลายเส้น ปลดการเชื่อมต่อสายไฟทั้งหมดเพื่อถอดกำลังไฟที่เป็นอันตรายออกไป
- เชื่อมต่อสายไฟทั้งหมดกับเต้ารับไฟฟ้าที่ต่อสายไฟและสายดินอย่างเหมาะสม ตรวจสอบให้แน่ใจว่าเต้ารับไฟฟ้าจ่ายไฟที่มีกำลังเหมาะสมและมีการหมุนเฟสตรงตามค่ากำหนดบนแผ่นโลหะของระบบ
- เชื่อมต่ออุปกรณ์ใดๆ ที่จะพ่วงต่อกับผลิตภัณฑ์นี้กับเต้ารับไฟฟ้าที่เดินสายไฟอย่างเหมาะสม
- หากเป็นไปได้ ควรใช้มือเพียงข้างเดียวในการเชื่อมต่อหรือปลดการเชื่อมต่อสายเคเบิลสัญญาณ
- ห้ามเปิดอุปกรณ์ใดๆ เมื่อพบว่า มีไฟ, น้ำ, หรือโครงสร้างได้รับความเสียหาย
- ปลดการเชื่อมต่อสายไฟ, ระบบโทรคมนาคม, เน็ตเวิร์ก, และโมเด็มที่พ่วงต่ออยู่ ก่อนที่คุณจะเปิดฝาครอบอุปกรณ์ ยกเว้นในกรณีที่ได้รับคำสั่งตามขั้นตอนการติดตั้งและคอนฟิกูเรชันเป็นอย่างอื่น
- เชื่อมต่อและปลดการเชื่อมต่อสายเคเบิลตามที่ได้อธิบายไว้ในขั้นตอนต่อไปนี เมื่อติดตั้ง, เคลื่อนย้าย, หรือเปิดฝาครอบผลิตภัณฑ์หรืออุปกรณ์ที่ต่อพ่วง

หากต้องการปลดการเชื่อมต่อ:

1. ปิดอุปกรณ์ทุกอย่าง (เว้นแต่มีคำแนะนำไว้เป็นอย่างอื่น)
2. ดึงสายไฟออกจากเต้ารับ
3. ดึงสายเคเบิลส่งสัญญาณออกจากตัวเชื่อมต่อ
4. ถอดสายเคเบิลทั้งหมดออกจากอุปกรณ์

หากต้องการเชื่อมต่อ:

1. ปิดอุปกรณ์ทุกอย่าง (เว้นแต่มีคำแนะนำไว้เป็นอย่างอื่น)
2. พ่วงต่อสายเคเบิลทั้งหมดเข้ากับอุปกรณ์
3. พ่วงต่อสายเคเบิลส่งสัญญาณเข้ากับตัวเชื่อมต่อ
4. พ่วงต่อสายไฟเข้ากับเต้ารับ
5. เปิดอุปกรณ์

(D005)

อันตราย

ขณะที่ทำงานอยู่กับชั้นวางระบบ IT หรือในบริเวณที่มีชั้นวางระบบ IT ของคุณ ให้สังเกตข้อควรระวังต่อไปนี้:

- อุปกรณ์ที่มีน้ำหนักมาก-อาจก่อให้เกิดการบาดเจ็บต่อร่างกายหรือความเสียหายต่ออุปกรณ์ได้ หากมีการจัดการที่ไม่ถูกต้อง
- ลดการวางระดับเสริมบนตู้ชั้นวางให้อยู่ต่ำเสมอ
- ควรติดตั้งแท่นยึดสเต็ปไลเซอร์บนตู้ชั้นวางเสมอ
- ติดตั้งอุปกรณ์ที่มีน้ำหนักมากที่สุดไว้ที่ด้านล่างสุดของตู้ชั้นวาง เพื่อหลีกเลี่ยงสภาวะการจัดวางเครื่องจักรที่ไม่สม่ำเสมอ ควรติดตั้งเซิร์ฟเวอร์และอุปกรณ์เสริมโดยเริ่มจากด้านล่างสุดของตู้ชั้นวางเสมอ
- ไม่ควรใช้อุปกรณ์ที่ประกอบเข้ากับชั้นวางเป็นชั้นวางหรือเป็นพื้นที่ใช้งาน ห้ามวางอ็อบเจกต์ต่างๆ ที่ด้านบนของอุปกรณ์ที่ประกอบเข้ากับชั้นวาง



- ตู้ชั้นวางแต่ละตู้อาจมีสายไฟมากกว่าหนึ่งสาย ตรวจสอบให้แน่ใจว่าได้ดึงสายไฟทั้งหมดในตู้ชั้นวางออกแล้ว เมื่อได้รับคำสั่งให้ปลดการเชื่อมต่อกำลังไฟในระหว่างให้บริการ
- เชื่อมต่ออุปกรณ์ทั้งหมดที่ติดตั้งในตู้ชั้นวางกับอุปกรณ์ไฟฟ้าที่ติดตั้งในตู้ชั้นวางเดียวกัน ห้ามเสียบปลั๊กสายไฟจากอุปกรณ์ที่ติดตั้งในตู้ชั้นวางตู้หนึ่งกับอุปกรณ์ไฟฟ้าที่ติดตั้งในตู้ชั้นวางอื่น
- เตารับไฟฟ้าที่ต่อสายไฟไม่ถูกต้อง สามารถทำให้เกิดอันตรายจากกำลังไฟต่อระบบ หรืออุปกรณ์ที่พ่วงต่อกับระบบที่เป็นโลหะ ลูกคามีหน้าที่รับผิดชอบในการตรวจสอบให้แน่ใจว่าเตารับไฟฟ้ามีการเดินสายไฟและสายดินอย่างถูกต้อง เพื่อป้องกันไฟฟ้าช็อต

ข้อควรระวัง

- ห้ามติดตั้งยูนิตในชั้นวางซึ่งมีอุณหภูมิภายในสูงกว่าอุณหภูมิที่ผู้ผลิตแนะนำไว้สำหรับอุปกรณ์ที่ประกอบเข้ากับชั้นวาง
- ห้ามติดตั้งยูนิตในชั้นวางซึ่งมีการไหลเวียนอากาศที่ไม่เหมาะสม ตรวจสอบให้แน่ใจว่า การไหลเวียนอากาศตามช่องสำหรับใช้ระบายอากาศที่ด้านข้าง, ด้านหน้า หรือด้านหลังของยูนิตไม่ได้ถูกกีดขวางหรือลดลง
- ในการเชื่อมต่ออุปกรณ์เข้ากับวงจรจ่ายไฟฟ้า ควรพิจารณาให้ถี่ว่าการใช้งานวงจรจนเกินพิกัดจะไม่ทำให้ความสามารถในการป้องกันสายจ่ายไฟหรือการป้องกันกระแสไฟเกินตัวยลดลง หากต้องการเตรียมการเชื่อมต่อสายไฟกับชั้นวางที่ถูกต้อง โปรดอ้างอิงถึงแถบป้ายการกำหนดค่าที่อยู่บนอุปกรณ์ในชั้นวางเพื่อกำหนดความต้องการกำลังไฟทั้งหมดของวงจรจ่ายไฟฟ้า
- (สำหรับลิ้นชักแบบเลื่อน) ห้ามดึงหรือติดตั้งลิ้นชัก หรือคุณลักษณะพิเศษ หากแท่นยึดสเต็ปไลเซอร์ของชั้นวางไม่ได้ยึดติดอยู่กับชั้นวาง ห้ามดึงลิ้นชักออกมากกว่าหนึ่งลิ้นชักในหนึ่งครั้ง ชั้นวางอาจไม่มั่นคง หากคุณดึงลิ้นชักออกมากกว่าหนึ่งลิ้นชักในหนึ่งครั้ง
- (สำหรับลิ้นชักแบบยึดตายตัว) ลิ้นชักนี้เป็นลิ้นชักแบบยึดตายตัว และห้ามไม่ให้เคลื่อนย้ายเพื่อรับบริการ ยกเว้นได้รับการระบุโดยผู้ผลิต ความพยายามในการเคลื่อนย้ายลิ้นชักบางส่วน หรือทั้งหมดออกจากชั้นวางอาจเป็นสาเหตุทำให้ชั้นวางไม่มั่นคง หรือเป็นสาเหตุทำให้ลิ้นชักตกลงมาจากชั้นวาง

(R001)

ข้อควรระวัง:

การถอดส่วนประกอบออกจากตำแหน่งด้านบนในตู้ชั้นวาง จะช่วยให้ชั้นวางมีความมั่นคงระหว่างที่มีการย้ายตำแหน่งใหม่ โปรดปฏิบัติตามคำแนะนำทั่วไปเหล่านี้ เมื่อคุณจัดตำแหน่งตู้ชั้นวางใหม่ภายในห้องหรืออาคาร:

- ลดน้ำหนักของตู้ชั้นวางโดยการถอดอุปกรณ์โดยเริ่มต้นจากด้านบนสุดของตู้ชั้นวาง หากเป็นไปได้ ให้จัดตู้ชั้นวางคืนสภาพตามคอนฟิกรูเรชันเดิมตั้งแต่ที่คุณได้รับมา ถ้าไม่ทราบคอนฟิกรูเรชันดังกล่าว คุณต้องปฏิบัติตามข้อควรระวังดังต่อไปนี้:
 - ถอดอุปกรณ์ทั้งหมดในตำแหน่ง 32U และด้านบนนอก
 - ตรวจสอบให้แน่ใจว่าได้ติดตั้งอุปกรณ์ที่หนักสุดไว้ที่ด้านล่างของตู้ชั้นวาง
 - ตรวจสอบให้แน่ใจว่า ไม่มีระดับ U ที่ว่างเปล่าระหว่างอุปกรณ์ที่ติดตั้งในตู้ชั้นวางต่ำกว่าระดับ 32U
- ถ้าตู้ชั้นวางที่คุณจัดตำแหน่งใหม่คือส่วนของห้องชุดของตู้ชั้นวาง ให้ดึงตู้ชั้นวางออกจากห้องชุด
- ตรวจสอบเรตที่คูกวางแผนที่จะกำจัดอันตรายที่อาจเกิดขึ้นได้
- ตรวจสอบว่าเรตที่คุณเลือกสามารถรองรับน้ำหนักของตู้ชั้นวางที่โหลดได้ อ้างอิงถึงเอกสารที่มาพร้อมกับตู้ชั้นวางของคุณเพื่อทราบข้อมูลเกี่ยวกับน้ำหนักของตู้ชั้นวางที่โหลด
- ตรวจสอบว่าประตูเปิดทั้งหมดมีขนาดอย่างน้อย 760 x 230 มม. (30 x 80 นิ้ว).
- ตรวจสอบให้แน่ใจว่าได้เก็บอุปกรณ์, ชั้น, ลิ้นชัก, ประตู, และสายเคเบิลทั้งหมดอยู่ในสภาพที่เรียบร้อย
- ตรวจสอบให้แน่ใจว่า การวางระดับเสริมทั้งสี่ระดับถูกยกไว้ที่ตำแหน่งสูงสุด
- ตรวจสอบให้แน่ใจว่า ไม่มีแท่นยึดสเตบิลไลเซอร์ที่ติดตั้งบนตู้ชั้นวางในขณะที่ทำการเคลื่อนย้าย
- ห้ามใช้ทางลาดที่เอียงเกิน 10 องศา
- เมื่อตู้ชั้นวางอยู่ในตำแหน่งใหม่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้โดยสมบูรณ์:
 - ลดการวางระดับเสริมทั้งสี่ระดับให้ต่ำลง
 - ติดตั้งแท่นยึดสเตบิลไลเซอร์บนตู้ชั้นวาง
 - ถ้าคุณถอดอุปกรณ์ใดๆ ออกจากตู้ชั้นวาง ให้ประกอบเข้าในตู้ชั้นวางใหม่จากตำแหน่งล่างสุด ไปยังตำแหน่งบนสุด
- หากจำเป็นต้องย้ายตำแหน่งเป็นระยะทางไกลๆ ให้จัดตู้ชั้นวางคืนสภาพตามคอนฟิกรูเรชันเดิมตั้งแต่ที่คุณได้รับมา บรรจุตู้ชั้นวางด้วยบรรจุภัณฑ์วัสดุเดิม หรือเทียบเท่า ลดการวางระดับเสริมให้ต่ำลง เพื่อยกฐานล้อให้ออกนอกพลาเลต และเลื่อนตู้ชั้นวางไปยังพลาเลต

(R002)

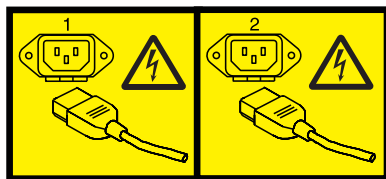
(L001)



(L002)



(L003)



or



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

ข้อควรระวัง:

ผลิตภัณฑ์นี้อาจมีอุปกรณ์ต่อไปนี้ตั้งแต่หนึ่งตัวขึ้นไป: ซีดีรอมไดรฟ์, ดีวีดีรอมไดรฟ์, ดีวีดีแรมไดรฟ์, หรือโมดูลเลเซอร์ ซึ่งเป็นผลิตภัณฑ์เลเซอร์ Class 1 หมายเหตุให้จดจำข้อมูลต่อไปนี้:

- ห้ามถอดฝาครอบออก การถอดฝาครอบของผลิตภัณฑ์เลเซอร์อาจเป็นผลทำให้เกิดการสัมผัสกับการแผ่รังสีเลเซอร์ที่เป็นอันตราย ไม่มีชิ้นส่วนที่สามารถถอดเปลี่ยนได้ภายในอุปกรณ์
- การใช้ตัวควบคุม หรือตัวปรับเปลี่ยน หรือใช้ประสิทธิภาพของขั้นตอนที่แตกต่างไปจากที่ระบุไว้ในนี้อาจเป็นสาเหตุทำให้เกิดการสัมผัสกับการแผ่รังสีที่เป็นอันตราย

(C026)

ข้อควรระวัง:

สภาพแวดล้อมการประมวลผลข้อมูลสามารถประกอบด้วยอุปกรณ์ซึ่งส่งผ่านระบบ ที่เชื่อมต่อกับโมดูลเลเซอร์ซึ่งปฏิบัติงานด้วยกำลังไฟมากกว่าระดับกำลังไฟของ Class 1 ด้วยเหตุนี้จึงห้ามมองที่ส่วนปลายของเส้นใยแก้วนำแสงหรือเคเบิลที่เปิดอยู่ (C027)

ข้อควรระวัง:

ผลิตภัณฑ์นี้ประกอบด้วยเลเซอร์ Class 1 M ห้ามมองที่อุปกรณ์ออปติคัลโดยตรง (C028)

ข้อควรระวัง:

ผลิตภัณฑ์เลเซอร์บางชนิดประกอบด้วยเลเซอร์ไดโอด Class 3A หรือ Class 3B ฝังอยู่ บันทึกข้อมูลดังต่อไปนี้: การแผ่รังสีเลเซอร์เมื่อเปิด ห้ามจ้องมองลำแสง, ห้ามใช้อุปกรณ์ออปติคัลในการมองโดยตรง, และหลีกเลี่ยงการสัมผัสกับลำแสงโดยตรง (C030)

ข้อควรระวัง:

แบตเตอรี่ประกอบด้วยลิเธียม หากต้องการหลีกเลี่ยงการระเบิดที่อาจเกิดขึ้นได้ ห้ามเผา หรือชาร์จแบตเตอรี่

ห้าม:

- __ ทิ้งหรือจุ่มลงในน้ำ
- __ ให้ความร้อนให้มากขึ้นกว่า 100°C (212°F)
- __ ซ่อมหรือถอดแยก

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

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** เชื่อมต่อแบบโลหะกับอินเตอร์เฟซที่เชื่อมต่อกับ OSP (outside plant) หรือสายไฟของอุปกรณ์เอง อินเตอร์เฟซเหล่านี้ได้รับการออกแบบมาเพื่อใช้เป็นอินเตอร์เฟซภายในอาคารเท่านั้น (พอร์ตชนิด 2 หรือชนิด 4 ตามที่อธิบายใน GR-1089-CORE) และต้องมีการแยกจากสายเคเบิล OSP แบบเปลี่ยน การเพิ่มตัวปกป้องหลักไม่ใช่การปกป้องที่เพียงพอสำหรับการเชื่อมต่อ อินเตอร์เฟซเหล่านี้ในแบบโลหะเข้ากับสาย OSP

หมายเหตุ: สายเคเบิลอีเทอร์เน็ตทั้งหมด ต้องมีฉนวนหุ้มและต่อสายดินที่ปลายทั้งสองด้าน

ระบบไฟฟ้ากระแสสลับไม่จำเป็นต้องใช้อุปกรณ์ป้องกันไฟกระชากหรือ surge protection device (SPD) ภายนอก

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

การติดตั้งและตั้งค่า Hardware Management Console

อธิบายถึงวิธีการติดตั้งฮาร์ดแวร์ HMC เชื่อมต่อ HMC เข้ากับระบบที่ถูกจัดการของคุณ และกำหนดคอนฟิก HMC สำหรับใช้งาน คุณสามารถดำเนินการกับงานเหล่านี้ได้ด้วยตนเอง หรือติดต่อผู้ให้บริการเพื่อดำเนินการกับงานเหล่านี้ให้คุณ คุณอาจถูกเรียกเก็บค่าธรรมเนียมจากผู้ให้บริการสำหรับการให้บริการนี้

มีอะไรใหม่สำหรับการติดตั้งและการกำหนดคอนฟิก HMC

อ่านข้อมูลที่มีการเปลี่ยนแปลงหรือข้อมูลใหม่เกี่ยวกับหัวข้อการติดตั้งและกำหนดคอนฟิก HMC เมื่อมีการอัปเดตการรวบรวมหัวข้อก่อนหน้านี้

ตุลาคม 2013

- ข้อมูลเพิ่มเติมเกี่ยวกับการติดตั้งหน้าจอและเคียบอร์ด หมายถึงเพิ่มเติมเกี่ยวกับความต้องการของระบบเพื่อรันฟังก์ชัน Power® Enterprise Pools

มีนาคม 2013

- เพิ่มข้อมูลเกี่ยวกับตำแหน่งพอร์ตของ HMC

พฤศจิกายน 2012

- เพิ่มข้อมูลเกี่ยวกับการกำหนดคอนฟิก HMC

พฤษภาคม 2012

- เพิ่มข้อมูลเกี่ยวกับการตั้งค่า HMC

พฤษภาคม 2011

- เพิ่มข้อมูลเกี่ยวกับเชื่อมต่อเครือข่าย HMC

กุมภาพันธ์ 2010

- เพิ่มข้อมูลเกี่ยวกับเซิร์ฟเวอร์ IBM Power Systems™ ที่มีตัวประมวลผล POWER7®

ภารกิจติดตั้งและคอนฟิกูเรชัน

เรียนรู้เกี่ยวกับภารกิจที่เชื่อมโยงกับภารกิจติดตั้งและ คอนฟิกูเรชัน HMC ต่างๆ

ส่วนนี้อธิบายงานที่คุณต้องดำเนินการ เมื่อคุณติดตั้ง และกำหนดคอนฟิก HMC ของคุณที่ระดับสูงสุด โดยมีวิธีการที่แตกต่างกันมากมาย สำหรับการติดตั้งและกำหนดคอนฟิก HMC ของคุณ ค้นหาสถานการณ์ที่เหมาะสมที่สุด กับภารกิจซึ่งคุณต้องการทำ

หมายเหตุ: ถ้าคุณกำลังจัดการกับเซิร์ฟเวอร์ POWER7 แบบอิงตัวประมวลผล HMC ต้องเป็นเวอร์ชัน 7.7.2 หรือสูงกว่า สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ” ในหน้า 84

การติดตั้งและการกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อติดตั้ง และกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

ตารางที่ 1. งานที่คุณต้องดำเนินการเมื่อติดตั้งและกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. รวบรวมข้อมูลและป้อนข้อมูล ในเวิร์กชีตคอนฟิกูเรชันการติดตั้งล่วงหน้า	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25 “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23
2. แกะกล่องบรรจุฮาร์ดแวร์	
3. ต่อสายเคเบิลฮาร์ดแวร์ HMC	“การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อะโลน” ในหน้า 32 “การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง” ในหน้า 44
4. เปิด HMC โดยกดปุ่มเปิด/ปิด	
5. ล็อกอินและเรียกทำงานเว็บแอปพลิเคชัน HMC	
6. เข้าใช้เวิร์กชีตตั้งค่าที่แนะนำ หรือใช้เมนู HMC เพื่อกำหนดคอนฟิก HMC	“การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ผ่านทางเวิร์กชีตตั้งค่าที่แนะนำ” ในหน้า 61 “การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 62
7. ต่อเซิร์ฟเวอร์เข้ากับ HMC	

การอัปเดตและอัปเดตรหัส HMC ของคุณ

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อคุณอัปเดตและอัปเดตโค้ด HMC ของคุณ

หากคุณมี HMC ที่มีอยู่ และต้องการอัปเดตหรืออัปเดต รหัส HMC ของคุณ คุณต้องทำงานระดับสูงต่อไปนี้ให้เสร็จสิ้น:

ตารางที่ 2. งานที่คุณต้องดำเนินการเมื่ออัปเดตหรืออัปเกรดรหัส HMC

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ขอรับอัปเกรด	“การอัปเดตซอฟต์แวร์ HMC ของคุณ” ในหน้า 87
2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	
3. สำรองข้อมูลโปรไฟล์ของระบบที่จัดการ	
4. สำรองข้อมูล HMC	
5. บันทึกข้อมูลคอนฟิกูเรชัน HMC ปัจจุบัน	
6. บันทึกสถานะคำสั่งรีโมต	
7. จัดเก็บข้อมูลอัปเกรด	
8. อัปเดตซอฟต์แวร์ HMC	
9. ตรวจสอบว่าการติดตั้งการอัปเกรดรหัสเครื่อง HMC เรียบร้อยแล้ว	

การโอนย้ายระบบ HMC โค้ดเวอร์ชัน 6 ไปเป็นโค้ดเวอร์ชัน HMC

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อคุณโอนย้ายจาก HMC เวอร์ชัน 6 เป็น HMC เวอร์ชัน 7

หากคุณมี HMC ที่มีอยู่ และต้องการโอนย้ายจากเวอร์ชัน 6 เป็นเวอร์ชัน 7 คุณต้องทำงานระดับสูงต่อไปนี้ให้เสร็จสิ้น:

ตารางที่ 3. งานที่คุณต้องดำเนินการเมื่อโอนย้ายระบบ HMC เวอร์ชัน 6 เป็น HMC เวอร์ชัน 7

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ตรวจสอบให้แน่ใจว่าฮาร์ดแวร์ HMC ของคุณสนับสนุนรหัส HMC เวอร์ชัน 7	
2. ตรวจสอบให้แน่ใจว่ารหัส HMC ของคุณอยู่ที่ระดับ 6.12 หรือสูงกว่า หากไม่ใช่ คุณต้องอัปเกรดรหัส HMC ที่มีอยู่	“การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ” ในหน้า 84 “การอัปเดตซอฟต์แวร์ HMC ของคุณ” ในหน้า 87
3. อัปเดต HMC ของคุณไปเป็นเวอร์ชัน 7	“การอัปเดตซอฟต์แวร์ HMC ของคุณ” ในหน้า 87
4. ทางเลือก: อัปเดตระดับเฟิร์มแวร์ของระบบที่จัดการของคุณ ไปเป็นระดับสูงสุดที่มีอยู่	2
5. หากคุณมี HMC ตัวที่สอง ดำเนินขั้นตอน 1-4 สำหรับ HMC นั้น	

การเพิ่ม HMC ตัวที่สองในการติดตั้งที่มีอยู่

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อเพิ่ม HMC ตัวที่สองลงในระบบที่จัดการของคุณ

หากคุณมี HMC ที่มีอยู่และระบบที่จัดการ และต้องการเพิ่ม HMC ตัวที่สองในคอนฟิกูเรชันนี้ให้ทำต่อไปนี้:

ตารางที่ 4. งาน ที่คุณต้องดำเนินการเมื่อเพิ่ม HMC ตัวที่สองลงในการติดตั้งที่มีอยู่

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ตรวจสอบให้แน่ใจว่าฮาร์ดแวร์ HMC ของคุณสนับสนุนรหัส HMC เวอร์ชัน 7	
2. รวบรวมข้อมูล และป้อนข้อมูลในเวิร์กชีต Configuration การติดตั้งล่วงหน้า	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25
3. แกะกล่องบรรจุฮาร์ดแวร์	
4. ต่อสายเคเบิลฮาร์ดแวร์ HMC	“การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อะโลน” ในหน้า 32 “การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง” ในหน้า 44
5. เปิด HMC โดยกดปุ่มเปิด/ปิด	
6. ล็อกอินเข้าสู่ HMC	
7. ระดับโค้ด HMC ต้องตรงกัน เปลี่ยนโค้ดบน เครื่องหนึ่งให้ตรงกับโค้ดบน HMC เครื่องอื่น	“การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ” ในหน้า 84 “การอัปเดตซอฟต์แวร์ HMC ของคุณ” ในหน้า 87
8. เข้าใช้ชาร์ตตั้งค่าที่แนะนำ หรือใช้เมนู HMC เพื่อกำหนดคอนฟิก HMC	“การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 62
9. คอนฟิก HMC นี้สำหรับเซิร์ฟเวอร์ที่ใช้ชาร์ตการติดตั้ง Call-Home	“การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้” ในหน้า 75
10. ต่อเซิร์ฟเวอร์เข้ากับ HMC	

การเชื่อมต่อเน็ตเวิร์ก HMC

คุณสามารถใช้การเชื่อมต่อเน็ตเวิร์กประเภทต่างๆ เพื่อเชื่อมต่อ HMC ของคุณกับระบบที่ถูกจัดการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีตั้งค่า HMC เพื่อเชื่อมต่อกับเน็ตเวิร์ก โปรดดูที่ “การกำหนดคอนฟิก HMC” ในหน้า 61 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ HMC บนเน็ตเวิร์ก โปรดดูดังต่อไปนี้:

ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC

ศึกษาเกี่ยวกับวิธีการใช้ฟังก์ชันการจัดการและการให้บริการแบบรีโมต HMC โดยใช้เน็ตเวิร์กของคุณ

HMC สนับสนุนการสื่อสารโลจิคัลในประเภทดังต่อไปนี้:

HMC to managed system

ใช้เพื่อดำเนินฟังก์ชันการจัดการฮาร์ดแวร์โดยส่วนใหญ่ ซึ่ง HMC ออกคำขอฟังก์ชันควบคุมผ่านทางเซิร์ฟเวอร์เซสเซอร์ของระบบที่ถูกจัดการ บางครั้ง การเชื่อมต่อระหว่าง HMC และเซิร์ฟเวอร์เซสเซอร์เรียกว่าเป็น *เน็ตเวิร์กบริการ* การเชื่อมต่อนี้ต้องใช้สำหรับการจัดการระบบที่ถูกจัดการ

HMC to logical partition

ใช้เพื่อรวบรวมข้อมูลเกี่ยวกับแพลตฟอร์ม (เหตุการณ์ข้อผิดพลาดฮาร์ดแวร์, คลังฮาร์ดแวร์) จากการรันระบบ

ปฏิบัติการในโลจิคัลพาร์ติชัน พร้อมทั้งเพื่อประสานกับ activity แพลตฟอร์มบางอย่าง (dynamic LPAR, การซ่อมพร้อมกัน) กับระบบปฏิบัติการนั้น หากคุณต้องการใช้บริการและคุณลักษณะการแจ้งข้อผิดพลาด คุณต้องสร้างการเชื่อมต่อ

HMC to remote users

ช่วยให้ผู้ใช้โมดสามารถเข้าถึงฟังก์ชัน HMC ผู้ใช้โมดสามารถ เข้าถึง HMC โดยวิธีดังต่อไปนี้:

- โดยการใช้เว็บเบราว์เซอร์เพื่อเข้าถึงฟังก์ชัน GUI ของ HMC ทั้งหมดแบบรีโมต
- โดยการใช้ Secure Socket Shell (SSH) เพื่อเข้าถึงฟังก์ชันบรรทัดคำสั่ง HMC จากระยะไกล

HMC to service and support

ใช้เพื่อส่งข้อมูล เช่น รายงานความผิดพลาดฮาร์ดแวร์ ข้อมูลคลัง และการอัปเดตไมโครโค้ด ไปยังและจากผู้ให้บริการของคุณ คุณสามารถใช้พาทาสื่อสารนี้เพื่อเรียกการให้บริการโดยอัตโนมัติ

HMC ของคุณสามารถสนับสนุนฟิสิคัลอินเทอร์เน็ตอินเทอร์เฟซได้มากถึงสี่อินเทอร์เน็ตเพลสขึ้นอยู่กับแต่ละรุ่น HMC เวอร์ชันสแตนด์อะโลนสนับสนุนอินเทอร์เน็ตเพลส HMC เพียงสามอินเทอร์เน็ตเพลสเท่านั้น ซึ่งใช้ฮาร์ดแวร์อินเทอร์เน็ตแบบในตัวหนึ่งตัวและมีปลั๊กอินอะแดปเตอร์ได้มากที่สุดสองตัว ใช้อินเทอร์เน็ตเพลส แต่ละตัวเหล่านี้ในวิธีดังต่อไปนี้:

- เน็ตเวิร์กอินเทอร์เน็ตเพลสตั้งแต่หนึ่งขึ้นไปสามารถใช้เฉพาะสำหรับการสื่อสารแบบ HMC-ไปที-ระบบที่ถูกจัดการเท่านั้น ซึ่งหมายความว่า เฉพาะ HMC และเซอวิวิโปรเซสเซอร์ของระบบที่ถูกจัดการเท่านั้นที่จะอยู่บนเน็ตเวิร์กนั้น แม้ว่าอินเทอร์เน็ตเพลส เครือข่ายที่อยู่ในตัวประมวลผลเซอวิวิมีการเข้ารหัสโปรโตคอล Secure Sockets Layer (SSL) และมีการป้องกันด้วยรหัสผ่าน การมีเครือข่าย เฉพาะงานที่แยกต่างหากสามารถช่วยให้อินเทอร์เน็ตเพลสเหล่านี้มีระดับความปลอดภัย สูงขึ้น
- โดยทั่วไปแล้ว อินเทอร์เน็ตเพลสเน็ตเวิร์กแบบเปิดใช้กับการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC และโลจิคัลพาร์ติชันบนระบบที่ถูกจัดการ สำหรับการสื่อสารแบบ HMC-ไปที-โลจิคัลพาร์ติชัน คุณยังสามารถใช้เน็ตเวิร์กอินเทอร์เน็ตเพลสแบบเปิดนี้เพื่อจัดการกับ HMC จากระยะไกล
- หรือคุณอาจใช้อินเทอร์เน็ตเพลสอื่นเพื่อเชื่อมต่อกับโลจิคัลพาร์ติชัน และจัดการ HMC จากระยะไกล อินเทอร์เน็ตเพลสนี้ยังสามารถใช้เป็นการเชื่อมต่อ HMC แยกต่างหากไปยังกลุ่มโลจิคัลพาร์ติชันอื่น ตัวอย่างเช่น คุณอาจต้องการให้มี LAN การจัดการที่แยกต่างหากจาก LAN ซึ่งธุรกรรมทางธุรกิจปกติทั้งหมดกำลัง รันอยู่ ผู้ดูแลรีโมตสามารถเข้าถึง HMC และหน่วยที่ถูกจัดการอื่นได้โดยใช้วิธีการนี้ ในบางครั้งโลจิคัลพาร์ติชันจะอยู่ใน โดเมนความปลอดภัยเน็ตเวิร์กอื่น อาจจะเป็นด้านหลังไฟร์วอลล์ และคุณอาจต้องการมี การเชื่อมต่อเน็ตเวิร์ก HMC ที่แตกต่างกันสำหรับสองโดเมนเหล่านั้น

ข้อกำหนดเว็บเบราว์เซอร์สำหรับ HMC

คอนโซล การจัดการฮาร์ดแวร์ (HMC) ได้รับการสนับสนุนจาก Microsoft Internet Explorer (IE) เวอร์ชัน 6.0 และ 7.0, Firefox เวอร์ชัน 1.5.0.7 และ 2.0

ถ้า เบราวเซอร์ของคุณมีการกำหนดคอนฟิกเพื่อใช้อินเทอร์เน็ตพรีอ็อกซี โคลด์ IP แอดเดรส ควรมีการรวมไว้ในรายการข้อยกเว้น โปรตปรักษาผู้ดูแลระบบเครือข่าย ของคุณสำหรับข้อมูลเพิ่มเติมเกี่ยวกับรายการข้อยกเว้น ถ้าคุณยังคง จำเป็นต้องใช้พรีอ็อกซีเพื่อเรียกใช้ HMC ให้เปิดใช้งาน การใช้ HTTP 1.1 ผ่านทาง การเชื่อมต่อพรีอ็อกซี ภายใต้แท็บขั้นสูง ในหน้าต่าง อ็อพชันอินเทอร์เน็ต

หมายเหตุ: สำหรับ Firefox เวอร์ชัน 2.0 ตรวจสอบให้แน่ใจว่าคุณเปิดใช้งาน อ็อพชัน JavaScript เพื่อเพิ่มหรือลดหน้าต่าง และย้ายหรือเปลี่ยนขนาด หน้าต่างที่มีอยู่ คุณลักษณะนี้ช่วยให้คุณสลับระหว่างภารกิจ HMC ได้ง่าย ปฏิบัติตามขั้นตอนต่อไปนี้จะเปิดใช้งานอ็อพชัน Javascript:

1. เลือก เครื่องมือ และคลิก อ็อพชัน

2. เลือก เนื้อหา และคลิก ขั้นสูง
3. เลือก ย้ายหรือเปลี่ยนขนาดหน้าต่างที่มีอยู่ หรือ เพิ่มหรือลดหน้าต่าง
4. คลิก ตกลง

ต้องเปิดใช้งานเซสชันคุกกี้เพื่อให้ ASMI สามารถทำงานได้เมื่อเชื่อมต่อกับ HMC แบบรีโมต รหัสพร็อกซี asm บันทึกและใช้ข้อมูลเซสชัน ปฏิบัติตามขั้นตอนต่อไปเพื่อเปิดใช้งาน เซสชันคุกกี้

การเปิดใช้งานเซสชันคุกกี้ใน Internet Explorer

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

การเปิดใช้งานเซสชันคุกกี้ใน Firefox

1. เลือก เครื่องมือ และคลิก อีพซัน
2. คลิก คุกกี้
3. เลือก อนุญาตให้ไซต์ตั้งค่าคุกกี้
4. เลือก ข้อยกเว้น และเพิ่ม HMC
5. คลิก ตกลง

เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC:

HMC สามารถกำหนดคอนฟิกเพื่อใช้เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดได้ เน็ตเวิร์กส่วนตัวอนุญาตให้ใช้ช่วงที่เลือกของ IP-address ที่เราต์ไม่ได้ เน็ตเวิร์กแบบ *พับลิค* หรือแบบ "เปิด" หมายถึงการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC กับโลจิสติกส์พาร์ติชันและ ระบบอื่นๆ บนเน็ตเวิร์กปกติของคุณ

เน็ตเวิร์กส่วนตัว

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

บนระบบส่วนใหญ่ FSP จะจัดหาอีเทอร์เน็ตพอร์ต 2 พอร์ต ซึ่งใช้เลเบล **HMC1** และ **HMC2** ซึ่งอนุญาตให้คุณเชื่อมต่อ HMC ไม่เกิน 2 เครื่อง

บางระบบมี อีพซัน dual-FSP ในสถานการณ์นี้ FSP ตัวที่สองทำหน้าที่เป็นอุปกรณ์ "สำรอง" โดยหลักๆ แล้ว ข้อกำหนดการติดตั้งระดับต้น สำหรับระบบที่มี FSP สองตัว เหมือนกับระบบที่ไม่มี FSP ตัวที่สอง โดย HMC ต้องเชื่อมต่อกับ FSP แต่ละตัว ดังนั้น ต้องมีเน็ตเวิร์กฮาร์ดแวร์เพิ่มเติม (เช่น สวิตช์หรือฮับ LAN) เมื่อมี FSP มากกว่าหนึ่งตัว หรือมีระบบที่ถูกจัดการหลายระบบ

หมายเหตุ: พอร์ต FSP แต่ละพอร์ตบนระบบที่ถูกจัดการจะต้องเชื่อมต่อกับ HMC เพียงเครื่องเดียวเท่านั้น

พับลิคเน็ตเวิร์ก

เน็ตเวิร์กแบบเปิดสามารถเชื่อมต่อกับไฟร์วอลล์หรือเราเตอร์สำหรับการเชื่อมต่ออินเทอร์เน็ต การเชื่อมต่อกับอินเทอร์เน็ตช่วยให้ HMC สามารถ "call home" ได้เมื่อมีข้อผิดพลาดฮาร์ดแวร์อื่นใดที่ต้องการรายงาน

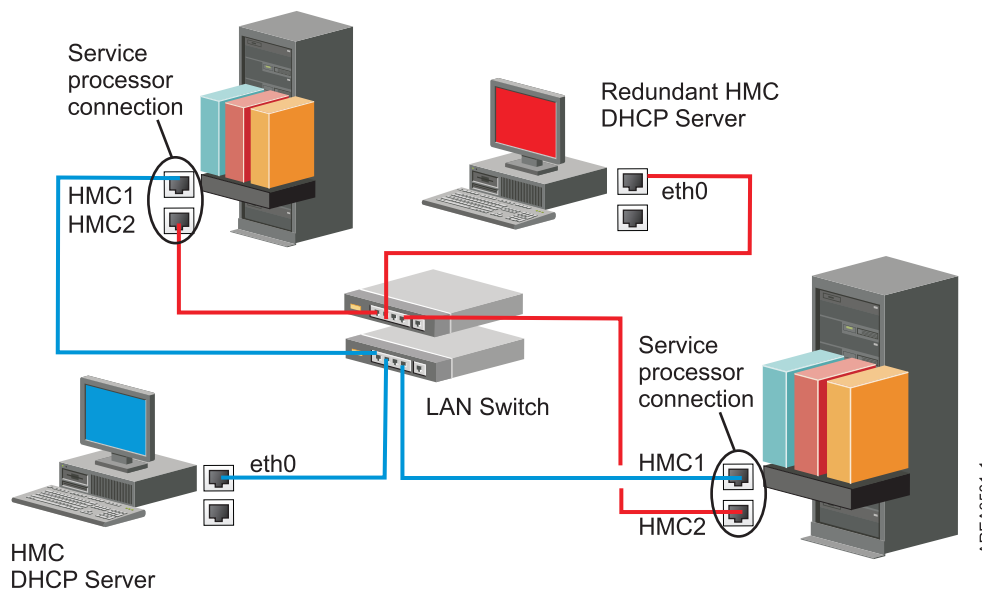
HMC ประกอบด้วยไฟร์วอลล์บนแต่ละ เน็ตเวิร์กอินเตอร์เฟซ ไฟร์วอลล์ระดับต้นจะถูกตั้งค่าโดยอัตโนมัติเมื่อคุณรันวิชวล HMC Guided Setup แต่คุณควรปรับการตั้งค่าไฟร์วอลล์หลังจากการติดตั้งและการคอนฟิก HMC เบื้องต้น

HMC เป็นเซิร์ฟเวอร์ DHCP:

คุณสามารถใช้ HMC เป็นเซิร์ฟเวอร์ Dynamic Host Configuration Protocol (DHCP)

หมายเหตุ: ถ้าคุณกำลังใช้ IPv6 กระบวนการค้นหาต้องทำด้วยตนเอง สำหรับ IPv6 ไม่มีการค้นหาแบบอัตโนมัติ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ “การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 70

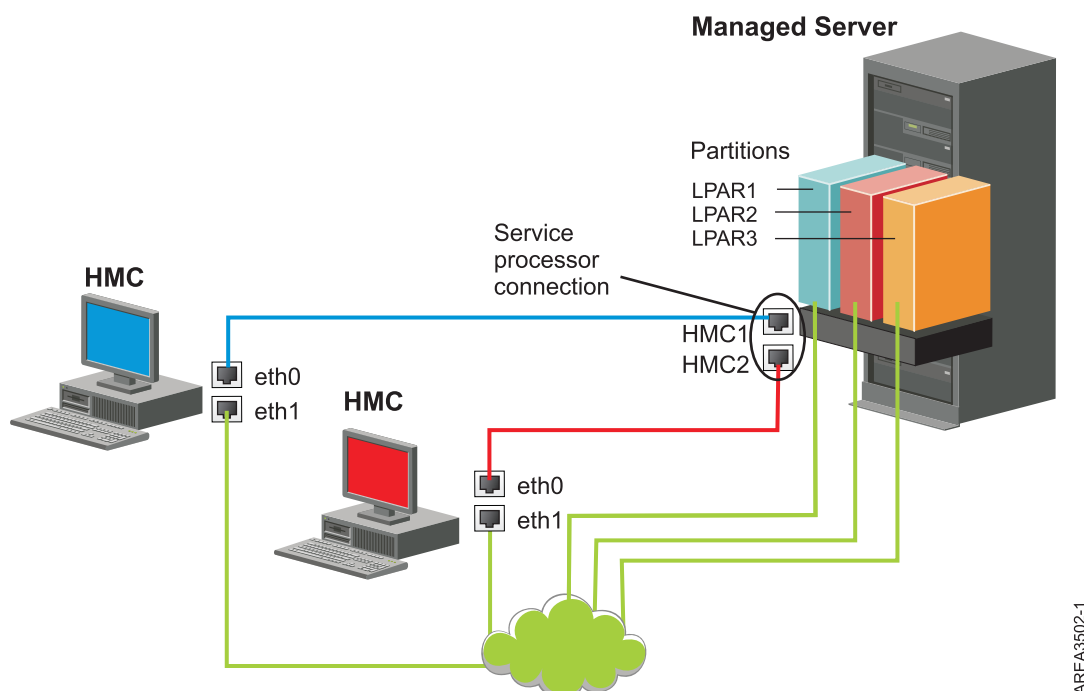


รูปภาพนี้แสดงสภาวะแวดล้อม HMC สำรอง พร้อมด้วย ระบบที่ถูกจัดการ 2 ระบบ HMC เครื่องแรกเชื่อมต่อกับพอร์ตแรกบนแต่ละ FSP และ HMC สำรองเชื่อมต่อกับพอร์ตที่สองบน HMC แต่ละเครื่อง HMC แต่ละเครื่องถูกตั้งค่าเป็นเซิร์ฟเวอร์ DHCP โดยใช้ช่วง IP แอดเดรสที่แตกต่างกัน การเชื่อมต่ออยู่บนเน็ตเวิร์กส่วนตัวที่แยกต่างหาก ด้วยเหตุนี้ จึงจำเป็นต้องตรวจสอบให้แน่ใจว่าพอร์ต 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 เช็กเมนต์ ส่วนตัวนี้สามารถมีอยู่ในรูปแบบหลายพอร์ตใน *virtual LAN (VLAN)* แบบไพรเวต บนสวิตช์ขนาดใหญ่ที่จัดการ ถ้าคุณมี VLAN แบบไพรเวตหลายๆ เน็ตเวิร์ก คุณจะต้องตรวจสอบให้แน่ใจว่า VLAN ดังกล่าวแยกออกจากกัน และไม่มีทราฟฟิกที่ตัดกัน

ถ้าคุณมี HMC มากกว่าหนึ่งเครื่อง คุณจะต้องเชื่อมต่อ HMC แต่ละเครื่องเข้ากับโลจิคัลพาร์ติชัน และเชื่อมต่อ HMC เข้าด้วยกัน บนเน็ตเวิร์กแบบเปิดเดียวกัน



รูปนี้แสดง HMC สองเครื่องที่เชื่อมต่อกับเซิร์ฟเวอร์ที่จัดการเดี่ยวบนเน็ตเวิร์กส่วนตัว และกับโลจิคัลพาร์ติชัน 3 พาร์ติชัน บนเน็ตเวิร์กสาธารณะ คุณสามารถมีอีเทอร์เน็ตอะแดปเตอร์เพิ่มเติมเพื่อให้ HMC มีเน็ตเวิร์กอินเตอร์เฟซ 3 ชุด คุณสามารถใช้เน็ตเวิร์กที่สามนี้เป็นเน็ตเวิร์กการจัดการ หรือเชื่อมต่อกับ CSM (Cluster Systems Manager) Management Server

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ “การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 70

การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ **call-home**

ศึกษาเพิ่มเติมเกี่ยวกับข้อพจน์ของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

คุณสามารถกำหนดคอนฟิก HMC เพื่อส่งข้อมูลเกี่ยวกับเซอรัวของฮาร์ดแวร์ให้กับ IBM โดยใช้การเชื่อมต่ออินเทอร์เน็ตแบบอิง LAN หรือการเชื่อมต่อผ่านสายโทรศัพท์ผ่านทางโมเด็ม

คุณมีทางเลือกในการสื่อสาร 2 ทางเลือก เมื่อกำหนดคอนฟิก การเชื่อมต่ออินเทอร์เน็ตผ่าน LAN ทางเลือกแรกคือใช้ Secure Sockets Layer (SSL) มาตรฐาน สามารถเปิดใช้การสื่อสาร SSL เพื่อเชื่อมต่อ อินเทอร์เน็ตผ่านพรีอ็อกซีเซิร์ฟเวอร์ การเชื่อมต่อ SSL มีแนวโน้มว่าจะสอดคล้องกับแนวทางความปลอดภัยขององค์กร ทางเลือกที่สองคือ การใช้การเชื่อมต่อ VPN

หมายเหตุ: หากการเชื่อมต่อเน็ตเวิร์กอินเทอร์เน็ตแบบเปิดของคุณใช้เฉพาะ Internet Protocol Version 6 (IPv6) เท่านั้น คุณจะไม่สามารถใช้ Internet VPN ในการเชื่อมต่อเพื่อการสนับสนุนได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรโตคอลที่ใช้โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 10

ข้อดีของการใช้การเชื่อมต่ออินเทอร์เน็ตอาจได้แก่:

- ความเร็วในการรับส่งข้อมูลสูงกว่ามาก
- ลดค่าใช้จ่ายสำหรับลูกค้า (เช่น ค่าสายโทรศัพท์ท่อนาล็อก ที่จัดเตรียมไว้โดยเฉพาะ)
- ความเชื่อถือได้สูงกว่า

ลักษณะความปลอดภัยต่อไปนี้มีผลบังคับใช้ไม่ว่าคุณจะใช้วิธีการเชื่อมต่อแบบใดก็ตาม:

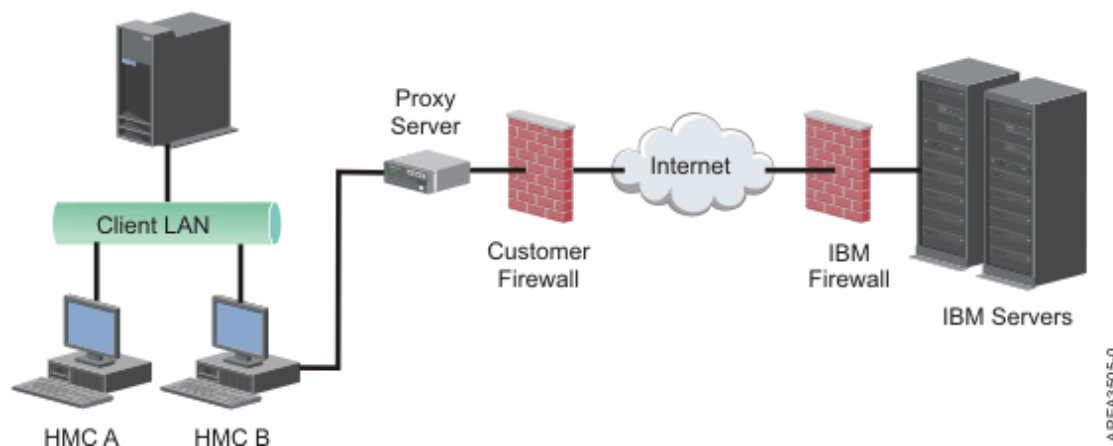
- คำร้องขอระบบสนับสนุนทางรีโมตจะถูกเริ่มต้นจาก HMC ไปยัง IBM การเชื่อมต่อเข้าไม่ได้เริ่มจาก IBM Service Support System
- ข้อมูลทั้งหมดที่ถ่ายโอนระหว่าง HMC และ IBM Service Support System จะถูกเข้ารหัสไว้โดยใช้การเข้ารหัสระดับสูง ข้อมูลดังกล่าวจะถูกเข้ารหัสโดยใช้ SSL หรือ IPSec Encapsulating Security Payload (ESP) ทั้งนี้ขึ้นอยู่กับวิธีการเชื่อมต่อที่เลือกใช้
- เมื่อ initialize การเชื่อมต่อที่เข้ารหัสไว้ HMC authenticates the HMC จะพิสูจน์ตัวตนปลายทางเป้าหมาย IBM Service Support System

ข้อมูลที่ส่งไปยัง IBM Service Support System ประกอบด้วยข้อมูลเกี่ยวกับปัญหาของฮาร์ดแวร์ และคอนฟิกูเรชัน ไม่มีข้อมูลแอพลิเคชันหรือข้อมูลลูกค้าที่ส่งผ่านไปยัง IBM

การใช้การเชื่อมต่ออินเทอร์เน็ตทางอ้อมด้วย พร็อกซีเซิร์ฟเวอร์

ถ้าคุณจำเป็นต้องติดตั้ง HMC ไว้บนเน็ตเวิร์กส่วนตัว คุณอาจสามารถเชื่อมต่ออินเทอร์เน็ตทางอ้อม โดยใช้พร็อกซี SSL ซึ่งสามารถส่งต่อคำร้องขอไปยังอินเทอร์เน็ต ข้อดี อีกประการหนึ่งของการใช้พร็อกซี SSL ก็คือ พร็อกซีดังกล่าว อาจสนับสนุนการล็อกและระบบตรวจสอบ

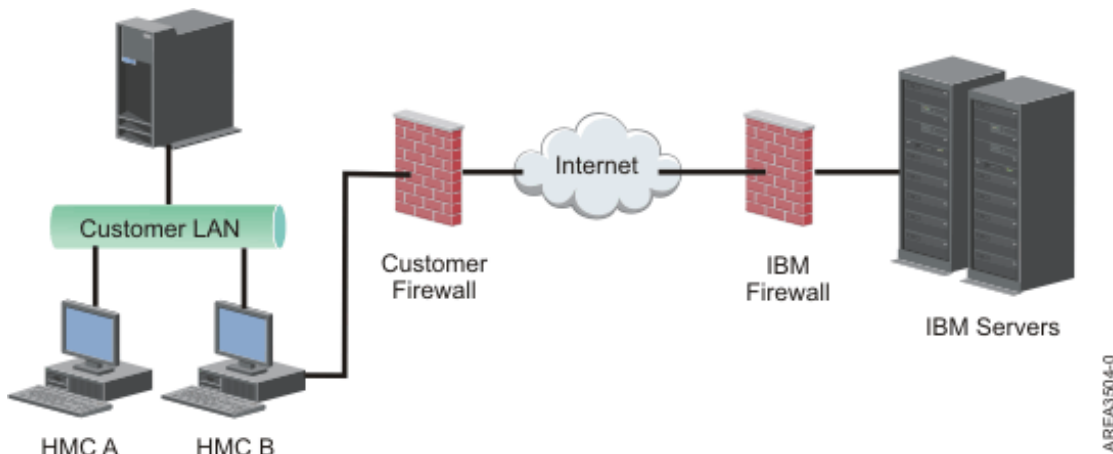
เมื่อต้องการส่งต่อ ข้อผิดพลาด SSL พร็อกซีเซิร์ฟเวอร์จะต้องสนับสนุนฟังก์ชันส่วนหัวพร็อกซีระดับต้น (ตามที่ระบุไว้ใน RFC 2616) และเมธอด CONNECT หรืออีกทางหนึ่ง อาจกำหนดคอนฟิกการพิสูจน์ตัวตนพร็อกซีระดับต้น (RFC 2617) เพื่อให้ HMC ทำการพิสูจน์ตัวตน ก่อนที่จะพยายามส่งต่อข้อผิดพลาดผ่าน พร็อกซีเซิร์ฟเวอร์



เพื่อให้ HMC สื่อสารได้สำเร็จ ฟร็อกซีเซิร์ฟเวอร์ของลูกค้าน่าจะต้องอนุญาตให้เชื่อมต่อกับพอร์ต 443 คุณสามารถกำหนดคอนฟิกฟร็อกซีเซิร์ฟเวอร์ของคุณเพื่อจำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 11 สำหรับ รายการ IP แอดเดรส

การใช้การเชื่อมต่อ SSL อินเทอร์เน็ตโดยตรง

ถ้า HMC ของคุณ สามารถเชื่อมต่ออินเทอร์เน็ต และสามารถตั้งค่าไฟร์วอลล์ภายนอก เพื่ออนุญาตให้ส่งแพ็กเก็ต TCP ไปยังปลายทางที่ระบุไว้ใน “รายการแอดเดรส Internet SSL” ในหน้า 11 คุณสามารถใช้ การเชื่อมต่ออินเทอร์เน็ตโดยตรงได้



การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต

การสื่อสารทั้งหมดถูกจัดการผ่านซ็อกเก็ต TCP ซึ่งเริ่มโดย HMC และใช้ SSL ระดับสูง เพื่อเข้ารหัสข้อมูลที่ส่งผ่าน แอดเดรส TCP/IP ปลายทางถูกเผยแพร่ (โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 11) เพื่อที่ว่าไฟร์วอลล์ภายนอก จะสามารถตั้งค่าเพื่ออนุญาตการเชื่อมต่อเหล่านี้

หมายเหตุ: พอร์ต HTTPS มาตรฐาน 443 ใช้สำหรับการสื่อสารทั้งหมด

HMC สามารถเปิดใช้งานเพื่อเชื่อมต่อโดยตรงกับอินเทอร์เน็ต หรือเพื่อเชื่อมต่อทางอ้อมจากฟร็อกซีเซิร์ฟเวอร์ที่ลูกค้าจัดหา ให้การตัดสินใจเกี่ยวกับแนวทางที่เหมาะสมที่สุดสำหรับการติดตั้งของคุณขึ้นอยู่กับข้อกำหนดความปลอดภัยและระบบเน็ตเวิร์กของ องค์กรของคุณ HMC (โดยตรง หรือผ่านฟร็อกซี SSL) ใช้แอดเดรสต่อไปนี้ เมื่อถูกตั้งค่าให้ใช้การเชื่อมต่อ Internet SSL

การเลือก อินเทอร์เน็ตโปรโตคอล

ระบุเวอร์ชันของ IP แอดเดรสที่จะใช้เมื่อ HMC เชื่อมต่อไปยังผู้ให้บริการของคุณ

ผู้ใช้งานมากจะใช้ Internet Protocol Version 4 (IPv4) เพื่อเชื่อมต่อไปยังผู้ให้บริการ IPv4 แอดเดรสปรากฏขึ้นในรูปแบบที่แสดงถึง ไบต์สี่ไบต์ของ IPv4 แอดเดรส ซึ่งคั่นด้วยจุด (ตัวอย่างเช่น 9.60.12.123) เพื่อเข้าถึงอินเทอร์เน็ต คุณยังสามารถใช้ Internet Protocol Version 6 (IPv6) เพื่อเชื่อมต่อไปยังผู้ให้บริการได้เช่นกัน ทั้งนี้ IPv6 มักถูกใช้งานโดยผู้ให้บริการเน็ตเวิร์ก เพื่อให้แน่ใจว่ามีพื้นที่ที่อยู่จะไม่ซ้ำกัน ถ้าคุณ ไม่แน่ใจเกี่ยวกับอินเทอร์เน็ตโปรโตคอลที่ใช้ในการติดตั้งของคุณ โปรดติดต่อ ผู้ดูแลระบบเครือข่ายของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เวอร์ชันแต่ละเวอร์ชัน โปรดดูที่ “การตั้งค่า IPv4 address” ในหน้า 70 และ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 70

รายการแอดเดรส Internet SSL

ศึกษาเกี่ยวกับแอดเดรสที่ HMC ใช้เมื่อใช้ภาวะเชื่อมต่อ Internet SSL

HMC ใช้ IPv4 address ต่อไปนี้เพื่อติดต่อกับส่วนบริการและส่วนสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้ภาวะเชื่อมต่ออินเทอร์เน็ตแบบ SSL

แอดเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่:

- 129.42.26.224
- 129.42.34.224
- 129.42.42.224
- 170.225.15.41
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216

แอดเดรส IPv4 ต่อไปนี้สำหรับทวีปอเมริกา:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

แอดเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่ที่ไม่ใช่อเมริกา:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.200
- 207.25.252.205

หมายเหตุ: เมื่อตั้งค่าไฟร์วอลล์เพื่ออนุญาตให้ HMC สามารถเชื่อมต่อกับเซิร์ฟเวอร์เหล่านี้จะต้องใช้ IP แอดเดรสที่เฉพาะเจาะจงสำหรับภูมิภาคดังกล่าวเท่านั้น

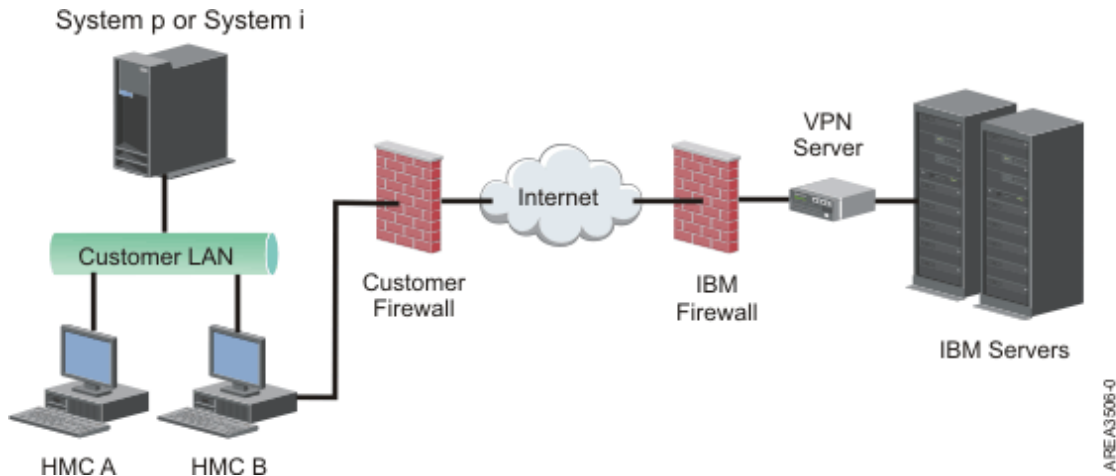
HMC ใช้ IPv6 แอดเดรสต่อไปนี้เพื่อติดต่อกับส่วนบริการและสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้ภาวะเชื่อมต่ออินเทอร์เน็ตแบบ SSL:

- 2620:0:6C0:1::1000
- 2620:0:6C1:1::1000
- 2620:0:6C2:1::1000

การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล

Virtual Private Network (VPN) ให้ความปลอดภัยเมื่อเชื่อมต่อกับระบบสนับสนุนระยะไกล

VPN ช่วยรักษาความเป็นส่วนตัวของเน็ตเวิร์กที่แยกต่างหากบนสายสาธารณะ โดยทดแทนการเข้ารหัสและมาตรการความปลอดภัยอื่นๆ สำหรับสายเน็ตเวิร์ก ที่แยกออกจากกันในทางกายภาพของเน็ตเวิร์กส่วนตัวแบบเก่า นอกจากนี้จะสามารถใช้สำหรับการเชื่อมต่อขาออกแล้ว การเชื่อมต่อ VPN ยังสามารถกำหนดคอนฟิกได้ตามต้องการ เพื่อสนับสนุน service request แบบรีโมต



เป็นความรับผิดชอบของ ผู้ดูแลระบบในการจัดเตรียมการเชื่อมต่อ อินเทอร์เน็ต นอกจากนี้ยังอาจ จำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ ถ้า คุณต้องการกำหนดคอนฟิกไฟร์วอลล์ของคุณ เพื่อจำกัด IP แอดเดรส โปรดดูที่ “รายการแอดเดรสเซิร์ฟเวอร์ VPN” สำหรับ รายการแอดเดรสที่คุณสามารถใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการเชื่อมต่ออินเทอร์เน็ตโดยใช้ VPN บน LAN โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65

รายการแอดเดรสเซิร์ฟเวอร์ VPN

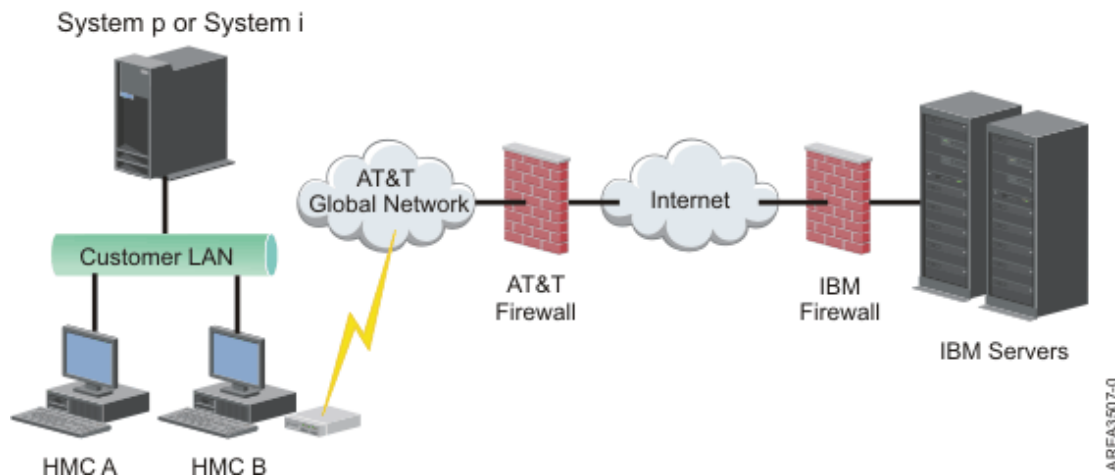
แสดงรายการเซิร์ฟเวอร์ที่ถูกใช้โดย HMC เมื่อกำหนดคอนฟิก HMC ให้ใช้ภาวะเชื่อมต่อกับอินเทอร์เน็ตโดยใช้ VPN

เซิร์ฟเวอร์ต่อไปนี้ใช้โดย HMC เมื่อถูกกำหนดคอนฟิกให้ใช้การเชื่อมต่อ VPN อินเทอร์เน็ต การเชื่อมต่อทั้งหมดใช้ ESP และ UDP บนพอร์ต 500 และพอร์ต 4500 เมื่อกำลังใช้ไฟร์วอลล์ Network Address Translation (NAT)

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต

ถ้าคุณต้องการใช้โมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต คุณจะต้องจัดหาสายอะนาล็อกแบบเฉพาะงานเพื่อเชื่อมต่อกับโมเด็ม HMC HMC ใช้โมเด็มเพื่อต่อเลขหมายโกลบอลเน็ตเวิร์กและเชื่อมต่อกับส่วนบริการ และส่วนสนับสนุนของ IBM



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเชื่อมต่อระบบสนับสนุนแบบรีโมต โดยใช้โทรศัพท์และโมเด็ม โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65

การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์

หัวข้อนี้จะอธิบายถึงสิ่งที่จำเป็นต้องทราบเมื่อตัดสินใจใช้เซิร์ฟเวอร์ Call-Home มากกว่าหนึ่งเครื่อง

เมื่อต้องการหลีกเลี่ยงไม่ให้เกิดความล้มเหลวแม้แต่จุดเดียว ให้คอนฟิก HMC ให้ใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานเซิร์ฟเวอร์แรก จะพยายามจัดการเหตุการณ์เซอร์วิสแต่ละเหตุการณ์ หากการเชื่อมต่อหรือการส่งข้อมูลล้มเหลว กับเซิร์ฟเวอร์ Call-Home นี้ จะมีการพยายามร้องขอเซอร์วิสอีกครั้งโดยใช้เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานอื่นจนกว่าจะประสบความสำเร็จหรือได้พยายามกับ ทุกเซิร์ฟเวอร์แล้ว

HMC ที่เชื่อมต่อที่ได้รับการระบุแล้วจากการวิเคราะห์ปัญหา ให้เป็นคอนโซลการวิเคราะห์หลักสำหรับระบบที่ถูกจัดการที่มีให้ จะรายงานปัญหา คอนโซลหลักนี้จะจำลองรายงานปัญหาให้กับ HMC รองใดๆ อีกด้วย HMC หลักจะต้องจดจำ HMC รองบนเน็ตเวิร์กได้ด้วย HMC หลักจะต้องจดจำ HMC รอง ว่าเป็นเซิร์ฟเวอร์ Call-Home เพิ่มเติมเมื่อ:

- HMC หลักถูกกำหนดคอนฟิกให้ใช้เซิร์ฟเวอร์ Call-Home ที่ “ค้นพบ” โดยเซิร์ฟเวอร์ Call-Home จะอยู่บนชั้นเน็ตเดียวกันกับ HMC หลัก หรือจัดการระบบเดียวกัน
- มีการเพิ่มเซิร์ฟเวอร์ Call-Home ด้วยตนเองลงในรายการ คอนโซลเซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานสำหรับการเชื่อมต่อภายนอก

การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC

เรียนรู้เกี่ยวกับค่าติดตั้งเน็ตเวิร์กที่คุณสามารถใช้นบน HMC

การเชื่อมต่อเน็ตเวิร์ก HMC

คุณสามารถใช้การเชื่อมต่อเน็ตเวิร์กประเภทต่างๆ เพื่อเชื่อมต่อ HMC ของคุณกับระบบที่ถูกจัดการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีตั้งค่า HMC เพื่อเชื่อมต่อกับเน็ตเวิร์ก โปรดดูที่ “การกำหนดคอนฟิก HMC” ในหน้า 61 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ HMC บนเน็ตเวิร์ก โปรดดูต่อไป:

ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC

ศึกษาเกี่ยวกับวิธีการใช้ฟังก์ชันการจัดการและการให้บริการแบบรีโมต HMC โดยใช้เน็ตเวิร์กของคุณ

HMC สนับสนุนการสื่อสารโลจิคัลในประเภทดังต่อไปนี้:

HMC to managed system

ใช้เพื่อดำเนินฟังก์ชันการจัดการฮาร์ดแวร์โดยส่วนใหญ่ ซึ่ง HMC ออกคำขอฟังก์ชันควบคุมผ่านทางเซอวิสโปรเซสเซอร์ของระบบที่ถูกจัดการ บางครั้ง การเชื่อมต่อระหว่าง HMC และเซอวิสโปรเซสเซอร์เรียกว่าเป็น *เน็ตเวิร์กบริการ* การเชื่อมต่อนี้ต้องใช้สำหรับการจัดการระบบที่ถูกจัดการ

HMC to logical partition

ใช้เพื่อรวบรวมข้อมูลเกี่ยวกับแพลตฟอร์ม (เหตุการณ์ข้อผิดพลาดฮาร์ดแวร์, คลังฮาร์ดแวร์) จากการรันระบบปฏิบัติการในโลจิคัลพาร์ติชัน พร้อมทั้งเพื่อประสานกับ activity แพลตฟอร์มบางอย่าง (dynamic LPAR, การซ่อมพร้อมกัน) กับระบบปฏิบัติการนั้น หากคุณต้องการใช้บริการและคุณลักษณะการแจ้งข้อผิดพลาด คุณต้องสร้างการเชื่อมต่อ

HMC to remote users

ช่วยให้ผู้ใช้รีโมตสามารถเข้าถึงฟังก์ชัน HMC ผู้ใช้รีโมตสามารถ เข้าถึง HMC โดยวิธีดังต่อไปนี้:

- โดยการใช้เว็บเบราว์เซอร์เพื่อเข้าถึงฟังก์ชัน GUI ของ HMC ทั้งหมดแบบรีโมต
- โดยการใช้ Secure Socket Shell (SSH) เพื่อเข้าถึงฟังก์ชันบรรทัดรับคำสั่ง HMC จากระยะไกล

HMC to service and support

ใช้เพื่อส่งข้อมูล เช่น รายงานความผิดพลาดฮาร์ดแวร์ ข้อมูลคลัง และการอัปเดตไมโครโค้ด ไปยังและจากผู้ให้บริการของคุณ คุณสามารถใช้พาดการสื่อสารนี้เพื่อเรียกการให้บริการโดยอัตโนมัติ

HMC ของคุณสามารถสนับสนุนฟิสิคัลอีเทอร์เน็ตอินเตอร์เฟซได้มากถึงสี่อินเตอร์เฟซขึ้นอยู่กับแต่ละรุ่น HMC เวอร์ชันสแตนด์อะโลนสนับสนุนอินเตอร์เฟซ HMC เพียงสามอินเตอร์เฟซเท่านั้น ซึ่งใช้อะแดปเตอร์อีเทอร์เน็ตแบบในตัวหนึ่งตัวและมีปลั๊กอินอะแดปเตอร์ได้มากที่สุดสองตัว ใช้อินเตอร์เฟซ แต่ละตัวเหล่านี้ในวิธีดังต่อไปนี้:

- เน็ตเวิร์กอินเตอร์เฟซตั้งแต่หนึ่งขึ้นไปสามารถใช้เฉพาะสำหรับการสื่อสารแบบ HMC-ไปที่-ระบบที่ถูกจัดการเท่านั้น ซึ่งหมายความว่า เฉพาะ HMC และเซอวิสโปรเซสเซอร์ของระบบที่ถูกจัดการเท่านั้นที่จะอยู่บนเน็ตเวิร์กนั้น แม้ว่าอินเตอร์เฟซ เครือข่ายที่อยู่ในตัวประมวลผลเซอวิสมีการเข้ารหัสโปรโตคอล Secure Sockets Layer (SSL) และมีการป้องกันด้วยรหัสผ่าน การมีเครือข่าย เฉพาะงานที่แยกต่างหากสามารถช่วยให้อินเตอร์เฟซเหล่านี้มีระดับความปลอดภัย สูงขึ้น
- โดยทั่วไปแล้ว อินเตอร์เฟซเน็ตเวิร์กแบบเปิดใช้กับการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC และโลจิคัลพาร์ติชันบนระบบที่ถูกจัดการ สำหรับการสื่อสารแบบ HMC-ไปที่-โลจิคัลพาร์ติชัน คุณยังสามารถใช้เน็ตเวิร์กอินเตอร์เฟซแบบเปิดนี้เพื่อจัดการกับ HMC จากระยะไกล
- หรือคุณอาจใช้อินเตอร์เฟซอื่นเพื่อเชื่อมต่อกับโลจิคัลพาร์ติชัน และจัดการ HMC จากระยะไกล อินเตอร์เฟซนี้ยังสามารถใช้เป็นการเชื่อมต่อ HMC แยกต่างหากไปยังกลุ่มโลจิคัลพาร์ติชันอื่น ตัวอย่างเช่น คุณอาจต้องการให้มี LAN การจัดการที่แยกต่างหากจาก LAN ซึ่งธุรกรรมทางธุรกิจปกติทั้งหมดกำลัง รันอยู่ ผู้ดูแลรีโมตสามารถเข้าถึง HMC และหน่วยที่ถูกจัดการอื่น ได้โดยใช้วิธีการนี้ ในบางครั้งโลจิคัลพาร์ติชันจะอยู่ใน โดเมนความปลอดภัยเน็ตเวิร์กอื่น อาจจะเป็นด้านหลังไฟร์วอลล์ และคุณอาจต้องการมี การเชื่อมต่อเน็ตเวิร์ก HMC ที่แตกต่างกันสำหรับสองโดเมนเหล่านั้น

ข้อกำหนดเว็บเบราว์เซอร์สำหรับ HMC

คอนโซล การจัดการฮาร์ดแวร์ (HMC) ได้รับการสนับสนุนจาก Microsoft Internet Explorer (IE) เวอร์ชัน 6.0 และ 7.0, Firefox เวอร์ชัน 1.5.0.7 และ 2.0

ถ้าเบราว์เซอร์ของคุณมีการกำหนดคอนฟิกเพื่อใช้อินเทอร์เน็ตพรีอ็อกซีโลคัล IP แอดเดรส ควรมีการรวมไว้ในรายการข้อยกเว้นโปรตปรักษาผู้ดูแลระบบเครือข่ายของคุณสำหรับข้อมูลเพิ่มเติมเกี่ยวกับรายการข้อยกเว้น ถ้าคุณยังคงจำเป็นต้องใช้พรีอ็อกซีเพื่อเรียกใช้ HMC ให้เปิดใช้งาน การใช้ HTTP 1.1 ผ่านทาง การเชื่อมต่อพรีอ็อกซี ภายใต้แท็บขั้นสูง ในหน้าต่าง อีพชันอินเทอร์เน็ต

หมายเหตุ: สำหรับ Firefox เวอร์ชัน 2.0 ตรวจสอบให้แน่ใจว่าคุณเปิดใช้งาน อีพชัน JavaScript เพื่อเพิ่มหรือลดหน้าต่างและย้ายหรือเปลี่ยนขนาด หน้าต่างที่มีอยู่ คุณลักษณะนี้ช่วยให้คุณสามารถสลับระหว่างภารกิจ HMC ได้ง่าย ปฏิบัติตามขั้นตอนต่อไปนีเพื่อเปิดใช้งานอีพชัน Javascript:

1. เลือก เครื่องมือ และคลิก อีพชัน
2. เลือก เนื้อหา และคลิก ขั้นสูง
3. เลือก ย้ายหรือเปลี่ยนขนาดหน้าต่างที่มีอยู่ หรือ เพิ่มหรือลดหน้าต่าง
4. คลิก ตกลง

ต้องเปิดใช้งานเซชันคุกกี้เพื่อให้ ASMI สามารถทำงานได้เมื่อเชื่อมต่อกับ HMC แบบรีโมต รหัสพรีอ็อกซี asm บันทึกและใช้ข้อมูลเซชัน ปฏิบัติตามขั้นตอนต่อไปนีเพื่อเปิดใช้งาน เซชันคุกกี้

การเปิดใช้งานเซชันคุกกี้ใน Internet Explorer

1. เลือก เครื่องมือ และคลิก อีพชันอินเทอร์เน็ต
2. เลือก ความเป็นส่วนตัว และคลิก ขั้นสูง
3. ตรวจสอบให้แน่ใจว่าได้เลือก อนุญาตเซชันคุกกี้เสมอ ถ้ายังไม่ได้เลือก ให้เลือก ยกเลิกการจัดการคุกกี้อัตโนมัติ และเลือก อนุญาต เซชันคุกกี้เสมอ
4. เลือก พร้อมท์ภายใต้คุกกี้ของบุคคลที่หนึ่งและคุกกี้ของบุคคลที่สาม
5. คลิก ตกลง

การเปิดใช้งานเซชันคุกกี้ใน Firefox

1. เลือก เครื่องมือ และคลิก อีพชัน
2. คลิก คุกกี้
3. เลือก อนุญาตให้ไซต์ตั้งค่าคุกกี้
4. เลือก ข้อยกเว้น และเพิ่ม HMC
5. คลิก ตกลง

เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC:

HMC สามารถกำหนดคอนฟิกเพื่อใช้เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดได้ เน็ตเวิร์กส่วนตัวอนุญาตให้ใช้ช่วงที่เลือกของ IP-address ที่เราต์ไม่ได้ เน็ตเวิร์กแบบ *พับลิก* หรือแบบ "เปิด" หมายถึงการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC กับโลจิสต์ลาร์ติชันและ ระบบอื่นๆ บนเน็ตเวิร์กปกติของคุณ

เน็ตเวิร์กส่วนตัว

เน็ตเวิร์กส่วนตัวของ HMC มีเพียงอุปกรณ์เดียว นั่นคือ HMC และระบบที่จัดการแต่ละระบบที่ HMC เชื่อมต่ออยู่ HMC ถูกเชื่อมต่อกับ FSP (Flexible Service Processor) ของแต่ละระบบที่จัดการ

บนระบบส่วนใหญ่ FSP จะจัดหาอีเทอร์เน็ตพอร์ต 2 พอร์ต ซึ่งใช้เลเบล **HMC1** และ **HMC2** ซึ่งอนุญาตให้คุณเชื่อมต่อ HMC ไม่เกิน 2 เครื่อง

บางระบบมี อ็อพชัน dual-FSP ในสถานการณ์นี้ FSP ตัวที่สองทำหน้าที่เป็นอุปกรณ์ "สำรอง" โดยหลักๆ แล้ว ข้อกำหนดการติดตั้งระดับต้น สำหรับระบบที่มี FSP สองตัว เหมือนกับระบบที่ไม่มี FSP ตัวที่สอง โดย HMC ต้องเชื่อมต่อกับ FSP แต่ละตัว ดังนั้น ต้องมีเน็ตเวิร์กฮาร์ดแวร์เพิ่มเติม (เช่น สวิตช์หรือฮับ LAN) เมื่อมี FSP มากกว่าหนึ่งตัว หรือมีระบบที่จัดการหลายระบบ

หมายเหตุ: พอร์ต FSP แต่ละพอร์ตบนระบบที่จัดการจะต้องเชื่อมต่อกับ HMC เพียงเครื่องเดียวเท่านั้น

พับลิคเน็ตเวิร์ก

เน็ตเวิร์กแบบเปิดสามารถเชื่อมต่อกับไฟร์วอลล์หรือเราเตอร์สำหรับการเชื่อมต่ออินเทอร์เน็ต การเชื่อมต่อกับอินเทอร์เน็ตช่วยให้ HMC สามารถ "call home" ได้เมื่อมีข้อผิดพลาดฮาร์ดแวร์อื่นใดที่ต้องการรายงาน

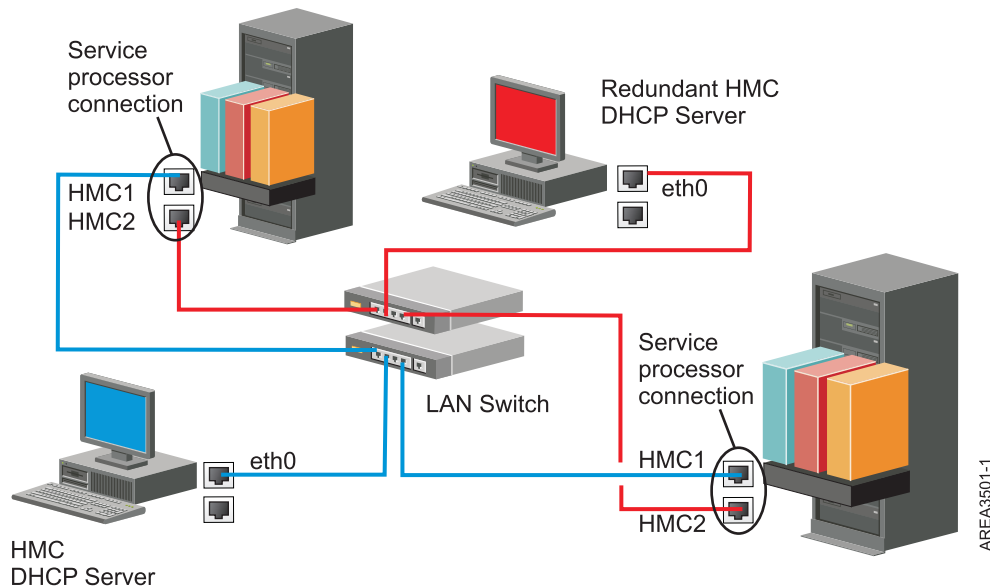
HMC ประกอบด้วยไฟร์วอลล์บนแต่ละ เน็ตเวิร์กอินเตอร์เฟซ ไฟร์วอลล์ระดับต้นจะถูกตั้งค่าโดยอัตโนมัติเมื่อคุณรันวิซาร์ด HMC Guided Setup แต่คุณควรปรับการตั้งค่าไฟร์วอลล์หลังจากการติดตั้งและการคอนฟิก HMC เบื้องต้น

HMC เป็นเซิร์ฟเวอร์ DHCP:

คุณสามารถใช้ HMC เป็นเซิร์ฟเวอร์ Dynamic Host Configuration Protocol (DHCP)

หมายเหตุ: ถ้าคุณกำลังใช้ IPv6 กระบวนการค้นหาต้องทำด้วยตนเอง สำหรับ IPv6 ไม่มีการค้นหาแบบอัตโนมัติ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ "การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP" ในหน้า 70

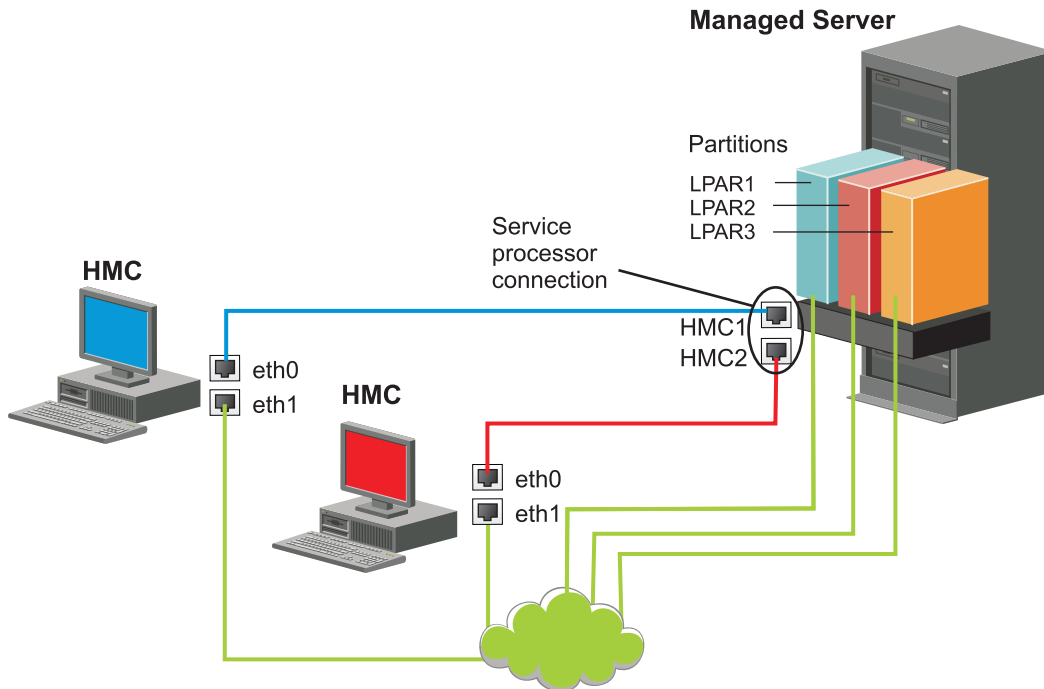


รูปภาพนี้แสดงสถานะแวดล้อม HMC สำรอง พร้อมด้วย ระบบที่ถูกจัดการ 2 ระบบ HMC เครื่องแรกเชื่อมต่อกับพอร์ตแรกบนแต่ละ FSP และ HMC สำรองเชื่อมต่อกับพอร์ตที่สองบน HMC แต่ละเครื่อง HMC แต่ละเครื่องถูกตั้งค่าเป็นเซิร์ฟเวอร์ DHCP โดยใช้ช่วง IP แอดเดรสที่แตกต่างกัน การเชื่อมต่ออยู่บนเน็ตเวิร์กส่วนตัวที่แยกต่างหาก ด้วยเหตุนี้จึงจำเป็นอย่างยิ่งที่จะต้องตรวจสอบให้แน่ใจว่าพอร์ต 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 เช็กเมนต์ ส่วนตัวนี้สามารถมีอยู่ในรูปแบบหลายพอร์ตใน *virtual LAN (VLAN)* แบบไพรเวต บนสวิตช์ขนาดใหญ่ที่ถูกจัดการ ถ้าคุณมี VLAN แบบไพรเวตหลายๆ เน็ตเวิร์ก คุณจะตรวจสอบให้แน่ใจว่า VLAN ดังกล่าวแยกออกจากกัน และไม่มีทราฟฟิกที่ติดกัน

ถ้าคุณมี HMC มากกว่าหนึ่งเครื่อง คุณจะต้องเชื่อมต่อ HMC แต่ละเครื่องเข้ากับโลจิคัลพาร์ติชัน และเชื่อมต่อ HMC เข้าด้วยกัน บนเน็ตเวิร์กแบบเปิดเดียวกัน



AREA3502-1

รูปนี้แสดง HMC สองเครื่องที่เชื่อมต่อกับเซิร์ฟเวอร์ที่ถูกจัดการเดี่ยวบนเน็ตเวิร์กส่วนตัว และกับโลจิคัลพาร์ติชัน 3 พาร์ติชันบนเน็ตเวิร์กสาธารณะ คุณสามารถมีอีเทอร์เน็ตอะแดปเตอร์เพิ่มเติมเพื่อให้ HMC มีเน็ตเวิร์กอินเตอร์เฟซ 3 ชุด คุณสามารถใช้เน็ตเวิร์กที่สามนี้เป็นเน็ตเวิร์กการจัดการ หรือเชื่อมต่อกับ CSM (Cluster Systems Manager) Management Server

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ “การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 70

การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home

ศึกษาเพิ่มเติมเกี่ยวกับข้อพจน์ของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

คุณสามารถกำหนดคอนฟิก HMC เพื่อส่งข้อมูลเกี่ยวกับเซิร์ฟเวอร์ของฮาร์ดแวร์ให้กับ IBM โดยใช้การเชื่อมต่ออินเทอร์เน็ตแบบอิง LAN หรือการเชื่อมต่อผ่านสายโทรศัพท์ผ่านทางโมเด็ม

คุณมีทางเลือกในการสื่อสาร 2 ทางเลือก เมื่อกำหนดคอนฟิก การเชื่อมต่ออินเทอร์เน็ตผ่าน LAN ทางเลือกแรกคือใช้ Secure Sockets Layer (SSL) มาตรฐาน สามารถเปิดใช้การสื่อสาร SSL เพื่อเชื่อมต่อ อินเทอร์เน็ตผ่านพรีอ็อกซีเซิร์ฟเวอร์ การเชื่อมต่อ SSL มีแนวโน้มว่าจะสอดคล้องกับแนวทางความปลอดภัยขององค์กร ทางเลือกที่สองคือ การใช้การเชื่อมต่อ VPN

หมายเหตุ: หากการเชื่อมต่อเน็ตเวิร์กอินเทอร์เน็ตแบบเปิดของคุณ ใช้เฉพาะ Internet Protocol Version 6 (IPv6) เท่านั้น คุณจะไม่สามารถใช้ Internet VPN ในการเชื่อมต่อเพื่อการสนับสนุนได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรโตคอลที่ใช้โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 10

ข้อดีของการใช้การเชื่อมต่ออินเทอร์เน็ตอาจได้แก่:

- ความเร็วในการรับส่งข้อมูลสูงกว่ามาก
- ลดค่าใช้จ่ายสำหรับลูกค้า (เช่น ค่าสายโทรศัพท์ท่อนาล็อก ที่จัดเตรียมไว้โดยเฉพาะ)
- ความเชื่อถือได้สูงกว่า

ลักษณะความปลอดภัยต่อไปนี้มีผลบังคับใช้ไม่ว่าคุณจะเลือกใช่วิธีการเชื่อมต่อแบบใดก็ตาม:

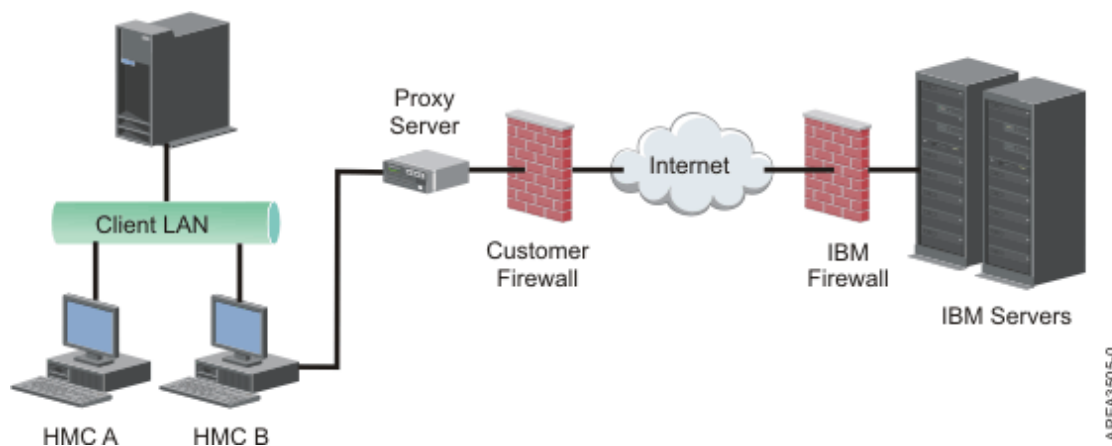
- คำร้องขอระบบสนับสนุนทางรีโมตจะถูกเริ่มต้นจาก HMC ไปยัง IBM การเชื่อมต่อเข้าไม่ได้เริ่มจาก IBM Service Support System
- ข้อมูลทั้งหมดที่ถ่ายโอนระหว่าง HMC และ IBM Service Support System จะถูกเข้ารหัสไว้โดยใช้การเข้ารหัสระดับสูง ข้อมูลดังกล่าวจะถูกเข้ารหัสโดยใช้ SSL หรือ IPSec Encapsulating Security Payload (ESP) ทั้งนี้ขึ้นอยู่กับวิธีการเชื่อมต่อที่เลือกใช้
- เมื่อ initialize การเชื่อมต่อที่เข้ารหัสไว้ HMC authenticates the HMC จะพิสูจน์ตัวตนปลายทางเป้าหมาย IBM Service Support System

ข้อมูลที่ส่งไปยัง IBM Service Support System ประกอบด้วยข้อมูลเกี่ยวกับปัญหาของฮาร์ดแวร์ และคอนฟิกูเรชัน ไม่มีข้อมูลแอพลิเคชันหรือข้อมูลลูกค้าที่ส่งผ่านไปยัง IBM

การใช้การเชื่อมต่ออินเทอร์เน็ตทางอ้อมด้วย พร็อกซีเซิร์ฟเวอร์

ถ้าคุณจำเป็นต้องติดตั้ง HMC ไว้บนเน็ตเวิร์กส่วนตัว คุณอาจสามารถเชื่อมต่ออินเทอร์เน็ตทางอ้อม โดยใช้พร็อกซี SSL ซึ่งสามารถส่งต่อคำร้องขอไปยังอินเทอร์เน็ต ข้อดีอีกประการหนึ่งของการใช้พร็อกซี SSL ก็คือ พร็อกซีดังกล่าว อาจสนับสนุนการล็อกและระบบตรวจสอบ

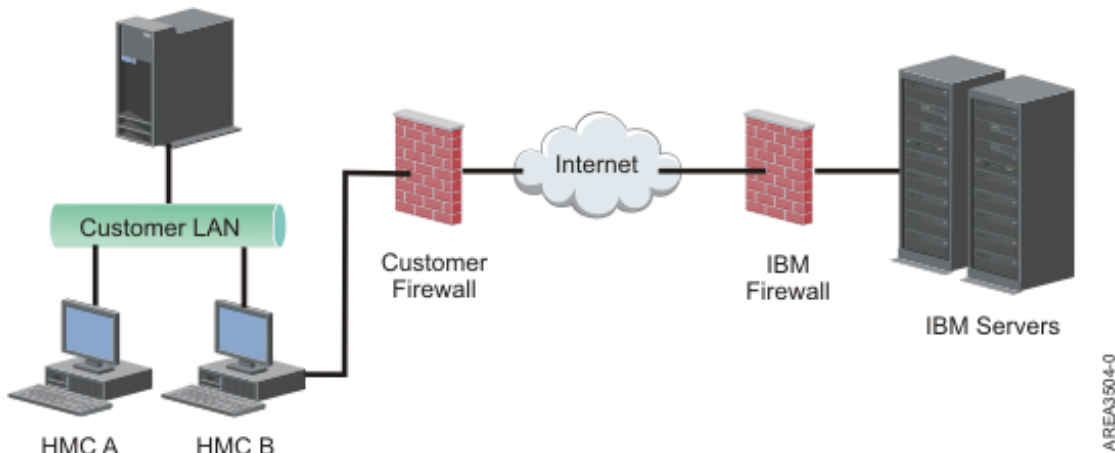
เมื่อต้องการส่งต่อข้อผิดพลาด SSL พร็อกซีเซิร์ฟเวอร์จะต้องสนับสนุนฟังก์ชันส่วนหัวพร็อกซีระดับต้น (ตามที่ระบุไว้ใน RFC 2616) และเมธอด CONNECT หรืออีกทางหนึ่ง อาจกำหนดคอนฟิกการพิสูจน์ตัวตนพร็อกซีระดับต้น (RFC 2617) เพื่อให้ HMC ทำการพิสูจน์ตัวตน ก่อนที่จะพยายามส่งต่อข้อผิดพลาดผ่าน พร็อกซีเซิร์ฟเวอร์



เพื่อให้ HMC สื่อสารได้สำเร็จ พร็อกซีเซิร์ฟเวอร์ของลูกค้าจะต้องอนุญาตให้เชื่อมต่อกับพอร์ต 443 คุณสามารถกำหนดคอนฟิกพร็อกซีเซิร์ฟเวอร์ของคุณเพื่อจำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ โปรดดูที่ “รายการแอตเตรส Internet SSL” ในหน้า 11 สำหรับ รายการ IP แอดเดรส

การใช้การเชื่อมต่อ SSL อินเทอร์เน็ตโดยตรง

ถ้า HMC ของคุณ สามารถเชื่อมต่ออินเทอร์เน็ต และสามารถตั้งค่าไฟร์วอลล์ภายนอก เพื่ออนุญาตให้ส่งแพ็กเก็ต TCP ไปยังปลายทางที่ระบุไว้ใน “รายการแอตเตรส Internet SSL” ในหน้า 11 คุณสามารถใช้ การเชื่อมต่ออินเทอร์เน็ตโดยตรงได้



การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต

การสื่อสารทั้งหมดถูกจัดการผ่านซ็อกเก็ต TCP ซึ่งเริ่มโดย HMC และใช้ SSL ระดับสูงเพื่อเข้ารหัสข้อมูลที่ส่งผ่าน แอดเดรส TCP/IP ปลายทางถูกเผยแพร่ (โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 11) เพื่อที่ว่าไฟร์วอลล์ภายนอกจะสามารถตั้งค่าเพื่ออนุญาตการเชื่อมต่อเหล่านี้

หมายเหตุ: พอร์ต HTTPS มาตรฐาน 443 ใช้สำหรับการสื่อสารทั้งหมด

HMC สามารถเปิดใช้งานเพื่อเชื่อมต่อโดยตรงกับอินเทอร์เน็ต หรือเพื่อเชื่อมต่อทางอ้อมจากพร็อกซีเซิร์ฟเวอร์ที่ลูกค้าจัดหา ให้การตัดสินใจเกี่ยวกับแนวทางที่เหมาะสมที่สุดสำหรับการติดตั้งของคุณขึ้นอยู่กับข้อกำหนดความปลอดภัยและระบบเน็ตเวิร์กขององค์กรของคุณ HMC (โดยตรง หรือผ่านพร็อกซี SSL) ใช้แอดเดรสต่อไปนี้ เมื่อถูกตั้งค่าให้ใช้การเชื่อมต่อ Internet SSL

การเลือก อินเทอร์เน็ตโปรโตคอล

ระบุเวอร์ชันของ IP แอดเดรสที่จะใช้เมื่อ HMC เชื่อมต่อไปยังผู้ให้บริการของคุณ

ผู้ใช้งานมากจะใช้ Internet Protocol Version 4 (IPv4) เพื่อเชื่อมต่อไปยังผู้ให้บริการ IPv4 แอดเดรสปรากฏขึ้นในรูปแบบที่แสดงถึง ไบต์สี่ไบต์ของ IPv4 แอดเดรส ซึ่งคั่นด้วยจุด (ตัวอย่างเช่น 9.60.12.123) เพื่อเข้าถึงอินเทอร์เน็ต คุณยังสามารถใช้ Internet Protocol Version 6 (IPv6) เพื่อเชื่อมต่อไปยังผู้ให้บริการได้เช่นกัน ทั้งนี้ IPv6 มักถูกใช้งานโดยผู้ให้บริการเน็ตเวิร์ก เพื่อให้แน่ใจว่ามีพื้นที่ที่อยู่ที่ไม่ซ้ำกัน หากคุณไม่แน่ใจเกี่ยวกับอินเทอร์เน็ตโปรโตคอลที่ใช้ในการติดตั้งของคุณ โปรดติดต่อผู้ดูแลระบบเครือข่ายของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เวอร์ชันแต่ละเวอร์ชัน โปรดดูที่ “การตั้งค่า IPv4 address” ในหน้า 70 และ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 70

รายการแอดเดรส Internet SSL

ศึกษาเกี่ยวกับแอดเดรสที่ HMC ใช้เมื่อใช้ภาวะเชื่อมต่อ Internet SSL

HMC ใช้ IPv4 address ต่อไปนี้เพื่อติดต่อกับส่วนบริการและส่วนสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้ภาวะเชื่อมต่ออินเทอร์เน็ตแบบ SSL

แอดเดรส IPv4 ต่อไปนี้ สำหรับทุกสถานที่:

- 129.42.26.224
- 129.42.34.224

- 129.42.42.224
- 170.225.15.41
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216

แอดเดรส IPv4 ต่อไปนี้สำหรับทวีปอเมริกา:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

แอดเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่ที่ไม่ใช่อเมริกา:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.200
- 207.25.252.205

หมายเหตุ: เมื่อตั้งค่าไฟร์วอลล์เพื่ออนุญาตให้ HMC สามารถเชื่อมต่อกับเซิร์ฟเวอร์เหล่านี้จะต้องใช้ IP แอดเดรสที่เฉพาะเจาะจงสำหรับภูมิภาคดังกล่าวเท่านั้น

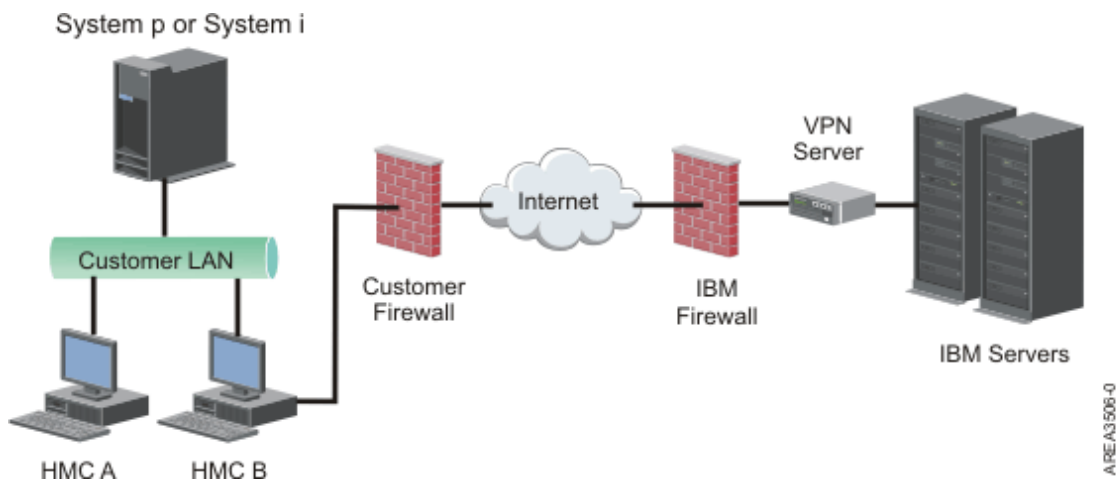
HMC ใช้ IPv6 แอดเดรสต่อไปเพื่อติดต่อกับส่วนบริการและสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้ภาวะเชื่อมต่ออินเทอร์เน็ตแบบ SSL:

- 2620:0:6C0:1::1000
- 2620:0:6C1:1::1000
- 2620:0:6C2:1::1000

การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล

Virtual Private Network (VPN) ให้ความปลอดภัยเมื่อเชื่อมต่อกับระบบสนับสนุนระยะไกล

VPN ช่วยรักษาความเป็นส่วนตัวของเน็ตเวิร์กที่แยกต่างหากบนสายสาธารณะ โดยทดแทนการเข้ารหัสและมาตรการความปลอดภัยอื่นๆ สำหรับสายเน็ตเวิร์กที่แยกออกจากกันในทางกายภาพของเน็ตเวิร์กส่วนตัวแบบเก่า นอกจากนี้ยังสามารถใช้สำหรับการเชื่อมต่อขาออกแล้ว การเชื่อมต่อ VPN ยังสามารถกำหนดคอนฟิกได้ตามต้องการ เพื่อสนับสนุน service request แบบรีโมต



เป็นความรับผิดชอบของผู้ดูแลระบบในการเตรียมการเชื่อมต่ออินเทอร์เน็ต นอกจากนี้ยังอาจจำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ ถ้าต้องการกำหนดคอนฟิกไฟร์วอลล์ของคุณ เพื่อจำกัด IP แอดเดรส โปรดดูที่ “รายการแอดเดรสเซิร์ฟเวอร์ VPN” ในหน้า 12 สำหรับ รายการแอดเดรสที่คุณสามารถใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการเชื่อมต่ออินเทอร์เน็ตโดยใช้ VPN บน LAN โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65

รายการแอดเดรสเซิร์ฟเวอร์ VPN

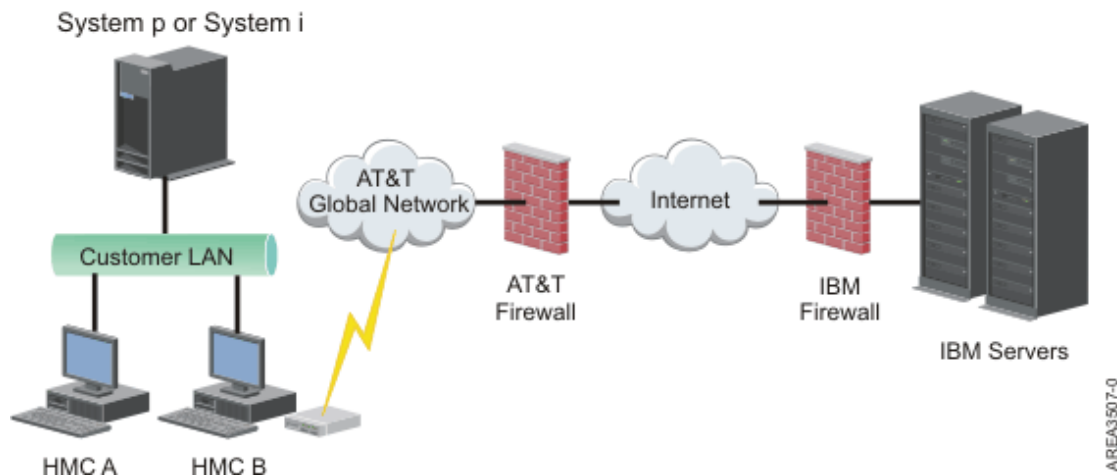
แสดงรายการเซิร์ฟเวอร์ที่ถูกใช้โดย HMC เมื่อกำหนดคอนฟิก HMC ให้ใช้ภาวะเชื่อมต่อกับอินเทอร์เน็ตโดยใช้ VPN

เซิร์ฟเวอร์ต่อไปนี้ใช้โดย HMC เมื่อถูกกำหนดคอนฟิกให้ใช้การเชื่อมต่อ VPN อินเทอร์เน็ต การเชื่อมต่อทั้งหมดใช้ ESP และ UDP บนพอร์ต 500 และพอร์ต 4500 เมื่อกำลังใช้ไฟร์วอลล์ Network Address Translation (NAT)

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต

ถ้าคุณต้องการใช้โมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต คุณจะต้องจัดหาสายอะนาล็อกแบบเฉพาะงานเพื่อเชื่อมต่อกับโมเด็ม HMC HMC ใช้โมเด็มเพื่อต่อเลขหมายโกลบอลเน็ตเวิร์กและเชื่อมต่อกับส่วนบริการ และส่วนสนับสนุนของ IBM



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเชื่อมต่อระบบสนับสนุนแบบรีโมต โดยใช้โทรศัพท์และโมเด็ม โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65

การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์

หัวข้อนี้จะอธิบายถึงสิ่งที่คุณจำเป็นต้องทราบเมื่อตัดสินใจใช้เซิร์ฟเวอร์ Call-Home มากกว่าหนึ่งเครื่อง

เมื่อต้องการหลีกเลี่ยงไม่ให้เกิดความล้มเหลวแม้แต่จุดเดียว ให้คอนฟิก HMC ให้ใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานเซิร์ฟเวอร์แรก จะพยายามจัดการเหตุการณ์เซอร์วิสแต่ละเหตุการณ์ หากการเชื่อมต่อหรือการส่งข้อมูลล้มเหลว กับเซิร์ฟเวอร์ Call-Home นี้ จะมีการพยายามร้องขอเซอร์วิสอีกครั้งโดยใช้เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานอื่นจนกว่าจะประสบความสำเร็จหรือได้พยายามกับ ทุกเซิร์ฟเวอร์แล้ว

HMC ที่เชื่อมต่อที่ได้รับการระบุแล้วจากการวิเคราะห์ปัญหา ให้เป็นคอนโซลการวิเคราะห์หลักสำหรับระบบที่ถูกจัดการที่มีให้ จะรายงานปัญหา คอนโซลหลักนี้จะจำลองรายงานปัญหาให้กับ HMC รองใดๆ อีกด้วย HMC หลักจะต้องจดจำ HMC รองบนเน็ตเวิร์กได้ด้วย HMC หลักจะต้องจดจำ HMC รอง ว่าเป็นเซิร์ฟเวอร์ Call-Home เพิ่มเติมเมื่อ:

- HMC หลักถูกกำหนดคอนฟิกให้ใช้เซิร์ฟเวอร์ Call-Home ที่ “ค้นพบ” โดยเซิร์ฟเวอร์ Call-Home จะอยู่บนชั้นเน็ตเดียวกันกับ HMC หลัก หรือจัดการระบบเดียวกัน
- มีการเพิ่มเซิร์ฟเวอร์ Call-Home ด้วยตนเองลงในรายการ คอนโซลเซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานสำหรับการเชื่อมต่อภายนอก

การจัดเตรียมสำหรับการตั้งค่าของ HMC

ใช้ส่วนนี้เพื่อรวบรวมการตั้งค่าการตั้งค่าที่จำเป็นที่คุณต้องทราบก่อนเริ่มขั้นตอนการตั้งค่า

เมื่อต้องการกำหนดคอนฟิก HMC คุณต้องเข้าใจ แนวคิดที่เกี่ยวข้อง ดำเนินการตัดสินใจ และจัดเตรียมการติดตั้ง

ส่วนนี้อธิบายข้อมูลที่คุณจะต้องใช้เพื่อเชื่อมต่อ HMC กับรายการต่อไปนี้:

- เซอร์วิสโปรเซสเซอร์ในระบบที่ถูกจัดการของคุณ

- โลจิสติกส์พาร์ติชันในระบบที่ถูกจัดการเหล่านั้น
- รีโมตเวิร์กสเตชัน
- IBM Service เพื่อนำฟังก์ชัน “call-home” ไปใช้

หมายเหตุ: มีข้อมูลการเชื่อมต่อและความปลอดภัยเพิ่มเติมพร้อมให้ใช้งาน สำหรับข้อมูลเพิ่มเติม โปรดดูที่ ความปลอดภัยของการเชื่อมต่อ HMC

เมื่อต้องการจัดเตรียมการตั้งค่า HMC ให้ทำดังต่อไปนี้:

1. ขอรับและติดตั้งระดับท้ายสุดของโค้ด HMC ในเวอร์ชันที่คุณต้องการติดตั้ง
2. กำหนดสถานที่ติดตั้ง HMC ในตำแหน่งที่ใกล้เคียงกับเซิร์ฟเวอร์ที่จะจัดการ หาก HMC อยู่ห่างจากระบบที่ถูกจัดการมากกว่า 25 ฟุต คุณต้องเตรียมการเข้าถึงเว็บเบราว์เซอร์ไปยัง HMC จากที่ตั้งของระบบที่ถูกจัดการนั้น เพื่อให้พนักงานฝ่ายบริการสามารถเข้าถึง HMC ได้
3. ระบุเซิร์ฟเวอร์ที่ HMC จะจัดการ
4. กำหนดว่าคุณจะใช้เน็ตเวิร์กส่วนตัวหรือเน็ตเวิร์กแบบเปิดในการจัดการเซิร์ฟเวอร์ หากคุณเลือกใช้เน็ตเวิร์กส่วนตัว ให้ใช้ DHCP เว้นแต่คุณกำลังใช้การตั้งค่า Cluster Systems Management (CSM) CSM ไม่ได้รับการสนับสนุน IPv6 เมื่อต้องการเข้าถึง CSM คุณต้องมีเน็ตเวิร์กสองวง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ CSM โปรดดูเอกสารคู่มือที่ให้พร้อมกับคุณลักษณะนั้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเน็ตเวิร์กแบบเปิดและเน็ตเวิร์กส่วนตัว โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 6
5. หากคุณใช้เน็ตเวิร์กเปิดเพื่อจัดการกับ FSP คุณต้องตั้งค่าแอตเตสเตอร์ของ FSP ผ่านเมนู Advanced System Management Interface ด้วยตนเอง ขอแนะนำให้ใช้เน็ตเวิร์กส่วนตัวที่ไม่สามารถกำหนดเรตได้
6. หากคุณมีสอง HMC ให้กำหนด HMC หลักและรอง HMC หลักควรมีตำแหน่งที่ใกล้กับเครื่องมากกว่า และควรเป็น HMC ที่คอนฟิกร์ให้ติดต่อผู้ให้บริการ
7. กำหนดการตั้งค่าเน็ตเวิร์กที่คุณจะต้องใช้เพื่อเชื่อมต่อ HMC กับรีโมตเวิร์กสเตชัน โลจิสติกส์พาร์ติชัน และอุปกรณ์เน็ตเวิร์ก
8. กำหนดวิธีที่ HMC จะ “call home” อีพซัน Call home รวมถึง การเชื่อมต่ออินเทอร์เนตแบบ Secure Socket Layer (SSL) ขาออกเท่านั้น โหมด หรือการเชื่อมต่อ Virtual Private Network (VPN)
9. กำหนดผู้ใช้ HMC ที่คุณจะสร้าง พร้อมทั้งรหัสผ่าน และบทบาทของผู้ใช้เหล่านั้น คุณต้องระบุรหัสผ่านให้กับผู้ใช้ hscroot และ hscope
10. จัดทำเอกสารแสดงข้อมูลติดต่อบริษัทดังต่อไปนี้ ซึ่งจะต้องใช้เมื่อกำหนดคอนฟิกร์ call home:
 - ชื่อบริษัท
 - การติดต่อผู้ดูแลระบบ
 - อีเมลแอตเตสเตอร์
 - หมายเลขโทรศัพท์
 - หมายเลขแฟกซ์
 - แอตเตสเตอร์ที่ตั้งทางกายภาพของ HMC
11. ถ้าคุณวางแผนที่จะใช้อีเมลเพื่อแจ้งเตือนผู้ควบคุมเครื่องหรือผู้ดูแลระบบ เมื่อส่งข้อมูลไปยัง IBM Service ผ่านระบบ call-home ให้ระบุเซิร์ฟเวอร์ Simple Mail Transfer Protocol (SMTP) และอีเมลแอตเตสเตอร์ที่คุณจะใช้
12. คุณต้องกำหนดรหัสผ่านต่อไปนี้:
 - รหัสผ่านเข้าถึงที่จะใช้เพื่อพิสูจน์ตัวตน HMC กับ FSP

- รหัสผ่าน ASMI ที่จะใช้กับผู้ใช้ **admin**
- รหัสผ่าน ASMI ที่จะใช้กับผู้ใช้ **general**

สร้างรหัสผ่านเมื่อคุณเชื่อมต่อจาก HMC ไปยังเซิร์ฟเวอร์ใหม่ เป็นครั้งแรก หาก HMC เป็น HMC สำรองหรือเครื่องที่สอง ให้ขอรับรหัสผ่านของผู้ใช้ HMC และเตรียมป้อนค่า เมื่อเชื่อมต่อกับ FSP ของเซิร์ฟเวอร์ที่ถูกจัดการในครั้งแรก

เมื่อคุณดำเนินขั้นตอนเตรียมการเหล่านี้เสร็จสิ้น ให้ป้อนข้อมูลใน “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC”

เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC

ใช้เวิร์กช็อปนี้เพื่อดูข้อมูลการติดตั้งที่คุณต้องเตรียมพร้อมสำหรับการติดตั้ง

ข้อกำหนดเน็ตเวิร์ก

อินเตอร์เฟซ LAN: เลือกอะแดปเตอร์ที่มี (เช่น eth0, eth1) ซึ่งจะใช้โดย HMC นี้เพื่อเชื่อมต่อกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน บริการและการสนับสนุน รวมถึงผู้ใช้โมด โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 4 สำหรับข้อมูลเพิ่มเติม การเชื่อมต่อจาก HMC สามารถอยู่บนเน็ตเวิร์กส่วนตัวหรือเน็ตเวิร์กแบบเปิด

ความเร็วของอีเทอร์เน็ตอะแดปเตอร์และ Duplex

ป้อนความเร็วของอีเทอร์เน็ตอะแดปเตอร์ที่ต้องการและโหมด duplex อีพชัณ autodetection จะระบุอ็อปชันใดเหมาะสมที่สุด ถ้าคุณไม่แน่ใจว่าความเร็ว และ duplex ใดจะก่อให้เกิดผลลัพธ์ที่ดีที่สุดสำหรับฮาร์ดแวร์ของคุณ ดีฟอลต์ = Autodetection ความเร็วของสื่อบันทึกที่ระบุความเร็วในโหมด duplex ของอีเทอร์เน็ตอะแดปเตอร์ เลือก Autodetection ยกเว้นว่าคุณมีข้อกำหนดในการระบุความเร็วสื่อบันทึกแบบคงที่ อุปกรณ์ใดๆ ที่เชื่อมต่อกับ FSP (สวิตช์/HMC) ต้องมีการตั้งค่าเป็นโหมด อัตโนมัต (ความเร็ว) / อัตโนมัต (ดูเพล็กซ์) เนื่องจากเป็นค่าติดตั้ง FSP ดีฟอลต์และไม่สามารถเปลี่ยนได้

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

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเน็ตเวิร์กแบบเปิดและเน็ตเวิร์กส่วนตัว โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC” ในหน้า 6

	eth0	eth1	eth2	eth3
ระบุเน็ตเวิร์กแบบ ส่วน ตัว หรือ เปิด สำหรับแอด อะแดปเตอร์				

Dynamic Host Configuration Protocol (DHCP) มีวิธีอัตโนมัติสำหรับการตั้งค่าคอนฟิกไคลเอนต์แบบไดนามิก คุณสามารถระบุ HMC นี้เป็นเซิร์ฟเวอร์ DHCP ถ้าเป็น HMC เครื่องแรกหรือเครื่องเดียวบนเน็ตเวิร์กส่วนตัว ให้เปิดใช้งาน HMC เป็นเซิร์ฟเวอร์ DHCP เมื่อคุณทำสิ่งนี้ ระบบที่ถูกจัดการบนเน็ตเวิร์ก จะถูกตั้งค่าและค้นพบโดย HMC โดยอัตโนมัติ

สำหรับฮอเทอร์เน็ตอะแดปเตอร์ที่ระบุ เป็นเน็ตเวิร์กส่วนตัว ให้ดำเนินการตามตารางต่อไปนี้:

	eth0	eth1
คุณต้องการระบุ HMC นี้เป็นเซิร์ฟเวอร์ DHCP หรือไม่? (ใช่/ไม่ใช่)		
หาก "ใช่" ให้บันทึกช่วง IP แอดเดรสที่คุณต้องการใช้		

สำหรับฮอเทอร์เน็ตอะแดปเตอร์ที่ระบุเป็นเน็ตเวิร์ก เปิดให้ดำเนินการตามตารางต่อไปนี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ อินเทอร์เน็ตโปรโตคอลเวอร์ชันอื่น โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 10

การใช้ IPv6

หากคุณกำลังใช้ IPv6 ให้ปรึกษากับผู้บริหารเน็ตเวิร์กของคุณ แล้วเลือกวิธีที่คุณต้องการใช้รับ IP แอดเดรส หลังจากนั้น ให้ดำเนินการตาม ตารางต่อไปนี้:

	eth0	eth1	eth2	eth3
คุณกำลังใช้ IP แอดเดรสที่มีการกำหนดไว้อย่างคงที่ใช่หรือไม่? หากใช่ ให้บันทึกแอดเดรสนั้นไว้ที่นี่				

	eth0	eth1	eth2	eth3
คุณกำลังรับ IP แอดเดรสจากเซิร์ฟเวอร์ DHCP ใช่หรือไม่? (ใช่/ไม่ใช่)				

	eth0	eth1	eth2	eth3
คุณกำลังรับ IP แอดเดรสจากเราเตอร์ IPv6 ใช่หรือไม่?				

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า IPv6 address โปรดดูที่ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 70 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ IPv6 แอดเดรสเท่านั้น โปรดดูที่ “การใช้ IPv6 แอดเดรสเท่านั้น” ในหน้า 71

การใช้ IPv4

ดำเนินการตามตารางต่อไปนี้สำหรับฮอเทอร์เน็ตอะแดปเตอร์ที่ระบุเป็น เน็ตเวิร์กเปิดโดยใช้ IPv4

	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)				
ถ้า ใช่ แสดงรายการแอปพลิเคชัน และ IP แอดเดรสที่ควรจะผ่านไฟร์วอลล์ได้:				

ข้อมูล TCP/IP

ต้องใช้แอดเดรส TCP/IP ที่ไม่ซ้ำกันสำหรับแต่ละโหนด ทั้งสำหรับ Support Element (SE) และ Hardware Management Console (HMC) โดย network mask ที่กำหนด จะถูกใช้ในการสร้างแอดเดรสที่ไม่ซ้ำกัน ตามค่าดีฟอลต์ สำหรับ LAN ส่วนตัวแบบโลคัล ถ้า โหนดจะถูกเชื่อมต่อกับเน็ตเวิร์กขนาดใหญ่ที่มีแอดเดรส TCP/IP ที่ถูกจัดการ คุณสามารถระบุแอดเดรส TCP/IP ที่จะใช้ ระบบจะสร้าง ค่าดีฟอลต์

ค่าติดตั้งไฟร์วอลล์

ค่าติดตั้งไฟร์วอลล์ HMC จะสร้างเครื่องกีดกันด้านความปลอดภัยที่อนุญาตหรือปฏิเสธ การเข้าถึงเน็ตเวิร์กแอปพลิเคชันที่เฉพาะเจาะจงบน HMC คุณสามารถระบุ ค่าติดตั้งการควบคุมเหล่านี้สำหรับฟิลิคัลเน็ตเวิร์กอินเทอร์เน็ตแต่ละชุด ซึ่งทำให้ คุณสามารถควบคุมว่าเน็ตเวิร์กอินเทอร์เน็ต HMC ใดจะสามารถเข้าถึงไต่บนแต่ละเน็ตเวิร์ก

ถ้าคุณได้ตั้งค่าอย่างน้อยหนึ่งอะแดปเตอร์เป็น เน็ตเวิร์กอะแดปเตอร์แบบเปิด คุณจะต้องจัดหาข้อมูลเพิ่มเติมต่อไปนี้เพื่อให้ HMC ของคุณสามารถเข้าถึง LAN:

ข้อมูลโฮสต์แบบโลคัล	
ชื่อโฮสต์ HMC:	

ข้อมูลโฮสต์แบบโลคัล	
โดเมนเนม:	
รายละเอียดของ HMC:	
ข้อมูลเกตเวย์	
แอดเดรสเกตเวย์: (nnn.nnn.nnn.nnn)	
อุปกรณ์เกตเวย์:	
การเปิดใช้ DNS	
คุณต้องการใช้ DNS หรือไม่? (ใช่/ไม่ใช่)	
หากตอบ “ใช่” ให้ระบุลำดับการค้นหาเซิร์ฟเวอร์ DNS ที่ด้านล่างนี้:	
1.	
2.	
ลำดับการค้นหาโดเมนซัพพลาย:	
1.	
2.	

ข้อมูลโฮสต์แบบโลคัล

เมื่อต้องการระบุ Hardware Management Console (HMC) ให้กับเน็ตเวิร์ก ให้ป้อนชื่อโฮสต์และโดเมนเนมของ HMC นอกจากนี้คุณยังใช้เฉพาะชื่อโฮสต์แบบย่อ บนเน็ตเวิร์กของคุณเท่านั้น ให้ป้อนชื่อโฮสต์แบบเต็ม ตัวอย่างโดเมนเนม: name.yourcompany.com

ข้อมูลเกตเวย์

เมื่อต้องการกำหนดเกตเวย์ดีฟอลต์ให้ใส่แอดเดรส TCP/IP ที่จะใช้สำหรับการเรดแพ็กเก็ต IP แอดเดรสเกตเวย์จะแจ้งคอมพิวเตอร์แต่ละเครื่องหรืออุปกรณ์ เน็ตเวิร์กแต่ละอุปกรณ์ว่าจะส่งข้อมูลเมื่อใด ถ้าสถานีเป้าหมายไม่ได้ระบุให้เน็ตเวิร์กย่อยเป็นต้นทาง

การเปิดใช้ DNS

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

ลำดับการค้นหาเซิร์ฟเวอร์ DNS

ป้อน IP แอดเดรสของเซิร์ฟเวอร์ DNS ที่จะถูกค้นหา สำหรับการแมปชื่อโฮสต์ และ IP แอดเดรส ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

ลำดับการค้นหาโดเมนซัพพลาย

ป้อนโดเมนซัพพลายที่คุณกำลังใช้ HMC จะใช้โดเมนซัพพลายเพื่อผนวกเข้ากับชื่อที่ไม่ถูกต้องสำหรับการค้นหา DNS ซัพพลายจะถูกค้นหา ตามลำดับที่แสดงอยู่ในรายการ ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

การแจ้งเตือนทางอีเมล

ลิสต์ข้อมูลติดต่อทางอีเมล ถ้าคุณต้องการได้รับแจ้งทางอีเมล เมื่อ เกิดปัญหาเกี่ยวกับฮาร์ดแวร์กับระบบของคุณ

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 เป็นโปรโตคอลที่ใช้ในการส่งอีเมล เมื่อใช้ SMTP ไคลเอ็นต์จะส่งข้อความและสื่อสาร กับเซิร์ฟเวอร์ SMTP โดยใช้โปรโตคอล SMTP

ถ้า คุณไม่ทราบแอดเดรส SMTP ของเซิร์ฟเวอร์ของคุณ หรือไม่แน่ใจ ให้ติดต่อ ผู้บริหารเน็ตเวิร์กของคุณ

พอร์ต พิมพ์หมายเลขพอร์ตของเซิร์ฟเวอร์ที่จะรับแจ้งเกี่ยวกับเหตุการณ์ของระบบ หรือ ใช้พอร์ตดีฟอลต์

อีเมลแอดเดรสที่จะรับแจ้ง

ป้อนอีเมลแอดเดรสที่ตั้งค่าให้รับข้อความแจ้งเตือน เมื่อเกิดเหตุการณ์ของระบบ

- เลือก Only call-home problem events เพื่อรับ การแจ้งเตือนเฉพาะในกรณีที่เกิดเหตุการณ์ที่สร้างฟังก์ชัน call-home
- เลือก All problem events เพื่อรับการแจ้งเตือน เมื่อเกิดเหตุการณ์ใดๆ

ข้อมูลติดต่อฝ่ายบริการ

ชื่อบริษัท	
ชื่อผู้ดูแล	
อีเมลแอดเดรส	
หมายเลขโทรศัพท์	
หมายเลขโทรศัพท์อื่น	
หมายเลขโทรสาร	
หมายเลขโทรสารอื่น	

ที่อยู่	
ที่อยู่ 2	
เมืองหรือเขต	
สถานะ	
รหัสไปรษณีย์	
ประเทศหรือภูมิภาค	
ตำแหน่งของ HMC (ถ้าเหมือนกับที่อยู่ของผู้ดูแลระบบข้างต้น ให้ระบุ “same”):	
ที่อยู่	
ที่อยู่ 2	
เมืองหรือเขต	
สถานะ	
รหัสไปรษณีย์	
ประเทศหรือภูมิภาค	

การให้สิทธิและการเชื่อมต่อส่วนบริการ

เลือก ประเภทของการเชื่อมต่อเพื่อติดต่อผู้ให้บริการของคุณ สำหรับรายละเอียด ของวิธีการเหล่านี้ รวมทั้งลักษณะด้านความปลอดภัยและข้อกำหนดการตั้งค่าคอนฟิก โปรดดูที่ “การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 8

- _____ Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต
- _____ เรียกเลขหมายจาก HMC แบบโลคัล
- _____ Virtual private network (VPN) ผ่านอินเทอร์เน็ต

Secure Sockets Layer (SSL) ผ่านอินเทอร์เน็ต:

ถ้าคุณมีการเชื่อมต่ออินเทอร์เน็ตจาก HMC ของคุณ คุณสามารถใช้ การเชื่อมต่อดังกล่าวเพื่อติดต่อผู้ให้บริการ คุณ สามารถเชื่อมต่อโดยตรงกับผู้ให้บริการ ของคุณ โดยใช้ Secure Sockets Layer (SSL) แบบเข้ารหัส ซึ่งใช้การเชื่อมต่อ อินเทอร์เน็ตที่มีอยู่ เลือก ใช้ฟรีอ็อกซี SSL ถ้าคุณต้องการกำหนดคอนฟิกการใช้ SSL ที่เข้ารหัส โดยใช้การเชื่อมต่อ ทางอ้อมซึ่งใช้ฟรีอ็อกซี SSL

ใช้ฟรีอ็อกซี SSL? (ใช่/ไม่ใช่)	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
แอดเดรส:	
พอร์ต:	

พิสูจน์ตัวตนด้วยพรีอ็อกซี SSL?	
ถ้าใช่ แสดงรายการข้อมูลด้านล่าง:	
ผู้ใช้:	
รหัสผ่าน:	

โปรโตคอลการเชื่อมต่ออินเทอร์เน็ตที่ใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอินเทอร์เน็ตโปรโตคอลอื่น โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 10

___ IPv4

___ IPv6

___ IPv4 และ IPv6

เรียกเลขหมายจาก HMC แบบโลคัล

ป้อนข้อมูลเรียกเลขหมาย เพื่อตั้งค่าโลคัลโมเด็มของคุณ ระบุหมายเลขโทรศัพท์ที่ใช้ในการต่อเลขหมายไปยังผู้ให้บริการ เมื่อคุณกำลังเชื่อมต่อ หมายเลขโทรศัพท์จะถูกต่อเลขหมายตามลำดับที่ แสดงในรายการ

คำแนะนำสำหรับต่อเลขหมาย: _____

Tone: _____

Pulse: _____

รอเสียงสัญญาณ? _____

เปิดใช้งานลำโพง? _____

Virtual Private Network (VPN)

ถ้าคุณมีการเชื่อมต่ออินเทอร์เน็ตจาก HMC ของคุณ คุณสามารถใช้การเชื่อมต่อดังกล่าวเพื่อติดต่อผู้ให้บริการ คุณสามารถเชื่อมต่อโดยตรงกับผู้ให้บริการของคุณ โดยใช้ virtual private network (VPN) ซึ่งใช้การเชื่อมต่ออินเทอร์เน็ตที่มีอยู่

หมายเหตุ: ถ้าคุณเลือก Virtual Private Network (VPN) ผ่านอินเทอร์เน็ต คุณจะไม่สามารถเลือก ออฟชั่นอื่นใด

เซิร์ฟเวอร์ Call-home

กำหนดว่า HMC ใดที่คุณต้องการคอนฟิกเพื่อให้เชื่อมต่อกับฝ่ายสนับสนุนและบริการเป็นเซิร์ฟเวอร์ Call-Home สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เซิร์ฟเวอร์ Call-Home หลายๆ เซิร์ฟเวอร์ โปรดดูที่ “การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์” ในหน้า 13

___ HMC นี้

___ HMC อื่น

หากคุณสามารถตรวจสอบ HMC อื่น ให้แสดงรายการ HMC อื่นที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home ที่นี้:

รายชื่อโฮสต์ HMC หรือ IP แอดเดรส ที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home

คุณสมบัติเพิ่มเติมสำหรับการสนับสนุน

My Systems และ Premium Search

แสดงรายการ IBM ID ของ _____

คุณ

แสดง IBM ID เพิ่มเติม _____

เพื่อเข้าถึงข้อมูลการสนับสนุนที่มีคุณค่าและกำหนดเองในส่วนระบบของเงินและการค้นหาแบบพิเศษของเว็บไซต์ Electronic Services ลูกค้าต้องลงทะเบียน IBM ID ของลูกค้าด้วยระบบนี้ ถ้าคุณยังไม่มี คุณสามารถลงทะเบียนสำหรับ IBM ID ได้ที่: www.ibm.com/account/profile

หมายเหตุ: IBM จัดเตรียมฟังก์ชันสำหรับเว็บที่ต้องการทำให้เป็นส่วนตัว ซึ่งใช้ข้อมูลที่เก็บรวบรวมโดยแอปพลิเคชัน IBM Electronic Service Agent™ เพื่อใช้ฟังก์ชันเหล่านี้ คุณต้องลงทะเบียนบนเว็บไซต์ IBM Registration ก่อนที่ <http://www.ibm.com/account/profile>

เมื่อต้องการอนุญาตให้ผู้ใช้สามารถใช้ข้อมูล Electronic Service Agent เพื่อกำหนดเว็บฟังก์ชันเป็นส่วนบุคคล ให้ป้อน IBM ID ที่คุณได้ลงทะเบียนไว้บนเว็บไซต์ IBM Registration ไปที่ <http://www.ibm.com/support/electronic> the valuable เพื่อดูข้อมูลการสนับสนุนที่มีประโยชน์ซึ่งพร้อมใช้งานสำหรับลูกค้าที่ลงทะเบียน IBM ID ไว้กับระบบ

การตั้งค่า HMC

คุณต้องตั้งค่าฮาร์ดแวร์ HMC ก่อนตั้งค่าซอฟต์แวร์ HMC ศึกษาเพิ่มเติมเกี่ยวกับการตั้งค่า HMC ที่มีดิสก์หรือ HMC ที่ติดตั้งล่วงหน้า

การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อโลน

วางตำแหน่ง HMC และวางสายเคเบิลให้กับส่วนประกอบฮาร์ดแวร์แต่ละชิ้น

ถ้า HMC ถูกใช้เพื่อจัดการกับระบบ POWER7 แบบอิงโปรเซสเซอร์ใดๆ HMC ต้องเป็น C05 หรือรุ่นใหม่กว่า ซึ่งเป็น HMC แบบสแตนด์อโลน

1. ตรวจสอบให้แน่ใจว่า คุณวาง HMC ไว้ในตำแหน่งที่ต้องการ

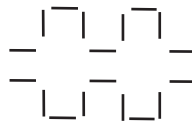
2. ติดตั้งสายเคเบิลมอเนเตอร์เข้ากับตัวเชื่อมต่อมอเนเตอร์, แล้วไขสกรูให้แน่น
3. ติดตั้งสายไฟเข้ากับมอเนเตอร์
4. ตรวจสอบให้แน่ใจว่า สวิตช์เลือกแรงดันไฟบน HMC ถูกตั้งค่าให้เป็นแรงดันไฟที่ใช้ในภูมิภาคของคุณ สวิตช์เลือกแรงดันไฟฟ้าจะเป็นสีแดง และอยู่ใกล้กับตัวเชื่อมต่อไฟฟ้า ขยับสวิตช์เพื่อแสดงแรงดันไฟที่ใช้ในตำแหน่งของคุณ
5. เสียบปลั๊กสายไฟเข้ากับ HMC
6. เชื่อมต่อคีย์บอร์ดและเมาส์เข้ากับ HMC
7. เชื่อมต่อกับโมเด็มเสริม:

หมายเหตุ: ในระหว่างการติดตั้ง และกำหนดคอนฟิกของ HMC โมเด็มอาจต่อเลขหมายอัตโนมัติตามขั้นตอน การ call-out ของ HMC ซึ่งถือเป็นพฤติกรรมปกติ

ถ้าคุณกำลัง เชื่อมต่อโมเด็มภายนอก ให้ปฏิบัติตามดังนี้:

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่นเพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM

- a. หากคุณยังไม่ได้ดำเนินการให้เชื่อมต่อสายเคเบิลข้อมูลของโมเด็มเข้ากับโมเด็มภายนอกของ HMC
- b. เชื่อมต่อสายเคเบิลข้อมูลเข้ากับพอร์ตระบบบน HMC ซึ่งมีเลเบลที่เป็นสัญลักษณ์ต่อไปนี้:

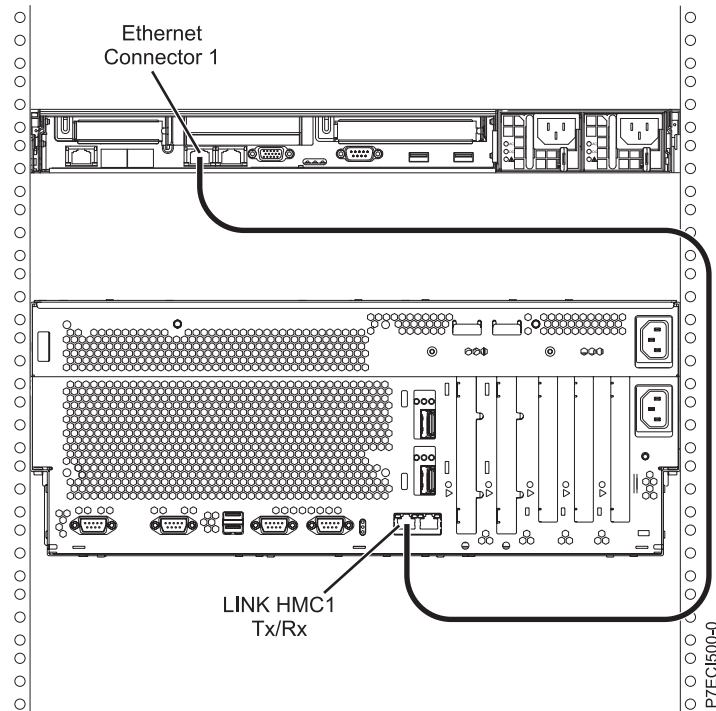


IPHA1522-0

- c. ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตของโมเด็มภายนอกเข้ากับปลั๊กโทรศัพท์แบบอนาล็อกบนผนัง
- หากคุณกำลังเชื่อมต่อกับโมเด็มภายใน ให้ใช้สายเคเบิลข้อมูลเพื่อเชื่อมต่อโมเด็มภายในของ HMC กับแหล่งข้อมูลที่เหมาะสม ตัวอย่างเช่น ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตโมเด็มของ HMC เข้ากับปลั๊กอนาล็อกบนผนังของคุณ

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่นเพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM

8. หากระบบที่จัดการได้รับการติดตั้งแล้ว คุณสามารถตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแอคทีฟอยู่หรือไม่โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่จัดการในขณะที่ขั้นตอนติดตั้งกำลังดำเนินไป
9. เชื่อมต่อ ตัวเชื่อมต่ออีเทอร์เน็ต 1 บน HMC กับพอร์ต LINK HMC1 บนระบบที่จัดการ



10. ถ้าคุณกำลังเชื่อมต่อกับ HMC สำรองกับเซิร์ฟเวอร์ที่ถูกจัดการให้เชื่อมต่อพอร์ตอีเทอร์เน็ตที่มีเลเบล **LINK HMC2** บนเซิร์ฟเวอร์ที่ถูกจัดการ
11. หากคุณใช้โมเด็มภายนอกให้เสียบสายตัวจ่ายไฟของโมเด็มเข้ากับโมเด็ม HMC
12. เสียบปลั๊กสายไฟสำหรับมอเตอร์ HMC และโมเด็มภายนอกของ HMC เข้ากับช่องเสียบระบบไฟฟ้า หากคุณกำลังเชื่อมต่อ HMC นี้กับระบบที่ถูกจัดการใหม่ ไม่ต้องเชื่อมต่อระบบที่ถูกจัดการเข้ากับแหล่งกำเนิดไฟฟ้าในเวลานี้

จากนั้นคุณจะต้องตั้งค่าซอฟต์แวร์ HMC ดำเนินการต่อด้วย “การกำหนดคอนฟิก HMC” ในหน้า 61

หลักการที่เกี่ยวข้อง:

“การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 8

ศึกษาเพิ่มเติมเกี่ยวกับข้อพจน์ของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

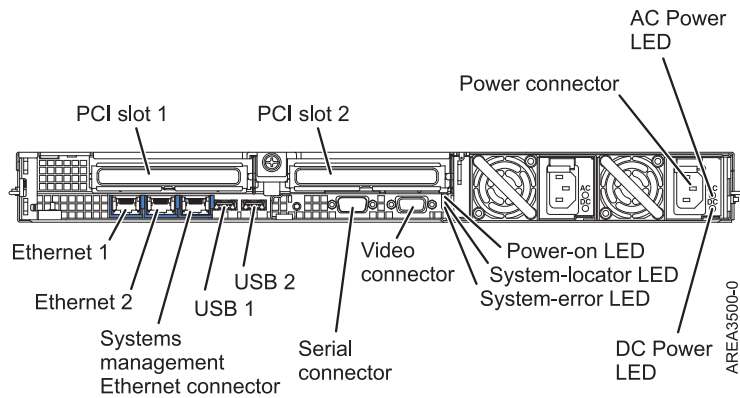
“การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 4

การติดตั้ง 7310-CR4 HMC ลงในชั้นวาง

ส่วนนี้อธิบายถึงวิธีการติดตั้ง 7310-CR4 HMC ลงในชั้นวาง นี่คืองานของลูกค้า

ถ้า HMC ถูกนำมาใช้เพื่อจัดการกับระบบ POWER7 แบบอิงโพรเซสเซอร์ใดๆ HMC ต้องเป็น CR3 หรือรุ่นใหม่กว่า ซึ่งเป็นโมเดล HMC ที่ประกอบเข้ากับชั้นวาง

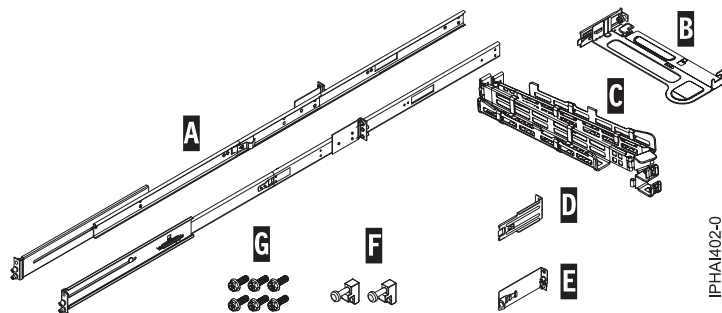
ต่อไปนี้เป็นด้านหลังของ 7310-CR4:



รูปที่ 1. ด้านหลังของ 7310-CR4

เมื่อต้องการติดตั้ง 7310-CR4 HMC ลงในชั้นวางให้ทำตามขั้นตอนต่อไปนี้:

1. ทำรายการชิ้นส่วนให้เสร็จสิ้น โปรดดูที่ ทำรายการชิ้นส่วนให้เสร็จสิ้น
2. ค้นหาตำแหน่งชุดฮาร์ดแวร์ที่ประกอบเข้ากับชั้นวาง และชุดรางของระบบ ซึ่งประกอบด้วยยูนิตรบบของคุณ



รูปที่ 2. ชุดราง

ตารางที่ 6. ชิ้นส่วนของชุดราง

ชิ้นส่วนของชุดรางแบบสไลด์

A รางแบบสไลด์

B จานที่ประกอบเข้ากับแขนยึดสายเคเบิล

C แขนยึดสายเคเบิล

D แท่นยึดสายเคเบิล

E สายเคเบิลที่สนับสนุนแท่นยึดและแท็บความปลอดภัย

F แลตซ์ (2)

G สกรู (6)

สำคัญ: ยูนิตรบบนี้เป็นยูนิต 1 EIA แบบสูง คุณอาจต้องการข้อมูลนี้เพื่อทำการติดตั้งให้เสร็จสิ้น

การทำให้รายการชิ้นส่วนให้เสร็จสิ้น

คุณอาจต้องการทำการรายการชิ้นส่วนให้เสร็จสิ้น ใช้โปรซีเดอร์ในส่วนนี้เพื่อปฏิบัติงานนี้

หากคุณยังไม่ได้ทำให้ทำการรายการชิ้นส่วนให้เสร็จสิ้น ก่อนที่จะดำเนินการติดตั้ง:

1. หาตำแหน่งรายงานชุดเครื่องมือในกล่องอุปกรณ์
2. ตรวจสอบให้แน่ใจว่า คุณได้รับชิ้นส่วนทุกชิ้นที่คุณได้สั่งซื้อ

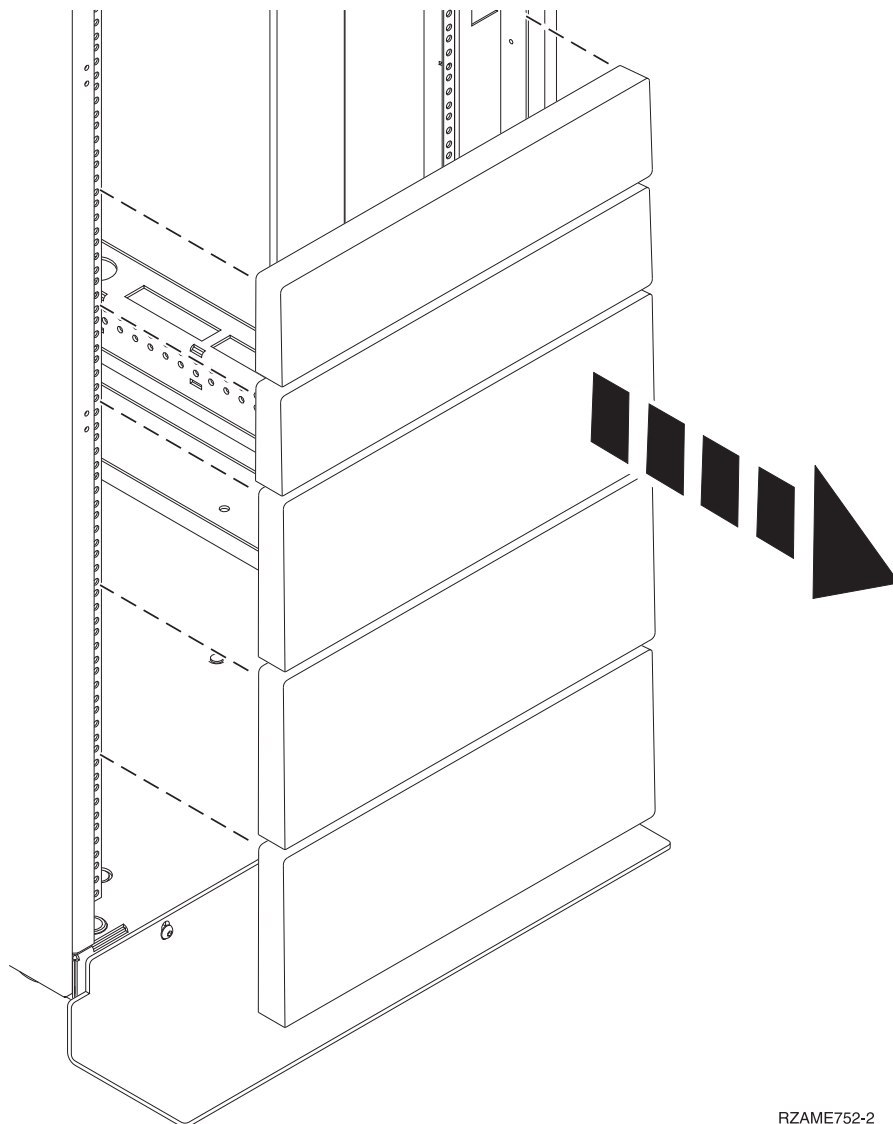
ถ้าชิ้นส่วนไม่ถูกต้อง หายไป หรือเสียหาย ให้ติดต่อผู้ขายของ IBM หรือฝ่ายขายและสนับสนุนของ IBM

การกำหนดตำแหน่ง

คุณอาจต้องการกำหนดตำแหน่งที่จะติดตั้งระบบ ในชั้นวาง ส่วนนี้ประกอบด้วยโปรซีเดอร์ที่คุณสามารถทำงานเหล่านี้ได้

ก่อนที่จะติดตั้ง HMC ลงในชั้นวาง ปฏิบัติตามขั้นตอนต่อไปนี้จะเสร็จสิ้น:

1. วางแผนสถานที่ที่คุณจะวางยูนิต วางยูนิตที่ใหญ่และหนักกว่า ในส่วนล่างของชั้นวาง
2. ถ้าชั้นวางมีแผงฟิลเลอร์ให้ถอดแผงฟิลเลอร์ออกเพื่อให้เข้าถึงด้านในของชั้นวางที่คุณวางแผน ที่จะวางยูนิต



RZAME752-2

รูปที่ 3. การถอดแผงฟิลเลอร์

3. ถอดประตูด้านหน้าและด้านหลังออก หากจำเป็น
4. ทำตามคำสั่งสำหรับการทำเครื่องหมายตำแหน่งโดยไม่มีเท็มเพลต โปรดดูที่ การทำเครื่องหมายตำแหน่งโดยไม่มีเท็มเพลตที่ประกอบเข้ากับชั้นวาง

การทำเครื่องหมายตำแหน่งโดยไม่มีเท็มเพลตประกอบเข้ากับชั้นวาง:

คุณสามารถทำเครื่องหมายตำแหน่งโดยไม่มีเท็มเพลต

เท็มเพลตที่ประกอบเข้ากับชั้นวางไม่ได้ประกอบเข้ากับระบบนี้ ระบบเหล่านี้คือยูนิต 1 EIA แบบสูง

เมื่อต้องการกำหนดตำแหน่งการประกอบเข้า ให้ปฏิบัติตามขั้นตอนเหล่านี้:

1. กำหนดที่จะวางระบบในชั้นวาง บันทึกตำแหน่ง EIA

หมายเหตุ: ยูนิต EIA บนชั้นวางของคุณประกอบด้วยกลุ่มของรูสามรู

2. หันด้านหน้าของชั้นวางและทำงานจากด้านขวา จุดยึดเหนี่ยวที่อยู่ถัดจากรูด้านบนสุดของยูนิต EIA

หมายเหตุ: จุดยึดเหนี่ยวจะถูกใช้เพื่อวัตถุประสงค์ในการระบุตำแหน่งบนชั้นวาง ถ้าคุณไม่มีจุดใดๆ ให้ใช้รูปแบบอื่นๆ ของเครื่องมือที่ใช้ทำเครื่องหมายเพื่อวัตถุประสงค์ในการระบุตำแหน่งรู (ตัวอย่างเช่น เทป ตัวทำเครื่องหมาย หรือดินสอ) ถ้าคุณกำลังติดตั้งรางแบบสไลด์ให้วางเครื่องหมายหรือจุดยึดเหนี่ยวที่ตำแหน่งด้านล่างและกึ่งกลางของยูนิต EIA แต่ละยูนิต

3. วางจุดยึดเหนี่ยวอื่นๆ ถัดจากรูด้านล่างของ ยูนิต EIA ข้างต้น

หมายเหตุ: ถ้าคุณกำลังนับรูให้เริ่มต้นด้วยรูที่ระบุโดยจุดแรกและนับไปอีกสองรู วางจุดที่สองให้อยู่ถัดจากรูที่สาม

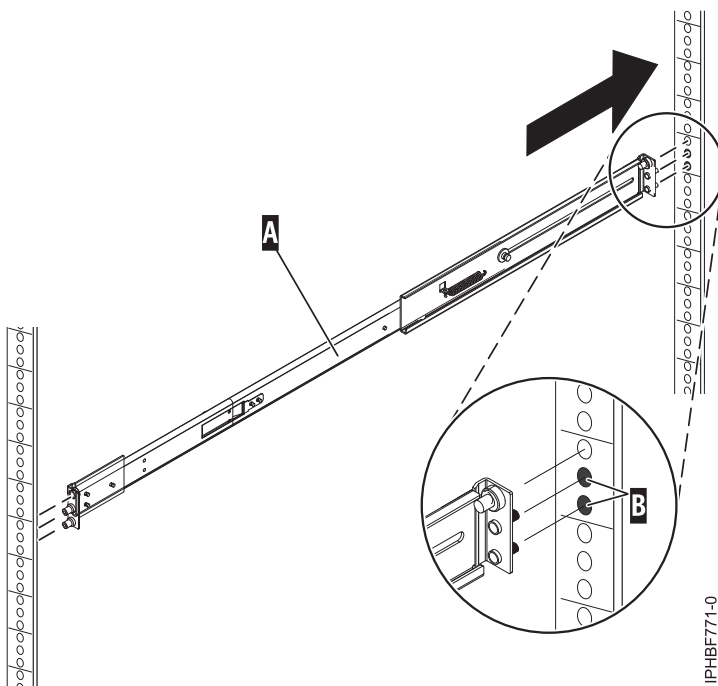
4. ทำซ้ำขั้นตอน 1 ในหน้า 37 สำหรับ รูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
5. ไปที่ด้านหลังของชั้นวาง
6. ที่ด้านขวา ให้หา ยูนิต EIA ที่ตรงกับยูนิต EIA ด้านล่างซึ่งทำเครื่องหมายอยู่บนด้านหน้าของชั้นวาง
7. วางจุดยึดเหนี่ยวที่ด้านล่างของยูนิต EIA
8. วางจุดยึดเหนี่ยวที่รูด้านบนสุดของยูนิต EIA
9. ทำเครื่องหมายที่รูทางด้านซ้ายของชั้นวาง

การติดตั้งรางแบบสไลด์ในชั้นวาง

เมื่อต้องการติดตั้งรางแบบสไลด์ในชั้นวาง ให้ปฏิบัติตามขั้นตอนต่อไปนี้

เมื่อต้องการ ติดตั้งรางแบบสไลด์ในชั้นวาง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

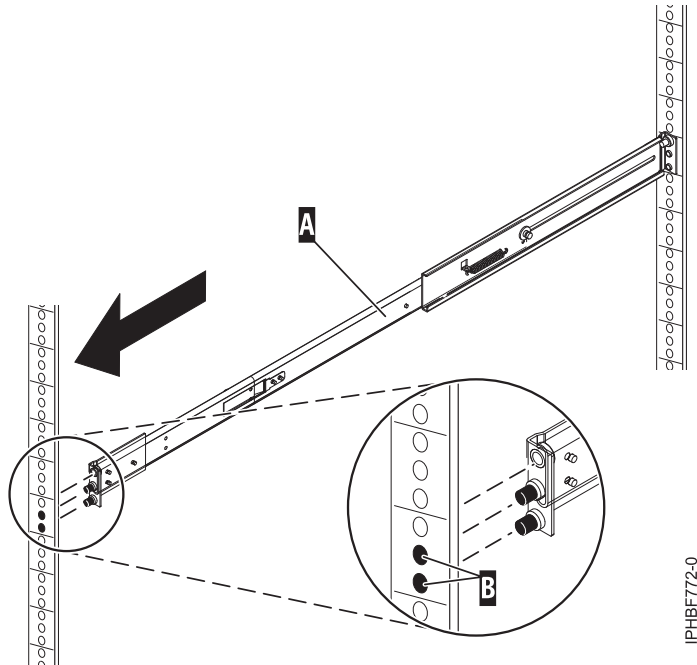
1. ใส่รางแบบสไลด์ด้านขวา (A) ที่มีเครื่องหมาย right (ขวา), เข้ากับหน้าแปลนที่ประกอบเข้ากับชั้นวางในตำแหน่ง (B) ที่ด้านหลังขวาของชั้นวาง ขั้วของรางสองขั้วจะยื่นผ่านรู (B) ที่อยู่ด้านล่างและตรงกลางบนยูนิต EIA



IPHBF771-0

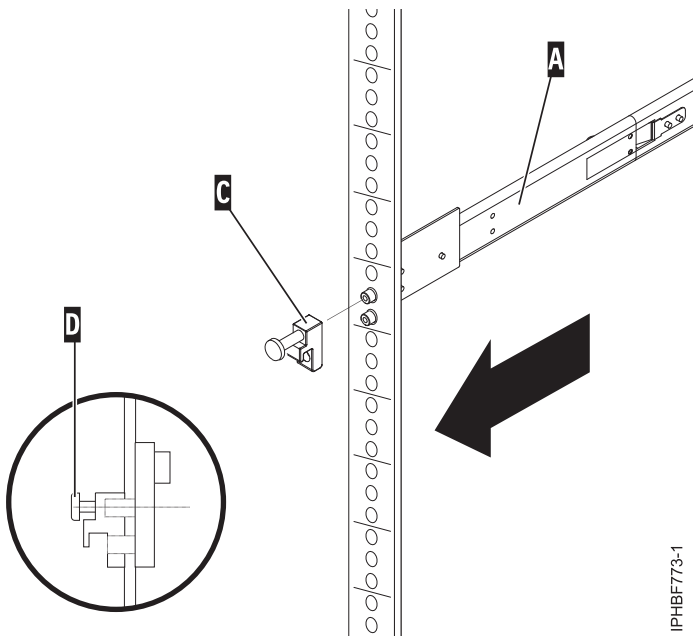
รูปที่ 4. การติดตั้งรางแบบสไลด์ที่ด้านหลังของชั้นวาง

2. ผลักที่ส่วนท้ายของชั้นวาง (A) เพื่อดันกลไกสปริงโหลตของราง และใส่รางลงในหน้าแปลนติดตั้งในตำแหน่ง (B) ทางด้านขวาของชั้นวาง รางจะคลายและขั้วของรางสองขั้วจะยื่นผ่านรู (B) ที่อยู่ด้านล่างและตรงกลางบนยูนิต EIA



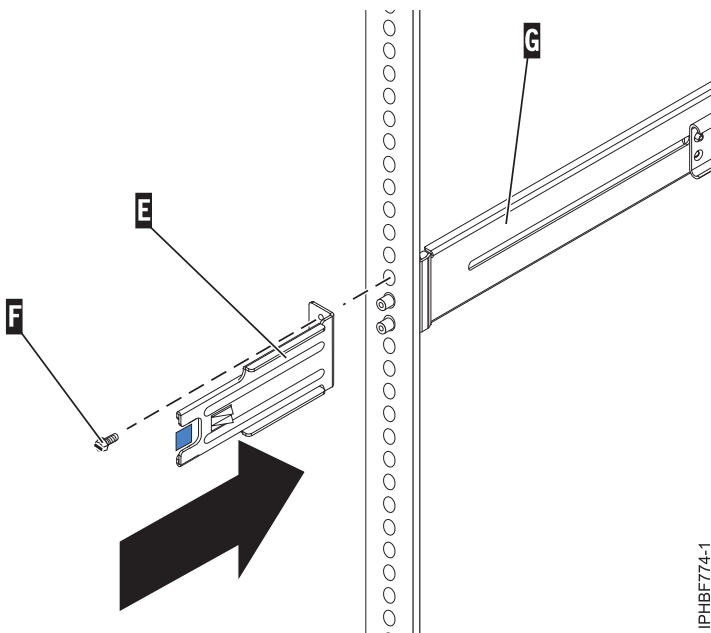
รูปที่ 5. การติดตั้งรางแบบสไลด์ด้านขวาที่ด้านหน้าของชั้นวาง

3. ทำซ้ำขั้นตอน 1 ในหน้า 38-2 เพื่อติดตั้ง รางแบบสไลด์ด้านซ้ายที่มีเครื่องหมาย *left* (ซ้าย) ลงในชั้นวาง
4. จากด้านหน้าของชั้นวาง ให้วางแลตซ์ (C) ไว้บนขั้ว ใช้มือหมุนสกรู (D) ลงในขั้วด้านบนของรางแบบสไลด์ด้านหน้าขวา (A)



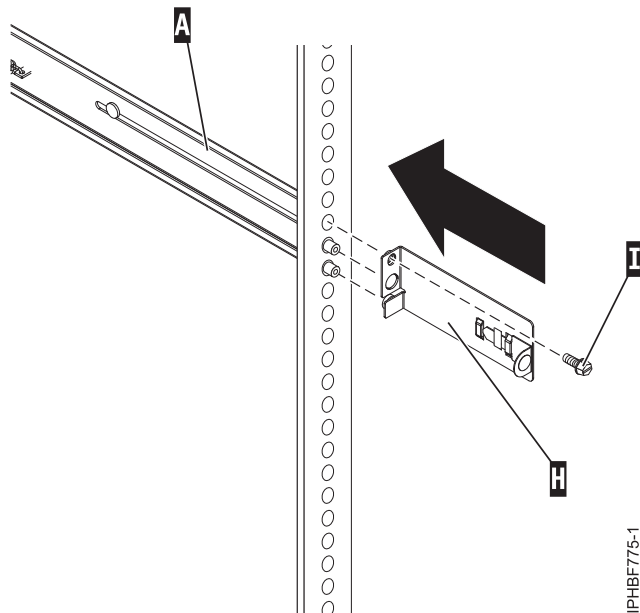
รูปที่ 6. การติดตั้งแลตซ์ที่ด้านหน้าของราง

5. ทำซ้ำขั้นตอนก่อนหน้านี้เพื่อติดตั้งแลตซ์บนรางแบบสไลด์ที่ด้านหน้าซ้าย
6. ย้ายไปยังด้านหลังของชั้นวาง ไส้กรู (F) ให้แน่นเพื่อยึดแท่นยึดที่ต่ออยู่กับแขนยึดสายเคเบิล (E) เข้ากับด้านหลังของรางด้านซ้าย (G)



รูปที่ 7. การยึดแท่นยึดสายเคเบิลเข้ากับรางด้านหลังซ้าย

7. ถ้าคุณไม่มีแผนที่จะย้ายระบบนี้ให้ดำเนินการต่อด้วย “การติดตั้ง HMC บนรางแบบสไลด์” ถ้าคุณ มีแผนที่จะเคลื่อนย้ายระบบนี้ ให้ใส่สกรู (I) เพื่อยึด แขนยึดสายเคเบิลที่รองรับแท่นยึด (H) เข้ากับ ด้านหลังขวาของราง (A) ไขสกรูให้แน่น แขนยึดสายเคเบิลที่รองรับแท่นยึด สามารถนำมาใช้เพื่อยึดแขนยึดสายเคเบิลในระหว่างการขนส่งได้ ถ้ากลไกถูกยึดหลังจากที่ติดตั้งแขนยึดสายเคเบิล คุณจะไม่สามารถเลื่อนระบบจากชั้นวางได้



รูปที่ 8. การยึด สายเคเบิลที่รองรับแท่นยึดกับรางด้านหลังขวา

การติดตั้ง HMC บนรางแบบสไลด์

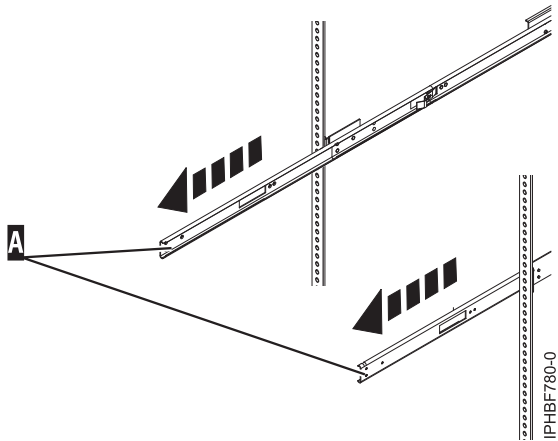
คุณอาจต้องการติดตั้ง HMC บนรางแบบสไลด์ใช้โปรซีเดอร์ในส่วนนี้เพื่อปฏิบัติงานนี้

ก่อนการติดตั้ง HMC บนรางแบบสไลด์โปรดแน่ใจว่า สเตบิลไลเซอร์ถูกต่อและแท่นยึดสเตบิลไลเซอร์ของชั้นวางจะถูกยึดกับชั้นวางด้านหน้าส่วนล่าง เพื่อป้องกันชั้นวางจากการตกหล่น เมื่อรางถูกดึงออกจากชั้นวาง

เมื่อต้องการ ติดตั้ง HMC บนชุดรางแบบสไลด์ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ถอด shipping bracket ที่ครอบตัวจ่ายไฟจาก ส่วนหลังทางด้านขวาของ HMC เมื่อต้องการถอด shipping bracket ให้ดัน bracket ไปทางด้านขวา และหมุน shipping bracket ออกจาก HMC
2. จากด้านหน้าของชั้นวางให้ต่อรางแบบสไลด์จนกว่ารางจะล็อกลงตามตำแหน่ง (A) ที่ได้ต่อไว้

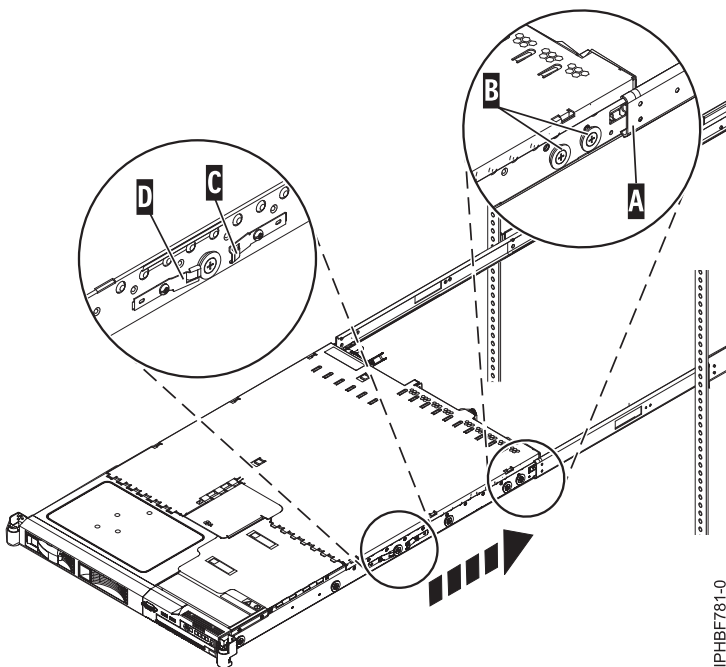
ข้อควรสนใจ: แลตซ์ที่อยู่ด้านหน้าของราง และแท่นยึดแขนยึดสายเคเบิลต้องถูกติดตั้ง ก่อน ที่จะติดตั้ง HMC บนราง ถ้าไม่ได้ติดตั้งชิ้นส่วนเหล่านี้ไว้ การติดตั้งอาจทำให้รางกดทับ และ HMC อาจตกหล่นจากชั้นวางได้



รูปที่ 9. การต่อรางแบบสไลด์

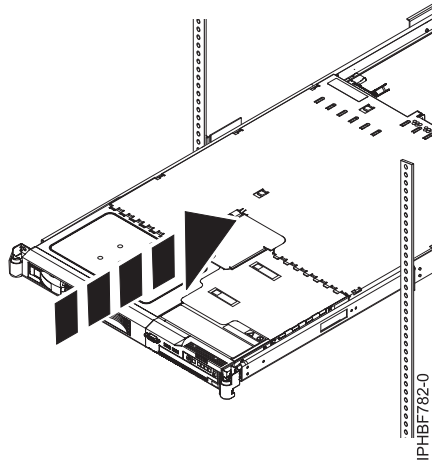
สำคัญ: ยูนิตนี้หนักประมาณ 17 กก. (37 ปอนด์) โปรดตรวจสอบให้แน่ใจว่าคุณสามารถรองรับน้ำหนักนี้ได้อย่างปลอดภัย
เมื่อวาง HMC ลงใน ชั้นวาง

3. ยก HMC ให้สูงเท่ากับราง และจัดตำแหน่งชุดของล้อ (B) ที่ด้านหลังของ HMC ระหว่างเส้นบอกแนวของราง



รูปที่ 10. การติดตั้ง HMC บนรางแบบสไลด์

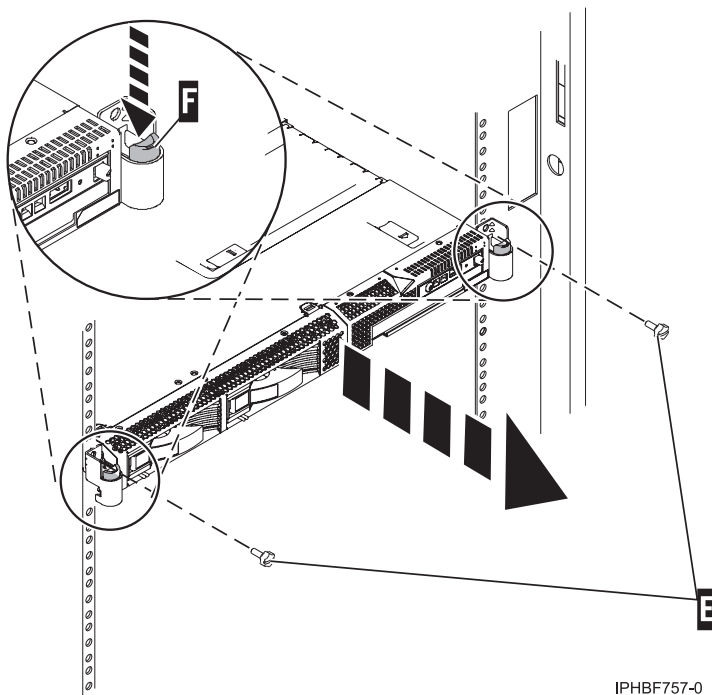
4. ผลัก HMC ลงในรางแบบสไลด์จนกระทั่งปล่อยสไลด์ (C) ล็อกเข้าที่ สิ่งนี้จะล็อกระบบในตำแหน่งการให้บริการบนสไลด์
คุณจะได้ยินเสียงคลิก
5. กดแลตช์ที่ปล่อยรางแบบสไลด์ด้านหน้า (D) ทั้งสองด้านของรางแบบสไลด์
6. เลื่อน HMC ไปยังและออกจากชั้นวาง เพื่อตรวจสอบว่า HMC เคลื่อนย้ายได้อย่างอิสระโดยไม่ถูกเชื่อมต่อ



รูปที่ 11. เลื่อน HMC เข้าในชั้นวาง

สำคัญ: ในสถานการณ์ใดๆ ห้ามกด HMC ลงในรางแบบสไลด์ ถ้า HMC ไม่เลื่อนอย่างอิสระในชั้นวาง ให้ถอด HMC ออกจากราง หลังจากที่ HMC ถูกถอดออกจากราง ให้วาง HMC ใหม่อีกครั้ง แล้วใส่ HMC ลงในรางอีกครั้ง ทำซ้ำขั้นตอนนี้จนกระทั่ง HMC เลื่อนไหลในรางได้อย่างอิสระ

7. พลัก HMC ให้เข้าที่จนกว่าແລตซ์ของราง (F) จะล็อกเข้าที่



รูปที่ 12. แลตซ์ของชั้นวางและสกรู

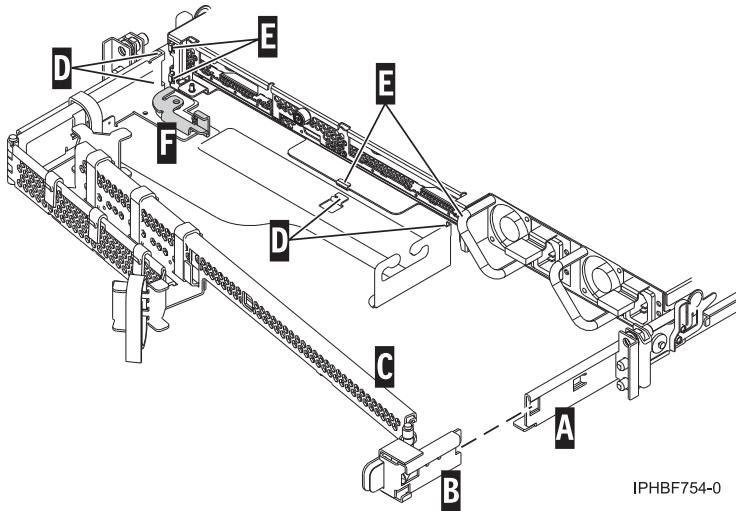
8. ขันสกรูทั้งสี่ที่ติดตั้งอยู่ที่ ด้านหน้าและด้านหลังของรางให้แน่น
9. ถ้าชั้นวางจะถูกขนส่งให้ใส่และขันสกรู (E) ของชั้นวางให้แน่น

การติดตั้งแขนยึดสายเคเบิล

คุณอาจต้องการติดตั้งแขนยึดสายเคเบิล ใช้โปรซีเดอร์ในส่วนนี้เพื่อปฏิบัติงานนี้

หากต้องการติดตั้งแขนยึดสายเคเบิล ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. จากด้านหลังของชั้นวางให้วางหน้าแปลนแขนยึดสายเคเบิล (A) ไว้บนด้านหลังของชุดรางระบบให้คงที่ (ดูจากด้านหลังของชั้นวาง)
2. ยึดแขนยึดสายเคเบิล (B) เข้ากับรางโดยผลักวงแขนไปบนรางจนกระทั่งวงแขนเข้าล็อก



รูปที่ 13. แขนยึดสายเคเบิลและยูนิตรระบบ

3. ยึดส่วนปลายสุดของแขนยึดสายเคเบิลอีกแขนหนึ่ง (C) เข้ากับด้านหลังของ HMC จัดตำแหน่งแท็บ (D) บนแขนยึดสายเคเบิลด้วยสล๊อต (E) บนด้านหลังของ HMC
4. เลื่อนแขนยึดสายเคเบิลไปยังด้านซ้าย ยึดแขนยึดสายเคเบิล ให้เข้าที่ ตรวจสอบให้แน่ใจว่า แท็บทั้งหมดอยู่ในสล๊อต
5. ผลักคันโยกสำหรับล็อก (F) ลงในตำแหน่งที่ล็อก ตรวจสอบให้แน่ใจว่า แขนยึดสายเคเบิล (C) อยู่ในระดับที่เคลื่อนที่ได้ อย่างอิสระ

การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง

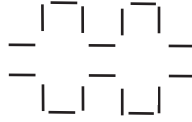
ศึกษาวิธีติดตั้ง HMC แบบติดตั้งชั้นวางของคุณ

1. ตรวจสอบให้แน่ใจว่า คุณวาง HMC ไว้ในตำแหน่งที่ถูกต้อง
2. ติดตั้ง HMC ลงในชั้นวาง สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การติดตั้ง 7310-CR4 HMC ลงในชั้นวาง” ในหน้า 34 เมื่อคุณเสร็จสิ้นการติดตั้ง HMC ลงในชั้นวางแล้ว ให้ทำขั้นตอนถัดไป
3. เสียบปลั๊กสายไฟเข้ากับ HMC
4. เชื่อมต่อคีย์บอร์ด มอนิเตอร์ และเมาส์
5. เชื่อมต่อโมเด็มที่เป็นอุปกรณ์เสริม:

ถ้าคุณกำลังเชื่อมต่อโมเด็มภายนอก ให้ปฏิบัติตามนี้:

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่นเพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 8

- a. ถ้าคุณต้องการติดตั้งโมเด็มภายนอกเข้ากับชั้นวาง ให้กระทำดังนี้
- b. หากคุณติดตั้งโมเด็มเรียบร้อยแล้ว ให้เชื่อมต่อสายเคเบิลข้อมูลของโมเด็มเข้ากับโมเด็มภายนอก HMC
- c. เชื่อมต่อสายเคเบิลข้อมูลโมเด็มเข้ากับพอร์ตระบบบน HMC ซึ่งมีเลเบลที่เป็นสัญลักษณ์ต่อไปนี้:



IPHA1522-0

- d. ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตของโมเด็มภายนอกเข้ากับปลั๊กโทรศัพท์แบบนาฬิกาบนผนัง
- e. เสียบสายตัวจ่ายไฟของโมเด็มเข้ากับโมเด็ม HMC

ถ้าคุณกำลังเชื่อมต่อกับโมเด็มภายใน ให้ใช้สายเคเบิลข้อมูลเพื่อเชื่อมต่อโมเด็ม HMC ภายในกับแหล่งข้อมูลที่เหมาะสม ตัวอย่างเช่น ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตของโมเด็ม HMC เข้ากับปลั๊กนาฬิกาบนกำแพงของคุณ

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่นเพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 8

6. เชื่อมต่อสายเคเบิลอีเทอร์เน็ต (หรือสายครอสโอเวอร์) จาก HMC ไปยังเซิร์ฟเวอร์ที่ถูกรจัดการ:

หมายเหตุ: เมื่อต้องการศึกษาเพิ่มเติมเกี่ยวกับการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 4

7. หากระบบที่ถูกรจัดการได้รับการติดตั้งแล้ว คุณสามารถตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแฉีกที่พอย์หรือไม่โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่ถูกรจัดการในขณะที่ขั้นตอนติดตั้งกำลังดำเนินไป
8. เชื่อมต่อพอร์ตอีเทอร์เน็ตบน HMC เข้ากับพอร์ตอีเทอร์เน็ตที่ชื่อ **HMC1** บนเซิร์ฟเวอร์ที่ถูกรจัดการ
9. ถ้าคุณกำลังเชื่อมต่อ HMC ตัวที่สองเข้ากับเซิร์ฟเวอร์ที่ถูกรจัดการ ให้เชื่อมต่อพอร์ตอีเทอร์เน็ตที่มีเลเบล **HMC2** บนเซิร์ฟเวอร์ที่ถูกรจัดการ
10. เสียบปลั๊กสายไฟสำหรับมอนิเตอร์, HMC และโมเด็มภายนอก HMC เข้ากับจุดจ่ายไฟ

หมายเหตุ: หากคุณกำลังเชื่อมต่อ HMC นี้ กับระบบที่ถูกรจัดการใหม่ ไม่ต้องเชื่อมต่อระบบที่ถูกรจัดการเข้ากับ แหล่งกำเนิดไฟฟ้าในเวลานี้

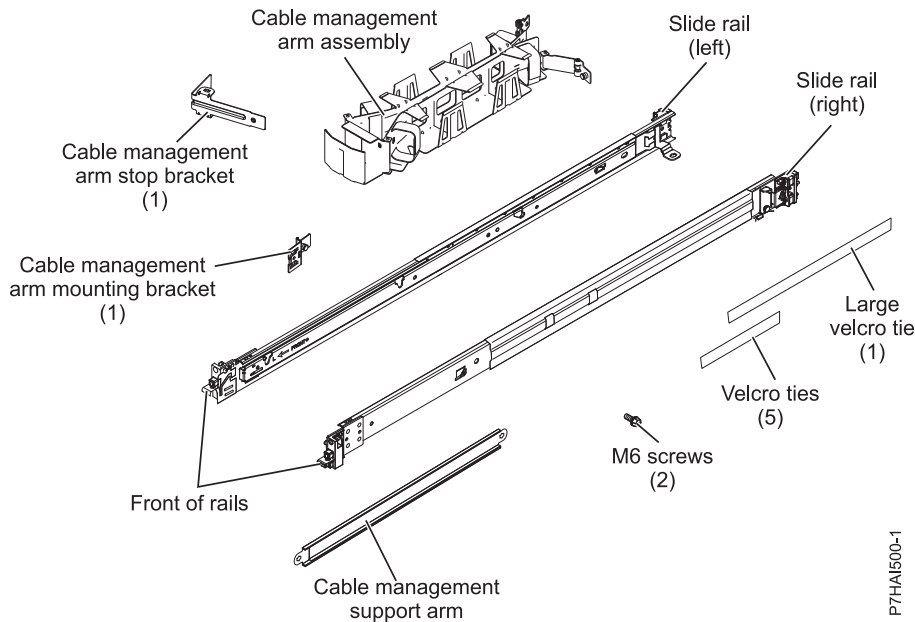
จากนั้น คุณจะต้องตั้งค่าซอฟต์แวร์ HMC ดำเนินการต่อด้วย “การกำหนดคอนฟิก HMC” ในหน้า 61

การติดตั้ง 7042-CR5, 7042-CR6 และ 7042-CR7 เข้ากับชั้นวาง

ส่วนนี้จะอธิบายวิธีการติดตั้ง 7042-CR5, 7042-CR6, และ 7042-CR7 HMC เข้ากับชั้นวาง

ถ้า HMC ถูกนำมาใช้เพื่อจัดการกับระบบ POWER7 แบบอิงโพรเซสเซอร์ใดๆ HMC ต้องเป็น CR3 หรือรุ่นใหม่กว่า ซึ่งเป็นโมเดล HMC ที่ประกอบเข้ากับชั้นวาง

ทำรายการชิ้นส่วนให้เสร็จสิ้น รูปประกอบต่อไปนี้แสดงรายการที่คุณต้องการติดตั้งเซิร์ฟเวอร์ในตู้ชั้นวาง ถ้ารายการใดๆ หายไปหรือเกิดความเสียหาย โปรดติดต่อสถานที่ที่คุณซื้อ

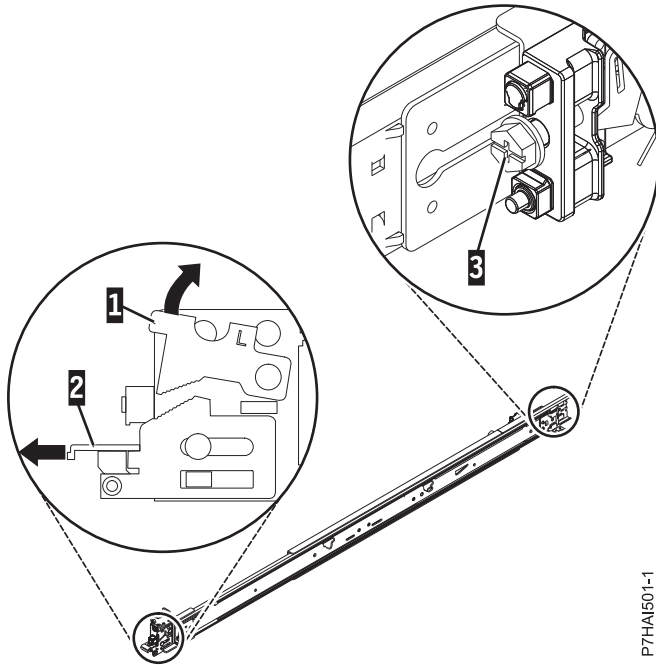


รูปที่ 14. รายการชิ้นส่วน

หมายเหตุ: คุณสามารถใช้สกรูสำหรับการจัดตั้ง หรือเพื่อให้มีความแข็งแรงมากขึ้น ในพื้นที่ที่มีการสั่นสะเทือนสูง

เพื่อติดตั้ง 7042-CR5, 7042-CR6, or 7042-CR7 HMC ลงในชั้นวาง ให้ดำเนินการต่อไปนี้:

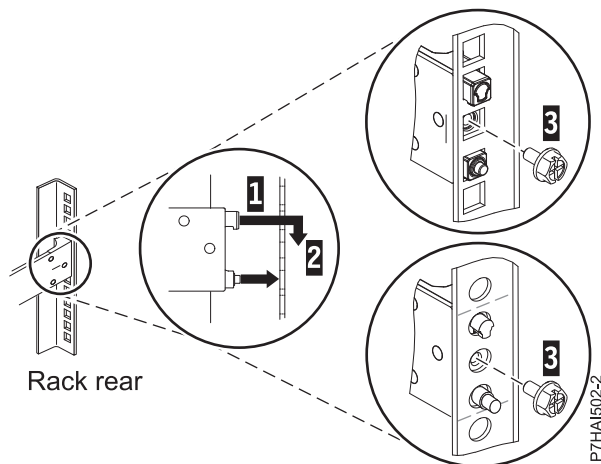
1. รางแบบสไลด์แต่ละรางมีเครื่องหมาย R (ด้านขวา) หรือ L (ด้านซ้าย) อย่างใดอย่างหนึ่ง เลือกหนึ่งในรางแบบสไลด์ และดันขึ้นบนแท็บด้านหน้าที่สามารถเคลื่อนย้ายได้ (1) จากนั้นดึงแลตซ์ด้านหน้า (2) เพื่อเลื่อนรางแบบสไลด์ด้านหน้า ถ้าติดตั้งตะปูควงไว้ในรางแบบสไลด์ (3) ให้ถอดออก



รูปที่ 15. รางแบบสไลด์และแท็บที่สามารถเคลื่อนย้ายได้

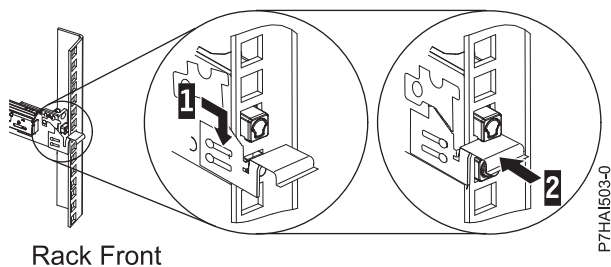
หมายเหตุ: ตรวจสอบให้แน่ใจว่าแท็บที่สามารถเคลื่อนย้ายได้ยังคงขยายได้ และไม่กลับสู่ตำแหน่งเดิม

2. จัดตำแหน่งขั้วสองขั้วที่ด้านหลังของรางแบบสไลด์ที่มีรูสามรูใน U ที่เลือกไว้บนด้านหลังของชั้นวาง กดราง เพื่อให้ขั้วเข้าไปอยู่ในรู (1) และปล่อยรางแบบสไลด์ (2) ลงจนกว่าแลตช์จะเข้าที่



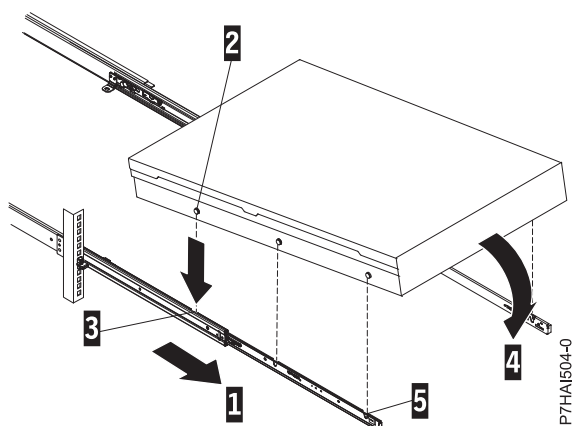
รูปที่ 16. จัดตำแหน่งขั้วภายในรูที่ด้านหลังของชั้นวาง

3. ดึงรางแบบสไลด์ไปข้างหน้าและใส่ขั้วสองขั้ว (1) ที่ด้านหน้าของรางลงในรูที่ต่ำกว่าสองรูใน U บนด้านหน้าของชั้นวาง รางลงในตำแหน่งจนกว่าจะเข้าที่ ผลักแลตช์ด้านหน้า (2) ในทุกทาง ทำซ้ำขั้นตอนที่ 1 ถึง 3 เพื่อติดตั้งรางอื่นลงในชั้นวาง ตรวจสอบให้แน่ใจว่าแลตช์ด้านหน้าแต่ละตัวอยู่ในตำแหน่งที่เหมาะสม



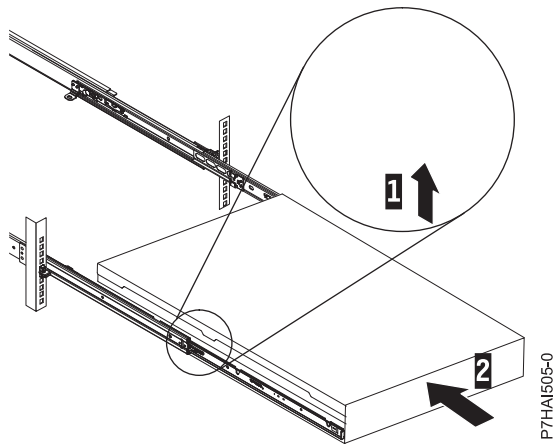
รูปที่ 17. รางและขั้วของชั้นวางด้านหน้า

4. ดึงรางแบบสไลด์ไปข้างหน้า (1) จนกว่าจะมีเสียงคลิกสองครั้งในตำแหน่งให้ยกเซิร์ฟเวอร์ด้วยความระมัดระวัง และเอียงลงในตำแหน่งที่อยู่เหนือรางแบบสไลด์ ดังนั้น หัวตะปูด้านหลัง (2) บนเซิร์ฟเวอร์จะอยู่แนวเดียวกับสล๊อตด้านหลัง (3) บนรางแบบสไลด์เลื่อนเซิร์ฟเวอร์ลงจนกว่าหัวตะปูด้านหลังจะเข้าไปอยู่ในสล๊อตด้านหลัง สองช่อง จากนั้นลดระดับเซิร์ฟเวอร์ด้านหน้าลง (4) จนกว่าหัวตะปูด้านหน้าจะเข้าไปอยู่ในสล๊อตด้านหน้า (5) เลื่อนผ่านหัวตะปูด้านหน้า



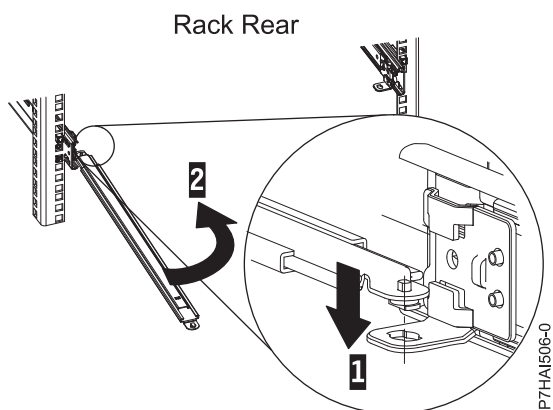
รูปที่ 18. รางแบบสไลด์ที่ขยาย หัวตะปูดของเซิร์ฟเวอร์ที่จัดตำแหน่งในแนวเดียวกับสล๊อตในราง

5. ยกแลตซ์สีน้ำเงินขึ้น (1) บนรางแบบสไลด์และผลักเซิร์ฟเวอร์ (2) ในทุกทิศทางเข้าไปในชั้นวางจนกว่าจะมีเสียงคลิกเพื่อให้เข้าตำแหน่ง



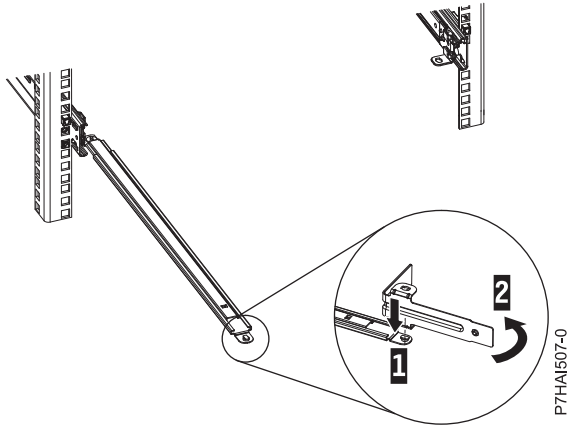
รูปที่ 19. ปลอยแลตซ์และเซิร์ฟเวอร์

6. แขนยึดสายเคเบิลสามารถติดตั้งบนด้านใดด้านหนึ่งของเซิร์ฟเวอร์ รูปภาพต่อไปนี้แสดงการติดตั้งแขนยึดสายเคเบิลบนด้านซ้าย เมื่อต้องการติดตั้งแขนยึดสายเคเบิลทางด้านขวา ให้ทำตามคำสั่งและติดตั้งฮาร์ดแวร์ในทิศทางตรงกันข้าม เชื่อมต่อส่วนปลายสุดด้านหนึ่งของแขนยึด (1) เข้ากับรางแบบสไลด์ตัวเดียวกันกับที่คุณวางแผนที่จะยึดแขนยึดสายเคเบิล ดังนั้น คุณสามารถหมุนปลายสุดอีกด้านหนึ่งของแขนยึด (2) ไปทางด้านหน้าของชั้นวาง



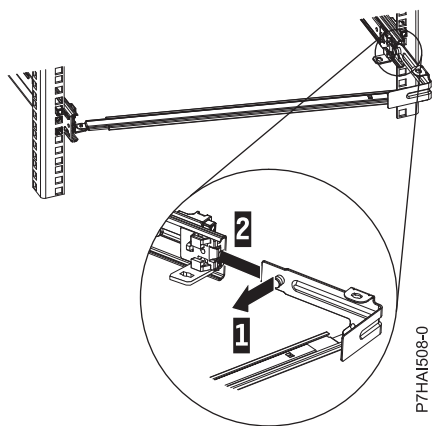
รูปที่ 20. การเชื่อมต่อแขนยึด

7. ติดตั้งแท่นยึดที่หยุดการยึดสายเคเบิลรูปตัว L (1) บนด้านปลายสุดของแขนยึดที่ไม่ได้ถูกยึดไว้ เปิดแท่นยึด (2) เพื่อยึดแท่นยึดเข้ากับแขนยึด



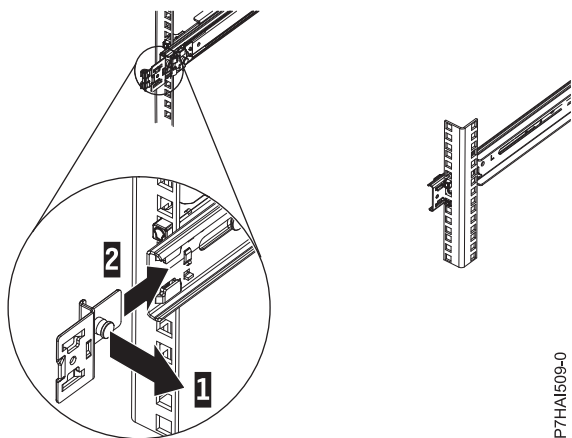
รูปที่ 21. แท่นยึดที่หยุดการยืดสายเคเบิล ซึ่งยึดกับแขนยึด

8. เมื่อต้องการยึดแขนยึดด้านอื่นกับด้านหลังของรางแบบสไลด์ให้ดึงข้อออก (1) จากนั้นเลื่อนแท่นยึด (2) เข้าไปในรางแบบสไลด์



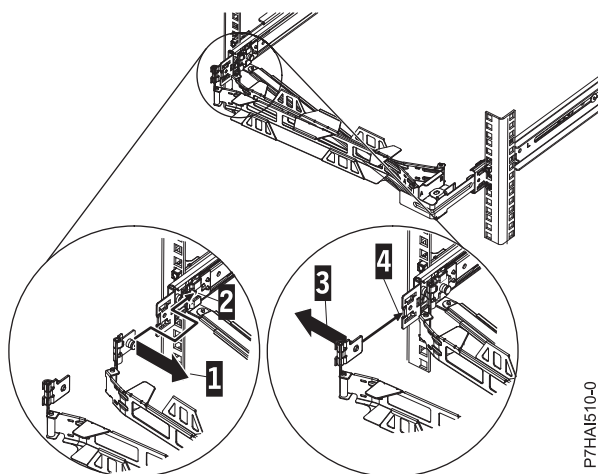
รูปที่ 22. ขั้วที่ขยายแท่นยึดที่ติดตั้งภายในรางแบบสไลด์

9. ดึงข้อของแท่นยึดที่ประกอบเข้าออก (1) และเลื่อนแท่นยึดที่ประกอบเข้า (2) ลงในรางแบบสไลด์ที่คุณกำลังติดตั้ง แขนยึดสายเคเบิล ผลักแท่นยึดลงในรางแบบสไลด์จนกว่าข้อสปริงจะเข้าสู่ตำแหน่ง



รูปที่ 23. ขั้วแทนยึดที่ประกอบเข้าซึ่งขยายได้และแทนยึดที่ประกอบเข้าซึ่งติดตั้งในรางแบบสไลด์

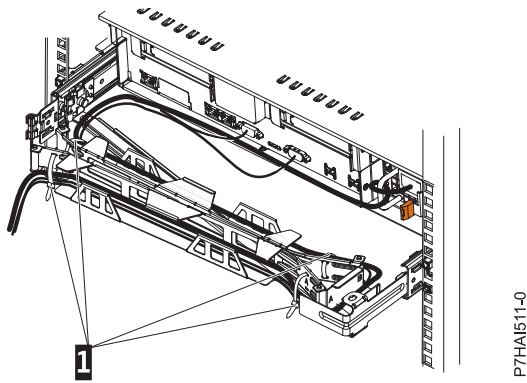
10. วางแขนยึดสายเคเบิลบนแขนยึด ดึงขั้วแขนยึดสายเคเบิล ออก (1) จากนั้น เลื่อนแท็บ แขนยึดสายเคเบิล (2) ลงในสล๊อตที่ด้านในของรางแบบสไลด์ ผลักแท็บจนกว่า จะเข้าตำแหน่ง ดึงขั้วแขนยึดสายเคเบิลด้านอื่นออก (3) จากนั้น เลื่อนแท็บแขนยึดสายเคเบิลลงในสล๊อต (4) ที่ด้านนอกของรางแบบสไลด์ ผลักแท็บจนกว่าจะเข้าตำแหน่ง



รูปที่ 24. การเชื่อมต่อแขนยึดสายเคเบิล

11. ยึดสายไฟและสายเคเบิลเข้ากับด้านหลังของเซิร์ฟเวอร์ (ซึ่งรวมถึงคีย์บอร์ด จอมอนิเตอร์และสายเมาส์ตามต้องการ) จัดเส้นทางสายเคเบิลและสายไฟบนแขนยึดสายเคเบิล (1) และยึดสายเหล่านั้นด้วยสายผูกเคเบิลหรือรัดด้วยสายรัด

หมายเหตุ: อนุญาตให้ หย่อนสายเคเบิลทั้งหมดเพื่อไม่ให้สายเคเบิลตึงเกินไปตามการย้ายแขนยึด สายเคเบิล



รูปที่ 25. การยึดสายไฟและการจัดเส้นทาง

12. เลื่อนเซิร์ฟเวอร์ลงในชั้นวางจนกระทั่งเข้าที่

การติดตั้งหน้าจอและคีย์บอร์ด

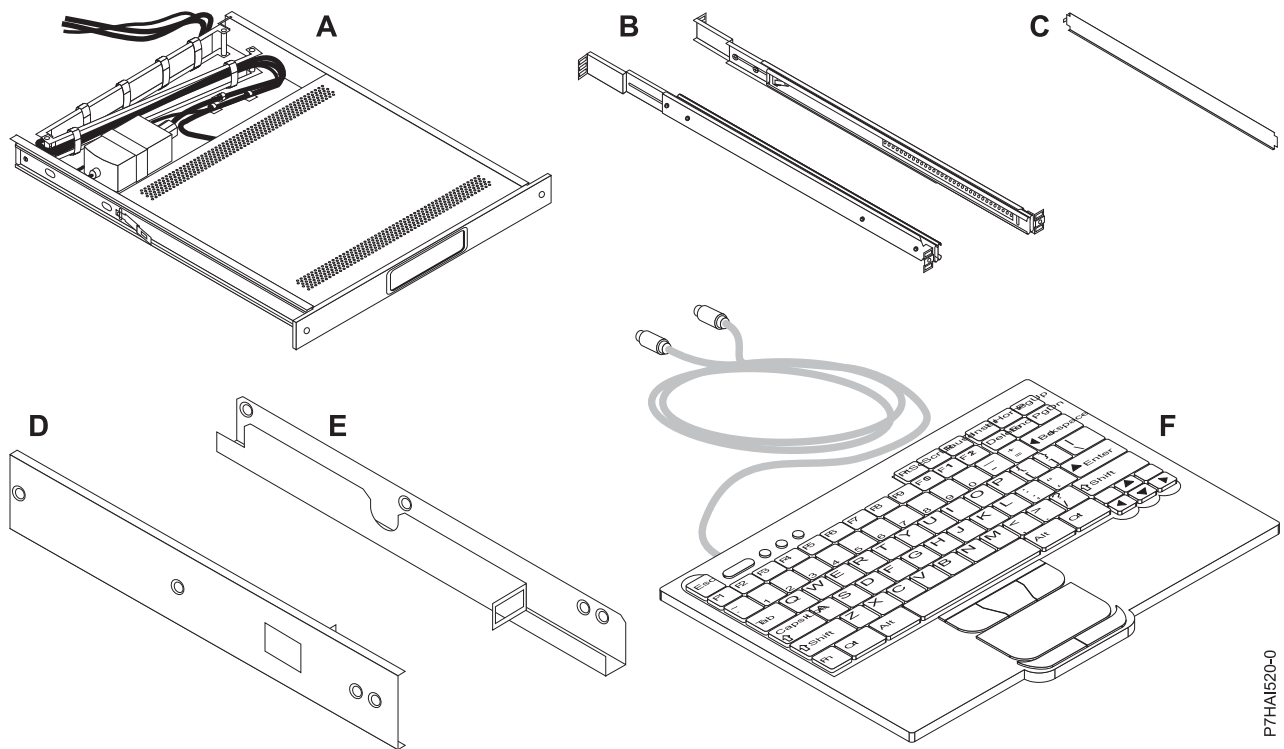
ศึกษาวิธีการติดตั้งหน้าจอและคีย์บอร์ด ซึ่ง มาพร้อมกับ 7042-CR6 HMC เข้ากับชั้นวาง นี่คือนงานของลูกค้า

ถ้า HMC ถูกนำมาใช้เพื่อจัดการกับระบบที่ใช้ตัวประมวลผล POWER7 HMC ต้องเป็น CR3 หรือใหม่กว่าซึ่งเป็นโมเดล HMC ที่ประกอบเข้ากับชั้นวาง IBM eserver 7316-TF3 มีหน้าจอแบบจอบนขนาด 17 นิ้ว และ ถาดวางหน้าจอคีย์บอร์ดและมอนิเตอร์ที่ประกอบเข้ากับชั้นวาง คีย์บอร์ดแบบพิเศษที่สามารถใช้ได้สำหรับภาษาต่างๆ พอดีกับภายในด้านหน้าของ ถาดคีย์บอร์ด ถาดคีย์บอร์ดและหน้าจอจะใช้พื้นที่ขนาด 1 ยูนิต Electronics Industries Association (EIA) ในตู้ชั้นวาง คุณ สามารถติดตั้งสวิตช์คอนโซลด้านหลังถาดเพื่อต่อคีย์บอร์ดและหน้าจอแบบจอบน เข้ากับเซิร์ฟเวอร์มากกว่าหนึ่งตัว

เพื่อติดตั้ง 7042-CR6 HMC ลงในชั้นวาง ให้ดำเนินการขั้นตอนต่อไปนี้:

ข้อควรสนใจ: การติดตั้งรางในชั้นวางเป็นโปรซีเดอร์ทที่ซับซ้อน เมื่อต้องการติดตั้งรางอย่างถูกต้อง คุณต้องปฏิบัติงานแต่ละงานตามลำดับดังนี้

1. ทำรายการชิ้นส่วนให้เสร็จสิ้น สำหรับคำแนะนำ โปรดดูที่ “การทำให้รายการชิ้นส่วนให้เสร็จสิ้น” ในหน้า 54 การทำรายการชิ้นส่วนให้เสร็จสิ้น
2. ค้นหาตำแหน่งชุดฮาร์ดแวร์ที่ประกอบเข้ากับชั้นวาง และชุดรางของระบบ ซึ่งประกอบด้วยยูนิตระบบของคุณ



P7HA520-0

รูปที่ 26. ชิ้นส่วนของชุดการติดตั้ง

A หนึ่งถาดคีย์บอร์ดที่มี หน้าจอแบบจอบนในตัว

B รางด้านนอก (2)

C สเปเซอร์การจัดตำแหน่งราง (1)

D ขายึดสวิตช์คอนโซล ด้านขวา (1)

E ขายึดสวิตช์คอนโซล ด้านซ้าย (1)

F คีย์บอร์ด อุปกรณ์ชี้ในตัว (1)

G ชุดฮาร์ดแวร์ เบ็ดเตล็ด: น็อตน็อต U ยึดอุปกรณ์ 12 ตัว, น็อตคลิป 12 ตัว, สกรูหัวร่องสี่แฉก 10 ตัว, สกรู 4 (8-32) ตัว และสกรูหางปลา 2 ตัว

H สายไฟความยาว 1.8 ม. (6 ฟุต) (1)

I ขั้วต่อสายไฟ International Electrotechnical Commission (IEC) ความยาว 2.4 ม. (8 ฟุต) (1)

J สายต่อ คีย์บอร์ด (1)

K สายต่อ เม้าส์ (1)

L แผ่น CD ที่มี ไตรเวอร์ของคีย์บอร์ดและเมาส์ที่ทำงานบน Windows (ห้ามใช้กับระบบ Eserver pSeries หรือระบบที่ใช้ AIX, Linux หรือ OS/400)

สำคัญ: ใช้เครื่องมือต่อไปนี้เพื่อติดตั้งคีย์บอร์ดและ หน้าจอแบบจอบนที่ประกอบเข้ากับชั้นวาง:

- กรรไกร

- ไชควงแจก
- ไชควงแบบแบน

การทำให้รายการชิ้นส่วนให้เสร็จสิ้น

คุณอาจต้องการทำรายการชิ้นส่วนให้เสร็จสิ้น

ถ้าคุณยังไม่ได้ทำให้ทำรายการชิ้นส่วนให้เสร็จสิ้น ก่อนที่จะดำเนินการติดตั้ง:

1. หาตำแหน่งรายงานชุดเครื่องมือในกล่องอุปกรณ์
2. ตรวจสอบให้แน่ใจว่า คุณได้รับชิ้นส่วนทุกชิ้นที่คุณได้สั่งซื้อ

ถ้าชิ้นส่วนไม่ถูกต้อง หายไป หรือเสียหาย ให้ติดต่อผู้ขายของ IBM หรือฝ่ายขายและสนับสนุนของ IBM

การทำเครื่องหมายตำแหน่งโดยไม่ใช่เท็มเพลตประกอบเข้ากับชั้นวาง

คุณสามารถทำเครื่องหมายตำแหน่งโดยไม่ใช่เท็มเพลต

เท็มเพลตที่ประกอบเข้ากับชั้นวางไม่ได้ประกอบเข้ากับระบบนี้ ระบบเหล่านี้คือยูนิต 1 EIA แบบสูง

เมื่อต้องการกำหนดตำแหน่งการประกอบเข้า ให้ปฏิบัติตามขั้นตอนเหล่านี้:

1. กำหนดที่จะวางระบบในชั้นวาง บันทึกตำแหน่ง EIA

หมายเหตุ: ยูนิต EIA บนชั้นวางของคุณประกอบด้วยกลุ่มของรูสามรู

2. หันด้านหน้าของชั้นวางและทำงานจากด้านขวา จุดยึดเหนี่ยวที่อยู่ถัดจากรูด้านบนสุดของยูนิต EIA

หมายเหตุ: จุดยึดเหนี่ยวจะถูกใช้เพื่อวัตถุประสงค์ในการระบุตำแหน่งบนชั้นวาง ถ้าคุณไม่มีจุดใดๆ ให้ใช้รูปแบบอื่นๆ ของเครื่องมือที่ใช้ทำเครื่องหมาย เพื่อวัตถุประสงค์ในการระบุตำแหน่ง (ตัวอย่างเช่น เทป ตัวทำเครื่องหมาย หรือดินสอ) ถ้าคุณกำลังติดตั้งรางแบบสไลด์ให้วางเครื่องหมายหรือจุดยึดเหนี่ยวที่ตำแหน่งด้านล่างและกึ่งกลางของยูนิต EIA แต่ละยูนิต

3. วางจุดยึดเหนี่ยวอื่นๆ ถัดจากรูด้านล่างของ ยูนิต EIA ข้างต้น

หมายเหตุ: ถ้าคุณกำลังนับรูให้เริ่มต้นด้วยรูที่ระบุโดยจุดแรกและนับไปอีกสองรู วางจุดที่สองให้อยู่ถัดจากรูที่สาม

4. ทำซ้ำขั้นตอน 1 ในหน้า 37 สำหรับ รูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
5. ไปที่ด้านหลังของชั้นวาง
6. ที่ด้านขวาให้หಾಯูนิต EIA ที่ตรงกับยูนิต EIA ด้านล่างซึ่งทำเครื่องหมายอยู่บนด้านหน้าของชั้นวาง
7. วางจุดยึดเหนี่ยวที่ด้านล่างของยูนิต EIA
8. วางจุดยึดเหนี่ยวที่รูด้านบนสุดของยูนิต EIA
9. ทำเครื่องหมายที่รูทางด้านซ้ายของชั้นวาง

การติดตั้งหน้าจอและคีย์บอร์ดเข้ากับชั้นวาง

ศึกษาวิธีการติดตั้งหน้าจอและคีย์บอร์ดที่ มาพร้อมกับ 7042-CR6 HMC เข้ากับชั้นวาง

IBM 7316-TF3 เป็นหน้าจอและคีย์บอร์ดที่มีจอแบนขนาด 17 นิ้วที่ประกอบเข้ากับชั้นวางที่ใช้พื้นที่การยึดเข้ากับชั้นวาง 1.75 นิ้ว (1 EIA) ในตู้ชั้นวาง คุณสามารถใช้ขายึดที่มีในชุดนี้ เพื่อติดตั้งสวิตช์คอนโซลในพื้นที่การติดตั้งบนชั้นวางเดียวกับชุดคอนโซลหน้าจอ

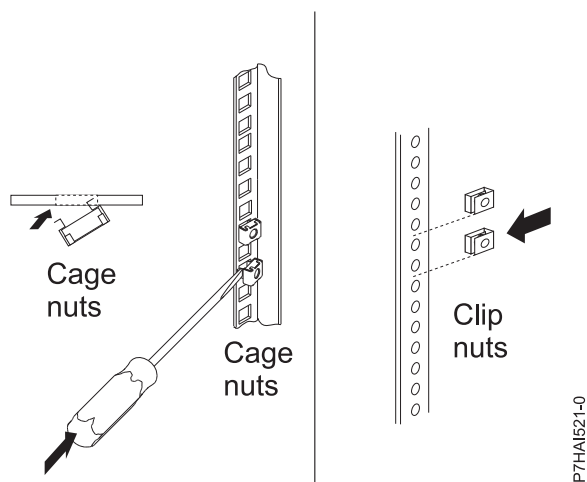
เพื่อติดตั้งหน้าจอและคีย์บอร์ดของ 7042-CR6 HMC ลงในชั้นวาง ให้ดำเนินการขั้นตอนต่อไป:

ข้อควรสนใจ: ถอดประตูด้านข้างและแผงด้านข้างออกเพื่อให้การเข้าถึงสำหรับการติดตั้งได้ง่ายขึ้น

ดำเนินการขั้นตอนต่อไปเพื่อติดตั้งหน้าจอและคีย์บอร์ด ลงในชั้นวาง:

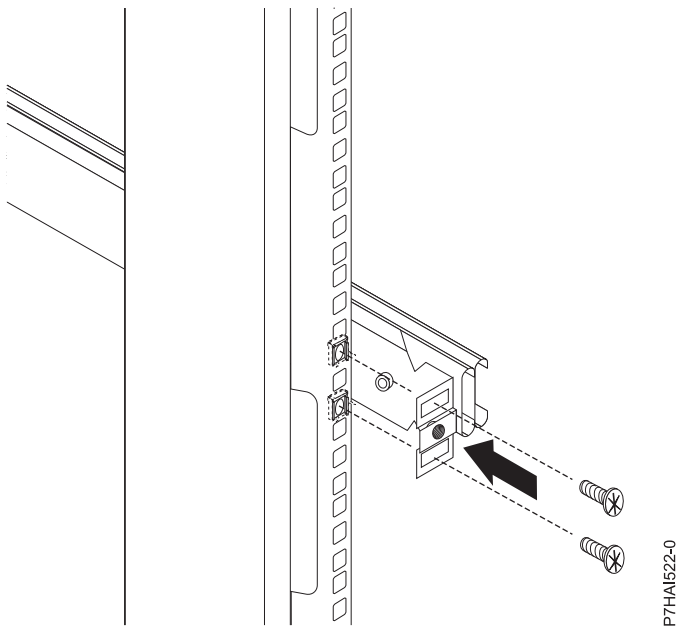
1. เลือกตำแหน่งในชั้นวางสำหรับถาดวางหน้าจอและคีย์บอร์ด สำหรับข้อมูลเพิ่มเติม โปรดดูที่ การทำเครื่องหมายตำแหน่ง.
2. ติดตั้งน็อต U ยึดอุปกรณ์ 4 ตัว (รูสล็อตบนหน้าแปลนชั้นวาง) หรือน็อตคลิป 4 ตัว (รูวงกลมบนหน้าแปลนชั้นวาง) ในตำแหน่ง EIA เดียวกันที่ด้านหน้า และด้านหลังของชั้นวาง

หมายเหตุ: หากคุณวางแผนที่จะติดตั้งสวิตช์คอนโซล ให้ติดตั้งน็อต U ยึดอุปกรณ์ หรือน็อตคลิปในตำแหน่งด้านหลังตรงกลาง ตามที่แสดงในรูปภาพต่อไปนี้



รูปที่ 27. การติดตั้ง น็อต U ยึดอุปกรณ์

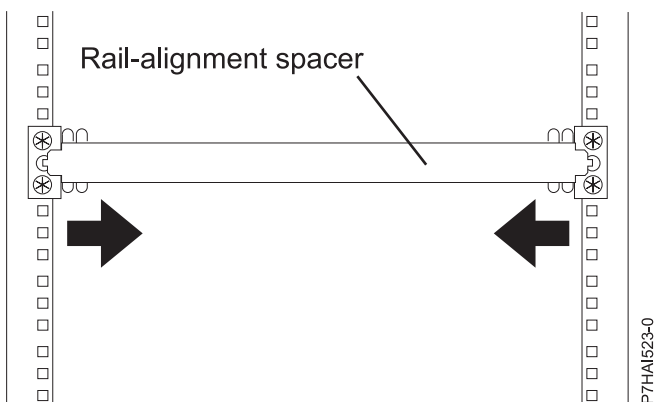
3. คลายสกรูปรับรางสองตัวที่อยู่บน รางเลื่อนด้านนอกแต่ละตัวออก ดึงรางออกไปยังการปรับด้านนอก สูงสุด
4. ปรับขยิดรางเลื่อนด้านนอกให้พอดีกับความลึกของ ตู้ชั้นวาง จากนั้น ติดตั้งขายึดรางเลื่อนให้พอดีกับ ความลึกของตู้ชั้นวางโดยใช้สกรูสี่ตัวจากชุดฮาร์ดแวร์ เบ็ดเตล็ด สกรูควรแน่นด้วยแรงนิ้วเพื่อให้สามารถปรับ ราง



รูปที่ 28. การปรับขายึดรางเลื่อน

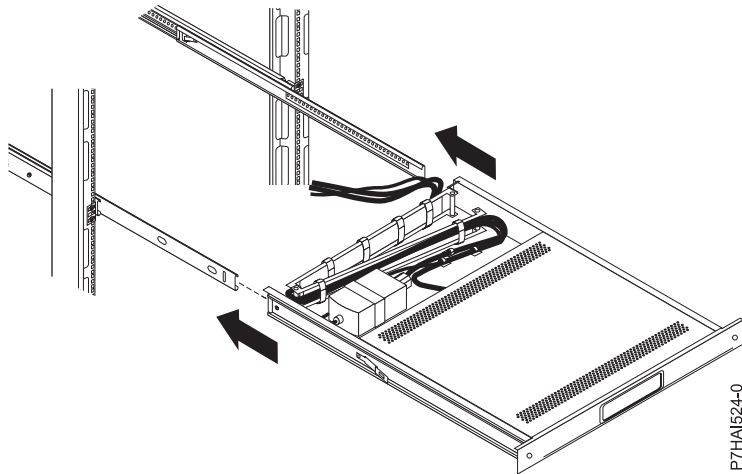
หมายเหตุ: ตรวจสอบให้แน่ใจว่าขายึดรางเลื่อน ขยายออกไปด้านนอกของหน้าแปลนการยึดตู้ชั้นวาง อย่าติดตั้ง สกรู ในรูตรงกลางทางด้านหน้าหรือด้านหลังของขายึด รางเลื่อน รูเหล่านี้จะใช้เพื่อติดตั้งสกรูทางปลา หรือขายึด การติดตั้ง สวิตช์คอนโซลตามลำดับต่อไปในขั้นตอนนี้

5. ใช้สกรูสี่ตัวจาก ชุดฮาร์ดแวร์เบ็ดเตล็ด and finger-tight them from the rear of the slide-rail brackets to the rack cabinet. ตรวจสอบให้แน่ใจว่าขายึดรางเลื่อน ขยายออกด้านนอกของหน้าแปลนการยึดตู้ชั้นวาง
6. ขันสกรูการปรับรางสองตัวบนรางด้านนอกแต่ละตัว ที่คุณคลายไว้ในขั้นตอน 5 ให้แน่น
7. ใส่สเปเซอร์จัดตำแหน่งรางลงในช่องตรงกลางรางเลื่อน ตรวจสอบให้แน่ใจว่าสเปเซอร์การจัดตำแหน่งรางหุ้มรอบราง ขัน สกรูสี่ตัวด้านหน้า จากนั้นถอดสเปเซอร์ออก



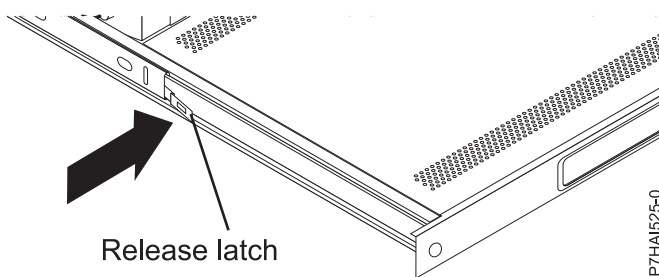
รูปที่ 29. การใส่สเปเซอร์การปรับราง

8. ดึงชิ้นส่วนด้านในของรางที่ยึดกับชั้นวางให้ยืดออก จากนั้น เลื่อนชุดล้อเลื่อนมาทางด้านหน้าของราง
9. เลื่อนถาดวางคีย์บอร์ดและหน้าจอแบบจอบนไปยังชุดล้อเลื่อน ในราง



รูปที่ 30. การเลื่อนหน้าจอและคีย์บอร์ด

10. กดสลักปลดล็อก และดันถาดวางคีย์บอร์ดและหน้าจอลงในชั้นวางให้สนิท คุณอาจพบแรงต้านทานบางอย่างในตอนเริ่มต้น เนื่องจากชุดล้อเลื่อนวางอยู่ระหว่างรางด้านในและด้านนอก ดึงถาดออกมาครึ่งทาง จากนั้นดันกลับไปที่ให้ถาดอยู่ในราง ทำเช่นนี้สองสามครั้งเพื่อให้แน่ใจว่า สามารถเลื่อนถาดในรางได้อย่างราบรื่น



รูปที่ 31. การใช้สลักปลดล็อก

หมายเหตุ:

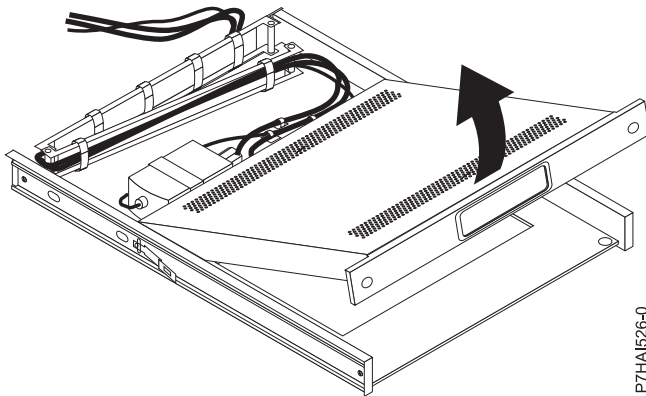
สายวิดีโอจะเชื่อมต่อ กับหน้าจอแบบจอแบน เมื่อคุณติดตั้งถาดลงในตู้ชั้นวาง ตรวจสอบให้แน่ใจว่าคุณไม่ได้พับหรือตัดสายวิดีโอ

11. วางถาดลงในราง และขันสกรูยึดขายึดรางเลื่อนด้านหลัง สี่ตัวให้แน่น
12. วางคีย์บอร์ดบนพื้นผิวเรียบที่มั่นคง และถอดแผ่นยาง ที่ปลายด้านล่างของคีย์บอร์ดใหม่ แต่ละด้านออก อย่าปล่อยแผ่นยางไว้บนคีย์บอร์ด เนื่องจาก แผ่นยางอาจขยายไปยังพื้นที่ด้านล่างถาด

หมายเหตุ:

อย่า ดึงขาตั้งคีย์บอร์ดออก หน้าจอแบบจอแบนอาจ เกิดความเสียหายหากขาตั้งถูกดึงออกเมื่ออยู่ใกล้หน้าจอ

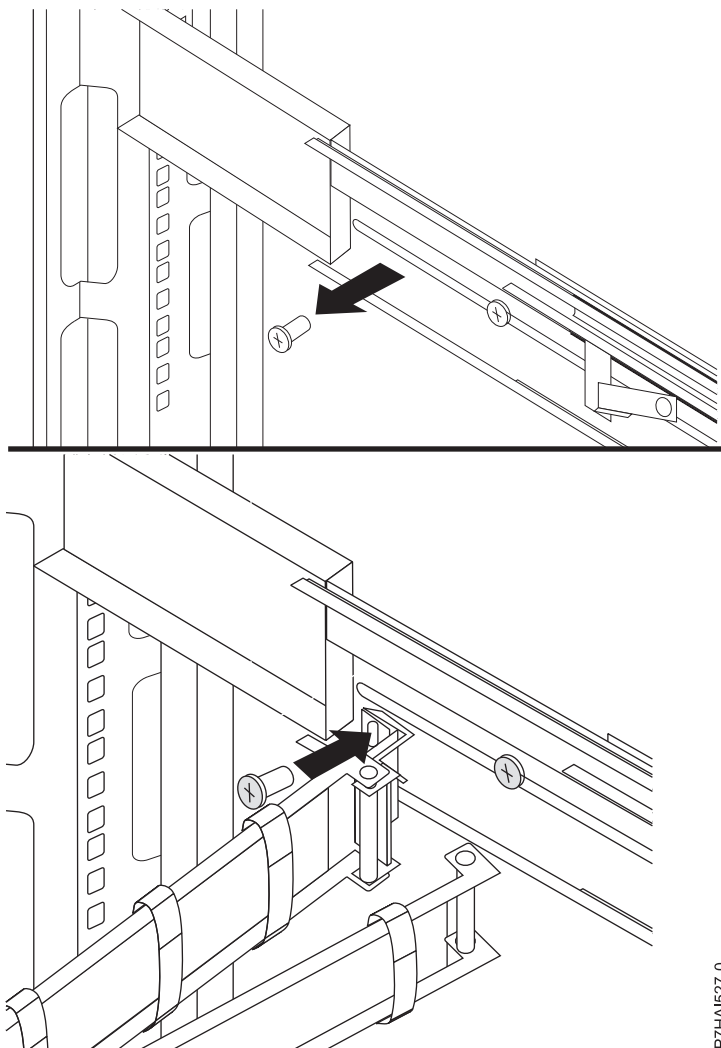
13. ดึงถาดออกจากชั้นวางจนสุด ราง
14. ยกด้านหน้าของหน้าจอแบบจอแบนขึ้น จากนั้นยกหน้าจอ ในตำแหน่งที่ยกสูงขึ้น



P7HA1E26-0

รูปที่ 32. การยกหน้าจอใน ตำแหน่งที่ยกสูงขึ้น

15. วางคีย์บอร์ดลงในถาด จากนั้นสอดสายเคเบิลของคีย์บอร์ดและ เมาส์ผ่านคลิปรัดสายทางด้านล่างของถาดผ่านช่องทางด้านขวาของถาด และไปยังแขนการจัด สายเคเบิล ดึงสายเคเบิลทั้งหมดผ่านช่อง
16. วางสายคีย์บอร์ดและเมาส์บนถาดด้านหลังหน้าจอ ตรวจสอบให้แน่ใจว่าสายเคเบิลขวางกับอุปกรณ์ต่างๆ ในชั้นวางเมื่อดันถาด กลับเข้าที่ในขั้นตอนต่อไปนี้ คุณต้อง สอดสายผ่านแขนการจัดสายเคเบิล
17. ลดหน้าจอให้ต่ำลง จากนั้นดันถาด กลับเข้าไปในชั้นวางจนสุด ใช้สกรูหางปลาเพื่อยึดด้านหน้าของถาด เข้ากับชั้นวาง
18. จากด้านหลังของชั้นวาง ให้ถอดแถบรัดสำหรับการขนส่งที่ยึด แขนการจัดสายเคเบิลเข้ากับถาดออก
19. สอดสายคีย์บอร์ดและเมาส์ผ่านแขนการจัด สายเคเบิล ใช้แถบรัดสายที่มีอยู่เพื่อยึดสายเคเบิล
20. ถอดสกรูการปรับรางที่อยู่ใกล้กับ ด้านหลังของชั้นวางออกจากรางเลื่อนด้านซ้าย ใช้สกรูเพื่อยึดติดตั้ง แขนการจัดสายเคเบิลเข้ากับราง



รูปที่ 33. การติดตั้งแขนการจัดสาย เคเบิล

21. เชื่อมต่อข้อต่อวิดีโอ, คีย์บอร์ด และเมาส์เข้ากับ เซิร์ฟเวอร์หรือสวิตช์คอนโซลในตู้ชั้นวาง หาก ติดตั้งสวิตช์คอนโซล โปรดดูที่ การติดตั้ง Optional Console Switch และดำเนินการขั้นตอนตามที่อธิบายไว้ หากไม่ได้ติดตั้ง ให้ปฏิบัติตาม ขั้นตอนจากขั้นตอน 21 เพื่อดำเนินการติดตั้งถาดวางหน้าจอและคีย์บอร์ด ของคุณ
22. เชื่อมต่อสายไฟ เข้ากับสายจัมเปอร์แบบสับบนแขนการจัดสายเคเบิล
23. ต่อสายเคเบิลและข้อต่อสัญญาณทั้งหมดเข้ากับข้อต่อหรือ อุปกรณ์ที่ต้องการ
24. ตรวจสอบให้แน่ใจว่าสวิตช์ไฟถูกปิดอยู่ ต่อสายไฟ เข้ากับปลั๊กเสียบไฟฟ้าที่มีกราวด์ หรือ Power Distribution Unit (PDU)

หมายเหตุ: ตรวจสอบให้แน่ใจว่า แรงดันไฟฟ้าของแหล่งจ่ายไฟในท้องถิ่นอยู่ในช่วงไฟกระแสสลับ 100 – 240 โวลต์ ก่อนที่คุณจะเชื่อมต่อสายไฟเข้ากับหัวแปลงปลั๊กไฟ กระแสตรง

25. ดึงถาดออกจากด้านหน้าของตู้ชั้นวาง สอดสายเคเบิล ภายในตู้ชั้นวาง และยึดด้วยแถบรัดสาย

การติดตั้งสวิตช์คอนโซล (ตัวเลือก)

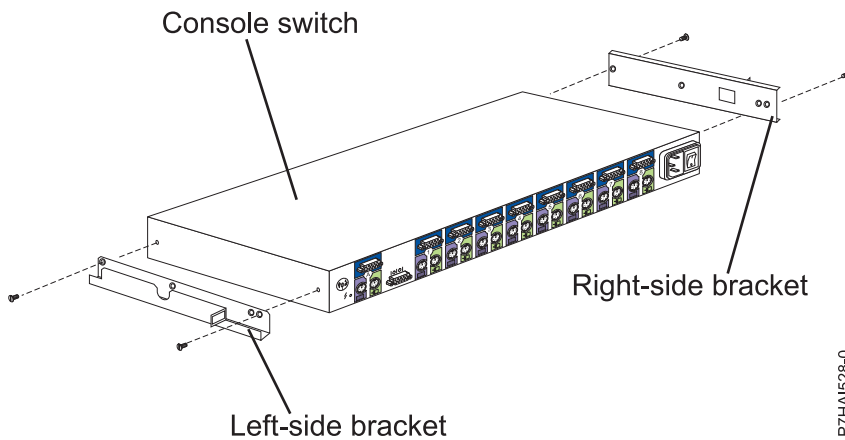
ศึกษาเกี่ยวกับวิธีการติดตั้งสวิตช์คอนโซลที่เป็นตัวเลือก

คุณสามารถใช้สวิตช์คอนโซลเพื่อเชื่อมต่อมากกว่าหนึ่งเซิร์ฟเวอร์ กับคีย์บอร์ดและหน้าจอเดียว ออฟชั่นของสวิตช์คอนโซลสามารถแยกออกจากกัน แต่ขั้วยึดที่กำหนดเองสำหรับสวิตช์จะมีอยู่ในชุดการติดตั้ง

โดยการติดตั้งสวิตช์คอนโซลที่ด้านหลังภาตวางหน้าจอและภาตวางคีย์บอร์ด ทั้งภาตวางหน้าจอและคีย์บอร์ดสามารถใช้พื้นที่ด้วยกัน ในชั้นวาง เพื่อติดตั้งสวิตช์คอนโซลหลังภาต ให้ใช้ขั้วยึดที่มาพร้อมกับชุดการติดตั้ง

ดำเนินการขั้นตอนต่อไปเพื่อติดตั้งสวิตช์คอนโซลด้านหลัง ภาต:

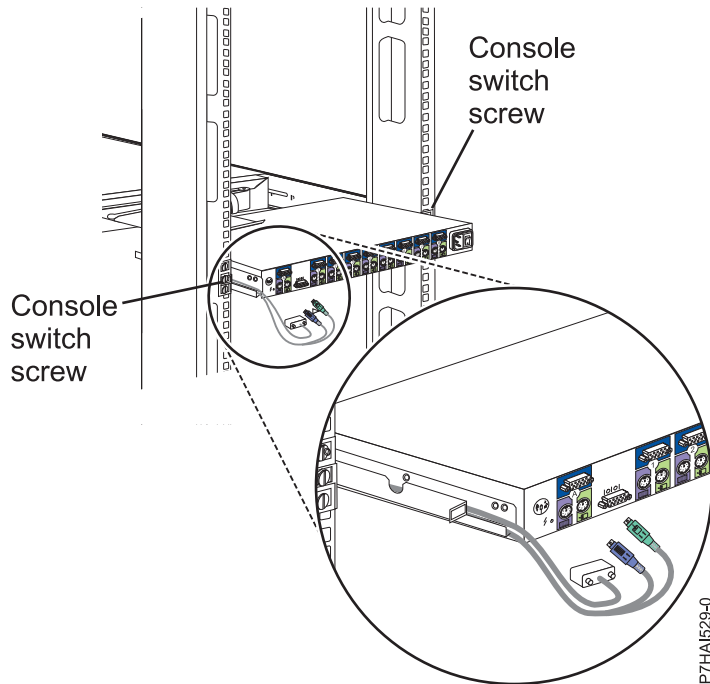
1. ใช้สกรู 8-32 ตัวเพื่อยึดขั้วยึดด้านขวาและซ้าย เข้ากับด้านขวาและด้านซ้ายของสวิตช์คอนโซลตามลำดับ



รูปที่ 34. การติดตั้งสวิตช์คอนโซล

หมายเหตุ: ขั้วยึด ด้านซ้าย จะมีช่องเพื่อสอดสายไฟ, วิดีโอ, คีย์บอร์ด และเมาส์ ตรวจสอบให้แน่ใจว่าคุณติดตั้งขั้วยึดเข้ากับสวิตช์คอนโซล โดยให้ช่องทางด้านซ้ายของขั้วยึดหันขึ้น

2. ติดตั้งสวิตช์คอนโซลด้านหลังภาตวางคีย์บอร์ดและหน้าจอแบน โดยใช้สกรูสี่ตัว (ด้านละสองตัว) ที่มาพร้อมกับชุดฮาร์ดแวร์ต่างๆ
3. สอดสายไฟ, วิดีโอ, คีย์บอร์ด และเมาส์ผ่าน ช่องในขั้วยึดทางด้านซ้ายบนสวิตช์คอนโซล จากนั้น เชื่อมต่อ ขั้วต่อวิดีโอ, คีย์บอร์ด และเมาส์เข้ากับสวิตช์คอนโซล



รูปที่ 35. การกำหนดเส้นทางสาย

4. เชื่อมต่อสายไฟ, การกำหนดเส้นทางสายเคเบิลต่างๆ และการรัดสายเคเบิล สำหรับ คำแนะนำ โปรดดูที่ การเชื่อมต่อ สายไฟเข้ากับสายจัมเปอร์แบบสันบนแผนการจัดการสาย

การกำหนดคอนฟิก HMC

กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก ความปลอดภัย เซอร์วิสแอพลิเคชัน และความต้องการส่วนตัวบางอย่างของผู้ใช้

ขึ้นอยู่กับระดับของการปรับแต่งค่าเองที่คุณต้องการกำหนดให้กับคอนฟิกูเรชัน HMC ของคุณ คุณมีตัวเลือกหลายตัวเลือกสำหรับการตั้งค่า HMC เพื่อให้เหมาะสมกับความต้องการของคุณ ตัวช่วยสร้างการติดตั้งที่แนะนำ คือเครื่องมือใน HMC ซึ่งได้รับการออกแบบมาเพื่อช่วยให้การตั้งค่า HMC เป็นไปอย่างง่ายดาย คุณสามารถเลือกใช้อัลลีต์ผ่านทางวิซาร์ดเพื่อสร้างสภาวะแวดล้อมของ HMC ตามที่แนะนำได้อย่างรวดเร็ว หรือคุณสามารถเลือกที่จะสำรวจการกำหนดค่าทั้งหมดที่วิซาร์ดแนะนำ คุณยังสามารถดำเนินขั้นตอนกำหนดคอนฟิกโดยใช้ความช่วยเหลือจากวิซาร์ด การกำหนดคอนฟิก HMC โดยใช้เมนู HMC

ก่อนที่คุณจะเริ่มต้น ให้รวบรวมข้อมูลคอนฟิกูเรชันที่ต้องการ ซึ่งคุณจำเป็นต้องปฏิบัติตามขั้นตอนต่างๆ ให้เสร็จสิ้นอย่างสมบูรณ์ โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23 สำหรับ รายการของข้อมูลที่ต้องการ เมื่อคุณเตรียมการเสร็จสิ้น ตรวจสอบให้แน่ใจว่าคุณเสร็จสิ้น “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25 และกลับไปสู่ส่วนนี้

การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ทางวิซาร์ดเซตอัพที่แนะนำ

ในหลายๆ กรณี, HMC ถูกติดตั้งเพื่อปฏิบัติงานได้อย่างมีประสิทธิภาพโดยใช้ค่ากำหนดดีฟอลต์หลายๆ ค่า ใช้รายการตรวจสอบวิธีลัดนี้เพื่อเตรียม HMC สำหรับการให้บริการ เมื่อคุณได้ปฏิบัติตามขั้นตอนเหล่านี้ในรายการตรวจสอบเรียบร้อยแล้ว HMC ของคุณจะถูกกำหนดค่าให้เป็นเซิร์ฟเวอร์ Dynamic Host Configuration Protocol (DHCP) ในเน็ตเวิร์กส่วนบุคคล (เชื่อมต่อโดยตรง)

เริ่มต้น HMC และปฏิบัติตามขั้นตอนในวิซาร์ดเซตอัพที่แนะนำ

ล็อกอินเข้าสู่อินเตอร์เฟซ HMC และตั้งค่า HMC ของคุณโดยใช้วิซาร์ด Guided Setup

หมายเหตุ: หากเป็นการติดตั้งใหม่ ตรวจสอบให้แน่ใจว่าระบบที่ถูกรจัดการ ไม่ได้เชื่อมต่อกับแหล่งกำเนิดไฟฟ้า สำหรับ HMC แบบติดตั้งกับชั้นวาง นี่หมายความว่า HMC จะเป็นเพียงอุปกรณ์ชิ้นเดียวเท่านั้นที่จะเสียบกับบัสกระจายกำลังไฟฟ้า (power distribution bus – PDB) ถ้าเป็น HMC เครื่องที่สองที่เชื่อมต่อกับระบบที่ถูกรจัดการระบบเดียวกัน ก็จะสามารถเชื่อมต่อกับระบบที่ถูกรจัดการเข้ากับแหล่งกำเนิดไฟฟ้า

1. เปิด HMC โดยกดปุ่มเปิด/ปิด.
2. โปรดรอให้ HMC เลือกภาษาดีฟอลต์และค่าติดตั้งโลแคล ประมาณ 30 วินาที
3. ยอมรับข้อตกลงไลเซนส์ของ คอนโซลการจัดการฮาร์ดแวร์ หากคุณไม่ยอมรับข้อตกลงไลเซนส์ของ คอนโซลการจัดการฮาร์ดแวร์ คุณก็จะไม่สามารถกำหนดคอนฟิกของ HMC ให้เสร็จสิ้นได้
4. คลิก **Log on and launch the Hardware Management Console web application**
5. ล็อกอินเข้าสู่ HMC:

หมายเหตุ: หากผู้ดูแลระบบของคุณ (hmcadmin) เปลี่ยนแปลงรหัสผ่าน ให้ป้อนค่าที่นี้

- ID: hscroot
- รหัสผ่าน: abc123

วิซาร์ด Guided Setup จะปรากฏขึ้น

6. คลิก ตกลง บนหน้าต่าง entry ของ Guided Setup

หมายเหตุ: หากตัวช่วยสร้างการติดตั้งที่แนะนำ ไม่ปรากฏขึ้นเมื่อคุณเริ่มต้น HMC ให้คลิก **Guided Setup Wizard** ในพื้นที่การนำทางของเพจต้อนรับเข้าสู่ HMC

7. ดำเนินการตามขั้นตอนใน Guided Setup wizard ให้เสร็จสิ้น โดยใช้เวิร์กชีตการติดตั้งคอนฟิกูเรชันก่อนล่วงหน้า ที่คุณได้ทำเสร็จสิ้นแล้ว คลิก **ใช่** เพื่อดำเนินการต่อและดำเนินการขั้นตอนต่างๆ ในวิซาร์ดการเชื่อมต่อ และเซิร์ฟเวอร์ Call-Home
8. ในหน้าต่าง Summary คลิก **Finish**
9. หากคุณยังไม่ได้เชื่อมต่ออีเทอร์เน็ตกับระบบที่ถูกรจัดการผ่านทางสายเคเบิล ให้เชื่อมต่อตอนนี้
10. ในพื้นที่การนำทาง HMC ให้คลิก การจัดการเซอว์วิส
11. ในพื้นที่เนื้อหา ให้คลิก ผู้ใช้ที่ได้รับสิทธิ หน้าต่าง Authorize User จะเปิด
12. ป้อน IBM ID ของคุณในช่อง และคลิก **OK**

ตรวจทานคอนฟิกูเรชันของคุณ

ในหน้าต่าง Status ให้ตรวจสอบความคืบหน้าของ ค่าติดตั้งคอนฟิกูเรชันต่างๆ ที่คุณได้เลือกไว้ หน้าต่างนี้อาจจะแสดงสถานะหยุดพัก สำหรับบางงานเป็นเวลา 2-3 นาที คลิก **View Log** เพื่อดูข้อความสถานะที่เกี่ยวข้องกับแต่ละงาน คลิก **Close** เมื่อไรก็ได้เพื่อปิดวิซาร์ด Guided Setup งานที่กำลังรันอยู่จะยังคงรันต่อไป ตอนนี้ HMC ของคุณได้ถูกกำหนดคอนฟิกแล้ว

การกำหนดคอนฟิก HMC โดยใช้เมนู HMC

ส่วนนี้มีรายการที่ครบถ้วนของงานคอนฟิกูเรชัน HMC ทั้งหมด ซึ่งช่วยแนะแนวทางตลอดกระบวนการกำหนดคอนฟิก HMC ของคุณ เลือก อีพพชันนี้ถ้าคุณไม่ต้องการใช้ตัวช่วยสร้างการติดตั้งที่แนะนำ

คุณต้องรีสตาร์ท HMC เพื่อให้ค่าที่ตั้งคอนฟิกูเรชันมีผลใช้งาน ดังนั้น คุณอาจต้องการพิมพ์รายการตรวจสอบนี้ และเก็บไว้กับคุณเมื่อทำการกำหนดคอนฟิก HMC

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

สิ่งที่ต้องการก่อน

ก่อนที่คุณจะเริ่มกำหนดคอนฟิก HMC โดยใช้เมนู HMC ตรวจสอบให้แน่ใจว่าได้ทำงานจัดเตรียมคอนฟิกูเรชัน ตามที่อธิบายใน “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23 แล้ว

ตารางที่ 7. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่สามารถหาข้อมูลที่เกี่ยวข้องได้

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. สตาร์ท HMC	“การเริ่มต้น HMC” ในหน้า 64
2. ตั้งค่าวันที่และเวลา	
3. เปลี่ยนรหัสผ่านที่กำหนดไว้ล่วงหน้า	
4. สร้างผู้ใช้เพิ่มเติม และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
5. กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก	“การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65
6. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิด และ IP แอดเดรสแบบฟิกซ์ ตั้งข้อมูล identification	
7. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิดและ IP แอดเดรสแบบฟิกซ์ ให้ตั้งค่า entry การเรดท์เป็นดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเรดท์เป็นดีฟอลต์เกตเวย์” ในหน้า 72
8. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิด และ IP แอดเดรสแบบฟิกซ์ ให้ตั้งค่าบริการโดเมนเนม	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 72
9. หากคุณกำลังใช้ IP แอดเดรสแบบฟิกซ์ และมีการใช้งาน DNS ให้ตั้งค่าโดเมนชัฟฟิกซ์	“การตั้งค่าคอนฟิกโดเมนชัฟฟิกซ์” ในหน้า 73
10. กำหนดคอนฟิกเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการ และสนับสนุน IBM และส่งคืนรายการตรวจสอบนี้ เมื่อคุณได้ทำขั้นตอนนี้เสร็จสิ้นแล้ว	“การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้” ในหน้า 75
11. เชื่อมต่อระบบที่ถูกจัดการเข้ากับแหล่งจ่ายไฟ	
12. ตั้งค่ารหัสผ่านให้กับระบบที่ถูกจัดการ และรหัสผ่านของ ASMI แต่ละรายการ (general และ admin)	“การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ” ในหน้า 80
13. เข้าใช้ ASMI เพื่อตั้งวันที่และเวลาบนระบบที่ถูกจัดการ	
14. สตาร์ทระบบที่ถูกจัดการ และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
15. ตรวจสอบว่า คุณมีหนึ่งโลจิคัลพาร์ติชันบนระบบที่ถูกจัดการ	

ตารางที่ 7. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่สามารถหาข้อมูลที่เกี่ยวข้องได้ (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
16. ทางเลือก: เพิ่มระบบที่ถูกจัดการอีก และกลับไปสู่รายการตรวจสอบเมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
17. ทางเลือก: หากคุณกำลังติดตั้งเซิร์ฟเวอร์ใหม่ด้วย HMC ของคุณ ให้ตั้งค่าโลจิสติกส์พาร์ติชันและติดตั้งระบบปฏิบัติการ	
18. หากคุณไม่ได้กำลังติดตั้งเซิร์ฟเวอร์ใหม่ในเวลานี้ให้ทำงาน postconfiguration ซึ่งเลือกดำเนินการได้ เพื่อปรับค่าคอนฟิกูเรชันของคุณต่อไปอีก	“ขั้นตอน Postconfiguration” ในหน้า 81

การเริ่มต้น HMC

คุณสามารถล็อกอินเข้าสู่ HMC และเลือกภาษาที่คุณต้องการจะแสดงในอินเทอร์เฟซ ใช้ User ID hscroot ที่เป็นค่าดีฟอลต์ และรหัสผ่าน abc123 เพื่อล็อกอินเข้าสู่ HMC ในครั้งแรก

ถ้าต้องการเริ่ม HMC, ให้ทำตามต่อไปนี้:

1. เปิด HMC โดยกดปุ่มเปิด/ปิด.
2. หากภาษาอังกฤษเป็น preference ภาษาของคุณ โปรดดำเนินการขั้นตอนที่ 4
ถ้าคุณต้องการใช้ภาษาอื่นที่นอกเหนือจากภาษาอังกฤษ ให้พิมพ์หมายเลข 2 เมื่อคุณได้รับข้อความเตือนให้เปลี่ยนโลแคล

หมายเหตุ: ข้อความแจ้งเตือนนี้จะปรากฏอยู่เป็นเวลา 30 นาทีหาก你不ดำเนินการใดๆ

3. เลือกโลแคลที่คุณต้องการแสดงผลจากรายการในหน้าต่าง Locale Selection และคลิก **OK** โลแคลจะระบุภาษาที่อินเทอร์เฟซ HMC ใช้
4. คลิก **Log on and launch the Hardware Management Console web application**
5. เข้าสู่ระบบ HMC โดยใช้ user ID และรหัสผ่านดีฟอลต์ต่อไปนี้:

ID: hscroot

รหัสผ่าน: abc123

6. และกด Enter

การเปลี่ยนวันที่และเวลา

นาฬิกาแบบใช้แบตเตอรี่จะบันทึกวันที่และเวลาไว้สำหรับ HMC คุณอาจต้องรีเซ็ตวันที่และเวลาของคอนโซลหากเปลี่ยนแบตเตอรี่หรือย้ายระบบของคุณไปยังเซตเวลาที่แตกต่าง ศึกษาเกี่ยวกับวิธีการเปลี่ยนวันที่และเวลาสำหรับ HMC

หากคุณเปลี่ยนข้อมูลของวันที่ และเวลา, การเปลี่ยนแปลงนั้นจะไม่ส่งผลกระทบต่อระบบ และโลจิสติกส์พาร์ติชันที่ HMC จัดการอยู่

ถ้าต้องการเปลี่ยนวันที่และเวลาสำหรับ HMC ให้ทำตามต่อไปนี้:

1. ตรวจสอบให้แน่ใจว่าคุณมีหนึ่งในบทบาทต่อไปนี้:
 - ผู้ดูแลระบบพิเศษ
 - ตัวแทนบริการ

- ผู้ควบคุมเครื่อง
 - ผู้ชม
2. ในพื้นที่การนำทางให้คลิก **HMC** การจัดการ
 3. ในหน้าต่างย่อยเนื้อหาให้คลิก **เปลี่ยน วันที่และเวลา**
 4. ถ้าคุณเลือก **UTC** ในฟิลด์ **Clock** การตั้งค่าเวลาจะมีการปรับโดยอัตโนมัติ เมื่อมีการเลื่อนเวลาใน เขตเวลาที่เลือกไว้ ใส่วนที่ เวลา และเขตเวลา แล้วคลิก **OK**

การตั้งค่าชนิดเน็ตเวิร์ก HMC

ตั้งค่า HMC ของคุณ เพื่อให้สามารถสื่อสารกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน ผู้ใช้ระยะไกล และบริการและการสนับสนุน ได้

การตั้งค่า HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ:

ตั้งค่า HMC เพื่อให้สามารถเชื่อมต่อกับและจัดการระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อ กับระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิด ให้ทำต่อไปนี้:

ตารางที่ 8. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

งาน	ที่ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ ขอแนะนำให้ใช้ eth0	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25
2. ระบุไอเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุไอเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0 ” ในหน้า 67
3. กำหนดคอนฟิกไอเทอร์เน็ตอะแดปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อต	“การตั้งค่าความเร็วของสล็อต” ในหน้า 69
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 69
c. ตั้งค่าสแตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 70
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 71
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” ในหน้า 72
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 72
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 80

การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อ กับระบบที่ถูกจัดการ:

กำหนดคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับ และจัดการระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กส่วนตัว

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับระบบที่ถูกจัดการโดยใช้เน็ตเวิร์กส่วนตัวให้ทำต่อไปนี้:

ตารางที่ 9. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กชิตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25
2. ระบุอ็อบเจกต์เน็ตเวิร์กให้กับ HMC ของคุณ	“การระบุอ็อบเจกต์เน็ตเวิร์กที่จะถูกกำหนดเป็น eth0” ในหน้า 67
3. กำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP	“การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 70
4. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 80

การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับ โลจิคัลพาร์ติชัน:

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ โลจิคัลพาร์ติชันได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 10. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กชิตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25
2. ระบุอ็อบเจกต์เน็ตเวิร์กให้กับ HMC ของคุณ	“การระบุอ็อบเจกต์เน็ตเวิร์กที่จะถูกกำหนดเป็น eth0” ในหน้า 67
3. กำหนดคอนฟิกอ็อบเจกต์เน็ตเวิร์กแต่ละตัวโดยการทำงานต่อไปนี้:	
a. ตั้งค่าความเร็วสล็อต	“การตั้งค่าความเร็วของสล็อต” ในหน้า 69
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 69
c. ตั้งค่าสแตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 70
d. ตั้งค่าไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 71
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าต์เป็นดีฟอลต์เกตเวย์” ในหน้า 72
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 72
4. ตั้งค่าอ็อบเจกต์เน็ตเวิร์กเพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 80

การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับ ผู้ใช้ระยะไกล:

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ ผู้ใช้ระยะไกลได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 11. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25
2. ระบุอีเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุอีเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0”
3. กำหนดคอนฟิกอีเทอร์เน็ตอะแดปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อต	“การตั้งค่าความเร็วของสล็อต” ในหน้า 69
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 69
c. ตั้งค่าสแตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 70
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 71
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” ในหน้า 72
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 72
g. ตั้งค่าซัพพลาย	“การตั้งค่าคอนฟิกโดเมนซัพพลาย” ในหน้า 73
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	

การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC:

เมื่อต้องการคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC เพื่อให้สามารถ รายงานปัญหาได้ให้ปฏิบัติตามต่อไปนี้:

ตารางที่ 12. การกำหนดคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ตรวจสอบให้แน่ใจว่าคุณมีข้อมูลลูกค้าที่จำเป็นทั้งหมด	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25
2. กำหนดคอนฟิก HMC นี้เพื่อรายงานข้อผิดพลาด หรือเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่เพื่อรายงานความผิดพลาด	“การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน” ในหน้า 75 “การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้” ในหน้า 78
3. ตรวจสอบว่าคอนฟิกูเรชัน Call-Home ของคุณใช้งานได้	“การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่” ในหน้า 79
4. ให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม	“การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” ในหน้า 79
5. จัดกำหนดการการส่งข้อมูลของข้อมูลระบบ	“ข้อมูลการบริการส่งข้อมูล” ในหน้า 79

การระบุอีเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0:

การเชื่อมต่ออีเทอร์เน็ตกับเซิร์ฟเวอร์ที่ถูกจัดการต้องกระทำโดยใช้อีเทอร์เน็ตพอร์ตที่กำหนดเป็น eth0 บน HMC ของคุณ

หากคุณยังไม่ได้ติดตั้งอีเทอร์เน็ตอะแดปเตอร์เสริมในสล็อต PCI บน HMC ของคุณ อีเทอร์เน็ตพอร์ตหลักภายในจะถูกกำหนดเป็น eth0 หรือ eth1 บน HMC ของคุณทุกครั้ง หากคุณต้องการใช้ HMC เป็นเซิร์ฟเวอร์ DHCP สำหรับระบบที่ถูกจัดการ

หากคุณติดตั้งอีเทอร์เน็ตอะแดปเตอร์เสริมไว้แล้วในสล็อต PCI พอร์ตที่กำหนดเป็น eth0 จะขึ้นกับตำแหน่งและประเภทของอีเทอร์เน็ตอะแดปเตอร์ที่คุณติดตั้ง

หมายเหตุ: กฎเหล่านี้เป็นกฎทั่วไป และอาจไม่มีผลกับ configuration ทั้งหมด

ตารางต่อไปนี้จะแสดงกฎของการติดตั้งอีเทอร์เน็ตตามประเภท HMC

ตารางที่ 13. ประเภท HMC และกฎที่เกี่ยวข้องสำหรับการติดตั้งอีเทอร์เน็ต

ประเภท HMC	กฎสำหรับการติดตั้งอีเทอร์เน็ต
HMC ที่ประกอบเข้ากับชั้นวางพร้อมอีเทอร์เน็ตพอร์ตภายในสองพอร์ต	HMC สนับสนุนอีเทอร์เน็ตอะแดปเตอร์เสริม 1 ตัวเท่านั้น - หากมีอีเทอร์เน็ตอะแดปเตอร์เสริมติดตั้งอยู่ พอร์ตนั้นจะถูกกำหนดเป็น eth0 ในกรณีนี้ อีเทอร์เน็ตพอร์ตหลักภายในจะถูกกำหนดเป็น eth1 และอีเทอร์เน็ตพอร์ตรองภายในจะถูกกำหนดเป็น eth2 - หากอีเทอร์เน็ตอะแดปเตอร์เป็นอีเทอร์เน็ตอะแดปเตอร์พอร์ตคู่ พอร์ตที่ติดเลเบล Act/Link A จะเป็น eth0 พอร์ตที่ติดเลเบล Act/link B จะเป็น eth1 ในกรณีนี้ อีเทอร์เน็ตพอร์ตหลักภายในจะถูกกำหนดเป็น eth2 และอีเทอร์เน็ตพอร์ตรองภายในจะถูกกำหนดเป็น eth3 - หากไม่มีอะแดปเตอร์ติดตั้งอยู่ อีเทอร์เน็ตพอร์ตหลักภายในจะถูกกำหนดเป็น eth0
รุ่นสแตนด์โลน 7310-C0x และ 7042-C0x ที่มีอีเทอร์เน็ตพอร์ตภายในเดียว	definition ขึ้นกับประเภทของอีเทอร์เน็ตอะแดปเตอร์ที่คุณติดตั้ง: - หากมีอีเทอร์เน็ตอะแดปเตอร์เดียวติดตั้งไว้ อะแดปเตอร์นั้นจะถูกกำหนดเป็น eth0 - หากอีเทอร์เน็ตอะแดปเตอร์เป็นอีเทอร์เน็ตอะแดปเตอร์พอร์ตคู่ พอร์ตที่ติดเลเบล Act/link A จะเป็น eth0 พอร์ตที่ติดเลเบล Act/link B จะเป็น eth1 ในกรณีนี้ อีเทอร์เน็ตพอร์ตภายในหลักจะถูกกำหนดเป็น eth2 - หากไม่มีอะแดปเตอร์ติดตั้งอยู่ อีเทอร์เน็ตพอร์ตภายในจะถูกกำหนดเป็น eth0 - หากมีอีเทอร์เน็ตอะแดปเตอร์ติดตั้งอยู่หลายตัว โปรดดูที่ “การพิจารณาชื่ออินเตอร์เฟซของอีเทอร์เน็ตอะแดปเตอร์”

การพิจารณาชื่ออินเตอร์เฟซของอีเทอร์เน็ตอะแดปเตอร์:

ถ้าคุณกำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP เซิร์ฟเวอร์นั้นสามารถดำเนินงานได้เฉพาะในตัวเชื่อมต่อ network interface card (NIC) ที่ HMC ระบุเป็น eth0 และ eth1 เท่านั้น คุณยังอาจต้องพิจารณาว่า ตัวเชื่อมต่อ NIC ใดที่คุณต้องการต่อเข้ากับเคเบิลอีเทอร์เน็ตด้วย ศึกษาเพิ่มเติมเกี่ยวกับการพิจารณาว่าตัวเชื่อมต่อ NIC ใดที่ HMC ระบุเป็น eth0 และ eth1

เมื่อต้องการพิจารณาชื่อที่ HMC กำหนดให้กับอีเทอร์เน็ตอะแดปเตอร์ให้ปฏิบัติตามนี้:

1. เปิดเชลล์เทอร์มินัลที่จำกัด เลือก **HMC Management > Open Restricted Shell Terminal**
2. พิมพ์ข้อความต่อไปนี้ที่บรรทัดคำสั่ง: `tail -f /var/log/messages` ไฟล์ล็อกข้อความจะเลื่อนไปเมื่อมีเหตุการณ์ใหม่เกิดขึ้น
3. ต่อสายเคเบิลอีเทอร์เน็ตของคุณ ถ้ามีการต่อสายเคเบิลนั้นแล้ว ให้ถอดออก รอประมาณ 5 วินาที แล้วต่อสายอีกครั้ง เชลล์ที่จำกัดจะเลื่อนไปเพื่อแสดงข้อความเมื่อคุณต่อสายเคเบิล entry ตัวอย่างต่อไปนี้แสดงว่าอีเทอร์เน็ตพอร์ตนี้อัปเดตเป็น `eth0: Aug 28 12:41:20 termite kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100`
4. ทำโปรซีเดอร์นี้ซ้ำสำหรับอีเทอร์เน็ตพอร์ตอื่นๆ ทั้งหมด และบันทึกผลลัพธ์ของคุณ
5. พิมพ์ `Ctrl+C` เพื่อหยุดคำสั่ง `tail`

การตั้งค่าความเร็วของสื่อบันทึก:

ศึกษาเกี่ยวกับวิธีการระบุความเร็วของสื่อบันทึก ซึ่งรวมถึง ความเร็วและโหมด duplex ของอะแดปเตอร์อีเทอร์เน็ต

ดีฟอลต์สำหรับค่าติดตั้งอะแดปเตอร์ HMC คือ **Autodetection** ถ้าอะแดปเตอร์นี้ถูกเชื่อมต่อกับสวิตช์ LAN คุณต้องจับคู่ค่าติดตั้งพอร์ตของสวิตช์ เมื่อต้องการ ตั้งค่าความเร็วสื่อบันทึกและ duplex ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก **HMC การจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน แล้วคลิก **Details**
5. ในส่วนข้อมูล Local area network ให้เลือก **Autodetection** หรือ ความเร็วสื่อบันทึกและ duplex ที่เหมาะสม
6. คลิก **OK**

การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด:

เน็ตเวิร์กส่วนบุคคล ประกอบด้วย HMC และระบบที่ถูกจัดการ เน็ตเวิร์กส่วนบุคคลจะถูกจำกัดอยู่แค่คอนโซลและระบบที่ถูกจัดการ และจะแยกต่างหากจากเน็ตเวิร์กภายในบริษัท *เน็ตเวิร์กแบบเปิด* ประกอบด้วยเน็ตเวิร์กส่วนบุคคล และเน็ตเวิร์กภายในบริษัท เน็ตเวิร์กแบบเปิดอาจประกอบด้วยจุดสิ้นสุดเน็ตเวิร์กนอกเหนือจากคอนโซล และระบบที่ถูกจัดการ และยังครอบคลุมถึงอุปกรณ์เน็ตเวิร์กย่อย และเน็ตเวิร์ก

เมื่อต้องการเลือกเน็ตเวิร์กส่วนบุคคลหรือพับลิคเน็ตเวิร์ก ให้ปฏิบัติตามนี้:

1. ในพื้นที่การนำทางให้คลิก **HMC การจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **Lan Adapter**
6. ในหน้าข้อมูล Local area network เลือก **Private** หรือ **Open**
7. คลิก **OK**

การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP:

Dynamic Host Configuration Protocol (DHCP) มีวิธีอัตโนมัติสำหรับการตั้งค่าคอนฟิกไคลเอ็นต์แบบไดนามิก

เมื่อต้องการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP ให้ทำดังนี้:

1. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
2. ในพื้นที่ใช้งาน ให้คลิก **Change network settings** หน้าต่าง Customize Network Settings จะเปิด
3. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
4. เลือก ส่วนตัว จากนั้นเลือก ชนิดของเน็ตเวิร์ก
5. ในส่วนเซิร์ฟเวอร์ DHCP เลือก **เปิดใช้งานเซิร์ฟเวอร์ DHCP** เพื่อ เปิดใช้งาน HMC เป็น เซิร์ฟเวอร์ DHCP

หมายเหตุ: คุณสามารถตั้งค่า HMC ที่จะเป็นเซิร์ฟเวอร์ DHCP บนเน็ตเวิร์กส่วนตัวเท่านั้น ถ้าคุณใช้เครือข่ายแบบเปิด คุณไม่มี อีอพชั่นในการเลือก **เปิดใช้งาน DHCP**

6. เลือกช่วงแอดเดรสของเซิร์ฟเวอร์ DHCP
7. คลิก **OK**

ถ้าคุณได้ตั้งค่า HMC ของคุณไปเป็นเซิร์ฟเวอร์ DHCP บนเน็ตเวิร์กส่วนตัวแล้ว คุณต้องตรวจสอบว่า คุณได้ตั้งค่าเน็ตเวิร์กส่วนตัว HMC DHCP อย่างถูกต้อง สำหรับข้อมูลเกี่ยวกับการเชื่อมต่อ HMC เข้ากับเน็ตเวิร์กส่วนตัว, โปรดดูที่ “การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 69

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 7

การตั้งค่า IPv4 address:

ศึกษาถึงวิธีการตั้งค่า IPv4 address ของคุณบน HMC

1. ใน พื้นที่การนำทาง ให้คลิก **HMC การจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **ค่าติดตั้งพื้นฐาน**
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:

ศึกษาเกี่ยวกับวิธีการตั้งค่า IPv6 ของคุณบน HMC

1. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**

5. คลิกแท็บ **IPv6 Settings**
6. เลือกอ็อปชัน **Autoconfig** หรือเพิ่ม IP แอดเดรสแบบสแตติก
7. ถ้าคุณได้เพิ่ม IP แอดเดรสแล้ว ให้ป้อน IPv6 แอดเดรสและความยาวของคำนำหน้า และคลิก **ตกลง**
8. คลิก **OK**

การใช้ IPv6 แอดเดรสเท่านั้น:

ศึกษาเกี่ยวกับวิธีการตั้งค่า HMC เพื่อให้ใช้ IPv6 แอดเดรสเท่านั้น

1. ในพื้นที่การนำทาง ให้คลิก **HMC การจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. เลือก **ไม่มีแอดเดรส IPv4**
6. คลิกแท็บ **IPv6 Settings**
7. เลือก **ใช้ DHCPv6** เพื่อตั้งค่า IP หรือ เพิ่ม IP แอดเดรสแบบสแตติก จากนั้นคลิก **ตกลง**

หลังจากที่คุณคลิก **ตกลง** คุณต้องรีบูต HMC ของคุณเพื่อให้การเปลี่ยนแปลงมีผลบังคับใช้

การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC

ในเน็ตเวิร์กแบบเปิด ไฟร์วอลล์จะถูกใช้เพื่อควบคุมการเข้าสู่เน็ตเวิร์กภายในบริษัทจากภายนอก HMC ก็มีไฟร์วอลล์ในอะแดปเตอร์อีเทอร์เน็ตแต่ละตัว เมื่อต้องการควบคุม HMC จากระยะไกล หรือให้รีโมตแอ็กเซสแก่บุคคลอื่น แกะไขการตั้งค่าคอนฟิกไฟร์วอลล์ของอีเทอร์เน็ตอะแดปเตอร์บน HMC ซึ่งเชื่อมต่อกับเน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิกไฟร์วอลล์, ให้ใช้ขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **HMC การจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **Firewall**
6. โดยการใช้วิธีใดวิธีหนึ่งต่อไปนี้ คุณสามารถอนุญาตให้ IP แอดเดรสใดๆ ใช้แอพลิเคชันเฉพาะผ่านไฟร์วอลล์ หรือคุณสามารถระบุ IP แอดเดรสมากกว่าหนึ่งได้:
 - อนุญาตให้ IP แอดเดรสใดๆ ที่ใช้แอพลิเคชันเฉพาะผ่านไฟร์วอลล์ได้:
 - a. จากช่องด้านบน, ให้เลือกแอพลิเคชัน
 - b. คลิก **Allow Incoming** แอปพลิเคชันจะไปปรากฏอยู่ในช่องด้านล่างเพื่อแสดงว่าถูกเลือกแล้ว
 - ระบุ IP แอดเดรสเพื่ออนุญาตให้ผ่านไฟร์วอลล์ได้:
 - a. จากช่องด้านบน ให้เลือกแอพลิเคชัน
 - b. คลิก **Allow Incoming by IP Address**
 - c. ในหน้าต่าง **Hosts Allowed**, ป้อน IP แอดเดรสและ network mask
 - d. คลิก **Add** และคลิก **OK**

7. คลิก OK

การเปิดใช้การเข้าถึงเซลล์ที่จำกัดแบบรีโมต:

คุณสามารถเปิดใช้การเข้าถึงเซลล์ที่จำกัดแบบรีโมตได้ เมื่อตั้งค่าไฟร์วอลล์

เมื่อต้องการเปิดใช้งานการเข้าถึงเซลล์ที่จำกัดแบบรีโมตให้ทำดังนี้:

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

ถึงตอนนี้ การเข้าถึงเซลล์ที่จำกัดแบบรีโมตถูกเปิดใช้งานแล้ว

การเปิดใช้งาน การเข้าถึงเว็บแบบรีโมต:

คุณสามารถเปิดใช้งานการเข้าถึงเว็บแบบรีโมตด้วย HMC ของคุณ

เมื่อต้องการเปิดใช้งานการเข้าถึงเว็บแบบรีโมตให้ทำดังนี้:

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

ถึงตอนนี้ การเข้าถึงเว็บแบบรีโมตถูกเปิดใช้งานแล้ว

การกำหนดคอนฟิก entry การเรตต์เป็นดีฟอลต์เกตเวย์

ศึกษาเกี่ยวกับวิธีการตั้งค่าการเรตต์ entry ตามดีฟอลต์เกตเวย์งานนี้สามารถใช้ได้กับการตั้งค่าที่ใช้เน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิก entry การเรตต์เป็นดีฟอลต์เกตเวย์ให้ปฏิบัติตามนี้:

1. ในพื้นที่การนำทาง ให้คลิก HMC การจัดการ
2. ในพื้นที่ใช้งาน ให้คลิก Change network settings หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ Routing
4. ในส่วนข้อมูลดีฟอลต์เกตเวย์ ป้อนเกตเวย์แอดเดรสและอุปกรณ์เกตเวย์ของ entry การเรตต์ที่คุณต้องการกำหนดเป็นดีฟอลต์เกตเวย์
5. คลิก OK

การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส

ถ้าคุณวางแผนที่จะติดตั้งเน็ตเวิร์กแบบเปิดให้ตั้งค่าโดเมนเนมเซอร์วิส

ถ้าคุณวางแผนที่จะติดตั้งเน็ตเวิร์กแบบเปิดให้ตั้งค่าโดเมนเนมเซอร์วิส Domain Name System (DNS) is a เป็นระบบฐานข้อมูลแบบกระจายสำหรับการจัดการชื่อของโฮสต์ และ Internet Protocol (IP) แอดเดรสที่เชื่อมโยงกัน การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิสประกอบด้วยการเปิดใช้งาน DNS และการระบุโดเมนซัพพลิคชันหา

1. ในพื้นที่การนำทาง ให้คลิก HMCการจัดการ

2. ในพื้นที่ใช้งาน ให้คลิก **Change network settings** หน้าต่าง Change Network Settings จะเปิด
3. คลิกแท็บ **Name Services**
4. เลือก **เปิดใช้งาน DNS** เพื่อเปิดใช้งาน DNS
5. ระบุเซิร์ฟเวอร์ DNS และโดเมนซัพพลิคส์ค้นหา แล้วคลิก **Add**
6. คลิก **OK**

การตั้งค่าคอนฟิกโดเมนซัพพลิคส์

รายการโดเมนซัพพลิคส์ใช้สำหรับ resolve IP แอดเดรส โดยเริ่มจาก entry แรกที่พบในรายการ

โดเมนซัพพลิคส์คือสตริงที่ต่อท้ายด้วยชื่อโฮสต์ซึ่งช่วยในการแปลงค่า IP แอดเดรสของรายการ ตัวอย่างเช่น ชื่อโฮสต์ของ myname อาจแปลงไม่ได้ อย่างไรก็ตาม หากสตริง myloc.mycompany.com เป็นสมาชิกของตารางโดเมนซัพพลิคส์ เครื่องจะพยายามแปลง myname.mloc.mycompany.com ด้วยเช่นกัน

เมื่อต้องการ กำหนดคอนฟิกของรายการโดเมนซัพพลิคส์ ให้ใช้ขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **การจัดการ HMC**
2. ในพื้นที่ใช้งาน ให้คลิก **Change network settings** หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ **Name Services**
4. ป้อนสตริงที่จะใช้เป็น entry ของโดเมนซัพพลิคส์
5. คลิก **Add** เพื่อเพิ่ม entry นั้นลงในรายการ

การคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP

คุณสามารถคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP (Lightweight Directory Access Protocol)

เมื่อผู้ใช้ลงชื่อเข้าใช้ HMC ระบบจะ ดำเนินการพิสูจน์ตัวตนของไฟล์รหัสผ่านภายในก่อน หากไม่พบไฟล์รหัสผ่านภายใน HMC สามารถติดต่อเซิร์ฟเวอร์ LDAP ระยะไกลสำหรับการพิสูจน์ตัวตนได้ คุณต้องคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP

หมายเหตุ: ก่อนที่คุณจะคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตน LDAP คุณต้อง ตรวจสอบให้แน่ใจว่ามีการเชื่อมต่อเน็ตเวิร์กการทำงานระหว่าง HMC และเซิร์ฟเวอร์ LDAP สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการคอนฟิกการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65

เมื่อต้องการคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตน LDAP ให้ปฏิบัติตามดังต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **การจัดการ HMC**
2. ในพื้นที่เนื้อหา ให้คลิก **คอนฟิกูเรชัน LDAP** หน้าต่างนิยามเซิร์ฟเวอร์ LDAP จะปรากฏขึ้น
3. เลือก **เปิดใช้งาน LDAP**
4. กำหนดเซิร์ฟเวอร์ LDAP ที่จะใช้สำหรับการพิสูจน์ตัวตน
5. กำหนดแอตทริบิวต์ LDAP ที่ใช้ในการระบุผู้ใช้ที่กำลังได้รับ การพิสูจน์ตัวตน ค่าดีฟอลต์คือ uid แต่คุณสามารถ ใช้แอตทริบิวต์ของคุณเองได้
6. กำหนดรหัสชื่อที่แตกต่าง ซึ่งเป็นฐานการค้นหาสำหรับเซิร์ฟเวอร์ LDAP
7. คลิก **OK**

8. ถ้าผู้ใช้ต้องการใช้การพิสูจน์ตัวตน LDAP ผู้ใช้ต้อง กำหนดคอนฟิกโปรไฟล์ของตนเพื่อให้มีการใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP แทนการพิสูจน์ตัวตนภายใน

การกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos

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

เมื่อผู้ใช้ลงชื่อเข้าใช้ HMC ระบบจะ ดำเนินการพิสูจน์ตัวตนของไฟล์รหัสผ่านภายในก่อน หากไม่พบไฟล์รหัสผ่านภายใน HMC สามารถติดต่อเซิร์ฟเวอร์ Kerberos ระยะไกลสำหรับการพิสูจน์ตัวตนได้ คุณต้องกำหนดคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย Kerberos

หมายเหตุ: ก่อนที่คุณจะกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos คุณต้องตรวจสอบให้แน่ใจว่ามีการเชื่อมต่อเน็ตเวิร์กการทำงาน ระหว่าง HMC และเซิร์ฟเวอร์ KDC สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 65

เมื่อต้องการกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตนระยะไกล ด้วย Kerberos ปฏิบัติดังต่อไปนี้:

1. เปิดใช้งานเซอวิส Network Time Protocol (NTP) บน HMC และตั้งค่าเซิร์ฟเวอร์ HMC และ KDC ให้ซิงโครไนซ์โดยใช้เซิร์ฟเวอร์ NTP เดียวกัน เมื่อต้องการเปิดใช้งานเซอวิส NTP บน HMC ให้ปฏิบัติตามดังต่อไปนี้:
 - a. ในพื้นที่การนำทาง ให้เลือก **HMC Management**
 - b. ในพื้นที่เนื้อหา ให้เลือก **เปลี่ยนวันที่ และเวลา**
 - c. เลือกแท็บ **คอนฟิกูเรชัน NTP**
 - d. เลือก **เปิดใช้งานเซอวิส NTP บน HMC นี้**
 - e. คลิก **OK**
2. คอนฟิกแต่ละโปรไฟล์ผู้ใช้ของ HMC ระยะไกลเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย Kerberos แทนที่จะใช้การพิสูจน์ตัวตนภายใน
3. ทางเลือก: คุณสามารถอิมพอร์ตไฟล์คีย์เซอวิสลงใน HMC นี้ได้ ไฟล์คีย์เซอวิสจะมีบัญชีโฮสต์ที่ระบุ HMC ให้แก่เซิร์ฟเวอร์ไฟล์คีย์เซอวิสรู้จักกันในชื่อของ **คีย์แท็บ** เมื่อต้องการอิมพอร์ตไฟล์คีย์เซอวิสลงใน HMC นี้ ให้ปฏิบัติตามดังต่อไปนี้:
 - a. ในพื้นที่การนำทาง ให้เลือก **HMC Management**
 - b. ในพื้นที่เนื้อหา ให้เลือก **กำหนดคอนฟิก KDC** หน้าต่างคอนฟิกูเรชัน Key Distribution Center จะปรากฏขึ้น
 - c. เลือก **การดำเนินการ > อิมพอร์ตเซอวิสคีย์** หน้าต่าง อิมพอร์ตคีย์เซอวิส จะปรากฏขึ้น
 - d. พิมพ์ตำแหน่งของไฟล์คีย์เซอวิส
 - e. คลิก **OK**
4. เพิ่มเซิร์ฟเวอร์ KDC ใหม่ลงใน HMC นี้ เมื่อต้องการเพิ่มเซิร์ฟเวอร์ KDC ใหม่ลงใน HMC นี้ ให้ปฏิบัติตามดังต่อไปนี้:
 - a. ในพื้นที่การนำทาง ให้เลือก **HMC Management**
 - b. ในพื้นที่เนื้อหา ให้เลือก **กำหนดคอนฟิก KDC** หน้าต่างคอนฟิกูเรชัน Key Distribution Center จะปรากฏขึ้น
 - c. เลือก **การดำเนินการ > เพิ่มเซิร์ฟเวอร์ KDC** หน้าต่าง อิมพอร์ตคีย์เซอวิส จะปรากฏขึ้น
 - d. พิมพ์ชื่อกลุ่มระบบเครือข่ายและชื่อโฮสต์ หรือ IP แอดเดรสของเซิร์ฟเวอร์ KDC

e. คลิก OK

การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้

คอนฟิก HMC ของคุณเพื่อให้สามารถแจ้งให้คุณทราบเมื่อเกิดปัญหาขึ้น

การคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับฝ่ายบริการและสนับสนุนได้โดยใช้ชาร์ตการติดตั้ง Call-Home:

คอนฟิก HMC เพื่อให้เป็นเซิร์ฟเวอร์ Call-Home โดยใช้ชาร์ต Call-Home

โปรซีเดอร์นี้จะอธิบายวิธีตั้งค่า HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้การเชื่อมต่อกับอินเทอร์เน็ตโดยตรง (ทาง LAN) และโดยอ้อม (SSL)

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23
- ถ้า คุณกำหนดคอนฟิกการสนับสนุนอินเทอร์เน็ตผ่านทางพรีอ็อกซีเซิร์ฟเวอร์ คุณยังต้องมีสิ่งต่อไปนี้ด้วย:
 - IP แอดเดรสและพอร์ตของพรีอ็อกซีเซิร์ฟเวอร์
 - ข้อมูลการพิสูจน์ตัวตนสำหรับพรีอ็อกซี
- มีการใช้อะแดปเตอร์ที่กำหนดเป็น eth1 (ซึ่งกำหนดเป็นเน็ตเวิร์กแบบเปิด) สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC” ในหน้า 13
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

เมื่อต้องการกำหนดคอนฟิก HMC เพื่อให้เป็นเซิร์ฟเวอร์ Call-Home โดยใช้ชาร์ต Call-Home ให้ทำดังนี้:

1. ในพื้นที่การนำทาง ให้เลือก การจัดการเซอวิส
2. ในพื้นที่เนื้อหา ให้เลือก ตัวช่วยสร้างเซตอัพ Call-Home วิชาร์ตการเชื่อมต่อและเซิร์ฟเวอร์ Call-Home จะเปิดขึ้น ปฏิบัติตามคำแนะนำในวิชาร์ตเพื่อกำหนดคอนฟิก Call-Home

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน:

คอนฟิก HMC นี้เพื่อให้สามารถติดต่อผู้ให้บริการเกี่ยวกับความผิดพลาดได้โดยใช้การเชื่อมต่อทาง LAN โทรศัพท์หรือโมเด็ม หรือ VPN

การคอนฟิก HMC เพื่อติดต่อบริการและสนับสนุนโดยใช้อินเทอร์เน็ต ทาง LAN และ SSL:

อธิบายถึงวิธีการกำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้การเชื่อมต่อกับอินเทอร์เน็ตโดยตรง (ทาง LAN) และโดยอ้อม (SSL)

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว ตรวจสอบค่านี้ โดยไปที่อินเทอร์เน็ตเฟส HMC และคลิก **Service Management > Manage Customer Information**
- ถ้าคุณกำหนดคอนฟิกการสนับสนุนอินเทอร์เน็ตผ่านทางพรีอ็อกซีเซิร์ฟเวอร์ คุณจะต้อง มีสิ่งต่างๆ ต่อไปนี้เช่นกัน:

- IP แอดเดรสและพอร์ตของพรีอ็อกซีเซิร์ฟเวอร์
- ข้อมูลการพิสูจน์ตัวตนสำหรับพรีอ็อกซี
- คุณจำเป็นต้องคอนฟิกอย่างน้อยหนึ่งเน็ตเวิร์กอินเตอร์เฟซที่เปิดอยู่ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “เน็ตเวิร์กส่วนตัว และเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 6
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

เมื่อต้องการกำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ Call-home โดยใช้อินเทอร์เน็ตทาง LAN และ SSL ให้ทำดังนี้:

1. ในพื้นที่การนำทาง ให้คลิก **Service Management**
2. ในส่วน **Connectivity** ให้คลิก **Manage Outbound Connectivity** หน้าต่างคอนโซลเซิร์ฟเวอร์ Call-Home จะปรากฏขึ้น
3. คลิก **Configure...**
4. ในหน้าต่าง คำติดตั้งการเชื่อมต่อขาออก ให้เลือก **เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ Call-Home**
5. ยอมรับข้อตกลง
6. ในหน้าต่าง คำติดตั้งการเชื่อมต่อขาออก ให้เลือกแท็บ **Internet**
7. ทำเครื่องหมายในกล่อง **Allow an existing internet connections for service**
8. ถ้าคุณกำลังใช้พรีอ็อกซี SSL ให้เลือก **Use SSL proxy**
9. ถ้าคุณใช้พรีอ็อกซี SSL ให้ใส่แอดเดรสและพอร์ตของพรีอ็อกซี ขอรับข้อมูลนี้ได้จากผู้บริหารเน็ตเวิร์ก
10. ถ้าคุณเลือก **Use SSL proxy** และพรีอ็อกซีต้องการพิสูจน์ตัวตนด้วย user ID และรหัสผ่าน ให้เลือก **Authenticate with the SSL proxy** พิมพ์ userid และรหัสผ่าน ขอรับข้อมูล user ID และรหัสผ่านได้จากผู้บริหารเน็ตเวิร์ก
11. เลือก **โปรโตคอลของอินเทอร์เน็ต** ที่คุณต้องการใช้
12. บนแท็บ **Internet** ให้คลิก **Test...**
13. ในหน้าต่าง Test Internet ให้คลิก **Start**
14. ตรวจสอบว่าการทดสอบเสร็จสิ้นสมบูรณ์
15. ในหน้าต่าง Test Internet ให้คลิก **Cancel**
16. ในหน้าต่างคำติดตั้งการเชื่อมต่อขาออก ให้คลิก **OK**

การเชื่อมต่อระบบให้บริการและสนับสนุนโดยใช้โทรศัพท์และโมเด็ม:

อธิบายวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้โมเด็มเป็นตัวเข้าถึงระบบสนับสนุนของ IBM

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- คุณมีสายโทรศัพท์นาล็อกที่จัดเตรียมไว้โดยเฉพาะ
- คุณมีข้อมูลที่จำเป็นสำหรับการตั้งค่าโมเด็ม สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว คุณอาจตรวจสอบ โดยการไปที่อินเตอร์เฟซ HMC และคลิก **Service Management > Manage Customer Information**
- ตรวจสอบว่าคุณมีข้อมูลต่อไปนี้:
 - ประเภทของสายนาล็อก กล่าวคือ เป็น tone หรือ pulse สายส่วนใหญ่ เป็นประเภท tone แต่บางสายยังคงเป็นประเภท rotary หรือ pulse แบบเดิม

- เมื่อยกหูโทรศัพท์แล้ว สายโทรศัพท์ที่มีเสียงสัญญาณ หรือไม่ สายโทรศัพท์ส่วนใหญ่มีเสียง แต่บางสายอาจไม่มีเสียง
- ต้องใช้หมายเลขนำหน้าสำหรับการหมุนโทรศัพท์หรือไม่ หมายเลขนำหน้า สำหรับการหมุนโทรศัพท์คือหมายเลขหรือชุดหมายเลขที่ช่วยให้โทรออกได้

เมื่อต้องการกำหนดคอนฟิก HMC ให้เป็นเซิร์ฟเวอร์ call-home โดยใช้โมเด็มเป็นตัวเข้าถึง การสนับสนุนของ IBM support, ให้ทำดังต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **Service Management**
2. ในส่วน **Connectivity** ให้คลิก **Manage Outbound Connectivity**
3. คลิก **Configure**
4. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้เลือก **เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ call-home**
5. ยอมรับข้อตกลง
6. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้คลิกแท็บ **โลคัล โมเด็ม**
7. บนหน้าโลคัลโมเด็ม ให้เลือกเช็kb็อกซ์อนุญาตให้ใช้ การหมุนโลคัลโมเด็มสำหรับเซอร์วิส
8. บนหน้าโลคัลโมเด็ม ให้เลือกเช็kb็อกซ์โมเด็มคอนฟิกรูชัน
9. ในหน้าต่าง **Customize Modem Settings** ให้คลิก **Dial type, Tone or Pulse** ถ้าสายโทรศัพท์ที่มีเสียงสัญญาณ เมื่อยกหูโทรศัพท์ ให้เลือกเช็kb็อกซ์ **รอสัญญาณหมุน** กรอกหมายเลขนำหน้าสำหรับการหมุนโทรศัพท์ เพื่อให้คุณสามารถโทรออกได้
10. คลิก **OK**
11. บนหน้าโลคัลโมเด็ม ให้คลิก **เพิ่ม**
12. เลือกหมายเลขจากรายการ
13. ถ้าเป็นหมายเลขในท้องถิ่น ให้ลบรหัสพื้นที่ออกจากฟิลด์ **Telephone number**
14. ในพาเนล **Add Telephone Number** ให้คลิก **Add**
15. ในพาเนล **Customize Modem Settings** ให้คลิก **Test**
16. ในพาเนล **Test Telephone Number** ให้คลิก **Start**
17. ตรวจสอบว่าการทดสอบเสร็จสิ้นสมบูรณ์
18. ในหน้าต่าง **Test Telephone Number** ให้คลิก **Cancel**
19. คุณสามารถกำหนดคอนฟิกหมายเลขโทรศัพท์ได้ไม่เกินห้าหมายเลข กำหนดคอนฟิก หมายเลขโทรศัพท์อย่างน้อยสองหมายเลข (หลักและรอง) ระบบจะ ลองหมุนหมายเลขตามลำดับที่กำหนดคอนฟิกไว้ เมื่อต้องการเพิ่ม หมายเลขเพิ่มเติมลงในรายการที่สามารถโทรได้ ให้ทำซ้ำขั้นตอนต่างๆ ในกระบวนการนี้
20. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้คลิก **OK**

การเชื่อมต่อระบบให้บริการและสนับสนุนโดยใช้ VPN บน LAN:

ตั้งค่าเซิร์ฟเวอร์ call-home โดยใช้ VPN

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 23

- มีการใช้แอสแตริสค์ที่กำหนดเป็น eth1 (ซึ่งกำหนดเป็นเน็ตเวิร์กแบบเปิด) สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC” ในหน้า 13
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว ตรวจสอบค่านี้โดยคลิก **Service Management > Manage Customer Information** บนอินเทอร์เฟซ HMC

เมื่อต้องการกำหนดคอนฟิกเซิร์ฟเวอร์ call-home โดยใช้ VPN ให้ทำตามต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก **Service Management**
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity**
3. คลิก **Configure**
4. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้เลือก เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ call-home
5. ยอมรับข้อตกลง
6. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้คลิกแท็บ **Internet VPN**
7. บนหน้าอินเทอร์เฟซ VPN ให้เลือก อนุญาตให้ใช้ VPN และการเชื่อมต่ออินเทอร์เน็ตที่มีอยู่สำหรับเซิร์ฟเวอร์
8. บนหน้าอินเทอร์เฟซ VPN ให้คลิกเช็กล่องทดสอบ
9. ในหน้าต่าง Test Internet VPN ให้คลิก **Start**
10. ตรวจสอบว่าการทดสอบเสร็จสิ้นสมบูรณ์
11. ในหน้าต่าง Test Internet VPN ให้คลิก **Cancel**
12. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้คลิก **OK**

การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้:

เลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วของ HMC ซึ่งมีการจดจำไว้แล้ว หรือ “ค้นพบ” โดย HMC นี้เพื่อรายงานข้อผิดพลาด

HMC ที่ค้นพบเป็น HMC ที่เปิดใช้งานเป็นเซิร์ฟเวอร์ Call-Home และอยู่บนชั้นเน็ตเดียวกัน หรือจัดการระบบที่ถูกจัดการเดียวกันกับ HMC นี้

เมื่อต้องการเลือก HMC ที่ค้นพบเพื่อติดต่อผู้ให้บริการเมื่อ HMC นี้รายงานข้อผิดพลาด ให้ปฏิบัติตามต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก **การจัดการเซิร์ฟเวอร์**
2. ในพื้นที่เนื้อหาให้คลิก **จัดการการเชื่อมต่อขาออก** หน้าต่างคอนโซลเซิร์ฟเวอร์ Call-Home จะปรากฏขึ้น
3. คลิก **ใช้คอนโซลเซิร์ฟเวอร์ call-home** ที่พบ HMC จะแสดง IP แอดเดรสหรือชื่อโฮสต์ของ HMC ที่คอนฟิกสำหรับ Call-Home
4. คลิก **OK**

หมายเหตุ: ไม่ควรเพิ่ม HMC ที่ต่ำกว่าเวอร์ชัน 7.1.0 เป็นพรีอ็อกซีเซิร์ฟเวอร์ Call-Home ใน HMC ที่เท่ากับ หรือสูงกว่าเวอร์ชัน 7.1.0

คุณยังสามารถเพิ่มเซิร์ฟเวอร์ Call-Home ของ HMC ที่มีอยู่ซึ่งอยู่บนชั้นเน็ตอื่นได้เอง เลือก IP แอดเดรสหรือชื่อโฮสต์ของ HMC ที่ถูกกำหนดคอนฟิกสำหรับการติดต่อโฮม และคลิก **เพิ่ม** จากนั้นคลิก **ตกลง**

การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่:

ทดสอบการรายงานปัญหาเพื่อตรวจสอบให้แน่ใจว่า การเชื่อมต่อไปยังส่วนบริการ และสนับสนุนกำลังทำงานอยู่

เมื่อต้องการตรวจสอบว่าคอนฟิгурेशन call-home ทำงานอยู่ให้ทำดังนี้:

1. ในพื้นที่การนำทางให้คลิก **Service Management**
2. ในพื้นที่ใช้งาน ให้คลิก **Create Event**
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. ตรวจสอบว่ามีกำหนดเหตุการณ์ PMH และหมายเลขให้กับหมายเลขปัญหา ที่คุณเปิด
8. เลือกเหตุการณ์และเลือกปิด
9. บนหน้าต่าง ปิด ให้พิมพ์ชื่อของคุณและความคิดเห็นสั้นๆ

การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม:

คุณต้องให้สิทธิ์แก่ผู้ใช้ในการดูข้อมูลเกี่ยวกับระบบของคุณ

ก่อนที่คุณจะให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวมมา คุณต้องขอรับ IBM ID ก่อน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการขอรับ IBM ID โปรดดูที่ “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 25

เมื่อต้องการให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม ให้ปฏิบัติตามดังต่อไปนี้:

1. ในพื้นที่การนำทาง ให้เลือก การจัดการเซอวิส
2. ในพื้นที่เนื้อหา ให้เลือก ผู้ใช้ที่ได้รับสิทธิ์
3. ป้อน IBM ID ของคุณ
4. คลิก **OK**

ข้อมูลการบริการส่งข้อมูล:

คุณสามารถส่งข้อมูลไปยังผู้ให้บริการของคุณได้ในทันที หรือคุณสามารถจัดกำหนดการให้ส่งข้อมูลเป็นประจำได้

IBM จัดเตรียมฟังก์ชันสำหรับเว็บที่ทำให้เป็นส่วนตัว ซึ่งใช้ข้อมูลที่เก็บรวบรวมโดย IBM Electronic Service Agent เพื่อใช้ฟังก์ชันเหล่านี้ คุณต้องลงทะเบียนบนเว็บไซต์ IBM Registration ก่อนที่ <http://www.ibm.com/account/profile> เมื่อต้องการอนุญาตให้ผู้ใช้งานใช้ข้อมูล Electronic Service Agent เพื่อทำฟังก์ชันสำหรับเว็บให้เป็นส่วนตัว โปรดดูที่ “การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ข้อดีของการลงทะเบียน IBM ID กับระบบของคุณ โปรดดูที่ <http://www.ibm.com/support/electronic>

หมายเหตุ: คุณควรส่งผ่านข้อมูลผู้ให้บริการหลังจากที่ได้ติดตั้งและกำหนดคอนฟิก HMC เพื่อใช้งาน

เมื่อต้องการส่งข้อมูลการบริการให้ทำดังนี้:

1. ในพื้นที่การนำทางให้คลิก **Service Management**

2. ในพื้นที่เนื้อหาให้คลิก **Transmit Service Information**
3. ดำเนินงานให้เสร็จสมบูรณ์ในหน้าต่างรายละเอียดเซอวิซการกระจายสัญญาณ แล้วคลิก **OK**.

การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ

คุณต้องตั้งรหัสผ่านสำหรับเซิร์ฟเวอร์และ Advanced System Management (ASM) ของคุณ อ่านเพิ่มเติมเกี่ยวกับวิธีการใช้อินเตอร์เฟซ HMC เพื่อตั้งรหัสผ่านเหล่านี้

หากคุณได้รับข้อความ Authentication Pending HMC จะเตือนให้คุณตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ

หาก你不ได้รับข้อความ Authentication Pending ให้ทำขั้นตอนต่อไปนี้ให้เสร็จสิ้น เพื่อตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ

การอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณ:

เมื่อต้องการอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณให้ทำดังนี้:

1. ในพื้นที่การนำทางให้เลือกระบบที่ถูกจัดการ
2. ในพื้นที่งานให้คลิก **Operations**
3. คลิก **Change Password** หน้าต่าง Update Password จะเปิด
4. พิมพ์ข้อมูลที่จำเป็น และคลิก **OK**

การอัปเดตรหัสผ่านทั่วไปสำหรับ Advanced System Management (ASM):

หมายเหตุ: คำศัพท์ของรหัสผ่านสำหรับ ID ผู้ใช้ทั่วไปคือ general และคำศัพท์ของรหัสผ่านสำหรับ ID ผู้ดูแลระบบคือ admin

เมื่อต้องการ อัปเดตรหัสผ่านทั่วไปของ ASM ให้ทำดังนี้:

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

การรีเซ็ตรหัสผ่านผู้ดูแลระบบ Advanced System Management (ASM):

เมื่อต้องการรีเซ็ตรหัสผ่านของผู้ดูแลระบบ ให้ติดต่อผู้ให้บริการที่ได้รับสิทธิ

การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ

อ็พชั่นนี้ช่วยให้คุณตรวจสอบว่า คุณได้เชื่อมต่อกับเน็ตเวิร์ก อย่างถูกต้องหรือไม่

เมื่อต้องการทดสอบภาวะเชื่อมต่อเน็ตเวิร์ก, คุณต้องมีบทบาทใดบทบาทหนึ่ง ดังต่อไปนี้:

- ผู้ดูแลระบบพิเศษ

- ตัวแทนบริการ

เมื่อต้องการทดสอบการเชื่อมต่อระหว่าง HMC และระบบที่ถูกจัดการ ให้ปฏิบัติตามนี้:

1. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
2. คลิก **Test Network Connectivity**
3. ในแท็บ Ping ให้พิมพ์ชื่อโฮสต์หรือ IP แอดเดรสของระบบใดๆ ซึ่งคุณต้องการเชื่อมต่อ เมื่อต้องการทดสอบเน็ตเวิร์กแบบเปิดให้พิมพ์เกตเวย์ คลิก **Ping**

หากคุณยังไม่ได้สร้างโลจิคัลพาร์ติชันอื่นใด คุณจะไม่สามารถ ping แอดเดรสได้ คุณสามารถใช้ HMC เพื่อสร้าง โลจิคัลพาร์ติชันบนเซิร์ฟเวอร์ของคุณ หากต้องการดูไฟล์ PDF ของ การแบ่งพาร์ติชันแบบโลจิคัล ซึ่งมีขนาดประมาณ 1 MB โปรดดูที่ <http://publib.boulder.ibm.com/infocenter/systems/scope/hw/topic/p7hat/p7hat.pdf>.

เมื่อต้องการทำความเข้าใจ กับวิธีการใช้ HMC ในเน็ตเวิร์ก โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 4

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดคอนฟิก HMC เพื่อเชื่อมต่อกับเน็ตเวิร์ก โปรดดูที่ “การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 62

ขั้นตอน Postconfiguration

เมื่อคุณติดตั้งและตั้งค่าคอนฟิก HMC แล้ว ให้สำรองข้อมูล HMC ตามที่จำเป็น

การสำรองข้อมูล HMC ที่สำคัญ

คุณสามารถสำรองข้อมูลคอนโซลที่สำคัญลงในอุปกรณ์หน่วยความจำแฟลชแบบ USB ดีวีดี ผ่านทาง FTP หรือทางเน็ตเวิร์ก

เมื่อใช้ HMC, คุณสามารถสำรองข้อมูลที่สำคัญทั้งหมด, เช่น ข้อมูล ดังต่อไปนี้:

- ไฟล์การกำหนดตามความชอบของผู้ใช้
- ข้อมูลเกี่ยวกับผู้ใช้
- ไฟล์คอนฟิกูเรชัน-แพลตฟอร์ม HMC
- ล็อกไฟล์ HMC
- HMC อัปเดตผ่าน Install Corrective Service

ฟังก์ชันการสำรองข้อมูลจะบันทึกข้อมูล HMC ที่จัดเก็บอยู่บนฮาร์ดดิสก์ของ HMC ไปที่:

- สื่อบันทึกดีวีดี
- อุปกรณ์หน่วยความจำแฟลชแบบ USB
- ระบบรีโมตที่ประกอบเข้ากับระบบไฟล์ของ HMC (เช่น NFS)
- รีโมตโฮสต์ผ่านทาง FTP

สำรองข้อมูล HMC หลังจากที่คุณทำการเปลี่ยนแปลงใน HMC หรือในข้อมูลที่เกี่ยวข้องกับโลจิคัลพาร์ติชัน

หมายเหตุ: ก่อนที่จะบันทึกข้อมูลลงในสื่อบันทึกแบบถอดได้ ต้องจัดรูปแบบสื่อบันทึกนั้นก่อน เมื่อต้องการจัดรูปแบบสื่อบันทึก ให้คลิก **HMC Management > Format Media** และปฏิบัติตามขั้นตอน

ถ้าต้องการสำรองข้อมูล HMC คุณต้องมีบทบาทใดบทบาทหนึ่ง ดังต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ผู้ควบคุมเครื่อง
- ตัวแทนบริการ

เมื่อต้องการสำรองข้อมูลที่สำคัญของ HMC ให้ทำสิ่งต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก การจัดการ HMC
2. เลือก **Back up HMC Data**
3. เลือกอ็อปชันการเก็บถาวร คุณสามารถสำรองข้อมูลลงในสื่อบันทึกบนระบบภายในเครื่อง ระบบระยะไกลที่เชื่อมต่อ หรือส่งข้อมูลสำรองไปยังไคลเอนต์ระยะไกล
4. ปฏิบัติตามคำสั่งบนหน้าต่างเพื่อสำรองข้อมูล

การสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ทั้งหมดไว้บนระบบปริโมต

คุณสามารถใช้ HMC เพื่อสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ทั้งหมด ของ HMC ไว้บน ระบบปริโมต

ระบบปริโมตของคุณต้องมี Network File System (NFS) หรือ Secure Shell (ssh) ที่ถูกกำหนดคอนฟิกไว้ และเน็ตเวิร์กนี้ต้องสามารถเข้าถึงได้จาก HMC เมื่อต้องการทำงานนี้ให้เสร็จสิ้น คุณต้องปิดและรีบูต HMC ใช้เฉพาะ HMC เพื่อดำเนินงานนี้

เมื่อต้องการสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ไว้บนระบบปริโมต คุณต้องเป็นสมาชิกของบทบาทอย่างใดอย่างหนึ่ง ต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ผู้ควบคุมเครื่อง
- ตัวแทนบริการ

เมื่อต้องการสำรองข้อมูลฮาร์ดไดรฟ์ HMC ให้กับระบบปริโมต ให้ทำสิ่งต่อไปนี้:

1. บันทึกหมายเลขอินเตอร์เฟซ (eth0, eth1 เป็นต้น), MAC แอดเดรส และ IP แอดเดรสของแต่ละอะแดปเตอร์เครือข่ายบน HMC เมื่อต้องการดำเนินการดังกล่าว ให้คลิก **HMC Management > เปลี่ยนค่าติดตั้งเน็ตเวิร์ก > LAN อะแดปเตอร์**
2. ปิดและหยุดการจ่ายไฟ HMC
3. เปิดคอนโซล HMC ด้วยสื่อบันทึกการกู้คืน HMC ในไดรฟ์ดีวีดี หากต้องการเริ่มต้นอินเตอร์เฟซ HMC จากเน็ตเวิร์กบูตเซิร์ฟเวอร์ที่กำหนดคอนฟิกไว้ให้แน่ใจว่าเน็ตเวิร์กอินเตอร์เฟซคือหนึ่งในอุปกรณ์ต่อไปนี้ในลำดับการเริ่มทำงาน เมื่อต้องการดูรายการของอุปกรณ์สตาร์ทอัพให้กด F12 เมื่อเปิด HMC และเลือกเน็ตเวิร์กอินเตอร์เฟซที่คุณต้องการบูต
4. เลือกอ็อปชันสำรองข้อมูล และคลิก **Next**
5. เลือกเน็ตเวิร์กอินเตอร์เฟซเพื่อใช้สำหรับสื่อสารกับ รีโมตเซิร์ฟเวอร์ หากคุณกำลังเริ่มต้น HMC โดยติดต่อกับเน็ตเวิร์กบูตเซิร์ฟเวอร์ และเซิร์ฟเวอร์นี้ยังเป็นรีโมตเซิร์ฟเวอร์ที่คุณต้องการสำรองข้อมูล ให้เลือกค่ากำหนดดีฟอลต์จากนั้นให้คลิก **ถัดไป** และไปยังขั้นตอนที่ 7 ถ้าคุณไม่ได้เลือกค่ากำหนดดีฟอลต์ไว้ให้ดำเนินการต่อด้วยขั้นตอนถัดไป

หมายเหตุ: หมายเลขอินเตอร์เฟซ (eth0, eth1) อาจไม่ตรงกับหมายเลขที่บันทึกในขั้นตอนที่ 1 สามารถใช้ MAC address ที่แสดงรายการไว้เพื่อระบุอินเตอร์เฟซที่ต้องการได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การระบุอินเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 67

6. ถ้าคุณไม่ได้เลือกค่าติดตั้งดีฟอลต์ คุณต้องเลือก โปรโตคอลเครือข่ายเพื่อใช้กับอินเตอร์เฟซที่เลือกไว้ คุณสามารถเลือกที่จะรับ IP แอดเดรสจากเซิร์ฟเวอร์ DHCP ในเน็ตเวิร์กของคุณ หรือกำหนด IP แอดเดรส แบบคงที่ให้กับเน็ตเวิร์กอินเตอร์เฟซที่เลือก ทำการเลือก และคลิก Next
7. หากคุณไม่ได้เลือกค่าติดตั้งดีฟอลต์ ให้พิมพ์ IP แอดเดรสหรือชื่อโฮสต์ของรีโมตเซิร์ฟเวอร์ของคุณ ไฟล์สำรองข้อมูลจะถูกสร้างขึ้นโดยใช้ยูทิลิตี้บีบอัด gzip และคำสั่ง tar ระบุไฟล์ด้วยนามสกุล .tgz ในฟิลด์ **File on remote host** หากคุณสามารถเลือกค่ากำหนดดีฟอลต์เน็ตเวิร์กไว้ คุณต้องใช้ เซิร์ฟเวอร์ไคลเอนต์ในการกำหนดคอนฟิกเน็ตเวิร์กบูตของคุณ ข้อมูลนี้จะถูกแสดงในฟิลด์ **File on remote host** หลังจากที่คุณ ป้อนข้อมูลที่ต้องการทั้งหมดเสร็จสิ้นแล้ว ให้คลิก Next
8. เลือกวิธีที่คุณต้องการใช้เพื่อถ่ายโอนข้อมูล จาก HMC ของคุณ ให้กับรีโมตเซิร์ฟเวอร์ หากคุณเลือกการเข้ารหัสข้อมูล รีโมตโฮสต์ของคุณจะต้องมีเซิร์ฟเวอร์ Secure Shell (SSH) ที่กำลังรันอยู่ หากคุณเลือก การถ่ายโอนข้อมูลโดยไม่มีการเข้ารหัส รีโมตโฮสต์ของคุณต้องมี Network File Server (NFS) ที่กำลังรันอยู่ และไคลเอนต์ที่คุณต้องการ สำรองข้อมูล ต้องถูกเอ็กซ์พอร์ตเพื่อทำการบันทึก ทำการเลือก และคลิก Next
9. ถ้าคุณเลือกถ่ายโอนข้อมูลโดยใช้การเข้ารหัส คุณต้องพิมพ์ ID ผู้ใช้และรหัสผ่านของรีโมตเซิร์ฟเวอร์
10. ตรวจสอบข้อมูลที่คุณป้อนให้ถูกต้อง และคลิก **Finish** เมื่อการสำรองข้อมูลเสร็จสิ้น อินเตอร์เฟซของ HMC จะปรากฏขึ้น

ถ้าคุณปรับเปลี่ยนลำดับของการเริ่มทำงานโดยกด F1 เมื่อคุณเปิด HMC คุณต้องบูต HMC และเปลี่ยนค่าติดตั้งอีกครั้ง เมื่อคุณเปลี่ยนลำดับการเริ่มทำงาน ให้แน่ใจว่าฮาร์ดดิสก์ของคุณจะถูกแสดงก่อนเน็ตเวิร์กอินเตอร์เฟซ ในลำดับการเริ่มทำงาน

การอัปเดต การอัเกรด และการโอนย้ายรหัสเครื่อง HMC ของคุณ

การอัปเดตและอัเกรดควรดำเนินการเป็นระยะๆ เพื่อให้ HMC สามารถเพิ่มคุณสมบัติการทำงานใหม่ๆ และปรับปรุงคุณลักษณะที่มีอยู่ ศึกษาเพิ่มเติมเกี่ยวกับความแตกต่างระหว่างการอัปเดต การอัเกรด และการโอนย้ายรหัสเครื่อง HMC ของคุณ รวมทั้งศึกษาวิธีดำเนินการอัปเดต อัเกรด หรือโอนย้ายรหัสเครื่อง HMC

เมื่อคุณทำงานแต่ละงานเหล่านี้เสร็จสิ้น HMC จะรีบูต แต่พาร์ติชันไม่รีบูต

การอัปเดตรหัส HMC

ใช้การบำรุงรักษาระดับ HMC ที่มีอยู่

คุณไม่จำเป็นต้องทำงาน **Save upgrade data**

การอัเกรดรหัส HMC

แทนที่ซอฟต์แวร์ HMC ด้วยรหัสใหม่หรือระดับโปรแกรมฟิร์มแวร์ของโปรแกรมเดียวกัน

คุณต้องบูตจากสื่อบันทึกที่ถูกต้อง

การโอนย้ายรหัส HMC

ย้ายข้อมูล HMC จาก HMC เวอร์ชันหนึ่งเป็นเวอร์ชันอื่น

การโอนย้ายระบบเป็นการอัเกรดชนิดหนึ่ง

การกำหนดเวอร์ชันและรีลีสของรหัสเครื่อง HMC ของคุณ

เรียนรู้วิธีการดูเวอร์ชันและรีลีสของรหัสเครื่อง HMC

ระดับของรหัสเครื่องบน HMC จะกำหนดคุณลักษณะที่มีอยู่ รวมถึงการบำรุงรักษาเซิร์ฟเวอร์เฟิร์มแวร์และการปรับปรุงสำหรับการอัปเดตเป็นรีลีสใหม่

เมื่อต้องการดูเวอร์ชันและรีลีสของรหัสเครื่อง HMC ให้ทำดังนี้:

1. ในพื้นที่การนำทาง ให้คลิก **อัปเดต**
2. ในพื้นที่ใช้งาน ให้ดู และบันทึกข้อมูลที่ปรากฏภายใต้หัวข้อ HMC Code Level รวมทั้งเวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน

การขอรับและการใช้การอัปเดตรหัสเครื่องสำหรับ HMC เมื่อมีการเชื่อมต่ออินเทอร์เน็ต

ศึกษาวิธีขอรับอัปเดตรหัสเครื่องสำหรับ HMC เมื่อ HMC มีการเชื่อมต่ออินเทอร์เน็ต

เมื่อต้องการขอรับอัปเดตรหัสเครื่องสำหรับ HMC ให้ปฏิบัติตามขั้นตอนที่ 1 ถึง 5

ขั้นตอนที่ 1. ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต

เมื่อต้องการดาวน์โหลดอัปเดตจากระบบส่วนบริการ และสนับสนุนหรือเว็บไซต์ไปยัง HMC หรือเซิร์ฟเวอร์ของคุณ คุณต้องมีอย่างใดอย่างหนึ่งต่อไปนี้:

- การเชื่อมต่อ SSL โดยมีหรือไม่มีพรีออกซี SSL
- VPN อินเทอร์เน็ต

เพื่อให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **Service Management**
2. เลือก **Manage Outbound Connectivity**
3. เลือกแท็บสำหรับชนิดของการเชื่อมต่อขาออก ที่คุณเลือกใช้สำหรับ HMC ของคุณ (VPN อินเทอร์เน็ต หรือ SSL)

หมายเหตุ: ถ้าไม่มีการเชื่อมต่อกับส่วนบริการและสนับสนุน ให้ตั้งค่าการเชื่อมต่อบริการ ก่อนที่จะดำเนินการต่อสำหรับขั้นตอนนี้ สำหรับคำแนะนำเกี่ยวกับวิธีการตั้งค่าการเชื่อมต่อกับส่วนบริการและสนับสนุน โปรดดูที่ การตั้งค่าเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการและสนับสนุน IBM

4. คลิก **Test**
5. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์ ถ้าการทดสอบไม่เสร็จสมบูรณ์ ให้แก้ปัญหการเชื่อมต่อและแก้ไข ปัญหา ก่อนที่จะดำเนินการต่อตามขั้นตอนนี้ อีกทางหนึ่ง คุณสามารถขอรับอัปเดตบนดีวีดี
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **อัปเดต**

2. ในพื้นที่ใช้งาน ให้ดูและบันทึกข้อมูล ที่ปรากฏภายใต้หัวข้อ HMC Code Level รวมทั้งเวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน
3. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอน ต่อไปนี้:

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ตให้ไปที่ <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

หมายเหตุ: ถ้าคุณต้องการ คุณสามารถติดต่อ ส่วนบริการและสนับสนุน

6. ดำเนินการต่อด้วย “ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC”

ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC

เมื่อต้องการใช้การอัปเดตรหัสเครื่อง HMC ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ก่อนที่คุณจะติดตั้งอัปเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูลคอนโซลที่สำคัญบน HMC ของคุณ สำหรับคำแนะนำ โปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 81 จากนั้น ให้ดำเนินการขั้นตอนถัดไป
2. ในพื้นที่การนำทาง ให้คลิก อัปเดต
3. คลิก **Update HMC** วิซาร์ด Install Corrective Service จะเปิดขึ้น
4. ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อติดตั้งอัปเดต
5. ปิดเครื่อง แล้วรีสตาร์ท HMC เพื่อให้ อัปเดตมีผล
6. คลิก **Log on and launch the Hardware Management Console web application**
7. ล็อกอินเข้าสู่อินเทอร์เฟซ HMC

ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งอย่างถูกต้องแล้ว ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก อัปเดต
2. ในพื้นที่ใช้งาน เวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน จะแสดงอยู่ภายใต้ หัวข้อ HMC Code Level
3. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
4. หากระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. เลือกการเชื่อมต่อเครือข่ายบน HMC
 - b. ลองทำการอัปเดตเฟิร์มแวร์อีกครั้ง โดยใช้ที่เก็บอื่น
 - c. ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP

เรียนรู้วิธีการขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP

เมื่อต้องการขอรับส่วนอัปเดตรหัสเครื่องของ HMC ให้ปฏิบัติตามขั้นตอนที่ 1-5

ขั้นตอนที่ 1. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก อัปเดต
2. ในพื้นที่ใช้งาน ให้ดูและบันทึกข้อมูล ที่ปรากฏภายใต้หัวข้อ HMC Code Level รวมทั้งเวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน
3. ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มี การเชื่อมต่ออินเทอร์เน็ต ให้ไปที่เว็บไซต์ Hardware Management Console ที่ <http://www-933.ibm.com/support/fixcentral/>
2. เลื่อนลงไปยังระดับเวอร์ชัน HMC ของคุณ เพื่อ ดูระดับ HMC ที่มีอยู่

หมายเหตุ: ถ้าคุณต้องการ คุณสามารถติดต่อส่วนบริการและสนับสนุน IBM

3. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. ขอรับอัปเดตรหัสเครื่อง HMC”

ขั้นตอนที่ 3. ขอรับอัปเดตรหัสเครื่อง HMC

เมื่อต้องการขอรับอัปเดตรหัสเครื่อง HMC ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

คุณสามารถสั่งซื้ออัปเดตรหัสเครื่อง HMC ผ่านทางเว็บไซต์ Fix Central โดยติดต่อส่วนบริการและสนับสนุน หรือดาวน์โหลดไปยังเซิร์ฟเวอร์ FTP

การสั่งซื้ออัปเดตรหัสเครื่อง HMC ผ่านเว็บไซต์ Fix Central

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่ เว็บไซต์ Hardware Management Console ที่ <http://www-933.ibm.com/support/fixcentral/>
2. ภายใต้ Supported HMC products ให้เลือกระดับ HMC ล่าสุด
3. เลื่อนลงไปยังพื้นที่ File name(s) / Package และระบุอัปเดตที่คุณ ต้องการสั่งซื้อ
4. ในคอลัมน์ Order ให้เลือก Go
5. คลิก Continue เพื่อลงชื่อเข้าใช้ด้วย IBM ID ของคุณ
6. ปฏิบัติตามพร้อมต้นหน้าจอเพื่อทำการสั่งซื้อ

การดาวน์โหลดอัปเดตรหัสเครื่อง HMC ลงในสื่อบันทึกแบบถอดออกได้

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่ เว็บไซต์ Hardware Management Console ที่ <http://www-933.ibm.com/support/fixcentral/>

2. ภายใต้ Supported HMC products ให้เลือกกระดุม HMC ล่าสุด
3. เลื่อนลงไปยังพื้นที่ File name(s) / Package และระบุอัปเดตที่คุณ ต้องการดาวน์โหลด
4. คลิกอัปเดตที่คุณต้องการดาวน์โหลด
5. ยอมรับข้อตกลงไลเซนส์ และบันทึกอัปเดตลงในสื่อบันทึกแบบถอดออกได้

เมื่อเสร็จเรียบร้อยแล้วให้ดำเนินการต่อด้วย “ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC”

ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC

เมื่อต้องการใช้การอัปเดตรหัสเครื่อง HMC ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ก่อนที่คุณจะติดตั้งอัปเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูล HMC ของคุณ สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 81
2. ถ้าคุณได้รับหรือสร้างอัปเดตบนทีวีดีแรม ให้ใส่แผ่นดิสก์ดังกล่าวในไดรฟ์ทีวีดีบน HMC ถ้าคุณได้รับหรือสร้างอัปเดตบนอุปกรณ์หน่วยความจำแบบ USB ให้เสียบอุปกรณ์หน่วยความจำนั้น
3. ในพื้นที่การนำทางให้คลิก อัปเดต
4. คลิก Update HMC วิซาร์ด Install Corrective Service จะเปิดขึ้น
5. ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อติดตั้งอัปเดต
6. ปิดเครื่อง รีเซ็ต และกลับเข้าสู่ระบบ HMC เพื่อให้การอัปเดตมีผล
7. ดำเนินการต่อด้วย “ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์”

ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์แล้ว ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก อัปเดตในพื้นที่ใช้งาน เวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน จะแสดงอยู่ภายใต้ หัวข้อ HMC Code Level
2. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
3. หากระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. ลองอัปเดตรหัสเครื่องอีกครั้ง ถ้าคุณสร้างทีวีดีในขั้นตอนนี้ ให้ใช้สื่อบันทึกใหม่
 - b. ถ้ายังคงมีปัญหาอยู่ให้ติดต่อระดับของการสนับสนุนถัดไป

การอัปเดตซอฟต์แวร์ HMC ของคุณ

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากรีลีสหนึ่งเป็นรีลีสถัดไป ในขณะที่ยังคงรักษาข้อมูลคอนฟิกูเรชัน HMC ของคุณ

เมื่อต้องการอัปเดตรหัสเครื่องบน HMC ให้ปฏิบัติตามขั้นตอนที่ 1-9

หมายเหตุ: ถ้า คุณกำลังอัปเดตจาก HMC ด้วยเวอร์ชัน 6 กับ HMC เวอร์ชัน 7 โปรดอ้างอิง “การโอนย้ายรหัสเครื่องบน HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7” ในหน้า 91

ขั้นตอนที่ 1. ขอรับอัปเดต

คุณสามารถสั่งซื้ออัปเดตรหัสเครื่อง HMC ผ่านทางเว็บไซต์ Fix Central

เมื่อต้องการขอรับอัปเดตผ่านทางเว็บไซต์ Fix Central ให้ทำดังต่อไปนี้:

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่เว็บไซต์ Hardware Management Console ที่ <http://www-933.ibm.com/support/fixcentral/>
2. คลิกทำต่อไปยัง Hardware Management Console จะปรากฏขึ้น
3. นำทางไปยังเวอร์ชัน HMC ที่คุณต้องการอัปเดต
4. ค้นหาตำแหน่งส่วนดาวน์โหลดและสั่งซื้อ

หมายเหตุ: ถ้าคุณไม่มีการเข้าถึงอินเทอร์เน็ต โปรดติดต่อส่วนบริการและสนับสนุน IBM เพื่อสั่งซื้อการอัปเดตบนทีวีดี

5. ปฏิบัติตามพร้อมด้นหน้าจอเพื่อทำการสั่งซื้อ
6. หลังจากเสร็จเรียบร้อยแล้ว ให้ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

เมื่อต้องการกำหนดระดับรหัสเครื่องที่มีอยู่บน HMC ให้ปฏิบัติตามขั้นตอนเหล่านี้:

1. ในพื้นที่ การนำทาง ให้คลิก **อัปเดต**
2. ในพื้นที่ใช้งาน ให้ดูและบันทึกข้อมูลปรากฏภายใต้หัวข้อ HMC Code Level รวมทั้งเวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน
3. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ”

ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ

เมื่อต้องการสำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการให้ทำดังนี้:

1. ในพื้นที่การนำทาง ให้เลือก **การจัดการระบบ**
2. เลือก **Servers**
3. เลือกเซิร์ฟเวอร์ และตรวจสอบให้แน่ใจว่าสถานะคือ *Operating* หรือ *Standby*
4. ภายใต้ Tasks ให้เลือก **Configuration > Manage Partition Data > Backup**
5. พิมพ์ชื่อไฟล์สำรองและบันทึก ข้อมูลนี้
6. คลิก **OK**
7. ทำซ้ำขั้นตอนเหล่านี้สำหรับแต่ละระบบที่ถูกจัดการ
8. ดำเนินการต่อด้วย “ขั้นตอนที่ 4. สำรองข้อมูล HMC”

ขั้นตอนที่ 4. สำรองข้อมูล HMC

สำรองข้อมูล HMC ก่อนที่จะติดตั้งซอฟต์แวร์ HMC เวอร์ชันใหม่ เพื่อให้สามารถเรียกคืนระดับก่อนหน้านี้นี้ในกรณีที่เกิดปัญหา ในระหว่างการอัปเดตซอฟต์แวร์ ห้ามใช้ข้อมูลคอนโซลที่สำคัญนี้หลังจากที่อัปเดตเป็น ซอฟต์แวร์ HMC เวอร์ชันใหม่ได้สำเร็จ

หมายเหตุ: เมื่อต้องการ สำรองข้อมูลไปยังสื่อบันทึกแบบถอดออกได้ คุณจะต้องเตรียมสื่อบันทึกดังกล่าวไว้ให้พร้อม

เมื่อต้องการ สำรองข้อมูล HMC ให้ทำดังนี้:

1. ถ้าคุณวางแผนที่จะ สำรองข้อมูลไปยังสื่อบันทึก ให้ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อจัดรูปแบบ สื่อบันทึก:
 - a. ใส่สื่อบันทึกลงในไดรฟ์
 - b. ในพื้นที่การนำทาง ให้เลือก **Service Management**

- c. เลือก **Format Media**
- d. เลือกชนิดของสื่อบันทึก
- e. เลือกชนิดการจัดรูปแบบ
- f. คลิก **OK**
2. ในพื้นที่การนำทาง ให้เลือก **HMC Management**
3. เลือก **Back up HMC Data** หน้าต่าง Back up HMC Data จะเปิดขึ้น
4. เลือกอ็อปชันการเก็บถาวร คุณสามารถสำรองข้อมูลลงในสื่อบันทึกบนระบบภายในเครื่อง ระบบระยะไกลที่เชื่อมต่อกับระบบไฟล์ HMC (ตัวอย่างเช่น NFS) หรือส่งสำเนาสำรองไปยังไซต์ระยะไกลโดยใช้ 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”

ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน

ก่อนที่คุณจะอัปเดตเป็นซอฟต์แวร์ HMC เวอร์ชันใหม่ ให้บันทึกข้อมูลคอนฟิกูเรชัน HMC เพื่อเป็นการป้องกัน

เมื่อต้องการ บันทึกข้อมูลคอนฟิกูเรชัน HMC ปัจจุบัน ให้ทำดังนี้:

1. เมื่อต้องการดูการดำเนินการที่กำหนดการสำหรับระบบที่ถูกจัดการ หรือโลจิคัลพาร์ติชัน เปิด **Systems Management** หากคุณต้องการบันทึกการดำเนินการตามกำหนดการสำหรับ HMC เลือก **HMC Management** และข้ามไปยังขั้นตอนที่ 3
2. เลือกระบบที่ถูกจัดการและพาร์ติชันใดๆ ที่คุณต้องการบันทึกข้อมูลคอนฟิกูเรชัน HMC
3. ในรายการงาน ให้เลือก **Schedule Operations** การดำเนินการตามกำหนดการสำหรับปลายทางที่คุณเลือกทั้งหมด จะปรากฏขึ้น
4. เลือก **Sort > By Object**
5. เลือกแต่ละอ็อบเจกต์และบันทึกรายละเอียดต่อไปนี้:
 - ชื่ออ็อบเจกต์
 - วันที่กำหนดการ
 - เวลาดำเนินการ (ในรูปแบบ 24 ชั่วโมง)
 - ทำซ้ำ (ถ้าเลือก Yes ให้ปฏิบัติตามขั้นตอนต่อไปนี้):
 - a. เลือก **View > Schedule Details**
 - b. บันทึกข้อมูลช่วงเวลา
 - c. ปิดหน้าต่างการดำเนินการตามกำหนดการ
 - d. ทำซ้ำสำหรับการดำเนินการตามกำหนดการแต่ละอย่าง
6. ปิดหน้าต่าง **Customize Scheduled Operations**
7. ดำเนินการต่อด้วย “ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล” ในหน้า 90

ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล

เมื่อต้องการบันทึกสถานะคำสั่งระยะไกลให้ทำดังนี้:

1. ในพื้นที่การนำทางให้เลือก **HMC Management**
2. ในรายการงานให้คลิก **Remote Command Execution**.
3. บันทึกว่าเช็กบ็อกซ์ **Enable remote command execution using the ssh facility** ถูกเลือกหรือไม่
4. คลิก **Cancel**
5. ดำเนินการต่อด้วย “ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต”

ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต

คุณสามารถบันทึกคอนฟิกูเรชัน HMC ปัจจุบันลงในพาร์ติชันของดิสก์ที่กำหนดบน HMC หรือในสื่อบันทึกภายในเครื่องก็ได้ ให้บันทึกข้อมูลอัปเดตในพื้นที่ก่อนที่จะอัปเดตซอฟต์แวร์ HMC ของคุณให้เป็นรหัสใหม่ แอ็คชันนี้อนุญาตให้คุณเรียกคืนคอนฟิกูเรชัน HMC ได้หลังจากการอัปเดต

หมายเหตุ: อนุญาตให้มีข้อมูลสำรองได้เพียงระดับเดียวเท่านั้น แต่ทุกครั้งที่คุณบันทึกข้อมูลอัปเดต ระดับก่อนหน้านั้นจะถูกเขียนทับ

เมื่อต้องการบันทึกข้อมูลอัปเดตให้ทำดังนี้:

1. ในพื้นที่การนำทางให้เลือก **HMC Management**
2. ในพื้นที่เนื้อหา ภายใต้การดำเนินงาน เลือก **Save Upgrade Data** wizard Save Upgrade Data จะเปิดขึ้น
3. เลือกสื่อบันทึกที่คุณต้องการบันทึกข้อมูล อัปเดต ถ้าคุณเลือกที่จะบันทึกสื่อบันทึกแบบถอดได้ ให้ใส่สื่อบันทึกในตอนนี้คลิก **Next**
4. คลิก **Finish**.
5. รอให้งานเสร็จสมบูรณ์ ถ้างาน Save Upgrade Data ล้มเหลว ให้ติดต่อระดับของการสนับสนุนถัดไปก่อนที่จะดำเนินการ

หมายเหตุ: ถ้างานบันทึกข้อมูลอัปเดตล้มเหลว ห้ามดำเนินการกระบวนการอัปเดต

6. คลิก **OK**
7. ดำเนินการต่อด้วย “ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC”

ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC

เมื่อต้องการอัปเดตซอฟต์แวร์ HMC ให้รีสตาร์ทระบบโดยใช้สื่อบันทึกแบบถอดออกได้ในไดรฟ์ DVD

1. ใส่สื่อบันทึกสำหรับการติดตั้งผลิตภัณฑ์ HMC ลงในไดรฟ์ดีวีดี
2. ในแถบการนำทางให้เลือก **การจัดการ HMC**
3. ในพื้นที่เนื้อหา เลือก **ปิดหรือรีสตาร์ท HMC**
4. ตรวจสอบว่า **Restart the HMC** ถูกเลือกไว้
5. คลิก **OK** HMC จะเริ่มทำงานอีกครั้ง และข้อมูลระบบจะเลื่อนอยู่บนหน้าจอต่าง
6. เลือก **Upgrade** และคลิก **Next**
7. เลือกจากอ็อปชันต่อไปนี้:
 - ถ้าคุณบันทึกข้อมูลอัปเดตที่บันทึกไว้ในระหว่างงานก่อนหน้านี้ ให้ทำขั้นตอนถัดไป

- ถ้าคุณไม่ได้บันทึกข้อมูลอัปเดตก่อนหน้านี้ในขั้นตอนนี้ คุณจะต้อง บันทึกข้อมูลอัปเดตในตอนนี้ ก่อนที่คุณจะดำเนินการต่อ

- เลือก **Upgrade from media** และคลิก **Next**
- ยืนยันค่าติดตั้ง และคลิก **Finish**
- ปฏิบัติตามพร้อมท์

หมายเหตุ:

- ถ้าหน้าจอว่างเปล่า ให้กด space bar เพื่อดูข้อมูล
- ดีวีดีแผ่นแรกอาจใช้เวลาประมาณ 20 ในการติดตั้ง

- ที่พร้อมท์ล็อกอิน ให้ล็อกอินโดยใช้ user ID และรหัสผ่านของคุณ การติดตั้งรหัส HMC เสร็จสมบูรณ์
- ดำเนินการต่อด้วย “ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์”

ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับ HMC ได้รับการติดตั้งเสร็จสมบูรณ์แล้ว ให้ทำดังนี้:

- ในพื้นที่การนำทาง ให้คลิก **อัปเดต** ในพื้นที่ใช้งาน เวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน จะแสดงอยู่ภายใต้ หัวข้อ HMC Code Level
- ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
- ถ้าระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ลองทำการอัปเดตอีกครั้งโดยใช้ดีวีดีใหม่ ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การโอนย้ายรหัสเครื่องบน HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7

ศึกษาวิธีย้ายรหัสเครื่องบน HMC จาก เวอร์ชัน 6 เป็นเวอร์ชัน 7 พร้อมทั้งการรักษาข้อมูลคอนฟิกูเรชัน HMC ของคุณ

เมื่อต้องการโอนย้ายรหัสเครื่องบน HMC จากเวอร์ชัน 6 ไปเป็นเวอร์ชัน 7 ให้ปฏิบัติตามขั้นตอนที่ 1-9

สำคัญ: เมื่อต้องการโอนย้ายเป็น เวอร์ชัน 7 รีลีส 0 รหัสเครื่อง HMC ของคุณต้องเป็นเวอร์ชัน 6 รีลีส 1.2 เป็นอย่างน้อย

ตรวจสอบให้แน่ใจว่าสอดคล้องตามข้อกำหนดขั้นต่ำ

เมื่อต้องการโอนย้ายรหัสเครื่องบน HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7 คุณต้องตรวจสอบให้แน่ใจก่อนว่าสอดคล้องตามข้อกำหนดขั้นต่ำต่อไปนี้:

- HMC ของคุณอยู่ที่ระดับ 6.12 หรือสูงกว่า สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบระดับรหัส และรีลีส HMC ของคุณ โปรดดูที่ “การกำหนดเวอร์ชันและรีลีสของรหัสเครื่อง HMC ของคุณ” ในหน้า 84
- เฟิร์มแวร์ระบบของคุณอยู่ที่ระดับล่าสุด
- คุณได้ดำเนินการตรวจสอบความสมบูรณ์ของเน็ตเวิร์กแล้ว
- ฮาร์ดแวร์ HMC ของคุณสนับสนุนอัปเดตนี้

ขั้นตอนที่ 1. ขอรับอัปเดต

เมื่อต้องการขอรับอัปเดต ให้ทำดังนี้:

คุณสามารถสั่งซื้อ อุปกรณ์รหัสเครื่อง HMC ผ่านทางเว็บไซต์ Fix Central โดยติดต่อ ส่วนบริการและสนับสนุน หรือดาวน์โหลดไปยังเซิร์ฟเวอร์ FTP

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ ที่มีการเชื่อมต่ออินเทอร์เน็ตให้ไปที่ <http://www.ibm.com/eserver/support/fixes>
2. เลือกตระกูลที่เหมาะสมในรายการตระกูล ผลิตภัณฑ์
3. เลือก **Hardware Management Console** ใน รายการชนิดผลิตภัณฑ์หรือโปรแกรมฟิกซ์
4. คลิก ทำต่อไป ซิต Hardware Management Console จะปรากฏขึ้น
5. นำทางไปยังเวอร์ชัน HMC ที่คุณต้องการ
6. ค้นหาตำแหน่งส่วนดาวน์โหลดและสั่งซื้อ

หมายเหตุ: ถ้าคุณไม่มีการเข้าถึงอินเทอร์เน็ต โปรดติดต่อส่วนบริการและ สนับสนุน เพื่อสั่งซื้ออุปกรณ์บนดีวีดี

7. ปฏิบัติตามพร้อมท์เพื่อส่งการสั่งซื้อของคุณ
8. หลังจากเสร็จเรียบร้อยแล้ว ให้ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่

เมื่อต้องการกำหนดระดับรหัสเครื่องที่มีอยู่บน HMC ให้ปฏิบัติตาม ขั้นตอนเหล่านี้:

1. ในพื้นที่การนำทางให้คลิกโฟลเดอร์ **Licensed Internal Code Maintenance**
2. เลือก **HMC Code Update**
3. ในพื้นที่สถานะ ให้มองหาเวอร์ชัน และรหัสของรหัสเครื่อง HMC ของคุณ
4. บันทึกเวอร์ชันและรหัสปัจจุบัน

Important: เมื่อต้องการอัปเดตจาก HMC รหัสเครื่อง 6.1.3 ถึง 7.3.4.0 คุณต้องใช้โปรแกรมฟิกซ์เป็นอันดับแรก สำหรับข้อมูลเพิ่มเติม โปรดดูที่ <http://www.ibm.com/eserver/support/fixes>

5. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ”

ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ

เมื่อต้องการสำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการให้ทำดังนี้:

1. ในพื้นที่เนื้อหาให้เลือกระบบที่ถูกจัดการ
2. จากเมนู คลิก **Selected > Profile Data > Backup**
3. พิมพ์ชื่อไฟล์สำรองและบันทึกข้อมูลนี้
4. คลิก **OK**
5. ทำซ้ำขั้นตอนที่ 1 ถึง 4 สำหรับระบบที่ถูกจัดการแต่ละระบบ

ขั้นตอนที่ 4. สำรองข้อมูลคอนโซลที่สำคัญ

สำรองข้อมูลคอนโซลที่สำคัญ ก่อนที่จะติดตั้งซอฟต์แวร์ HMC เวอร์ชันใหม่ เพื่อให้สามารถเรียกคืนระดับก่อนหน้านั้นในกรณีที่เกิดปัญหา ในระหว่างการอัปเดตซอฟต์แวร์ ห้ามใช้ข้อมูลคอนโซลที่สำคัญนี้หลังจากที่อัปเดตเป็น ซอฟต์แวร์ HMC เวอร์ชันใหม่ได้สำเร็จ

หมายเหตุ: ถ้าคุณเลือกที่จะสำรองข้อมูลคอนโซล ไปยังสื่อบันทึกแบบถอดออกได้ คุณจะต้องเตรียมสื่อบันทึกดังกล่าวไว้ให้พร้อม

เมื่อต้องการสำรองข้อมูลคอนโซลที่สำคัญให้ทำดังนี้:

1. เลือกจากอ็อปชันต่อไปนี้:

- ถ้าคุณ *ไม่มี*แผนที่จะสำรองข้อมูลลงใน DVD-RAM ให้ทำขั้นตอน ถัดไป
- ถ้าคุณวางแผนที่จะสำรองข้อมูลลงใน DVD-RAM ให้ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. ใส่แผ่น DVD-RAM ลงในไดรฟ์
 - b. ในพื้นที่การนำทาง ให้คลิก **Licensed Internal Code Maintenance**
 - c. เลือก **HMC Code Update**
 - d. เลือก **Format Removable Media**
 - e. เลือก **Format DVD-RAM**
 - f. คลิก **OK**
 - g. ดำเนินการขั้นตอนถัดไป

2. เลือก **Back up Critical Console Data**

3. เลือกอ็อปชันการเก็บถาวร คุณสามารถสำรองข้อมูลลงในทีวีดีใน HMC, ระบบรีโมตที่ติดตั้งกับระบบไฟล์ HMC (เช่น NFS) หรือส่งข้อมูลสำรองไปยังรีโมตไซต์โดยใช้ File Transfer Protocol (FTP)

- เมื่อต้องการสำรองข้อมูลลงในทีวีดี ให้เลือก **Back up to DVD on local system** และ ปฏิบัติตามคำแนะนำ
- เมื่อต้องการสำรองข้อมูลไปยังระบบรีโมตที่ประกอบเข้าด้วยกัน ให้เลือก **Backup to mounted remote system** และ ปฏิบัติตามคำแนะนำ
- เมื่อต้องการสำรองข้อมูลไปยังไซต์ FTP แบบรีโมต ให้เลือก **Send backup critical data to remote site** และปฏิบัติตามคำแนะนำ

4. ดำเนินการต่อด้วย “ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน”

ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน

ก่อนที่จะอัปเดตเป็นซอฟต์แวร์ HMC เวอร์ชันใหม่ ให้บันทึกข้อมูลคอนฟิกูเรชัน HMC เพื่อเป็นการป้องกัน

เมื่อต้องการ บันทึกข้อมูลคอนฟิกูเรชัน HMC ให้ทำตามขั้นตอนต่อไปนี้:

1. เมื่อต้องการดูการดำเนินการที่กำหนดการสำหรับระบบที่ถูกจัดการ หรือโลจิคัลพาร์ติชัน เปิด **Systems Management** หากคุณต้องการบันทึกการดำเนินการตามกำหนดการสำหรับ HMC เลือก **HMC Management** และเข้าไปยังขั้นตอนที่ 3
2. เลือกระบบที่ถูกจัดการและพาร์ติชันใดๆ ที่คุณต้องการบันทึกข้อมูลคอนฟิกูเรชัน HMC
3. ในรายการงาน ให้เลือก **Schedule Operations** การดำเนินการตามกำหนดการสำหรับปลายทางที่คุณเลือกทั้งหมด จะปรากฏขึ้น
4. เลือก **Sort > By Object**
5. เลือกแต่ละอ็อบเจกต์ และบันทึกรายละเอียดต่อไปนี้:
 - ชื่ออ็อบเจกต์
 - วันที่กำหนดการ
 - เวลาดำเนินการ (ในรูปแบบ 24 ชั่วโมง)
 - ทำซ้ำ (ถ้าเลือก Yes ให้ปฏิบัติตามขั้นตอนต่อไปนี้):
 - a. เลือก **View > Schedule Details**

- b. บันทึกข้อมูลช่วงเวลา
 - c. ปิดหน้าต่างการดำเนินการตามกำหนดการ
 - d. ทำซ้ำสำหรับการดำเนินการตามกำหนดการแต่ละอย่าง
6. ปิดหน้าต่าง Customize Scheduled Operations
7. ดำเนินการต่อด้วย “ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล”

ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล

1. ในพื้นที่การนำทางให้เลือก **HMC Management**
2. เลือก **HMC Configuration**
3. ในรายการงาน ให้คลิก **Enable/Disable Remote Command Execution**
4. บันทึกว่าเช็กบ็อกซ์ **Enable remote command execution using the ssh facility** ถูกเลือกหรือไม่
5. คลิก **Cancel**
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต”

ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต

คุณสามารถบันทึกคอนฟิกูเรชัน HMC ปัจจุบันในดิสก์พาร์ติชันที่กำหนดบน HMC ให้บันทึกข้อมูลอัปเดตในทันทีก่อนที่จะอัปเดตซอฟต์แวร์ HMC ของคุณให้เป็นวิธีใหม่ แอ็คชันนี้ช่วยให้คุณเรียกคืนคอนฟิกูเรชัน HMC ได้หลังจากการอัปเดต

ข้อมูลอัปเดต จะถูกเรียกคืนโดยอัตโนมัติในระหว่างกระบวนการติดตั้ง

หมายเหตุ: อนุญาตให้มีข้อมูลสำรองได้เพียงระดับเดียวเท่านั้น แต่ครั้งที่คุณบันทึกข้อมูลอัปเดต ระดับก่อนหน้านี้อาจถูกเขียนทับ

1. ในพื้นที่การนำทางให้เปิดโฟลเดอร์ **Licensed Internal Code**
2. เลือก **HMC Code Update**
3. เลือก **Save Upgrade Data**
4. เลือก **DVD** และคลิก **Continue**
5. ใส่แผ่นดีวีดีลงในไดรฟ์
6. คลิก **Continue** เพื่อเริ่มงาน
7. รอให้งานเสร็จสมบูรณ์ ถ้างาน Save Upgrade Data ล้มเหลว ให้ติดต่อระดับของการสนับสนุนถัดไปก่อนที่จะดำเนินการ

หมายเหตุ: ถ้างานบันทึกข้อมูลอัปเดตล้มเหลว อย่าดำเนินการกระบวนการอัปเดต

8. คลิก **OK**
9. คลิก **Cancel**
10. ดำเนินการต่อด้วย “ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7”

ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC จากเวอร์ชัน 6 เป็นเวอร์ชัน 7

Important: เมื่อต้องการอัปเดตจาก HMC รหัสเครื่อง 6.1.3 ไปเป็น 7.3.4.0 คุณต้องใช้ ptf เป็นสิ่งแรก สำหรับข้อมูลเพิ่มเติม โปรดดูที่ <http://www.ibm.com/eserver/support/fixes>

เมื่อต้องการอัปเดตซอฟต์แวร์ HMC ให้รีสตาร์ทระบบ ด้วย DVD-RAM ในไดรฟ์ DVD

1. ใส่สื่อบันทึกสำหรับการติดตั้งผลิตภัณฑ์ HMC
2. ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. จากแถบเมนู HMC ให้เลือก **Console > Exit**
 - b. คลิก **Exit now**
 - c. จากรายการลือกเอาต์ให้เลือก **Reboot Console** และ คลิก **OK** HMC จะเริ่มทำงานอีกครั้ง และ ข้อมูลระบบจะเลื่อนอยู่บนหน้าต่าง
3. เลือก **Upgrade** และคลิก **Next**
4. เมื่อคำเตือนปรากฏขึ้น ให้เลือกจาก อีพจน์ต่อไปนี้:
 - ถ้าคุณบันทึกข้อมูลอัปเดตที่บันทึกไว้ในระหว่างงานก่อนหน้านี้ ให้ทำ ขั้นตอนถัดไป
 - ถ้าคุณไม่ได้บันทึกข้อมูลอัปเดตก่อนหน้านี้ในขั้นตอนนี้ คุณจะ ต้อง บันทึกข้อมูลอัปเดตในตอนนี้ ก่อนที่คุณจะดำเนินการต่อ
5. เลือก **Upgrade from media** และคลิก **Next**
6. ยืนยันค่าติดตั้ง และคลิก **Finish**
7. ปฏิบัติตามพร้อมต์

หมายเหตุ:

- ถ้าหน้าจอว่างเปล่า ให้กด space bar เพื่อดูข้อมูล
 - ดีวีดีแผ่นแรกอาจใช้เวลาประมาณ 20 ในการติดตั้ง
8. เมื่อมีพร้อมต์ปรากฏขึ้น ให้เอาสื่อบันทึกแผ่นแรกออก แล้วใส่สื่อบันทึก แผ่นที่สอง
 9. เลือก **1. Install additional software from media** และ กด Enter กดคีย์ใดๆ เพื่อยืนยันการติดตั้ง HMC จะแสดงข้อความสถานะ เมื่อติดตั้งแพ็คเกจ
 10. คลิก **Log on and launch the Hardware Management Console web application**
 11. ล็อกอินเข้าสู่อินเตอร์เฟซ HMC
 12. ดำเนินการต่อด้วย “ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์”

ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์

1. ในพื้นที่การนำทาง ให้คลิก อัปเดต ในพื้นที่ใช้งาน เวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน จะแสดงอยู่ภายใต้ หัวข้อ HMC Code Level
2. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
3. ถ้าระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ลองทำการอัปเดตอีกครั้งโดยใช้ดีวีดีใหม่ ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

ขั้นตอนที่ 10. ขอรับแพ็คเกจอัปเดต

คุณสามารถสั่งซื้อแพ็คเกจอัปเดต HMC ผ่านทางเว็บไซต์ Fix Central โดยติดต่อส่วนบริการและสนับสนุน หรือดาวน์โหลดไปยังเซิร์ฟเวอร์ FTP

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ ที่มีการเชื่อมต่ออินเทอร์เน็ตให้ไปที่ <http://www.ibm.com/eserver/support/fixes>
2. เลือกตระกูลที่เหมาะสมในรายการตระกูล ผลิตภัณฑ์

3. เลือก **Hardware Management Console** ใน รายการชนิดผลิตภัณฑ์หรือโปรแกรมฟิร์มแวร์
4. คลิก **ทำต่อไป** ไซต์ Hardware Management Console จะปรากฏขึ้น
5. นำทางไปยังเวอร์ชัน HMC ที่คุณต้องการ
6. ค้นหาตำแหน่งส่วนดาวน์โหลดและสั่งซื้อ

หมายเหตุ: ถ้าคุณไม่มีการเข้าถึงอินเทอร์เน็ต โปรดติดต่อส่วนบริการและ สนับสนุน เพื่อสั่งซื้อฮาร์ดแวร์บนตัวดี

7. ปฏิบัติตามพร้อมดเพื่อดาวน์โหลดแพ็คเกจอัปเดตไปยัง สื่อบันทึกแบบถอดออกได้ หรือส่งคำสั่งซื้อของคุณ

ขั้นตอนที่ 11. เปลี่ยนกำหนดการของการดำเนินการสำหรับ HMC

เมื่อคุณอัปเดต HMC คุณจะต้องเปลี่ยนกำหนดการสำหรับการดำเนินการ ที่คุณได้ตั้งกำหนดการเอาไว้โดยใช้ HMC เวอร์ชันก่อนหน้า

1. ในพื้นที่การนำทางให้คลิก **การจัดการ HMC**
2. ในพื้นที่ใช้งาน ให้คลิก **Schedule Operations**

การอัปเดต HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตบนเครือข่าย

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตเครือข่าย

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตเครือข่าย ใช้ขั้นตอนต่อไปนี้เพื่ออัปเดต HMC ที่ระดับ V6R1.2 หรือสูงกว่า ซึ่งรวมถึงระดับ HMC V7 ทั้งหมด

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ไปที่เว็บไซต์ Hardware Management Console (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)
2. ดาวน์โหลดอิมเมจเครือข่าย HMC V7 ที่เหมาะสมและบันทึก บนเซิร์ฟเวอร์ FTP คุณไม่สามารถดาวน์โหลดไฟล์เหล่านี้โดยตรงไปยัง HMC คุณต้องดาวน์โหลดไฟล์อิมเมจไปยังเซิร์ฟเวอร์ ที่ยอมรับคำร้องขอ FTP
3. ตรวจสอบให้แน่ใจว่าคุณดาวน์โหลดไฟล์ต่อไปนี้:
 - initrd.gz
 - bzImage
 - disk1.img
 - disk2.img
 - disk3.img
 - hmcnetworkfiles.sum
4. บันทึกข้อมูลการอัปเดตบน HMC ดำเนินการบรรทัดคำสั่ง ต่อไปนี้เพื่อบันทึกข้อมูลการอัปเดต:
 - เพื่อบันทึกข้อมูลบนทั้ง DVD และ HDD ดำเนินการคำสั่งต่อไปนี้:


```
mount /media/cdrom
saveupgdata -r diskdvd
```
 - เพื่อบันทึกข้อมูลบน HDD ดำเนินการคำสั่งต่อไปนี้:


```
saveupgdata -r disk
```
5. คัดลอกไฟล์การอัปเดตไปยังพาร์ติชันดิสก์ที่สามารถบูตได้บน HMC รันคำสั่ง `getupgfiles` เพื่อคัดลอกไฟล์ ตัวอย่างเช่น: `getupgfiles -h <ftp server> -u <user id> -d <remote directory>`

โดย

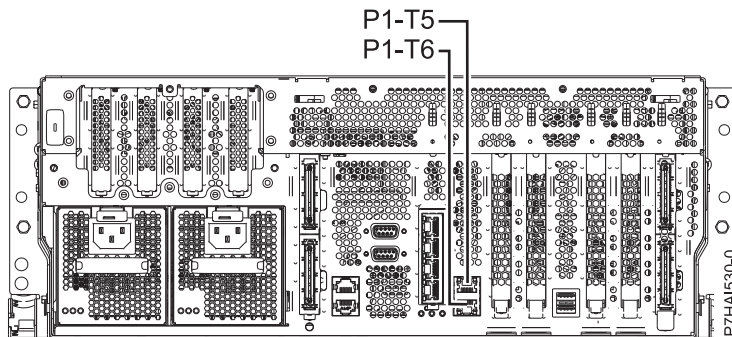
- ftp server คือชื่อโฮสต์หรือ ip แอดเดรสของ เซิร์ฟเวอร์ FTP ที่คุณดาวน์โหลดอิมเมจเครือข่าย HMC ไว้
 - user id คือ id ผู้ใช้ที่ถูกต้องบนเซิร์ฟเวอร์ FTP หากคุณไม่ได้ระบุรหัสผ่านด้วยอาร์กิวเมนต์ --passwd คุณจะได้รับพร้อมท์สำหรับรหัสผ่าน
 - remote directory คือไดเรกทอรีบนเซิร์ฟเวอร์ FTP ของคุณที่บันทึกอิมเมจเครือข่าย HMC ไว้
6. รีบูต HMC เพื่ออัปเดตโค้ดที่คัดลอกไปยังพาร์ติชันดิสก์ ที่บูตได้ รัน `chhmc -c altdiskboot -s enable --mode upgrade` เพื่อรีบูต HMC
 7. รีบูต HMC และเริ่มต้นการอัปเดต รันคำสั่ง `hmcshutdown -r -t now` เพื่อเริ่มต้นการอัปเดต

ตำแหน่งพอร์ตของ HMC

คุณสามารถค้นหาตำแหน่งพอร์ตได้โดยใช้โค้ดตำแหน่ง ใช้ภาพประกอบ ตำแหน่งพอร์ตของ HMC เพื่อแมปโค้ดตำแหน่งกับตำแหน่งพอร์ตของ HMC บนเซิร์ฟเวอร์

8202-E4B หรือ 8205-E6B ตำแหน่งพอร์ตของ HMC

ใช้แผนผัง และตารางนี้เพื่อแมปพอร์ต HMC บน 8202-E4B หรือ 8205-E6B



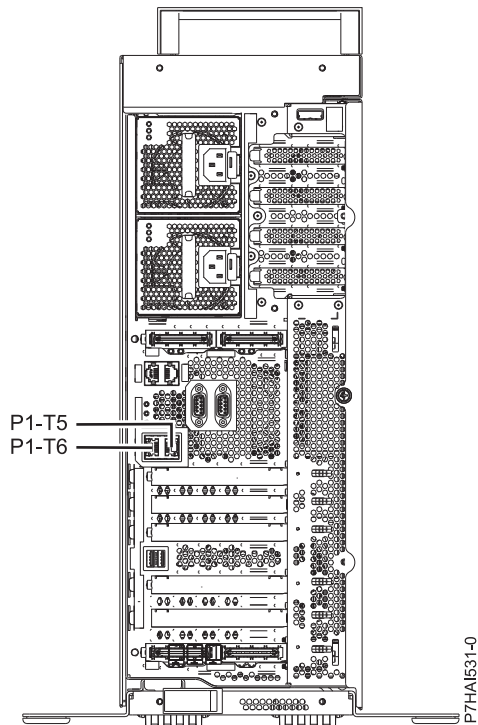
รูปที่ 36. 8202-E4B หรือ 8205-E6B ตำแหน่งพอร์ตของ HMC

ตารางที่ 14. 8202-E4B หรือ 8205-E6B ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T5	ไม่มี
พอร์ต HMC 2	Un-P1-T6	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ตของ HMC บน 8202-E4B หรือ 8205-E6B โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8202-E4B หรือ 8205-E6B		

8202-E4C หรือ 8205-E6C ตำแหน่งพอร์ตของ HMC

ใช้แผนผัง และตารางนี้เพื่อแม่พพอร์ต HMC บน 8202-E4C หรือ 8205-E6C



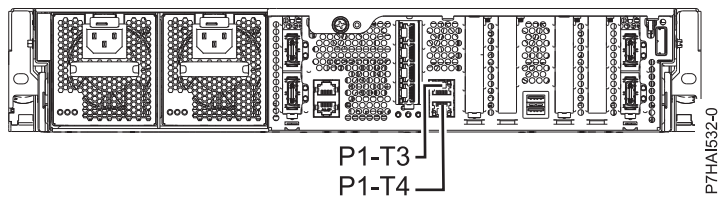
รูปที่ 37. 8202-E4C หรือ 8205-E6C ตำแหน่งพอร์ตของ HMC

ตารางที่ 15. 8202-E4C หรือ 8205-E6C ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T5	ไม่มี
พอร์ต HMC 2	Un-P1-T6	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ตของ HMC บน 8202-E4C หรือ 8205-E6C โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8202-E4C หรือ 8205-E6C		

8231-E2B ตำแหน่งพอร์ตของ HMC

ใช้แผนผังและตารางนี้เพื่อแม่พ พอร์ต HMC บน 8231-E2B



รูปที่ 38. 8231-E2B ตำแหน่งพอร์ตของ HMC

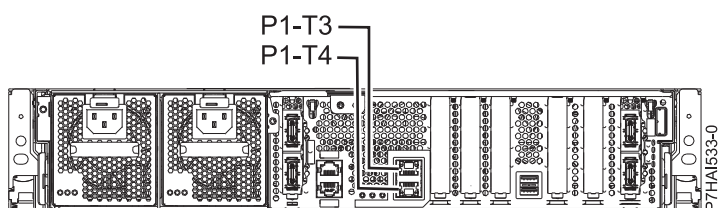
ตารางที่ 16. 8231-E2B ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T3	ไม่มี
พอร์ต HMC 2	Un-P1-T4	ไม่มี

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ตของ HMC บน 8231-E2B, โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8231-E2B

8231-E1C หรือ 8231-E2C ตำแหน่งพอร์ตของ HMC

ใช้แผนผัง และตารางนี้เพื่อแมปพอร์ต HMC บน 8231-E1C หรือ 8231-E2C



รูปที่ 39. 8231-E1C หรือ 8231-E2C ตำแหน่งพอร์ตของ HMC

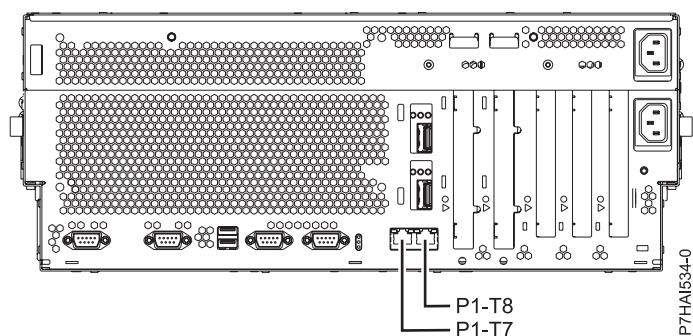
ตารางที่ 17. 8231-E1C หรือ 8231-E2C ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T3	ไม่มี
พอร์ต HMC 2	Un-P1-T4	ไม่มี

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ตของ HMC บน 8231-E1C หรือ 8231-E2C, see ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8231-E1C หรือ 8231-E2C

8233-E8B หรือ 8236-E8C ตำแหน่งพอร์ตของ HMC

ใช้แผนผัง และตารางนี้เพื่อแมปพอร์ต HMC บน 8233-E8B หรือ 8236-E8C



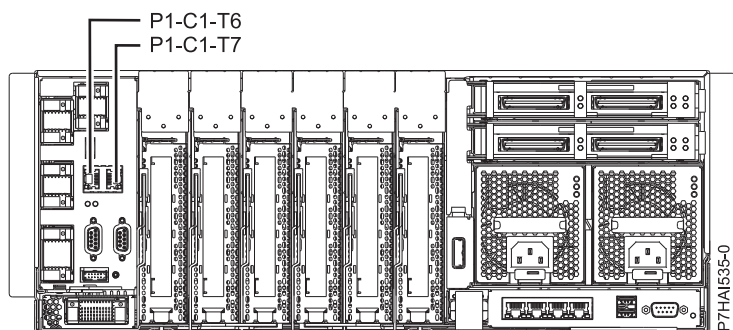
รูปที่ 40. 8233-E8B or 8236-E8C ตำแหน่งพอร์ตของ HMC

ตารางที่ 18. 8233-E8B or 8236-E8C ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T7	ไม่มี
พอร์ต HMC 2	Un-P1-T8	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ตของ HMC บน 8233-E8B หรือ 8236-E8C โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8233-E8B หรือ 8236-E8C		

8408-E8D 8248-L4T หรือ 9109-RMD ตำแหน่งพอร์ตของ HMC

ใช้แผนผัง และตารางนี้เพื่อแมปพอร์ต HMC บน 8408-E8D 8248-L4T หรือ 9109-RMD



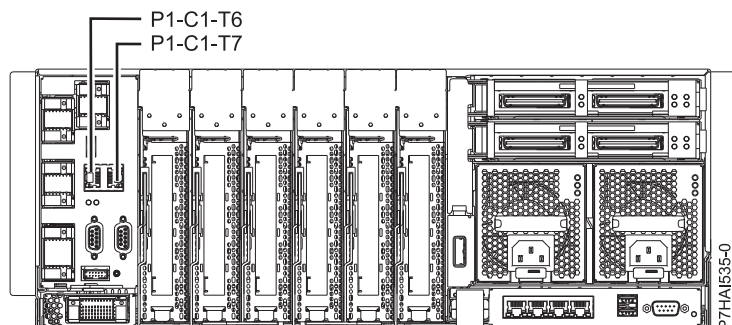
รูปที่ 41. 8408-E8D 8248-L4T or 9109-RMD ตำแหน่งพอร์ตของ HMC

ตารางที่ 19. 8408-E8D 8248-L4T or 9109-RMD ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-C1-T6	ใช่
พอร์ต HMC 2	Un-P1-C1-T7	ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ พอร์ตของ HMC บน 8408-E8D หรือ 9109-RMD โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8408-E8D หรือ 9109-RMD		

9117-MMB หรือ 9179-MHB ตำแหน่งพอร์ตของ HMC

ใช้แผนผังและตารางนี้เพื่อแม็พพอร์ต HMC บน 9117-MMB หรือ 9179-MHB



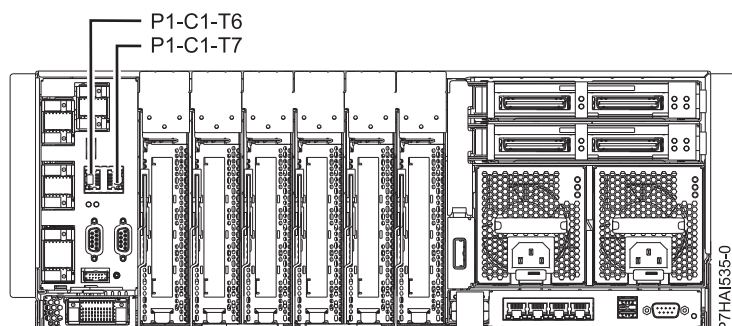
รูปที่ 42. 9117-MMB or 9179-MHB ตำแหน่งพอร์ตของ HMC

ตารางที่ 20. 9117-MMB or 9179-MHB ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-C1-T6	ใช่
พอร์ต HMC 2	Un-P1-C1-T7	ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ พอร์ต HMC บน 9117-MMB or 9179-MHB โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 9117-MMB หรือ 9179-HMC		

9117-MMC, 9117-MMD, 9179-MHC, 9179-MHD หรือตำแหน่งพอร์ต 8412-EAD HMC

ใช้แผนภาพและตารางนี้เพื่อแม็พพอร์ต HMC บน 9117-MMC, 9117-MMD, 9179-MHC, 9179-MHD หรือ 8412-EAD



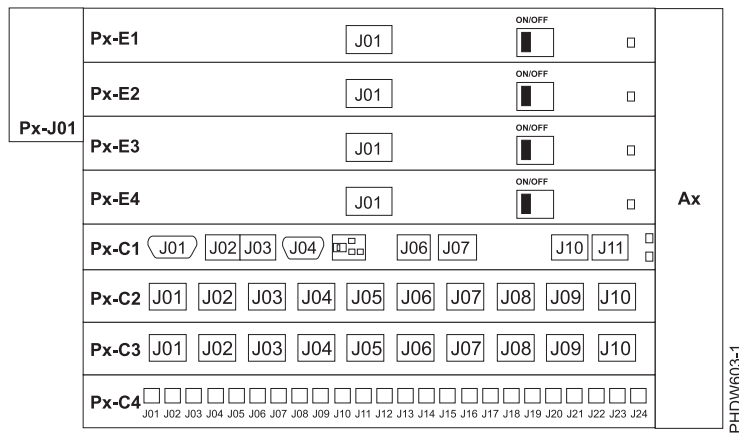
รูปที่ 43. 9117-MMC, 9117-MMD, 9179-MHC, 9179-MHD หรือตำแหน่งพอร์ต 8412-EAD HMC

ตารางที่ 21. 9117-MMC, 9117-MMD, 9179-MHC, 9179-MHD หรือตำแหน่งพอร์ต 8412-EADHMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-C1-T6	ใช่
พอร์ต HMC 2	Un-P1-C1-T7	ใช่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ พอร์ต HMC บน 9117-MMC, 9117-MMD, 9179-MHC หรือ 9179-MHD โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 9117-MMC, 9117-MMD, 9179-MHC หรือ 9179-MHD		

9119-FHB ตำแหน่งพอร์ตของ HMC

ใช้แผนผังและตารางนี้เพื่อแม็ป พอร์ต HMC บน 9119-FHB



รูปที่ 44. 9119-FHB ตำแหน่งพอร์ตของ HMC

ตารางที่ 22. 9119-FHB ตำแหน่งพอร์ตของ HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
HMC (ตัวเชื่อมต่อ J02, อีเทอร์เน็ตเข้ากับ Bulk power hub-BPH)	Un-Px-C1-J02	ไม่
HMC (ตัวเชื่อมต่อ J03, อีเทอร์เน็ตเข้ากับ Bulk power hub-BPH)	Un-Px-C1-J03	ไม่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ พอร์ต HMC บน 9119-FHB โปรดดูที่ ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 9119-FHB		

คำประกาศ

ข้อมูลนี้ถูกพัฒนาสำหรับผลิตภัณฑ์และการบริการในประเทศสหรัฐอเมริกา

ผู้ผลิตอาจจะไม่เสนอผลิตภัณฑ์ การให้บริการ หรือคุณลักษณะที่ได้อธิบายในเอกสารนี้ให้กับประเทศอื่น ปกติเกี่ยวกับข้อมูลของผลิตภัณฑ์และการให้บริการที่มีในพื้นที่ของ คุณได้จากตัวแทนของผู้ผลิต การอ้างถึง ผลิตภัณฑ์ โปรแกรม หรือการให้บริการของผู้ผลิต ไม่ได้มีจุดมุ่งหมายที่จะบอก หรือมีความหมายว่าผลิตภัณฑ์ โปรแกรม หรือ บริการนั้นจะสามารถใช้ได้ ฟังก์ชันอื่นๆที่คล้ายกันกับผลิตภัณฑ์ โปรแกรม หรือบริการซึ่ง ไม่ละเมิดทรัพย์สินทางปัญญาของผู้ผลิตสามารถใช้แทนได้ อย่างไรก็ตาม เป็นหน้าที่ของผู้ใช้ที่จะประเมิน และตรวจสอบการทำงานของผลิตภัณฑ์ โปรแกรมหรือการให้บริการนั้นเอง

ผู้ผลิตอาจได้รับสิทธิบัตรหรือยื่นขอรับการจดสิทธิบัตร ที่ครอบคลุมถึงสิ่งที่ได้อธิบายในเอกสารฉบับนี้ การตกแต่งเอกสารนี้ไม่ได้ทำให้คุณได้รับไลเซนส์สำหรับ สิทธิบัตรนี้ โดยคุณสามารถเขียนถึงผู้ผลิต เพื่อสอบถามข้อมูลเกี่ยวกับไลเซนส์

>ย่อหน้าต่อไปนี้อาจไม่สามารถใช้ได้ ในสหราชอาณาจักร หรือในประเทศที่มีกฎหมายท้องถิ่นที่แตกต่างกัน ออกไป: เอกสารนี้จัดเตรียมไว้ “ตามสภาพที่เป็น” โดยไม่มีการรับประกันใดๆ ไม่ว่าจะโดยเปิดเผยหรือโดยนัย รวมถึงแต่ไม่จำกัดถึง การรับประกันโดยนัยเกี่ยวกับความสามารถในการจำหน่าย การไม่ละเมิด และความเหมาะสมสำหรับวัตถุประสงค์เฉพาะอย่างใดอย่างหนึ่ง ในบางรัฐที่ไม่ยอมรับการสลละสิทธิ์โดยคำพูด หรือ การรับประกันโดยนัยสำหรับรายการใดๆ ดังนั้น ข้อความนี้จะใช้ไม่ได้

ข้อมูลนี้อาจเกิดความผิดพลาดทางเทคนิค หรือการพิมพ์ ซึ่งจะมีการแก้ไขข้อมูลเหล่านั้นเป็นระยะๆ ซึ่งข้อมูลที่ถูกแก้ไขนี้จะอยู่ในเอกสารฉบับ ถัดไป ผู้ผลิตอาจทำการปรับปรุง และ/หรือ แก้ไข ผลิตภัณฑ์ และ/หรือ โปรแกรม ที่กล่าวถึงในเอกสารฉบับนี้ ได้โดยไม่มีการแจ้งล่วงหน้า

การอ้างอิงในข้อมูลนี้ไปยังเว็บไซต์ซึ่ง ไม่ได้เป็นของผู้ผลิต มีการนำเสนอเพื่อความสะดวกเท่านั้นและ ไม่ได้เป็นการรับรองเว็บไซต์ดังกล่าวในลักษณะใดๆ เอกสารประกอบ ที่เว็บไซต์เหล่านั้นไม่ได้เป็นส่วนหนึ่งของเอกสารประกอบสำหรับผลิตภัณฑ์นี้ และการใช้เว็บไซต์ดังกล่าวถือเป็นความเสี่ยงของคุณเอง

ผู้ผลิตอาจใช้หรือเผยแพร่ข้อมูลที่ คุณให้ตามความเหมาะสมโดยไม่มี ข้อผูกมัดใดๆกับคุณ

ข้อมูลประสิทธิภาพการทำงานที่กล่าวถึงในเอกสารนี้ถูกวัด ในสภาวะแวดล้อมที่ถูกควบคุม ดังนั้นผลที่ได้จากสภาวะแวดล้อมการทำงานอื่น อาจมีความแตกต่างอย่างมาก การวัดค่าบางอย่างอาจถูกกระทำ บนระบบในระดับที่ใช้ในการพัฒนา และไม่มี การรับประกันว่า ค่าเหล่านั้นจะเหมือนกันในระบบทั่วไป อย่างไรก็ตาม การวัดค่าอาจเกิดจากการประมาณการจนถึงการคาดการณ์ ผลที่ได้จึงอาจแตกต่างกัน ผู้ใช้เอกสารนี้จึงควรตรวจสอบ ข้อมูลที่สามารถใช้ได้สำหรับสภาวะแวดล้อมของตน

ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ได้ผลิตโดยผู้ผลิตนี้ ได้รับมาจากผู้ผลิตผลิตภัณฑ์นั้น เอกสารประชาสัมพันธ์ หรือแหล่งข้อมูลสาธารณะ ผู้ผลิตไม่ได้ทำการ ทดสอบผลิตภัณฑ์ดังกล่าวและไม่สามารถยืนยัน ความเที่ยงตรงในประสิทธิภาพในการทำงาน ความเข้าใจกันได้ และการกล่าวอ้างอื่นๆ เกี่ยวกับผลิตภัณฑ์นั้นที่ไม่ได้ผลิตโดยผู้ผลิต หากมีคำถามเกี่ยวกับความสามารถของผลิตภัณฑ์ที่ไม่ได้ผลิตโดยผู้ผลิตควรจะ ติดต่อกับผู้ผลิตผลิตภัณฑ์นั้น

ข้อความใดๆเกี่ยวกับทิศทาง หรือเป้าหมายในอนาคตของผู้ผลิต อาจมีการเปลี่ยนแปลงหรือยกเลิก โดยไม่มีการแจ้งล่วงหน้า และมีการนำเสนอใหม่เฉพาะเป้าหมายและวัตถุประสงค์เท่านั้น

ราคาของผู้ผลิตที่แสดงให้เห็นเป็นราคาขายปลีกในปัจจุบัน และอาจมีการเปลี่ยนแปลงโดยไม่ต้องแจ้งให้ทราบล่วงหน้า ราคาของผู้แทนจำหน่ายอาจแตกต่างกันออกไป

โดยข้อมูลนี้มีวัตถุประสงค์เพื่อใช้ในการวางแผนเท่านั้น ข้อมูลเหล่านี้ อาจมีการเปลี่ยนแปลงก่อนที่จะมีคำอธิบาย ของผลิตภัณฑ์ออกมา

ข้อมูลนี้จะประกอบด้วยตัวอย่างของข้อมูล และรายงาน ที่ใช้ในการดำเนินธุรกิจในแต่ละวัน เพื่อให้การยกตัวอย่างสมบูรณ์ที่สุดเท่าที่จะทำได้ อาจมีการยกตัวอย่างชื่อบุคคล บริษัท ยี่ห้อ หรือผลิตภัณฑ์ ซึ่งชื่อเหล่านี้ อาจเป็นชื่อที่แต่งขึ้นซึ่งอาจเหมือนกับชื่อหรือที่อยู่ขององค์กรทางธุรกิจจริง ได้โดยบังเอิญ

ถ้าคุณดูเอกสารฉบับนี้โดยใช้สำเนาชั่วคราว รูปและสีของรูปประกอบอาจไม่แสดงให้เห็น

ห้ามทำการตกแต่งรูปภาพและข้อกำหนดคุณสมบัติในเอกสารนี้ ไม่ว่าจะเป็นบางส่วนหรือทั้งหมดโดยไม่มีคำอนุญาตเป็นลายลักษณ์อักษรจากผู้ผลิต

ผู้ผลิตเตรียมข้อมูลนี้เพื่อให้ใช้กับเครื่องที่ระบุไว้ ผู้ผลิตไม่ได้เป็นตัวแทน เพื่อวัตถุประสงค์อื่น

ระบบคอมพิวเตอร์ของผู้ผลิตมีกลไก ที่ถูกออกแบบให้ลดความเป็นไปได้ที่จะเกิดของความล้มเหลวของข้อมูลที่ไม่สามารถตรวจพบได้หรือ ข้อมูลสูญหาย อย่างไรก็ตามความเสี่ยงเหล่านี้ยังไม่สามารถจำกัดให้หมดไปได้ ผู้ใช้ที่ประสบการณเกี่ยวกับสัญญาณขาดหายที่ไม่ได้วางแผนไว้ล่วงหน้า ระบบขัดข้อง ระบบกำลังไฟฟ้าที่ไม่แน่นอนหรือขาดหาย หรือส่วนประกอบขัดข้อง ควรจะทำการตรวจสอบความถูกต้องของการดำเนินการ และข้อมูลที่ถูกรบกวนหรือส่งโดยระบบ ในช่วงเวลาหรือเวลาใกล้เคียงกับที่ สัญญาณขาดหายหรือขัดข้อง นอกจากนี้ ในการดำเนินงานที่มีความอ่อนไหว หรือสำคัญมาก ผู้ใช้ควรมีขั้นตอนเพื่อให้มั่นใจว่ามีการตรวจสอบข้อมูลอย่างเป็นอิสระก่อนที่จะเชื่อถือ ข้อมูลเหล่านั้น ผู้ใช้ควรทำการตรวจสอบ ข้อมูลล่าสุด และโปรแกรมฟิร์มแวร์สำหรับระบบและซอฟต์แวร์ที่เกี่ยวข้อง จากเว็บไซต์สนับสนุนของผู้ผลิตเป็นระยะๆ

ข้อความการให้สัตยาบัน

ผลิตภัณฑ์นี้อาจไม่ได้รับการรับรองในประเทศของคุณสำหรับการเชื่อมต่อด้วย สื่อใดๆ ก็ตามไปยังอินเทอร์เน็ตเฟสของเครือข่ายโทรคมนาคมแบบพบลิงก์ การรับรองเพิ่มเติมอาจเป็นข้อบังคับตามกฎหมายก่อนทำการเชื่อมต่อ ดังกล่าว โปรดติดต่อตัวแทนหรือผู้ค้าปลีกของ IBM ถ้ามีคำถามใดๆ

เครื่องหมายการค้า

IBM, โลโก้ IBM และ ibm.com เป็นเครื่องหมายการค้า หรือ เครื่องหมายการค้าที่จดทะเบียนของ International Business Machines Corp., โดยจดทะเบียน ภายในของเขตอำนาจของศาลและกฎหมายหลายแห่งทั่วโลก ผลิตภัณฑ์อื่นและชื่อการให้บริการ อาจเป็นเครื่องหมายการค้าของ IBM หรือบริษัทอื่น รายชื่อของเครื่องหมายการค้า IBM ปัจจุบัน สามารถดูได้บนเว็บไซต์ ข้อมูล เกี่ยวกับลิขสิทธิ์และเครื่องหมายการค้า ที่ www.ibm.com/legal/copytrade.shtml

Java และเครื่องหมายการค้าและตราสัญลักษณ์ที่สร้างขึ้นจาก Java ทั้งหมดเป็น เครื่องหมายการค้าหรือเครื่องหมายการค้าที่จดทะเบียนของ Oracle และ/หรือบริษัทในเครือ

Microsoft เป็นเครื่องหมายการค้าของ Microsoft Corporation ใน สหรัฐอเมริกา ประเทศอื่น หรือทั้งสองอย่าง

ประกาศเกี่ยวกับการปล่อยกำลังไฟฟ้า

เมื่อแนบมอนิเตอร์กับอุปกรณ์ คุณต้องใช้สายมอนิเตอร์ที่กำหนดให้ และอุปกรณ์ยังการแทรกแซงใดๆ ที่ให้มากับมอนิเตอร์

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A ต่อไปนี้ นำไปใช้กับเซิร์ฟเวอร์ IBM ที่มีตัวประมวลผล POWER7 และคุณลักษณะของเซิร์ฟเวอร์ ยกเว้นถูกกำหนดให้เป็นความเข้ากันได้ทางแม่เหล็กไฟฟ้า (EMC) คลาส B ใน ข้อมูลคุณลักษณะ

ข้อกำหนดของ Federal Communications Commission (FCC)

หมายเหตุ: เครื่องมือนี้ได้รับการทดสอบ และพบว่าเป็นไปตามข้อกำหนดของอุปกรณ์ดิจิทัลคลาส A ตามหมวด 15 ของกฎ FCC ข้อกำหนดเหล่านี้ถูกออกแบบมา เพื่อให้มีการป้องกันในระดับที่สมเหตุสมผลต่อการรบกวนที่เป็นอันตรายเมื่อเครื่องมือถูกใช้งานในสภาพการใช้งานเชิงพาณิชย์ อุปกรณ์นี้สามารถจะสร้าง ใช้งาน และสามารถแผ่คลื่นความถี่วิทยุ และหากไม่ได้ติดตั้งและใช้งานตามคู่มือการใช้งาน อาจเป็นเหตุให้เกิดการรบกวนที่สร้างความเสียหายต่อการสื่อสารทางวิทยุ การทำงานของอุปกรณ์นี้ในบริเวณที่ปกอภัยอาจก่อให้เกิดการรบกวนที่เป็นอันตราย ในกรณีนี้ ผู้ใช้งานจำเป็นต้องแก้ไขสัญญาณรบกวนโดยที่ต้องรับผิดชอบค่าใช้จ่ายด้วยตนเอง

สายเคเบิลและตัวเชื่อมต่อที่ได้รับการหุ้มฉนวน และมีการเดินสายดินเอาไว้เรียบร้อยแล้ว จะต้องถูกนำมาใช้งาน เพื่อให้เป็นไปตามข้อกำหนดต่างๆ ในเรื่องการแผ่สัญญาณของ FCC IBM ไม่มีส่วนรับผิดชอบต่อสัญญาณรบกวนเครื่องรับวิทยุหรือโทรทัศน์ที่เกิดขึ้น เนื่องจากการใช้สายเคเบิลและตัวเชื่อมต่อที่นอกเหนือไปจากที่แนะนำ หรือโดยการเปลี่ยนแปลงหรือปรับแต่งอุปกรณ์นี้โดยไม่ได้รับอนุญาต การเปลี่ยนแปลงหรือปรับแต่งโดยไม่ได้รับอนุญาต อาจทำให้สิทธิในการใช้งานอุปกรณ์นี้ของผู้ใช้เป็นโมฆะ

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

คำประกาศเกี่ยวกับความสอดคล้องของอุตสาหกรรมประเทศแคนาดา

อุปกรณ์ดิจิทัลคลาส A นี้สอดคล้องกับ Canadian ICES-003

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

คำประกาศความสอดคล้องของประชาคมยุโรป

ผลิตภัณฑ์นี้สอดคล้องกับข้อกำหนดในการป้องกันของข้อกำหนด EU Council Directive 2004/108/EC ตามร่างกฎหมายของรัฐสมาชิกที่เกี่ยวข้องกับความสามารถในความเข้ากันได้ทางแม่เหล็กไฟฟ้า IBM ไม่รับผิดชอบต่อความผิดพลาดเสียหายใดๆ ตามข้อกำหนดในการป้องกันซึ่งอันเกิดจากการดัดแปลงผลิตภัณฑ์โดยไม่ได้รับการแนะนำ รวมถึงการใช้การ์ดต่างๆ ที่ไม่ใช่ตัวเลือกของ IBM

ผลิตภัณฑ์นี้ได้รับการทดสอบ และพบว่าสอดคล้องกับข้อกำหนดของอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศคลาส A ตามมาตรฐานแห่งยุโรป EN 55022 ข้อกำหนดต่างๆ สำหรับอุปกรณ์คลาส A ได้รับการกำหนดขึ้นมาเพื่อใช้กับสภาวะแวดล้อมเชิงพาณิชย์และด้านอุตสาหกรรม ทั้งนี้เพื่อให้มีการป้องกันที่สมเหตุสมผลต่อสัญญาณรบกวนที่เกิดขึ้นกับอุปกรณ์การสื่อสารที่ได้รับอนุญาตแล้ว

ข้อมูลติดต่อสำหรับประชาคมยุโรป:

IBM Deutschland GmbH

Technical Regulations, Department M372

IBM-Allee 1, 71139 Ehningen, Germany

โทรศัพท์: +49 7032 15 2941

อีเมล: lugi@de.ibm.com

คำเตือน: ผลิตภัณฑ์นี้เป็นผลิตภัณฑ์คลาส A ผลิตภัณฑ์นี้อาจก่อให้เกิดการรบกวนคลื่นวิทยุในสภาพแวดล้อมการใช้งานภายในครัวเรือน ซึ่งผู้ใช้งานอาจจำเป็นต้องใช้มาตรการที่เหมาะสม

คำประกาศ VCCI - ญี่ปุ่น

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

ข้อความต่อไปนี้เป็นข้อสรุปของคำประกาศ VCCI ของประเทศญี่ปุ่นในกรอบข้างต้น

ผลิตภัณฑ์นี้เป็นผลิตภัณฑ์ในคลาส A ที่อิงตามมาตรฐานของสภา VCCI ผลิตภัณฑ์นี้อาจก่อให้เกิดการรบกวนคลื่นวิทยุในสภาพแวดล้อมการใช้งานภายในครัวเรือน ซึ่งผู้ใช้งานอาจจำเป็นต้องใช้มาตรการที่เหมาะสม

แนวทางปฏิบัติเกี่ยวกับความสอดคล้องที่มีหลักฐานยืนยันของ **Japanese Electronics and Information Technology Industries Association (JEITA)** (ผลิตภัณฑ์ที่มีกำลังไฟฟ้าน้อยกว่า หรือเท่ากับ 20 A ต่อเฟส)

高調波ガイドライン適合品

แนวทางปฏิบัติเกี่ยวกับความสอดคล้องที่มีหลักฐานยืนยันของ **Japanese Electronics and Information Technology Industries Association (JEITA)** ที่มีการปรับปรุงแก้ไข (ผลิตภัณฑ์ที่มีกำลังไฟฟ้ามากกว่า 20 A ต่อเฟส)

高調波ガイドライン準用品

คำประกาศเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (EMI) - สาธารณรัฐประชาชนจีน

声 明

此为 A 级产品, 在环境中,
该产品可能会造成无线电干扰。
在这种情况下, 可能需要用户对其
干扰采取切实可行的措施。

คำประกาศ: ผลิตภัณฑ์นี้เป็นผลิตภัณฑ์คลาส A ผลิตภัณฑ์นี้อาจก่อให้เกิดการรบกวนของคลื่นวิทยุในสภาพแวดล้อมการใช้งานภายในครัวเรือน ซึ่งผู้ใช้งานอาจจำเป็นต้องดำเนินการตามความเหมาะสม

คำประกาศเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (EMI) - ประเทศไต้หวัน

警告使用者：

這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這種
情況下，使用者會被要求
採取某些適當的對策。

ข้อความต่อไปนี้เป็นข้อสรุปคำประกาศ EMI ของประเทศไต้หวันข้างต้น

คำเตือน: ผลิตภัณฑ์นี้เป็นผลิตภัณฑ์คลาส A ผลิตภัณฑ์นี้อาจก่อให้เกิดการรบกวนของคลื่นวิทยุตามสภาพแวดล้อมการใช้งานภายในครัวเรือน ซึ่งผู้ใช้งานอาจจำเป็นต้องใช้มาตรการที่เหมาะสม

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

คำประกาศเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (EMI) - ประเทศเกาหลี

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

คำประกาศเกี่ยวกับความสอดคล้องของประเทศเยอรมนี

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 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 55022 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) 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 Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany

โทรศัพท์: +49 7032 15 2941

อีเมล: lugi@de.ibm.com

Generelle Informationen:

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

คำประกาศเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (Electromagnetic Interference (EMI) - ประเทศไทย)

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

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส B

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส B ต่อไปนี้นำไปใช้กับคุณลักษณะที่ถูกระบุให้เป็น ความเข้ากันได้ทางแม่เหล็กไฟฟ้า (EMC) คลาส B ในข้อมูลการติดตั้งคุณสมบัติ

ข้อกำหนดของคณะกรรมการกลางกำกับดูแลกิจการสื่อสาร (Federal Communications Commission - FCC)

อุปกรณ์นี้ได้รับการทดสอบ และพบว่าเป็นไปตามข้อกำหนดของอุปกรณ์ดิจิทัลคลาส B ตามหมวดที่ 15 ของ กฎ FCC ข้อกำหนดเหล่านี้ถูกออกแบบมาเพื่อให้การป้องกันในระดับที่สมเหตุสมผลต่อการรบกวนที่เป็นอันตรายเมื่ออุปกรณ์ถูกใช้งานในสภาพการใช้งานเชิงพาณิชย์

อุปกรณ์นี้สามารถที่จะก่อให้เกิด ใช้งาน และแผ่คลื่นความถี่วิทยุ และถ้าหากไม่ได้ติดตั้งและใช้งานตามคู่มือการใช้งาน อาจเป็นเหตุให้เกิดการรบกวนที่สร้างความเสียหายต่อการสื่อสารทางวิทยุ อย่างไรก็ตาม ไม่สามารถรับรองได้ว่าการรบกวนจะไม่เกิดขึ้นใน การติดตั้ง

หากอุปกรณ์นี้ ทำให้เกิดการรบกวนที่สร้างความเสียหายต่อการรับสัญญาณวิทยุ หรือโทรทัศน์ ซึ่งสามารถตรวจสอบโดยการ ปิดและเปิดอุปกรณ์ ผู้ใช้ จะได้รับการแนะนำให้พยายามแก้ไขการรบกวนโดยใช้หนึ่งในมาตรการต่อไปนี้:

- การปรับเปลี่ยน หรือย้ายเสาอากาศ
- เพิ่มระยะห่างระหว่างอุปกรณ์กับตัวรับสัญญาณ

- เชื่อมอุปกรณ์ไปยังปลั๊กบนวงจรที่ต่างจากวงจรที่ตัวรับเชื่อมต่ออยู่
- ปรีกษาตัวแทนจำหน่ายที่ได้รับอนุญาตของ IBM หรือตัวแทนบริการเพื่อขอความช่วยเหลือ

สายเคเบิลและตัวเชื่อมต่อที่ได้รับการหุ้มฉนวน และมีการเดินสายดินเอาไว้เรียบร้อยแล้ว จะต้องถูกนำมาใช้งาน เพื่อให้เป็นไปตามข้อกำหนดต่างๆ ในเรื่องการแผ่สัญญาณของ FCC สายเคเบิลและตัวเชื่อมต่อที่เหมาะสมสามารถหาซื้อได้จากตัวแทนจำหน่ายที่ได้รับอนุญาตของ IBM IBM ไม่มีส่วนรับผิดชอบต่อสัญญาณรบกวนเครื่องรับวิทยุหรือโทรทัศน์ที่เกิดขึ้น จากการเปลี่ยนแปลงหรือปรับแต่งอุปกรณ์นี้โดยไม่ได้รับอนุญาต การเปลี่ยนแปลงหรือปรับแต่งโดยไม่ได้รับอนุญาต อาจทำให้สิทธิในการใช้งานอุปกรณ์นี้ของผู้ใช้เป็นโมฆะ

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

คำประกาศเกี่ยวกับความสอดคล้องของอุตสาหกรรมแคนาดา

อุปกรณ์ดิจิทัล คลาส B นี้สอดคล้องกับข้อกำหนด ICES-003 ของแคนาดา

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

คำประกาศเกี่ยวกับความสอดคล้องของประชาคมยุโรป

ผลิตภัณฑ์นี้สอดคล้องกับข้อกำหนดในการป้องกันของ EU Council Directive 2004/108/EC ตามร่างกฎหมายของรัฐสมาชิกที่เกี่ยวข้องกับความสามารถในความเข้ากันได้ทางแม่เหล็กไฟฟ้า IBM ไม่สามารถรับผิดชอบต่อความผิดพลาดเสียหายใดๆ เพื่อให้เป็นไปตามข้อกำหนดในการป้องกันอันเกิดจากการดัดแปลงผลิตภัณฑ์โดยไม่ได้รับการแนะนำ รวมถึง การใช้การ์ดต่างๆ ที่ไม่ใช่ตัวเลือกของ IBM

ผลิตภัณฑ์นี้ได้รับการทดสอบ และพบว่าสอดคล้องกับข้อกำหนดของอุปกรณ์ด้านเทคโนโลยีสารสนเทศคลาส B ตามมาตรฐานยุโรป EN 55022 ข้อกำหนดต่างๆ สำหรับอุปกรณ์คลาส B ได้รับการกำหนดขึ้นมาเพื่อใช้กับสภาพแวดล้อมเชิงพาณิชย์และอุตสาหกรรม เพื่อให้มีการป้องกันที่สมเหตุสมผลต่อสัญญาณรบกวนที่เกิดขึ้นกับอุปกรณ์การสื่อสารที่ได้รับอนุญาตแล้ว

ข้อมูลติดต่อในประชาคมยุโรป:

IBM Deutschland GmbH

Technical Regulations, Department M372

IBM-Allee 1, 71139 Ehningen, Germany

โทรศัพท์: +49 7032 15 2941

อีเมล: lugi@de.ibm.com

คำประกาศ VCCI - ญี่ปุ่น

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

แนวทางปฏิบัติเกี่ยวกับความสอดคล้องที่มีหลักฐานยืนยันของ Japanese Electronics and Information Technology Industries Association (JEITA) (ผลิตภัณฑ์ที่มีกำลังไฟน้อยกว่า หรือเท่ากับ 20 A ต่อเฟส)

高調波ガイドライン適合品

แนวทางปฏิบัติเกี่ยวกับความสอดคล้องที่มีหลักฐานยืนยันของ Japanese Electronics and Information Technology Industries Association (JEITA) ที่มีการปรับปรุงแก้ไข (ผลิตภัณฑ์ที่มีกำลังไฟมากกว่า 20 A ต่อเฟส)

高調波ガイドライン準用品

ข้อมูลติดต่อ IBM ในประเทศไทย

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

คำประกาศเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (EMI) - ประเทศเกาหลี

이 기기는 가정용(B급)으로 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

คำประกาศเกี่ยวกับความสอดคล้องของประเทศเยอรมนี

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) 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 Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany

โทรศัพท์: +49 7032 15 2941

อีเมล: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

ข้อตกลงและเงื่อนไข

คำอนุญาตในการใช้เอกสารเหล่านี้เป็นไปตามข้อกำหนด และเงื่อนไขต่อไปนี้

ความสามารถในการใช้งาน: ข้อกำหนดและเงื่อนไขเหล่านี้เป็นข้อกำหนดและเงื่อนไขเพิ่มเติมในเรื่องของเงื่อนไขการใช้งานสำหรับเว็บไซต์ผู้ผลิต IBM IBM

การใช้งานส่วนบุคคล: คุณสามารถจัดทำสำเนาของเอกสารเหล่านี้เพื่อใช้ในการส่วนตัว มิใช่เพื่อการพาณิชย์ โดยมีเงื่อนไขว่าจะต้องคงข้อความประกาศความเป็นเจ้าของไว้โดยครบถ้วน คุณไม่สามารถแจกจ่าย แสดง หรือสร้างงานที่สืบเนื่องจากเอกสารเหล่านี้ หรือมาจากบางส่วนของเอกสารเหล่านี้ โดยไม่ได้รับความยินยอมอย่างชัดแจ้งจากผู้ผลิต IBM IBM.

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

สิทธิ์: นอกเหนือจากคำอนุญาตที่ได้แสดงไว้ในที่นี้ ผู้ผลิตไม่ได้ให้อำนาจดำเนินการ ลิขสิทธิ์หรือสิทธิอื่นใด ทั้งโดยเปิดเผยและโดยนัยเกี่ยวกับเอกสารหรือข้อมูลใดๆ เหล่านี้ ข้อมูล ซอฟต์แวร์ หรือทรัพย์สินทางปัญญาอื่นๆ ที่อยู่ในภายในที่นี้

ผู้ผลิต ขอสงวนสิทธิ์ในการเพิกถอนคำอนุญาตที่ให้ไว้ในที่นี้เมื่อใดก็ตามที่พิจารณาแล้วว่าการใช้เอกสารเหล่านี้ก่อนให้เกิดความเสียหาย ต่อผลประโยชน์ของบริษัท หรือเมื่อ IBM ได้พิจารณาแล้วว่าไม่มีการปฏิบัติตามข้อกำหนดข้างต้นไว้อย่างเหมาะสม

คุณไม่สามารถดาวน์โหลด ส่งออก หรือทำการส่งออกข้อมูลนี้เข้าได้ ยกเว้นได้ปฏิบัติตามกฎหมายและข้อบังคับที่กำหนดไว้ รวมถึงกฎหมายและข้อบังคับในการส่งออกทั้งหมดของสหรัฐอเมริกา

ผู้ผลิตไม่ขอรับประกันเกี่ยวกับเนื้อหาของเอกสารเหล่านี้ เอกสารเหล่านี้จัดเตรียมไว้ "ตามสภาพที่เป็น" โดยไม่มีการรับประกันใดๆ ไม่ว่าจะเป็นโดยเปิดเผยหรือโดยนัย รวมถึงแต่ไม่จำกัดเพียงการรับประกันโดยนัยของการขายสินค้า การไม่ละเมิด และความเหมาะสม สำหรับวัตถุประสงค์เฉพาะทาง



พิมพ์ในสหรัฐอเมริกา