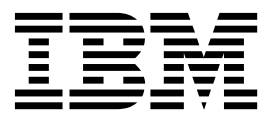


ระบบพลังงาน

การติดตั้งและตั้งค่า Hardware
Management Console



ระบบพลังงาน

การติดตั้งและตั้งค่า Hardware
Management Console



หมายเหตุ
ก่อนการใช้ข้อมูลนี้และผลิตภัณฑ์ที่ข้อมูลนี้สนับสนุน โปรดอ่านข้อมูลใน “ประกาศด้านความปลอดภัย” ในหน้า vii, “หมายเหตุ” ในหน้า 195, คู่มือ *IBM Systems Safety Notices*, G229-9054 และ *IBM Environmental Notices and User Guide*, Z125-5823

เอ็ดจันนี้ใช้กับ IBM Hardware Management Console เวอร์ชัน 8 รีลีส 8.7.0 ระดับการซ่อมบำรุง 0 และกับรีลีสและโมดิไฟเคชันถัดมาทั้งหมดจนกว่าจะระบุไว้เป็นอย่างอื่น ในเอ็ดจันใหม่

© ลิขสิทธิ์ของ IBM Corporation 2014, 2017.

© Copyright IBM Corporation 2014, 2017.

สารบัญ

ประกาศด้านความปลอดภัย	vii
การติดตั้งและการตั้งค่าคอนฟิก คอนโซลการจัดการฮาร์ดแวร์	1
มีอะไรใหม่สำหรับการติดตั้งและการกำหนดคอนฟิก HMC	1
ภารกิจการติดตั้งและคอนฟิกูเรชัน	2
การติดตั้งและการกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่	2
การอัปเดตและอัปเดตรหัส HMC ของคุณ	3
การเพิ่ม HMC ตัวที่สองในการติดตั้งที่มีอยู่	3
การตั้งค่า HMC	4
การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อโลน	4
การติดตั้ง 7310-CR4 HMC ลงในชั้นวาง	6
การทำให้รายการชิ้นส่วนให้เสร็จสิ้น	8
การกำหนดตำแหน่ง	8
การทำเครื่องหมายตำแหน่งโดยไม่ใช่แท้มเพลตประกอบเข้ากับชั้นวาง	9
การติดตั้งรางแบบสไลด์ในชั้นวาง	10
การติดตั้ง HMC บนรางแบบสไลด์	13
การติดตั้งแขนยึดสายเคเบิล	16
การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง	16
ตำแหน่งพอร์ตของ HMC	17
การติดตั้ง 7042-CR5 และ 7042-CR6 ในชั้นวาง	21
การติดตั้ง 7042-CR7 และ 7042-CR8 ในชั้นวาง	27
การติดตั้ง 7042-CR9 HMC ลงในชั้นวาง	36
การติดตั้ง 7063-CR1 ในชั้นวาง	46
สิ่งที่จำเป็นต้องมีสำหรับการติดตั้งระบบ 7063-CR1 บนชั้นวาง	46
การจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ	47
การกำหนดและทำเครื่องหมายตำแหน่งในชั้นวางสำหรับระบบ 7063-CR1	47
การติดตั้ง HMC ลงในชั้นวางโดยใช้รางยึด	48
การยึดรางกับโครงเครื่องและยึดกับชั้นวาง	49
การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ	50
การติดตั้ง HMC ลงในชั้นวางโดยใช้รางสไลด์	52
การติดตั้งรางสไลด์กับระบบและชั้นวาง	52
การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ	55
การวางสายเคเบิล 7063-CR1 HMC ที่ติดตั้งในชั้นวาง	56
การกำหนดค่า 7063-CR1 HMC	57
การติดตั้ง เครื่องมือเสมือน HMC	59
การติดตั้ง เครื่องมือเสมือน HMC บน x86	59
การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ KVM	59
การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ Xen	60
การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ VMware ESXi	61
การติดตั้ง เครื่องมือเสมือน HMC บน PowerVM (โลจิคัลพาร์ติชัน)	61
การใช้ Activation Engine สำหรับ เครื่องมือเสมือน HMC	62
การตั้งค่าโปรไฟล์คอนฟิกูเรชันสำหรับ Activation Engine	63

การติดตั้งหน้าจอและคีย์บอร์ด	71
การทำให้รายการขึ้นส่วนให้เสร็จสิ้น	72
การทำเครื่องหมายตำแหน่งโดยไม่ใช่เพิ่มเฟลตประกอบเข้ากับชั้นวาง	72
การติดตั้งหน้าจอและคีย์บอร์ดเข้ากับชั้นวาง	73
การติดตั้งสวิตช์คอนโซล (ตัวเลือก)	77
การกำหนดค่า HMC โดยใช้อินเทอร์เฟซ HMC Classic หรือ HMC Enhanced	79
การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC	80
การเชื่อมต่อเน็ตเวิร์ก HMC	80
ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC	80
การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home	84
ภาวะเชื่อมต่อแบบง่าย	86
การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต	87
การเลือก อินเทอร์เน็ตโปรโตคอล	87
รายการแอตเตส Internet SSL	87
การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล	88
รายการแอตเตสเซิร์ฟเวอร์ VPN	89
การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต	89
การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์	89
การจัดเตรียมสำหรับการตั้งค่าของ HMC	90
เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC	91
การกำหนดคอนฟิก HMC	100
การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ผ่านทางวิซาร์ดเซตอัพที่แนะนำ	100
เริ่มต้น HMC และปฏิบัติตามขั้นตอนในวิซาร์ดเซตอัพที่แนะนำ	100
ตรวจทานคอนฟิกูเรชันของคุณ	101
การกำหนดคอนฟิก HMC โดยใช้เมนู HMC	101
การเริ่มต้น HMC	103
การเปลี่ยนวันที่และเวลา	104
การตั้งค่าชนิดเน็ตเวิร์ก HMC	104
การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC	111
การกำหนดคอนฟิก entry การเรตเป็นดีฟอลต์เกตเวย์	112
การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส	112
การตั้งค่าคอนฟิกโดเมนซัพพลิ	112
การคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP	113
การกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos	113
การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้	114
การกำหนดคอนฟิก Events Manager for Call Home	120
การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ	121
การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ	122
ขั้นตอน Postconfiguration	122
การสำรองข้อมูล HMC ที่สำคัญ	122
การสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ทั้งหมดไว้บนระบบรีโมต	123
การอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ	124
การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ	125
การขอรับและการใช้การอัปเดตรหัสเครื่องสำหรับ HMC เมื่อมีการเชื่อมต่ออินเทอร์เน็ต	125
ขั้นตอนที่ 1. ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต	125
ขั้นตอนที่ 2. ดาวน์โหลดรหัสเครื่อง HMC ที่มีอยู่	126
ขั้นตอนที่ 3. ดาวน์โหลดรหัสเครื่อง HMC ที่มีอยู่	126

ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC	126
ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	126
การขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP	127
ขั้นตอนที่ 1. ดัชนีรหัสเครื่อง HMC ที่มีอยู่	127
ขั้นตอนที่ 2. ดัชนีรหัสเครื่อง HMC ที่มีอยู่	127
ขั้นตอนที่ 3. ขอรับอัปเดตรหัสเครื่อง HMC	127
ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC	128
ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	128
การอัปเดตซอฟต์แวร์ HMC ของคุณ	128
ขั้นตอนที่ 1. ขอรับอัปเดต	128
ขั้นตอนที่ 2. ดัชนีรหัสเครื่อง HMC ที่มีอยู่	129
ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ	129
ขั้นตอนที่ 4. สำรองข้อมูล HMC	129
ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน	130
ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล	130
ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต	131
ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC	131
ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	132
การอัปเดต HMC จากตำแหน่งรีโมทโดยใช้อีเมลการอัปเดตบนเครือข่าย	132
การกำหนดค่า HMC โดยใช้อินเตอร์เฟซ HMC Enhanced+	133
การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC	133
การเชื่อมต่อเน็ตเวิร์ก HMC	133
ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC	133
การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home	137
การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมท	139
การเลือก อินเทอร์เน็ตโปรโตคอล	140
รายการแอตเตส Internet SSL	140
การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล	141
รายการแอตเตสเซิร์ฟเวอร์ VPN	142
การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมท	142
การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์	142
การจัดเตรียมสำหรับการตั้งค่าของ HMC	143
เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC	144
การกำหนดคอนฟิก HMC	153
การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ทางวิซาร์ดเซตอัปที่แนะนำ	153
เริ่มต้น HMC และปฏิบัติตามขั้นตอนในวิซาร์ดเซตอัปที่แนะนำ	153
ตรวจทานคอนฟิกูเรชันของคุณ	154
การกำหนดคอนฟิก HMC โดยใช้เมนู HMC	154
การเริ่มต้น HMC	156
การเปลี่ยนวันที่และเวลา	157
การตั้งค่าชนิดเน็ตเวิร์ก HMC	157
การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC	165
การกำหนดคอนฟิก entry การเรตเป็นดีฟอลต์เกตเวย์	166
การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส	166
การตั้งค่าคอนฟิกโดเมนซัพพลิ	167
การคอนฟิก HMC เพื่อให้การพิสูจน์ตัวตนระยะไกลด้วย LDAP	167
การกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos	168

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน	169
การกำหนดคอนฟิก Events Manager for Call Home	176
การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ	177
การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ	178
ขั้นตอน Postconfiguration	178
การสำรองข้อมูล HMC ที่สำคัญ	178
การสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ทั้งหมดไว้บนระบบรีโมต	179
การอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ	180
การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ	181
การขอรับและการใช้การอัปเดตรหัสเครื่องสำหรับ HMC เมื่อมีการเชื่อมต่ออินเทอร์เน็ต	181
ขั้นตอนที่ 1. ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต	181
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	182
ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	182
ขั้นตอนที่ 4. ใช้การอัปเดตรหัสเครื่อง HMC	182
ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	183
การขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP	183
ขั้นตอนที่ 1. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	183
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	183
ขั้นตอนที่ 3. ขอรับอัปเดตรหัสเครื่อง HMC	184
ขั้นตอนที่ 4. ใช้การอัปเดตรหัสเครื่อง HMC	184
ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	185
การอัปเดตซอฟต์แวร์ HMC ของคุณ	185
ขั้นตอนที่ 1. ขอรับอัปเดต	185
ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	185
ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ	186
ขั้นตอนที่ 4. สำรองข้อมูล HMC	186
ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกูเรชัน HMC ปัจจุบัน	187
ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล	187
ขั้นตอนที่ 7. บันทึกข้อมูลอัปเดต	188
ขั้นตอนที่ 8. อัปเดตซอฟต์แวร์ HMC	188
ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์	189
การอัปเดต HMC จากตำแหน่งรีโมตโดยใช้อีเมลและการอัปเดตบนเครือข่าย	189
ตำแหน่งพอร์ตของ HMC	190
หมายเหตุ	195
คุณลักษณะความสามารถเข้าถึงได้สำหรับเซิร์ฟเวอร์ IBM Power Systems	196
ขอควรพิจารณานโยบายความเป็นส่วนตัว	198
เครื่องหมายการค้า	198
ประกาศเกี่ยวกับการปล่อยกำลังไฟฟ้า	198
คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A	198
คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส B	203
ข้อตกลงและเงื่อนไข	207

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: เมื่อทำงานเกี่ยวกับระบบหรือแวดล้อมไปด้วยระบบ ให้สังเกตข้อควรระวังต่อไปนี้:

กำลังไฟและกระแสไฟที่มาจากสายไฟ, สายโทรศัพท์, และสายสื่อสารเป็นอันตราย เพื่อหลีกเลี่ยงอันตรายที่เกิดจากไฟฟ้าช็อต:

- ถ้า IBM จัดส่งสายไฟให้เชื่อมต่อกำลังไฟเข้ากับยูนิตนี้ด้วยสายไฟที่ IBM จัดเตรียมให้เท่านั้น ห้ามใช้สายไฟของ IBM สำหรับผลิตภัณฑ์อื่นใด
- ห้ามเปิดหรือให้บริการตัวจ่ายไฟ
- ห้ามเชื่อมต่อ หรือปลดการเชื่อมต่อสายเคเบิลใดๆ หรือทำการติดตั้ง, บำรุงรักษา, หรือตั้งค่าคอนฟิกูเรชันผลิตภัณฑ์นี้ใหม่ ในระหว่างที่มีพายุฟ้าคะนอง
- ผลิตภัณฑ์นี้อาจประกอบด้วยสายไฟหลายเส้น ปลดการเชื่อมต่อสายไฟทั้งหมดเพื่อถอดกำลังไฟที่เป็นอันตรายออกไป
 - สำหรับไฟกระแสสลับ ถอดสายไฟทั้งหมดออกจากแหล่งจ่ายไฟกระแสสลับ
 - สำหรับชั้นวางที่มี DC power distribution panel (PDP) ให้ถอดแหล่งจ่ายไฟกระแสตรงของลูกค้าย เป็น PDP

- เมื่อเชื่อมต่อไฟฟ้กับผลิตภัณฑ์ตรวจสอบให้แน่ใจว่าสายไฟทั้งหมดเชื่อมต่อเหมาะสม
 - สำหรับชั้นวางที่มีไฟกระแสสลับ เชื่อมต่อสายไฟทั้งหมดกับเต้ารับที่ต่อสายไฟและสายดิน อย่างเหมาะสม ตรวจสอบให้แน่ใจว่าเต้ารับไฟฟ้าจ่ายไฟที่มีกำลังเหมาะสมและมีการหมุนเฟสตรงตามข้อกำหนดบนแผ่นโลหะของระบบ
 - สำหรับชั้นวางที่มี DC power distribution panel (PDP) ให้เชื่อมต่อแหล่งจ่ายไฟกระแสตรงของลูกค้ เป็น PDP ตรวจสอบให้แน่ใจว่าใช้ขั้วเหมาะสมเมื่อต่อเชื่อมต่อสายไฟกระแสตรงและส่งกลับไฟกระแสตรง
- เชื่อมต่ออุปกรณ์ใดๆ ที่จะพ่วงต่อกับผลิตภัณฑ์นี้กับเต้ารับไฟฟ้าที่เดินสายไฟอย่างเหมาะสม
- หากเป็นไปได้ ควรใช้มือเพียงข้างเดียวในการเชื่อมต่อ หรือปลดการเชื่อมต่อสายเคเบิลสัญญาณ
- ห้ามเปิดอุปกรณ์ใดๆ เมื่อพบว่าม้ไฟ, น้ำ, หรือโครงสร้างได้รับความเสียหาย
- อย่าพยายามเปิดเครื่อง จนกว่าแก้ไขสภาพที่ไม่ปลอดภัย ทั้งหมดแล้ว
- สมมติว่ามีอันตรายจากความปลอดภัยด้านอิเล็กทรอนิกส์ทำการตรวจสอบ ความต่อเนื่อง การต่อสายดิน และกำลังไฟทั้งหมดที่ระบุระหว่างโปรซีเดอร์ การติดตั้งระบบย่อย เพื่อให้แน่ใจว่าเครื่องตรงกับข้อกำหนดด้านความปลอดภัย
- อย่าตรวจสอบต่อไปถ้ามีสภาพความไม่ปลอดภัยใดๆ
- ก่อนคุณเปิดฝาอุปกรณ์ ยกเว้นว่ามีคำแนะนำเป็นอย่างอื่นในโปรซีเดอร์ การติดตั้งและการกำหนดคอนฟิก: ให้ถอดสายไฟกระแสตรงที่เสียบอยู่ ปิดตัวตัดวงจร ที่มีอยู่ใน rack power distribution panel (PDP) และถอดระบบ สื่อสารทางไกล เครือข่าย และโมเด็มที่มี

อันตราย:

- เชื่อมต่อและปลดการเชื่อมต่อสายเคเบิลตามที่ได้อธิบายไว้ในขั้นตอนต่อไปนี เมื่อติดตั้ง, เคลื่อนย้าย, หรือเปิดฝากรอบผลิตภัณฑ์หรืออุปกรณ์ที่ต่อพ่วง
- หากต้องการปลดการเชื่อมต่อ:
1. ปิดอุปกรณ์ทุกอย่าง (เว้นแต่มีคำแนะนำไว้เป็นอย่างอื่น)
 2. สำหรับไฟกระแสสลับ ถอดสายไฟออกจากเต้ารับ
 3. สำหรับชั้นวางที่มี DC power distribution panel (PDP) ปิดตัวตัดวงจรที่อยู่ใน PDP และถอดสายไฟออกจากแหล่งจ่ายไฟกระแสตรงของลูกค้
 4. ดึงสายเคเบิลส่งสัญญาณออกจากตัวเชื่อมต่อ
 5. ถอดสายเคเบิลทั้งหมดออกจากอุปกรณ์

หากต้องการเชื่อมต่อ:

1. ปิดอุปกรณ์ทุกอย่าง (เว้นแต่มีคำแนะนำไว้เป็นอย่างอื่น)
2. พ่วงต่อสายเคเบิลทั้งหมดเข้ากับอุปกรณ์
3. พ่วงต่อสายเคเบิลส่งสัญญาณเข้ากับตัวเชื่อมต่อ
4. สำหรับไฟกระแสสลับ เสียบสายไฟกับเต้ารับ
5. สำหรับชั้นวางที่มี DC power distribution panel (PDP) นำสายไฟออกจากแหล่งจ่ายไฟ กระแสตรงของลูกค้ และเปิดตัวตัดวงจรที่อยู่ใน PDP
6. เปิดอุปกรณ์

อาจมีขอบ มุม และข้อต่อที่แหลมคมอยู่ภายในและโดยรอบ ระบบ ใช้ความระมัดระวังเมื่อจัดการกับเครื่องมือเพื่อหลีกเลี่ยงการบาดเจ็บ การถลอก และการหนีบ (D005)

(R001 ส่วน 1 จากทั้งหมด 2):

อันตราย: ขณะที่ทำงานอยู่กับชั้นวางระบบ IT หรือในบริเวณที่มีชั้นวางระบบ IT ของคุณ ให้สังเกตข้อควรระวังต่อไปนี้:

- อุปกรณ์ที่มีน้ำหนักมาก—อาจก่อให้เกิดการบาดเจ็บต่อร่างกายหรือความเสียหายต่ออุปกรณ์ได้ หากมีการจัดการที่ไม่ถูกต้อง

- ลดการวางระดับเสริมบนตู้ชั้นวางให้อยู่ต่ำเสมอ
- ควรติดตั้งแท่นยึดสเตบิลไลเซอร์บนตู้ชั้นวางเสมอ
- ติดตั้งอุปกรณ์ที่มีน้ำหนักมากที่สุดไว้ที่ด้านล่างสุดของตู้ชั้นวาง เพื่อหลีกเลี่ยงสภาวะการจตุรัสเครื่องจักรที่ไม่สม่ำเสมอ ควรติดตั้งเซิร์ฟเวอร์และอุปกรณ์เสริมโดยเริ่มจากด้านล่างสุดของตู้ชั้นวางเสมอ
- ไม่ควรใช้อุปกรณ์ที่ประกอบเข้ากับชั้นวางเป็นชั้นวางหรือเป็นพื้นที่ใช้งาน ห้ามวางอ็อบเจกต์ต่างๆ ที่ด้านบนของอุปกรณ์ที่ประกอบเข้ากับชั้นวาง นอกจากนั้น อย่าพึ่งอุปกรณ์ที่ประกอบบนชั้นวาง และอย่า ใช้อุปกรณ์นั้นเพื่อทำให้ตำแหน่งร่างกายของคุณยืนได้มั่นคง (ตัวอย่างเช่น เมื่อทำงานจากบนได)



- ตู้ชั้นวางแต่ละตู้ต้องมีสายไฟมากกว่าหนึ่งสาย
 - สำหรับชั้นวางที่มีไฟกระแสสลับ ตรวจสอบให้แน่ใจว่าได้ดึงสายไฟทั้งหมดในตู้ชั้นวางออกแล้ว เมื่อได้รับคำสั่งให้ปลดการเชื่อมต่อกำลังไฟในระหว่างให้บริการ
 - สำหรับชั้นวางที่มี DC power distribution panel (PDP) ปิดตัวตัดวงจรที่ควบคุม กระแสไฟไปยังหน่วยอุปกรณ์ระบบหรือถอดแหล่งจ่ายไฟกระแสตรงของลูกค้า เมื่อได้รับคำสั่งให้ถอดสายไฟระหว่างการให้บริการ
- เชื่อมต่ออุปกรณ์ทั้งหมดที่ติดตั้งในตู้ชั้นวางกับอุปกรณ์ไฟฟ้าที่ติดตั้งในตู้ชั้นวางเดียวกัน ห้ามเสียบปลั๊กสายไฟจากอุปกรณ์ที่ติดตั้งในตู้ชั้นวางตู้หนึ่งกับอุปกรณ์ไฟฟ้าที่ติดตั้งในตู้ชั้นวางอื่น
- เต้ารับไฟฟ้าที่ต่อสายไฟไม่ถูกต้อง สามารถทำให้เกิดอันตรายจากกำลังไฟต่อระบบ หรืออุปกรณ์ที่พ่วงต่อกับระบบที่เป็นโลหะ ลูกค้านี้หน้าที่จะรับผิดชอบในการตรวจสอบให้แน่ใจว่าเต้ารับไฟฟ้ามีการเดินสายไฟและสายดินอย่างถูกต้อง เพื่อป้องกันไฟฟ้าช็อต

(R001 ส่วน 2 จากทั้งหมด 2):

ข้อควรระวัง:

- ห้ามติดตั้งยูนิตในชั้นวางซึ่งมีอุณหภูมิภายในสูงกว่าอุณหภูมิที่ผู้ผลิตแนะนำไว้สำหรับอุปกรณ์ที่ประกอบเข้ากับชั้นวาง
- ห้ามติดตั้งยูนิตในชั้นวางซึ่งมีการไหลเวียนอากาศที่ไม่เหมาะสม ตรวจสอบให้แน่ใจว่า การไหลเวียนอากาศตามช่องสำหรับใช้ระบายอากาศที่ด้านข้าง, ด้านหน้า หรือด้านหลังของยูนิตไม่ได้ถูกกีดขวางหรือลดลง
- ในการเชื่อมต่ออุปกรณ์เข้ากับวงจรจ่ายไฟฟ้า ควรพิจารณาให้ดีกว่าการใช้งานวงจรจนเกินพิกัดจะไม่ทำให้ความสามารถในการป้องกันสายจ่ายไฟหรือการป้องกันกระแสไฟเกินด้อยลง หากต้องการเตรียมการเชื่อมต่อสายไฟกับชั้นวางที่ถูกต้อง โปรดอ้างอิงถึงแถบป้ายการกำหนดค่าที่อยู่บนอุปกรณ์ในชั้นวางเพื่อกำหนดความต้องการกำลังไฟทั้งหมดของวงจรจ่ายไฟฟ้า
- (สำหรับลิ้นชักแบบเลื่อน) ห้ามดึงหรือติดตั้งลิ้นชัก หรือคุณลักษณะพิเศษ หากแท่นยึดสเตบิลไลเซอร์ของชั้นวางไม่ได้ยึดติดอยู่กับชั้นวาง ห้ามดึงลิ้นชักออกมากกว่าหนึ่งลิ้นชักในหนึ่งครั้ง ชั้นวางอาจไม่มั่นคง ถ้าคุณดึงลิ้นชักออกมากกว่าหนึ่งลิ้นชักในหนึ่งครั้ง



- (สำหรับลิ้นชักแบบยึดตายตัว) ลิ้นชักนี้เป็นลิ้นชักแบบยึดตายตัว และห้ามไม่ให้เคลื่อนย้ายเพื่อรับบริการ ยกเว้นได้รับการระบุโดยผู้ผลิต ความพยายามในการเคลื่อนย้ายลิ้นชักบางส่วน หรือทั้งหมดออกจากชั้นวางอาจเป็นสาเหตุทำให้ชั้นวางไม่มั่นคง หรือเป็นสาเหตุทำให้ลิ้นชักตกลงมาจากชั้นวาง

ข้อควรระวัง:

การถอดส่วนประกอบออกจากตำแหน่งด้านบนในตู้ชั้นวาง จะช่วยให้ชั้นวางมีความมั่นคงระหว่างที่มีการย้ายตำแหน่งใหม่ โปรดปฏิบัติตามคำแนะนำทั่วไปเหล่านี้ในทุกครั้งที่คุณเปลี่ยนตำแหน่ง ตู้ชั้นวางภายในห้องหรืออาคาร

- ลดน้ำหนักของตู้ชั้นวางโดยการถอดอุปกรณ์โดยเริ่มต้นจากด้านบนสุดของตู้ชั้นวาง หากเป็นไปได้ ให้จัดตู้ชั้นวางคืนสภาพตามคอนฟิกรูเรชันเดิมตั้งแต่ที่คุณได้รับมา ถ้าไม่ทราบคอนฟิกรูเรชันดังกล่าว คุณต้องปฏิบัติตามข้อควรระวังดังต่อไปนี้:
 - ถอดอุปกรณ์ทั้งหมดในตำแหน่ง 32U (compliance ID RACK-001 or 22U (compliance ID RR001) และด้านบนออก
 - ตรวจสอบให้แน่ใจว่าได้ติดตั้งอุปกรณ์ที่หนักสุดไว้ที่ด้านล่างของตู้ชั้นวาง
 - ตรวจสอบให้แน่ใจว่า มีน้อยมากหรือไม่มีระดับ U ที่วางระหว่างอุปกรณ์ต่างๆ ซึ่งติดตั้งในตู้ชั้นวางต่ำกว่าระดับ 32U (compliance ID RACK-001 หรือ 22U (compliance ID RR001) ยกเว้นว่าคอนฟิกรูเรชันที่ได้รับ อนุญาตเช่นนั้นเป็นพิเศษ
- ถ้าตู้ชั้นวางที่คุณจัดตำแหน่งใหม่คือส่วนของห้องชุดของตู้ชั้นวาง ให้ดึงตู้ชั้นวางออกจากห้องชุด
- ถ้าตู้ชั้นวางที่คุณกำลังเปลี่ยนตำแหน่งมีการจัดส่งมาพร้อมกับแขนค้ำซึ่ง ถอดออกได้ ต้องติดตั้งแขนค้ำนั้นอีกครั้ง ก่อนจะเปลี่ยนตำแหน่งตู้
- ตรวจสอบเรตต์ที่คุณวางแผนที่จะกำจัดอันตรายที่อาจเกิดขึ้นได้
- ตรวจสอบว่าเรตต์ที่คุณเลือกสามารถรองรับน้ำหนักของตู้ชั้นวางที่โหลดได้ อ้างอิงถึงเอกสารที่มาพร้อมกับตู้ชั้นวางของคุณเพื่อทราบข้อมูลเกี่ยวกับน้ำหนักของตู้ชั้นวางที่โหลด
- ตรวจสอบว่าประตูเปิดทั้งหมดมีขนาดอย่างน้อย 760 x 230 มม. (30 x 80 นิ้ว).
- ตรวจสอบให้แน่ใจว่าได้เก็บอุปกรณ์, ชั้น, ลินชัก, ประตู, และสายเคเบิลทั้งหมดอยู่ในสภาพที่เรียบร้อย
- ตรวจสอบให้แน่ใจว่า การวางระดับเสริมทั้งสี่ระดับถูกยกไว้ที่ตำแหน่งสูงสุด
- ตรวจสอบให้แน่ใจว่า ไม่มีแท่นยึดสเทปไลเซอร์ที่ติดตั้งบนตู้ชั้นวางในขณะที่ทำการเคลื่อนย้าย
- ห้ามใช้ทางลาดที่เอียงเกิน 10 องศา
- เมื่อตู้ชั้นวางอยู่ในตำแหน่งใหม่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้โดยสมบูรณ์:
 - ลดการวางระดับเสริมทั้งสี่ระดับให้ต่ำลง
 - ติดตั้งแท่นยึดสเทปไลเซอร์บนตู้ชั้นวาง
 - ถ้าคุณถอดอุปกรณ์ใดๆ ออกจากตู้ชั้นวาง ให้ประกอบเข้าในตู้ชั้นวางใหม่จากตำแหน่งล่างสุด ไปยังตำแหน่งบนสุด
- หากจำเป็นต้องย้ายตำแหน่งเป็นระยะทางไกลๆ ให้จัดตู้ชั้นวางคืนสภาพตามคอนฟิกรูเรชันเดิมตั้งแต่ที่คุณได้รับมา บรรจุตู้ชั้นวางด้วยบรรจุภัณฑ์วัสดุเดิม หรือเทียบเท่า ลดการวางระดับเสริมให้ต่ำลง เพื่อยกฐานล้อให้ออกนอกพลาเลต และเลื่อนตู้ชั้นวางไปยังพลาเลต

(R002)

(L001)



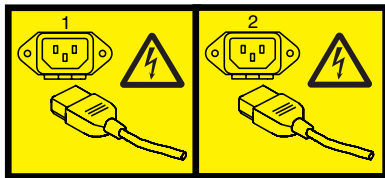
อันตราย: แรงดันไฟ กระแสไฟ หรือระดับพลังงานที่เป็นอันตรายจะแสดงอยู่ภายในส่วนประกอบต่างๆ ที่มีป้ายนี้ติดอยู่ ห้ามเปิดฝาครอบ หรือแผงกันที่ติดป้ายนี้อยู่ (L001)

(L002)

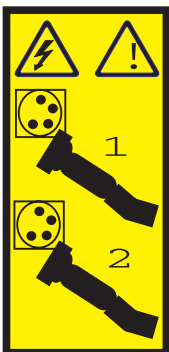


อันตราย: ไม่ควรใช้อุปกรณ์ที่ประกอบเข้ากับช่องว่างเป็นช่องว่างหรือเป็นพื้นที่ใช้งาน (L002)

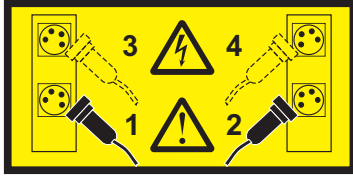
(L003)



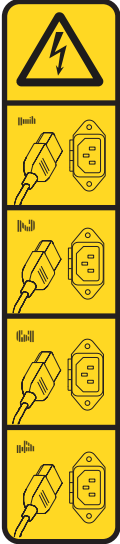
or



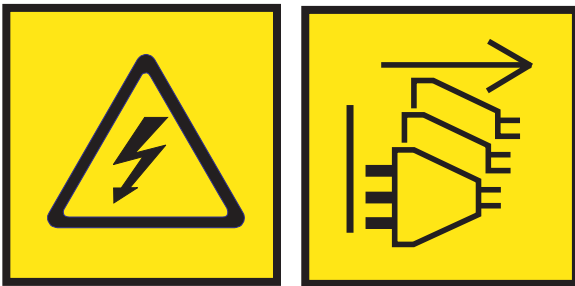
or



or



or



อันตราย: สายไฟหลายเส้น ผลิตภัณฑ์อาจมากับสายไฟกระแสดตรง หลายเส้น หรือสายไฟกระแสสลับหลายเส้น ปลดการเชื่อมต่อสายไฟทั้งหมดเพื่อถอดสายไฟ และสายเคเบิลที่เป็นอันตรายออกไป (L003)

(L007)



ข้อควรระวัง: พื้นผิวบริเวณใกล้เคียงร้อน (L007)

(L008)



ข้อควรระวัง: ชิ้นส่วนที่เคลื่อนไหวที่เป็นอันตรายในบริเวณใกล้เคียง (L008)

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

ข้อควรระวัง:

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

- ห้ามถอดฝาครอบออก การถอดฝาครอบของผลิตภัณฑ์เลเซอร์อาจเป็นผลทำให้เกิดการสัมผัสกับการแผ่รังสีเลเซอร์ที่เป็นอันตราย ไม่มีชิ้นส่วนที่สามารถถอดเปลี่ยนได้ภายในอุปกรณ์
- การใช้ตัวควบคุม หรือตัวปรับเปลี่ยน หรือใช้ประสิทธิภาพของขั้นตอนที่แตกต่างไปจากที่ระบุไว้ในที่นี้อาจเป็นสาเหตุทำให้เกิดการสัมผัสกับการแผ่รังสีที่เป็นอันตราย

(C026)

ข้อควรระวัง:

สภาพแวดล้อมการประมวลผลข้อมูลสามารถประกอบด้วยอุปกรณ์ซึ่งส่งผ่านบนระบบ ที่เชื่อมต่อกับโมดูลเลเซอร์ซึ่งปฏิบัติงานด้วยกำลังไฟมากกว่าระดับกำลังไฟของ Class 1 ด้วยเหตุนี้จึงห้ามมองที่ส่วนปลายของเส้นใยแก้วนำแสงหรือเตารับที่เปิดอยู่ แม้ว่าการส่องไฟเข้าไปใน ปลายด้านหนึ่ง และการมองเข้าไปในปลายอีกด้านหนึ่งของเส้นใยแก้วนำแสงที่ไม่ได้เชื่อมต่อเพื่อตรวจสอบความต่อเนื่องของ เส้นใยแก้วนำแสงอาจไม่ทำร้ายดวงตา แต่โพรมิเตอร์นี้อาจเป็นอันตรายได้ ดังนั้น จึงไม่แนะนำ การตรวจสอบความต่อเนื่องของเส้นใยแก้วนำแสงโดยการส่องไฟเข้าไปในปลายด้านหนึ่ง และการมองที่ ปลายอีกด้านหนึ่ง เมื่อต้องการตรวจสอบความต่อเนื่องของสายเส้นใยแก้วนำแสง ให้ใช้แหล่งไฟออปติคัลและมิเตอร์วัดพลังงาน (C027)

ข้อควรระวัง:

ผลิตภัณฑ์นี้ประกอบด้วยเลเซอร์ Class 1M ห้ามมองที่อุปกรณ์ออปติคัลโดยตรง (C028)

ข้อควรระวัง:

ผลิตภัณฑ์เลเซอร์บางชนิดประกอบด้วยเลเซอร์ไดโอด Class 3A หรือ Class 3B ผังอยู่ บนที่ข้อมูลดังต่อไปนี้: การแผ่รังสีเลเซอร์เมื่อเปิด ห้ามจ้องมองลำแสง, ห้ามใช้อุปกรณ์ออปติคัลในการมองโดยตรง, และหลีกเลี่ยงการสัมผัสกับลำแสงโดยตรง (C030)

ข้อควรระวัง:

แบตเตอรี่ประกอบด้วยลิเธียม หากต้องการหลีกเลี่ยงการระเบิดที่อาจเกิดขึ้นได้ ห้ามเผา หรือชาร์จแบตเตอรี่

ห้าม:

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

ให้แลกเปลี่ยนกับชิ้นส่วนที่ IBM เท่านั้น นำไปรีไซเคิล หรือทิ้งแบตเตอรี่ตามกฎหมายข้อบังคับท้องถิ่นของคุณในประเทศสหรัฐอเมริกา IBM มีขั้นตอนสำหรับการเก็บรวบรวมแบตเตอรี่นี้ สำหรับข้อมูลเพิ่มเติม โปรดโทรศัพท์ติดต่อที่ 1-800-426-4333 คุณต้องทราบหมายเลขชิ้นส่วนของแบตเตอรี่ขณะที่คุณโทรศัพท์ติดต่อ (C003)

ข้อควรระวัง:

เกี่ยวกับ ที่จัดเตรียมโดย IBM เครื่องมือยกของผู้จัดจำหน่าย:

- การใช้งานเครื่องมือยกควรทำโดยบุคลากรที่ได้รับอนุญาตเท่านั้น
- เครื่องมือยกใช้สำหรับการช่วยเหลือ ยก ติดตั้ง ถอดยูนิต์ (โหนด) เข้าในการยก ชั้่นวาง ไม่ได้ใช้สำหรับการขนส่ง ปริมาณมากบนทางลาด และไม่ได้ใช้แทน เครื่องมือที่กำหนด เช่น รถลากพาเลท, walkies, รถยก และแนวปฏิบัติในการย้ายตำแหน่งที่เกี่ยวข้อง เมื่อ ไม่สามารถปฏิบัติได้ ต้องใช้บุคคลที่ผ่านการฝึกอบรมมาเป็นพิเศษหรือเซอร์วิส (เช่น ผู้ควบคุมการยก หรือบริษัทรับจ้างย้ายของ)
- อ่าน และทำความเข้าใจกับเนื้อหาของผู้ใช้งานเครื่องมือยกโดยสมบูรณ์ก่อนจะใช้ การไม่อ่าน ไม่ทำความเข้าใจ ไม่เชื่อฟังกฎด้านความปลอดภัย และไม่ปฏิบัติตามคำแนะนำอาจส่งผล ให้ทรัพย์สินเสียหาย และ/หรือบาดเจ็บ หากมีคำถาม โปรดติดต่อเซอร์วิสและฝ่ายสนับสนุนของผู้จัดจำหน่าย เอกสารคู่มือต้องเก็บไว้กับเครื่องในพื้นที่ช่องเก็บ ซึ่งจัดเตรียมไว้ คู่มือฉบับแก้ไขล่าสุด มีอยู่บนเว็บไซต์ของผู้จัดจำหน่าย
- ทดสอบฟังก์ชันเบรกขาข่ายก่อนการใช้งานแต่ละครั้ง อย่าย้ายหรือเลื่อน เครื่องมือยกแรงเกินไปขณะใช้เบรกขาข่าย
- อย่าย้ายเครื่องมือยกขณะยกแพลตฟอร์มขึ้น ยกเว้นสำหรับการจัดตำแหน่งเล็กน้อย
- อย่าบรรทุกเกินความจุน้ำหนักบรรทุกที่กำหนด โปรดดูแผนภูมิความจุ้่นน้ำหนักบรรทุกเกี่ยวกับน้ำหนักบรรทุกสูงสุดที่ ศูนย์กลาง และที่ขอบของแพลตฟอร์มซึ่งขยาย
- เพิ่มน้ำหนักบรรทุกเฉพาะถ้าจัดตำแหน่งศูนย์กลางบนแพลตฟอร์มอย่างถูกต้อง อย่าวางของมากกว่า 200 ปอนด์ (91 กก.) บน ขอบของชั้นแพลตฟอร์มที่เลื่อนได้ และพิจารณาถึงแรงโน้มถ่วง (CoG) ของน้ำหนักบรรทุกด้วย
- อย่าติดตั้งอุปกรณ์เสริมตัวยกเอียงแพลตฟอร์มในลักษณะทำมุม ให้ยึดตัวยกเอียงแพลตฟอร์ม เข้ากับชั้นหลักให้ แน่นในทั้งหมดสี่ตำแหน่ง (4x) ด้วยฮาร์ดแวร์ที่จัดเตรียมไว้เท่านั้น ก่อนจะใช้ อ็อบเจกต์ ที่บรรทุกได้รับการออกแบบ มาเพื่อเลื่อนเข้า/ออกแพลตฟอร์มอย่างราบรื่นโดยไม่ต้องใช้แรง ดังนั้น ระวังอย่า ผลักหรือเอียง ควรรักษาตัวยกเอียง ให้อยู่ในแนวราบตลอดเวลา ยกเว้นสำหรับการปรับเล็กน้อยครั้งสุดท้ายเมื่อ จำเป็น
- อย่ายืนใต้น้ำหนักบรรทุกที่ยื่นออกมา
- อย่าใช้บนพื้นผิวที่ไม่ราบ เอียงขึ้น หรือเอียงลง (ทางลาดมาก)
- อย่าซ่อนทับน้ำหนักบรรทุก
- อย่าใช้งานขณะรับประทานยาหรือแอลกอฮอล์
- อย่าพาดบันไดกับเครื่องมือยก
- อันตรายจากการหนีบ อย่าผลักหรือดึงน้ำหนักบรรทุกด้วยแพลตฟอร์มที่ยกขึ้น
- อย่าใช้เป็นแพลตฟอร์มยกส่วนบุคคล หรือชั้นบันได ห้ามนั่งคร่อม
- อย่ายืนบนส่วนใดๆ ของเครื่องมือยก ไม่ใช่ชั้นบันได
- อย่าปีนบนเสา
- อย่าใช้เครื่องมือยกที่เสียหายหรือทำงานผิดปกติ
- จุดที่ขรุขระและไม่เรียบเป็นอันตรายต่อแพลตฟอร์มด้านล่าง บรรทุกสิ่งของด้านล่างในพื้นที่ซึ่งไม่มีบุคคลและ สิ่งกีดขวางเท่านั้น มือและเท้าไม่ควรมีส่วนกีดขวางระหว่างการใช้งาน
- ไม่ใช่รถยก ห้ามยกหรือย้ายเครื่องมือยกเปล่าด้วยรถลากพาเลท, jack หรือ รถยก
- เสาขยายได้มากกว่าแพลตฟอร์ม ระวังความสูงของเพดาน ถาดสายเคเบิล หัวฉีดดับเพลิง ดวงไฟ และอ็อบเจกต์ เหนือศีรษะอื่น
- อย่าปล่อยเครื่องมือยกที่มีน้ำหนักบรรทุกยกขึ้นโดยไม่มีการควบคุม
- ผ่าดู และอย่าให้มือ นิ้ว และเสื้อผ้ามี่กีดขวางเมื่อเครื่องมือเคลื่อนไหว
- ปรับเครื่องยกด้วยมือเท่านั้น ถ้าไม่สามารถหมุนที่จับเครื่องยกได้ง่ายด้วยมือเดียว แสดงว่า อาจบรรทุกเกินน้ำหนัก อย่าหมุนเครื่องยกต่อไปจนผ่านระดับบนสุดหรือล่างสุดของแพลตฟอร์ม การคลายออกมากเกินไปจะถอดที่จับ และ ทำให้สายเคเบิลเสียหาย จับที่จับไว้เสมอเมื่อลดระดับ หรือคลายออก ตรวจสอบให้แน่ใจเสมอว่า เครื่องยกมีน้ำหนัก

บรรทุกอยู่ก่อนจะปล่อยที่จับเครื่องยก

- อุบัติเหตุเกี่ยวกับเครื่องยกอาจทำให้บาดเจ็บร้ายแรง ไม่เหมาะสำหรับสถานที่ที่มีผู้คนพลุกพล่าน ส่งเสียงสัญญาณให้ได้ยินขณะเครื่องมือกำลังยก ตรวจสอบให้แน่ใจว่าเครื่องยกถูกล็อคไว้ในตำแหน่งก่อน จะปล่อยที่จับ อ่านหน้าคำแนะนำก่อนจะใช้เครื่องยกนี้ ห้ามปล่อยให้เครื่องยกคลายออก อย่างอิสระ ล้อที่หมุนอย่างอิสระจะทำให้สายเคเบิลพันรอบตรัมเครื่องยกอย่างไม่เท่าเทียมกัน ทำให้สายเคเบิลเสียหาย และอาจเป็นสาเหตุให้เกิดการบาดเจ็บร้ายแรง (C048)

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

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

อุปกรณ์เหมาะกับการติดตั้งในสถานที่ต่อไปนี้:

- สถานที่ที่อำนวยความสะดวกด้านเครือข่ายโทรคมนาคม
- ตำแหน่งที่สามารถใช้ NEC (National Electrical Code) ได้

พอร์ตภายในอาคารของอุปกรณ์นี้เหมาะกับการเชื่อมต่อภายในอาคาร หรือการวางสายไฟหรือสายเคเบิลที่มีฉนวนหุ้มเท่านั้น พอร์ตภายในอาคารของอุปกรณ์นี้ **ต้องไม่** เชื่อมต่อแบบโลหะกับอินเทอร์เฟซที่เชื่อมต่อกับ OSP (outside plant) หรือสายไฟของอุปกรณ์เอง อินเทอร์เฟซเหล่านี้ได้รับการออกแบบมาเพื่อใช้เป็นอินเทอร์เฟซภายในอาคารเท่านั้น (พอร์ตชนิด 2 หรือชนิด 4 ตามที่อธิบายใน GR-1089-CORE) และต้องมีการแยก จากสายเคเบิล OSP แบบเปลือย การเพิ่มตัวปกป้องหลักไม่ใช่การปกป้องที่เพียงพอสำหรับการเชื่อมต่อ อินเทอร์เฟซเหล่านี้ในแบบโลหะเข้ากับสาย OSP

หมายเหตุ: สายเคเบิลอีเทอร์เน็ตทั้งหมด ต้องมีฉนวนหุ้มและต่อสายดินที่ปลายทั้งสองด้าน

ระบบไฟฟ้ากระแสสลับไม่จำเป็นต้องใช้อุปกรณ์ป้องกันไฟกระชากหรือ surge protection device (SPD) ภายนอก

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

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

การติดตั้งและการตั้งค่าคอนฟิก คอนโซลการจัดการฮาร์ดแวร์

อธิบายถึงวิธีการติดตั้งฮาร์ดแวร์ HMC เชื่อมต่อ คอนโซลการจัดการฮาร์ดแวร์ (HMC) เชื่อมต่อ HMC เข้ากับระบบที่ถูกจัดการของคุณ และกำหนดคอนฟิก HMC สำหรับใช้งาน คุณสามารถดำเนินการกับงานเหล่านี้ได้ด้วยตนเอง หรือติดต่อผู้ให้บริการเพื่อดำเนินการกับงานเหล่านี้ให้คุณ คุณอาจถูกเรียกเก็บค่าธรรมเนียมจากผู้ให้บริการสำหรับการให้บริการนี้

หมายเหตุ: การจำลองเสมือนไม่สนับสนุนบนเซิร์ฟเวอร์ IBM Power® System S824L (8247-42L)

มีอะไรใหม่สำหรับการติดตั้งและการกำหนดคอนฟิก HMC

อ่านข้อมูลที่มีการเปลี่ยนแปลงหรือข้อมูลใหม่ที่เกี่ยวข้องกับหัวข้อการติดตั้งและกำหนดคอนฟิก HMC เมื่อมีการอัปเดตการรวบรวมหัวข้อก่อนหน้านี้

เดือนสิงหาคม 2017

- อินเทอร์เฟซ HMC Classic ไม่สนับสนุนแล้วบน Hardware Management Console (HMC) เวอร์ชัน 8.7.0 หรือใหม่กว่า ฟังก์ชันที่พร้อมใช้งานกับอินเทอร์เฟซ HMC Classic ก่อนหน้านี้พร้อมใช้งานกับ อินเทอร์เฟซ HMC Enhanced+ แล้วในตอนนี้อยู่
- เพิ่มหัวข้อต่อไปนี้:
 - “การติดตั้ง 7063-CR1 ในชั้นวาง” ในหน้า 46
 - “กำหนดค่าการเชื่อมต่อ BMC” ในหน้า 163
- เพิ่มหัวข้อ “การติดตั้ง 7063-CR1 ในชั้นวาง” ในหน้า 46

ตุลาคม 2016

- อัปเดตหัวข้อ “ตำแหน่งพอร์ตของ HMC” ในหน้า 17

พฤษภาคม 2016

- เพิ่มหัวข้อ “การติดตั้ง 7042-CR9 HMC ลงในชั้นวาง” ในหน้า 36

ตุลาคม 2015

- เพิ่มหัวข้อ “การติดตั้ง เครื่องมือเสมือน HMC” ในหน้า 59
- อัปเดตหัวข้อต่อไปนี้:
 - “รายการแอตเตส Internet SSL” ในหน้า 87
 - “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90

มิถุนายน 2015

- โพรซีเจอร์และฟังก์ชันของอินเทอร์เฟซ HMC Enhanced + Tech Preview (Pre-GA) ซึ่งเป็นอ็อปชันที่ถูกจัดเตรียมไว้พร้อมกับ HMC เวอร์ชัน 8.2.0 เหมือนกับอินเทอร์เฟซ HMC Enhanced+ ที่จัดเตรียมไว้พร้อมกับ HMC เวอร์ชัน 8.3.0 เฉพาะ HMC Enhanced+ เท่านั้นที่อ้างถึงในเอกสารคู่มือนี้ แต่เนื้อหานี้ยังใช้กับอินเทอร์เฟซ HMC Enhanced + Tech Preview (Pre-GA) ได้

- โพรซีเจอร์และฟังก์ชันของอินเทอร์เฟซ HMC Enhanced ซึ่งเป็นอ็อปชันที่ถูกจัดเตรียมไว้พร้อมกับ HMC เวอร์ชัน 8.2.0 เป็นส่วนหนึ่งของอินเทอร์เฟซ HMC Enhanced+ ที่ถูกจัดเตรียมไว้พร้อมกับ HMC เวอร์ชัน 8.3.0
- เพิ่มส่วน “การกำหนดค่า HMC โดยใช้อินเทอร์เฟซ HMC Enhanced+” ในหน้า 133
- อัปเดตหัวข้อ “การกำหนดคอนฟิก Events Manager for Call Home” ในหน้า 120

ตุลาคม 2014

- เพิ่มหัวข้อต่อไปนี้:
 - “การติดตั้ง 7042-CR7 และ 7042-CR8 ในชั้นวาง” ในหน้า 27
 - “การกำหนดคอนฟิก Events Manager for Call Home” ในหน้า 120
- อัปเดตหัวข้อ “การเริ่มต้น HMC” ในหน้า 103

มิถุนายน 2014

- เพิ่มข้อมูลเซิร์ฟเวอร์ IBM Power Systems ที่มี ตัวประมวลผล POWER8

ภารกิจการติดตั้งและคอนฟิกูเรชัน

เรียนรู้เกี่ยวกับภารกิจที่เชื่อมโยงกับภารกิจการติดตั้งและ คอนฟิกูเรชัน HMC ต่างๆ

ส่วนนี้อธิบายงานที่คุณต้องดำเนินการ เมื่อคุณติดตั้ง และกำหนดคอนฟิก HMC ของคุณที่ระดับสูงสุด โดยมีวิธีการที่แตกต่างกันมากมายสำหรับการติดตั้งและกำหนดคอนฟิก HMC ของคุณ ค้นหาสถานการณ์ที่เหมาะสมที่สุด กับภารกิจซึ่งคุณต้องการทำ

หมายเหตุ: หากคุณกำลังจัดการกับเซิร์ฟเวอร์ POWER8® แบบอิงตัวประมวลผล HMC ต้องเป็นเวอร์ชัน 8.1.0 หรือสูง สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดเวอร์ชันและรีลีสของรหัสเครื่อง HMC ของคุณ” ในหน้า 125

การติดตั้งและการกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อติดตั้ง และกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

ตารางที่ 1. งานที่คุณต้องดำเนินการเมื่อติดตั้งและกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. รวบรวมข้อมูลและป้อนข้อมูล ในเวิร์กชีตคอนฟิกูเรชันการติดตั้งล่วงหน้า	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91 “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
2. แกะกล่องบรรจุฮาร์ดแวร์	
3. ต่อสายเคเบิลฮาร์ดแวร์ HMC	“การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อโลน” ในหน้า 4 “การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง” ในหน้า 16
4. เปิด HMC โดยกดปุ่มเปิด/ปิด	
5. ล็อกอินและเรียกทำงานเว็บแอปพลิเคชัน HMC	

ตารางที่ 1. งานที่คุณต้องดำเนินการเมื่อติดตั้งและกำหนดคอนฟิก HMC ใหม่ที่มีเซิร์ฟเวอร์ใหม่ (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
6. เข้าใช้ชาร์ตตั้งค่าที่แนะนำ หรือใช้เมนู HMC เพื่อกำหนดคอนฟิก HMC	“การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ผ่านทางชาร์ตตั้งค่าที่แนะนำ” ในหน้า 100 “การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 101
7. ต่อเซิร์ฟเวอร์เข้ากับ HMC	

การอัปเดตและอัปเดตรหัส HMC ของคุณ

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อคุณอัปเดตและอัปเดตรหัส HMC ของคุณ

หากคุณมี HMC ที่มีอยู่และต้องการอัปเดตหรืออัปเดตรหัส HMC ของคุณ คุณต้องทำงานระดับสูงต่อไปนี้ให้เสร็จสิ้น:

ตารางที่ 2. งานที่คุณต้องดำเนินการเมื่ออัปเดตหรืออัปเดตรหัส HMC

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ขอรหัสอัปเดต	“การอัปเดตซอฟต์แวร์ HMC ของคุณ” ในหน้า 128
2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่	
3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ	
4. สำรองข้อมูล HMC	
5. บันทึกข้อมูลคอนฟิกูเรชัน HMC ปัจจุบัน	
6. บันทึกสถานะคำสั่งรีโมต	
7. จัดเก็บข้อมูลอัปเดต	
8. อัปเดตซอฟต์แวร์ HMC	
9. ตรวจสอบว่าการติดตั้งการอัปเดตรหัสเครื่อง HMC เสร็จเรียบร้อยแล้ว	

การเพิ่ม HMC ตัวที่สองในการติดตั้งที่มีอยู่

ศึกษาเพิ่มเติมเกี่ยวกับงานระดับสูงที่คุณต้องดำเนินการ เมื่อเพิ่ม HMC ตัวที่สองลงในระบบที่ถูกจัดการของคุณ

หากคุณมี HMC ที่มีอยู่และระบบที่ถูกจัดการ และต้องการเพิ่ม HMC ตัวที่สองในคอนฟิกูเรชันนี้ให้ทำต่อไปนี้:

ตารางที่ 3. งานที่คุณต้องดำเนินการเมื่อเพิ่ม HMC ตัวที่สองในการติดตั้งที่มีอยู่

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ตรวจสอบให้แน่ใจว่าฮาร์ดแวร์ HMC ของคุณสนับสนุนรหัส HMC เวอร์ชัน 7	

ตารางที่ 3. งาน ที่คุณต้องดำเนินการเมื่อเพิ่ม HMC ตัวที่สองลงในการติดตั้งที่มีอยู่ (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
2. รวบรวมข้อมูล และป้อนข้อมูลในเวิร์กชีต Configuration การติดตั้งล่วงหน้า	“เวิร์กชีตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
3. แกะกล่องบรรจุฮาร์ดแวร์	
4. ต่อสายเคเบิลฮาร์ดแวร์ HMC	“การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อะโลน” “การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง” ในหน้า 16
5. เปิด HMC โดยกดปุ่มเปิด/ปิด	
6. ล็อกอินเข้าสู่ HMC	
7. ระดับโค้ด HMC ต้องตรงกัน เปลี่ยนโค้ดบน เครื่องหนึ่งให้ตรงกับโค้ดบน HMC เครื่องอื่น	“การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ” ในหน้า 125 “การอัปเดตซอฟต์แวร์ HMC ของคุณ” ในหน้า 128
8. เข้าใช้เวิร์กชีตค่าที่แนะนำ หรือใช้เมนู HMC เพื่อกำหนดคอนฟิก HMC	“การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 101
9. คอนฟิก HMC นี้สำหรับเซิร์ฟเวอร์ที่ใช้เวิร์กชีตการติดตั้ง Call-Home	“การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้” ในหน้า 114
10. ต่อเซิร์ฟเวอร์เข้ากับ HMC	

การตั้งค่า HMC

คุณต้องตั้งค่าฮาร์ดแวร์ HMC ก่อนตั้งค่าซอฟต์แวร์ HMC ศึกษาเพิ่มเติมเกี่ยวกับการตั้งค่า HMC ที่มีดิสก์หรือ HMC ที่ติดตั้งชั้นวาง

การวางสายเคเบิลสำหรับ HMC แบบสแตนด์อะโลน

วางตำแหน่ง HMC และวางสายเคเบิลให้กับส่วนประกอบฮาร์ดแวร์แต่ละชิ้น

คุณสามารถต่อสายเคเบิล HMC แบบสแตนด์อะโลนของคุณไปยังระบบที่ถูกจัดการ

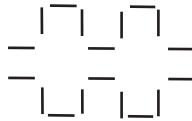
1. ตรวจสอบให้แน่ใจว่า คุณวาง HMC ไว้ในตำแหน่งที่ต้องการ
2. ติดตั้งสายเคเบิลมอนิเตอร์เข้ากับตัวเชื่อมต่อมอนิเตอร์, แล้วไขสกรูให้แน่น
3. ติดตั้งสายไฟเข้ากับมอนิเตอร์
4. ตรวจสอบให้แน่ใจว่า สวิตช์เลือกแรงดันไฟบน HMC ถูกตั้งค่าให้เป็นแรงดันไฟที่ใช้ในภูมิภาคของคุณ สวิตช์เลือกแรงดันไฟฟ้าจะเป็นสีแดง และอยู่ใกล้กับตัวเชื่อมต่อไฟฟ้า ขั้วสวิตช์เพื่อแสดงแรงดันไฟที่ใช้ในตำแหน่งของคุณ
5. เสียบปลั๊กสายไฟเข้ากับ HMC
6. เชื่อมต่อคีย์บอร์ดและเมาส์เข้ากับ HMC
7. เชื่อมต่อกับโมเด็มเสริม:

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

ถ้าคุณกำลัง เชื่อมต่อโมเด็มภายนอก ให้ปฏิบัติตามนี้:

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่น เพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM

- a. หากคุณยังไม่ได้ดำเนินการ ให้เชื่อมต่อสายเคเบิลข้อมูล ของโมเด็มเข้ากับโมเด็มภายนอกของ HMC
- b. เชื่อมต่อสายเคเบิลข้อมูลเข้ากับพอร์ตระบบบน HMC ซึ่งมีเลเบลที่เป็นสัญลักษณ์ต่อไปนี้:

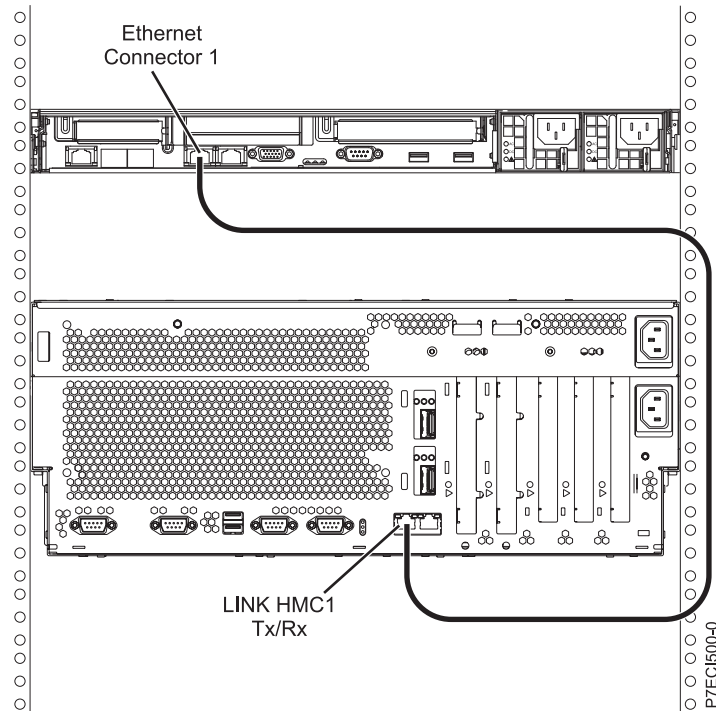


IPHA1522-0

- c. ใช้สายเคเบิลโทรศัพท์ เพื่อเชื่อมต่อสายพอร์ตของโมเด็มภายนอกเข้ากับปลั๊กโทรศัพท์แบบอนาล็อกบนผนัง หากคุณกำลังเชื่อมต่อกับโมเด็มภายใน ให้ใช้สายเคเบิลข้อมูลเพื่อเชื่อมต่อโมเด็มภายในของ HMC กับแหล่งข้อมูลที่เหมาะสม ตัวอย่างเช่น ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตโมเด็มของ HMC เข้ากับปลั๊กอนาล็อกบนผนังของคุณ

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่น เพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM

8. หากระบบที่ถูกระบุได้รับการติดตั้งแล้ว คุณจะตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแอคทีฟอยู่หรือไม่ โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่ถูกระบุในขณะที่ยื่นตอนติดตั้งกำลังดำเนินไป
9. เชื่อมต่อ ตัวเชื่อมต่ออีเทอร์เน็ต 1 บน HMC กับพอร์ต LINK HMC1 บนระบบที่ถูกระบุ



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 100

หลักการที่เกี่ยวข้อง:

“การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 84

ศึกษาเพิ่มเติมเกี่ยวกับข้อพจน์ของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

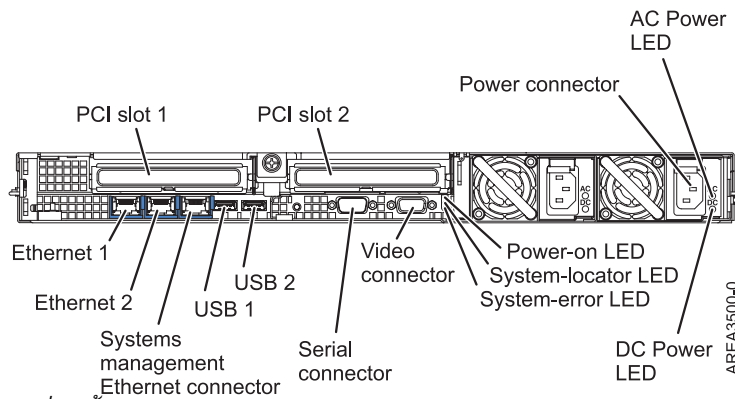
“การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80

การติดตั้ง 7310-CR4 HMC ลงในชั้นวาง

ส่วนนี้อธิบายถึงวิธีการติดตั้ง 7310-CR4 HMC ลงในชั้นวาง นี่คือนานของลูกค้า

ถ้า HMC ถูกนำมาใช้เพื่อจัดการกับระบบ POWER7® ถ้า HMC ถูกนำมาใช้เพื่อจัดการกับระบบ

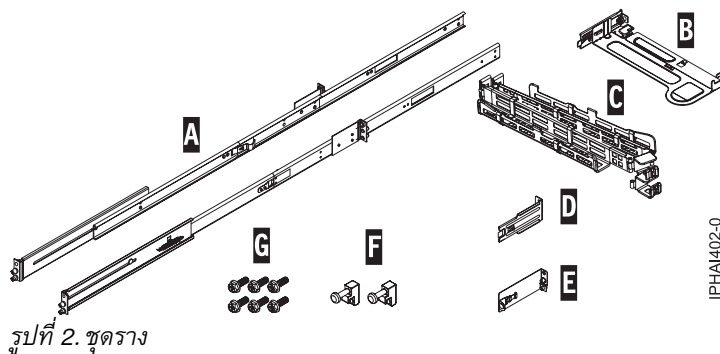
ต่อไปนี้เป็นด้านหลังของ 7310-CR4:



รูปที่ 1. ด้านหลังของ 7310-CR4

เมื่อต้องการติดตั้ง 7310-CR4 HMC ลงในชั้นวางให้ทำตามขั้นตอนต่อไปนี้:

1. ทำรายการชิ้นส่วนให้เสร็จสิ้น โปรดดูที่ ทำรายการชิ้นส่วนให้เสร็จสิ้น
2. ค้นหาตำแหน่งชุดฮาร์ดแวร์ที่ประกอบเข้ากับชั้นวาง และชุดวางของระบบ ซึ่งประกอบด้วยยูนิตรบบของคุณ



รูปที่ 2. ชุดวาง

ตารางที่ 4. ชิ้นส่วนของชุดวาง

ชิ้นส่วนของชุดวางแบบสไลด์

A รางแบบสไลด์

B งานที่ประกอบเข้ากับแขนยึดสายเคเบิล

C แขนยึดสายเคเบิล

D แท่นยึดสายเคเบิล

E สายเคเบิลที่สนับสนุนแท่นยึดและแท็บความปลอดภัย

F แลตซ์ (2)

G สกรู (6)

สำคัญ: ยูนิตรบบนี้คือยูนิต 1 EIA แบบสูง คุณอาจต้องการข้อมูลนี้เพื่อทำการติดตั้งให้เสร็จสิ้น

การทำให้รายการชิ้นส่วนให้เสร็จสิ้น

คุณอาจต้องการทำการรายการชิ้นส่วนให้เสร็จสิ้นใช้โปรซีเดอร์ในส่วนนี้เพื่อปฏิบัติงานนี้

ถ้าคุณยังไม่ได้ทำให้ทำการรายการชิ้นส่วนให้เสร็จสิ้น ก่อนที่จะดำเนินการติดตั้ง:

1. หาตำแหน่งรายงานชุดเครื่องมือในกล่องอุปกรณ์
2. ตรวจสอบให้แน่ใจว่าคุณได้รับชิ้นส่วนทุกชิ้นที่คุณได้สั่งซื้อ

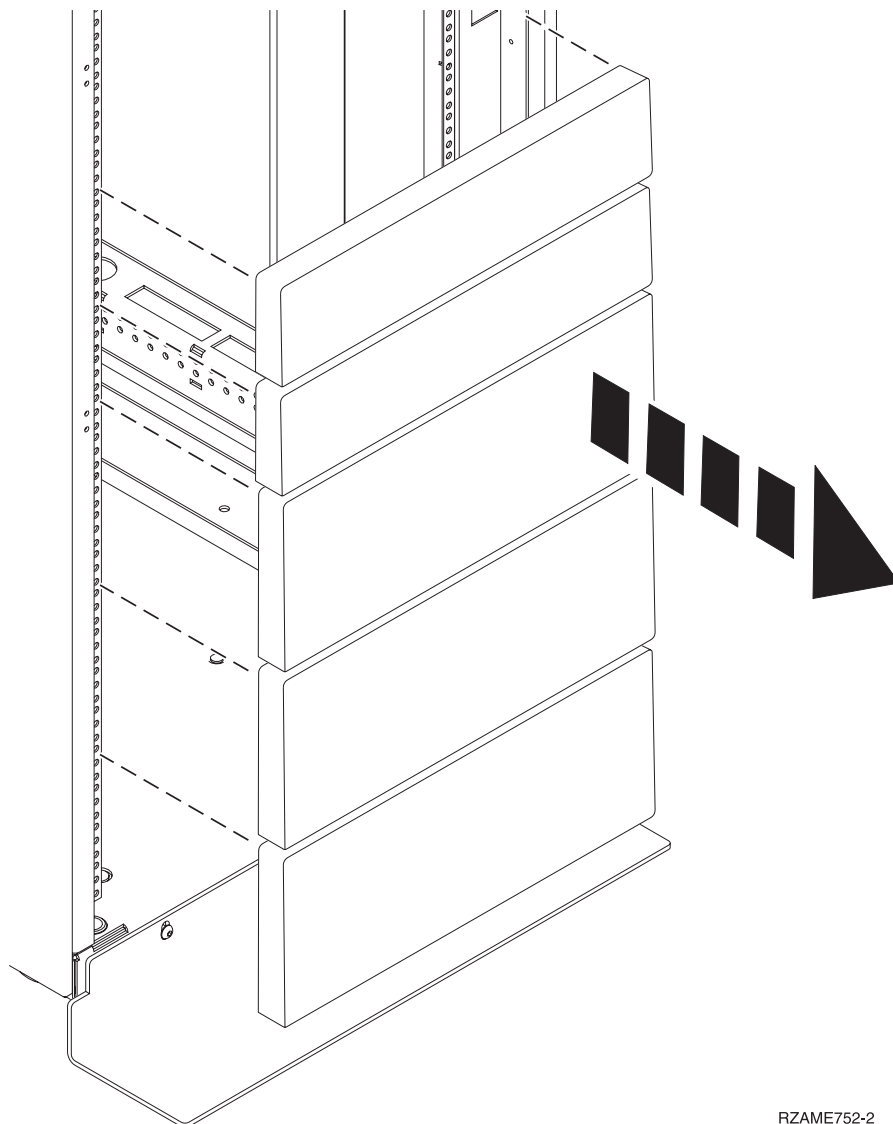
ถ้าชิ้นส่วนไม่ถูกต้อง หายไป หรือเสียหาย ให้ติดต่อผู้ขายของ IBM หรือฝ่ายขายและสนับสนุนของ IBM

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 หากคุณไม่มีจุดใดๆ ให้ใช้รูปแบบอื่นๆ ของเครื่องมือที่ใช้ทำเครื่องหมายเพื่อวัตถุประสงค์ในการระบุตำแหน่ง (ตัวอย่างเช่น เทป ตัวทำเครื่องหมาย หรือดินสอ) หากคุณกำลังติดตั้งรางแบบสไลด์ให้วางเครื่องหมายหรือจุดยึดเหนี่ยวที่ตำแหน่งด้านล่างและกึ่งกลางของยูนิต EIA แต่ละยูนิต

3. วางจุดยึดเหนี่ยวอื่นๆ ถัดจากรูด้านล่างของ ยูนิต EIA ข้างต้น

หมายเหตุ: หากคุณกำลังนับรูให้เริ่มต้นด้วยรูที่ระบุโดยจุดแรกและนับไปอีกสองรู วางจุดที่สองให้อยู่ถัดจากรูที่สาม

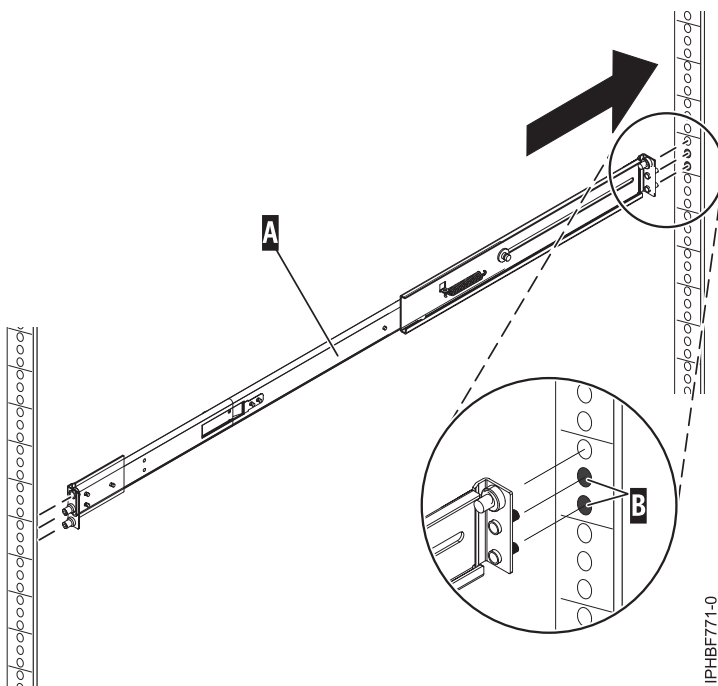
4. ทำซ้ำขั้นตอน 1 ในหน้า 9 สำหรับ รูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
5. ไปที่ด้านหลังของชั้นวาง
6. ที่ด้านขวา ให้หา ยูนิต EIA ที่ตรงกับยูนิต EIA ด้านล่างซึ่งทำเครื่องหมายอยู่บนด้านหน้าของชั้นวาง
7. วางจุดยึดเหนี่ยวที่ด้านล่างของยูนิต EIA
8. วางจุดยึดเหนี่ยวที่รูด้านบนสุดของยูนิต EIA
9. ทำเครื่องหมายที่รูทางด้านซ้ายของชั้นวาง

การติดตั้งรางแบบสไลด์ในชั้นวาง

ศึกษาเกี่ยวกับวิธีการติดตั้งสวิตช์คอนโซลที่เป็นตัวเลือก

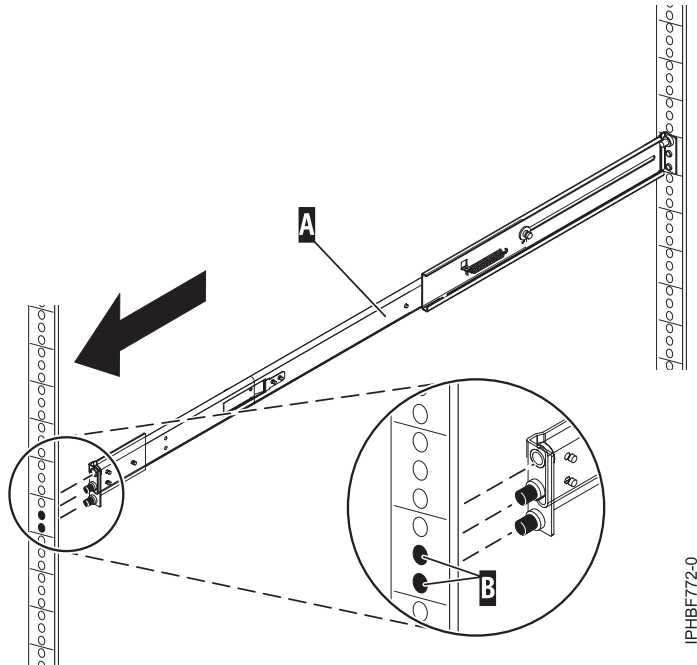
เมื่อต้องการ ติดตั้งรางแบบสไลด์ในชั้นวางให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ใส่รางแบบสไลด์ด้านขวา (A), ที่มีเครื่องหมาย right (B) เข้ากับหน้าแปลนที่ประกอบเข้ากับชั้นวางในตำแหน่ง ที่ด้าน หลังขวาของชั้นวาง ขั้วของรางสองขั้วจะยื่นผ่านรู (B) ที่อยู่ด้านล่างและตรงกลางบนยูนิต EIA



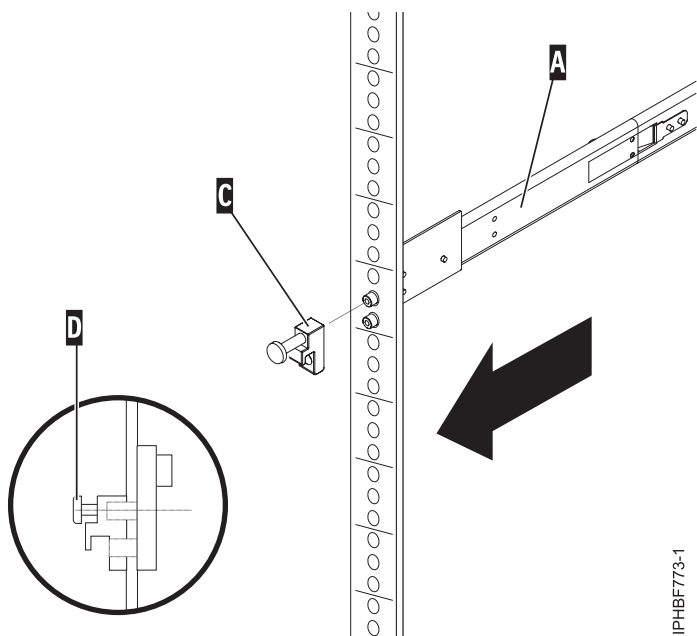
รูปที่ 4. การติดตั้งรางแบบสไลด์ที่ด้านหลังของชั้นวาง

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



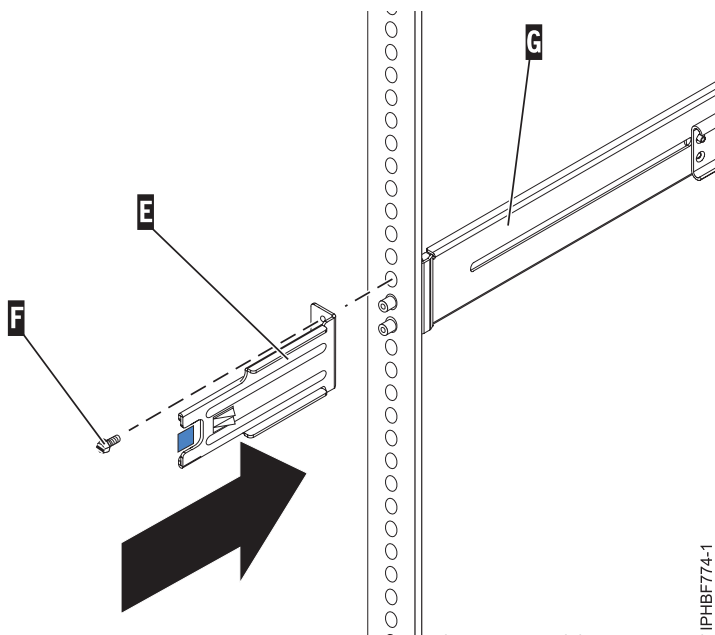
รูปที่ 5. การติดตั้งรางแบบสไลด์ด้านขวาที่ด้านหน้าของชั้นวาง

3. ทำซ้ำขั้นตอน 1 ในหน้า 10-2 เพื่อติดตั้ง รางแบบสไลด์ด้านซ้ายที่มีเครื่องหมาย *left* (ซ้าย) ลงในชั้นวาง
4. จากด้านหน้าของชั้นวาง ให้วางแลตซ์ (C) ไว้บนหัว ใช้มือหมุนสกรู (D) ลงในหัวด้านบนของรางแบบสไลด์ด้านหน้าขวา (A)



รูปที่ 6. การติดตั้งแลตซ์ที่ด้านหน้าของราง

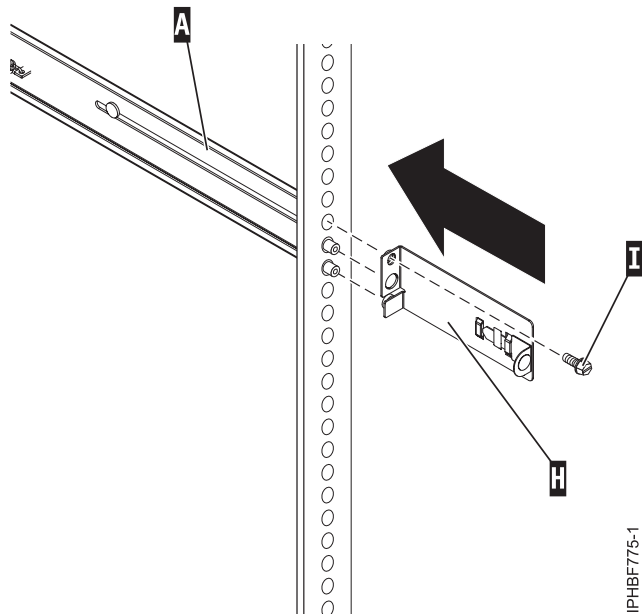
5. ทำซ้ำขั้นตอนก่อนหน้านี้เพื่อติดตั้งแลตซ์บนรางแบบสไลด์ที่ด้านหน้าซ้าย
6. ย้ายไปยังด้านหลังของชั้นวาง ไส้กรู (F) ให้แน่น เพื่อยึดแท่นยึดที่ต่ออยู่กับแขนการจัดการสายเคเบิล (E) เข้ากับ ด้านหลังของรางทางด้านซ้าย (G)



รูปที่ 7. การยึดแท่นยึดการจัดการสายเคเบิลเข้ากับรางที่อยู่ด้านหลังทางซ้ายมือ

7. ถ้าคุณไม่มีแผนที่จะย้ายระบบนี้ให้ดำเนินการต่อด้วย “การติดตั้ง HMC บนรางแบบสไลด์” หากคุณวางแผนที่จะขนส่งระบบของคุณให้ใส่สกรู (I) เพื่อยึดตัวยึดที่รองรับแขนการจัดการสายเคเบิล (H) เข้ากับ ด้านหลังขาของราง (A) ไขสกรูให้แน่น

แขนยึดสายเคเบิลที่รองรับแท่นยึด สามารถนำมาใช้เพื่อยึดแขนยึดสายเคเบิลในระหว่างการขนส่งได้ ถ้ากลไกถูกยึดหลังจากที่ติดตั้งแขนยึดสายเคเบิล คุณจะไม่สามารถเลื่อนระบบจากชั้นวางได้



รูปที่ 8. การยึด ตัวยึดที่รองรับแขนการจัดการสายเคเบิลเข้ากับรางที่อยู่ด้านหลังทางขวา

การติดตั้ง HMC บนรางแบบสไลด์

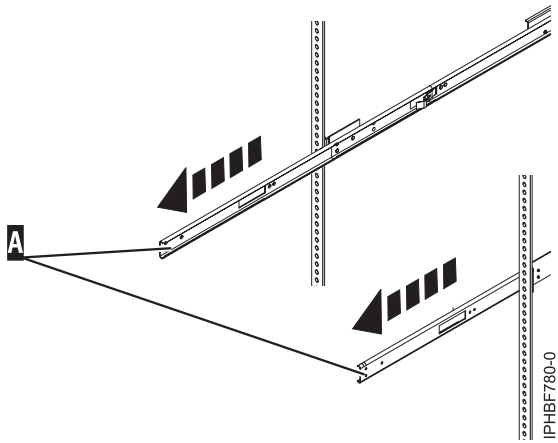
คุณอาจต้องการติดตั้ง HMC บนรางแบบสไลด์ใช้โพรซีเจอร์ในส่วนนี้เพื่อปฏิบัติงานนี้

ก่อนการติดตั้ง HMC บนรางแบบสไลด์ โปรดแน่ใจว่า สเตปีโลเซอร์ถูกต่อและแท่นยึดสเตปีโลเซอร์ของชั้นวางจะถูกยึดกับชั้นวางด้านหน้าส่วนล่าง เพื่อป้องกันชั้นวางจากการตกหล่น เมื่อรางถูกดึงออกจากชั้นวาง

เมื่อต้องการ ติดตั้ง HMC บนชุดรางแบบสไลด์ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

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

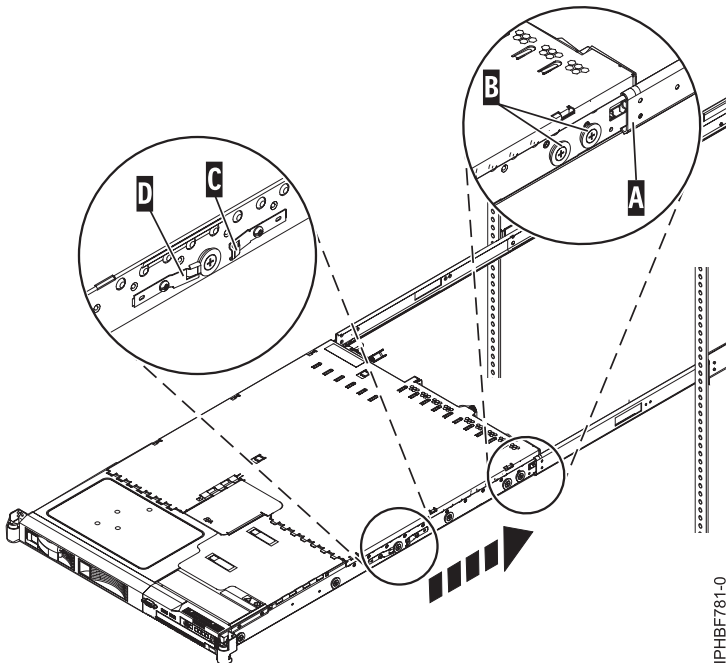
ข้อควรสนใจ: แลตซ์ที่อยู่ด้านหน้าของราง และแท่นยึดแขนยึดสายเคเบิลต้องถูกติดตั้ง ก่อน ที่จะติดตั้ง HMC บนราง ถ้าไม่ได้ติดตั้งชิ้นส่วนเหล่านี้ไว้ การติดตั้งอาจทำให้รางกดทับ และ HMC อาจตกหล่นจากชั้นวางได้



รูปที่ 9. การต่อรางแบบสไลด์

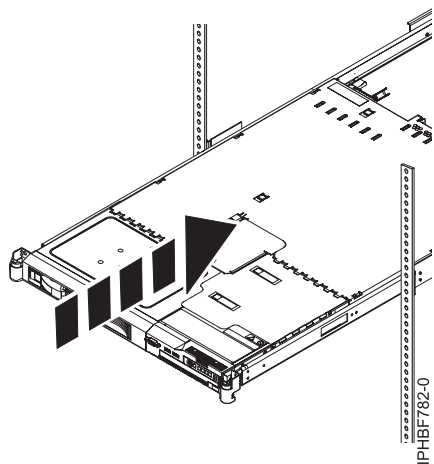
สำคัญ: หน่วยนี้หนักประมาณ 17 กก. (37 ปอนด์) โปรดตรวจสอบให้แน่ใจว่าคุณสามารถรองรับน้ำหนักนี้ได้อย่างปลอดภัย
เมื่อวาง HMC ลงในชั้นวาง

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



รูปที่ 10. การติดตั้ง HMC บนรางแบบสไลด์

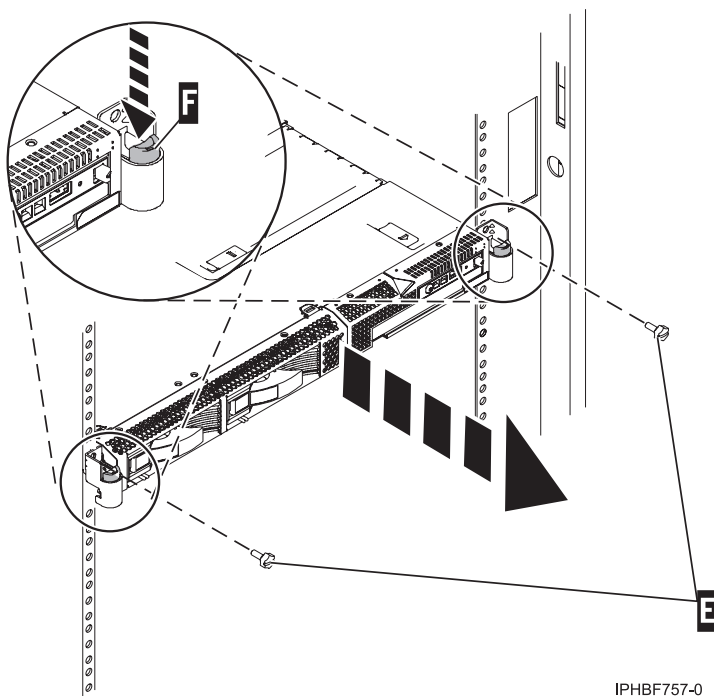
4. ผลัก HMC ลงในรางแบบสไลด์จนกระทั่งปล่อยสไลด์ (C) ล็อกเข้าที่ สิ่งนี้จะล็อกระบบในตำแหน่งการให้บริการบนสไลด์
คุณจะได้ยินเสียงคลิก
5. กดแลตซ์ที่ปล่อยรางแบบสไลด์ด้านหน้า (D) ทั้งสองด้านของรางแบบสไลด์
6. เลื่อน HMC ไปยังและออกจากชั้นวาง เพื่อตรวจสอบว่า HMC เคลื่อนย้ายได้อย่างอิสระโดยไม่ถูกเชื่อมต่อ



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. ผลัก HMC ให้เข้าที่จนกว่าแลตช์ของราง (F) จะล็อกเข้าที่



รูปที่ 12. แลตช์ของชั้นวางและสกรู

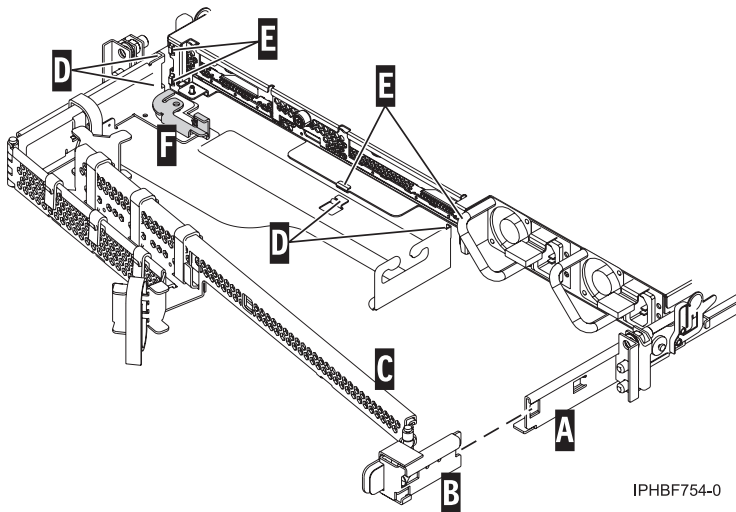
8. ขันสกรูทั้งสี่ที่ติดตั้งอยู่ที่ ด้านหน้าและด้านหลังของรางให้แน่น
9. ถ้าชั้นวางจะถูกขนส่งให้ใส่และขันสกรู (E) ของชั้นวางให้แน่น

การติดตั้งแขนยึดสายเคเบิล

คุณอาจต้องการติดตั้งแขนยึดสายเคเบิล ใช้โปรซีเจอร์ในส่วนนี้เพื่อปฏิบัติงานนี้

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. เลื่อนแขนยึดสายเคเบิลไปยังด้านซ้ายยึดแขนยึดสายเคเบิลให้เข้าที่ ตรวจสอบให้แน่ใจว่า แท็บทั้งหมดอยู่ในสล๊อต
5. ผลักคันโยกสำหรับล็อก (F) ลงในตำแหน่งที่ล็อก ตรวจสอบให้แน่ใจว่า แขนยึดสายเคเบิล (C) อยู่ในระดับที่เคลื่อนที่ได้ อย่างอิสระ

การวางสายเคเบิลสำหรับ HMC แบบติดตั้งชั้นวาง

ศึกษาวิธีติดตั้ง HMC แบบติดตั้งชั้นวางของคุณ

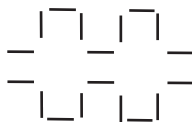
1. ตรวจสอบให้แน่ใจว่า คุณวาง HMC ไว้ในตำแหน่งที่ถูกต้อง
2. ติดตั้ง HMC ลงในชั้นวาง สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การติดตั้ง 7310-CR4 HMC ลงในชั้นวาง” ในหน้า 6 เมื่อคุณเสร็จสิ้นการติดตั้ง HMC ลงในชั้นวางแล้ว ให้ทำขั้นตอนถัดไป
3. เสียบปลั๊กสายไฟเข้ากับ HMC
4. เชื่อมต่อคีย์บอร์ด มอนิเตอร์ และเมาส์
5. เชื่อมต่อโมเด็มที่เป็นอุปกรณ์เสริม:

ถ้าคุณกำลังเชื่อมต่อโมเด็มภายนอก ให้ปฏิบัติตามนี้:

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่นเพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 84

- a. ถ้าคุณต้องการติดตั้งโมเด็มภายนอกเข้ากับชั้นวาง ให้กระทำดังนี้

- b. หากคุณติดตั้งโมเด็มเรียบร้อยแล้ว ให้เชื่อมต่อสายเคเบิลข้อมูลของโมเด็มเข้ากับโมเด็มภายนอก HMC
- c. เชื่อมต่อสายเคเบิลข้อมูลโมเด็มเข้ากับพอร์ตระบบบน HMC ซึ่งมีเลเบลที่เป็นสัญลักษณ์ต่อไปนี้:



IPHA1522-0

- d. ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตของโมเด็มภายนอกเข้ากับปลั๊กโทรศัพท์แบบอนาล็อกบนผนัง
- e. เสียบสายตัวจ่ายไฟของโมเด็มเข้ากับโมเด็ม HMC

ถ้าคุณกำลังเชื่อมต่อกับโมเด็มภายใน ให้ใช้สายเคเบิลข้อมูลเพื่อเชื่อมต่อโมเด็ม HMC ภายในกับแหล่งข้อมูลที่เหมาะสม ตัวอย่างเช่น ใช้สายเคเบิลโทรศัพท์เพื่อเชื่อมต่อสายพอร์ตของโมเด็ม HMC modem line port to the analog jack on your wall.

หมายเหตุ: คุณสามารถใช้วิธีการเชื่อมต่อแบบอื่นเพื่อส่งข้อมูลข้อผิดพลาดไปยัง IBM สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home” ในหน้า 84

6. เชื่อมต่อสายเคเบิลอีเทอร์เน็ต (หรือสายครอสโอเวอร์) จาก HMC ไปยังเซิร์ฟเวอร์ที่จัดการ:

หมายเหตุ: เมื่อต้องการศึกษาเพิ่มเติมเกี่ยวกับการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80

7. หากระบบที่จัดการได้รับการติดตั้งแล้ว คุณจะสามารถตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแฉีคที่พอย์หรือไม่โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่จัดการในขณะที่ขั้นตอนติดตั้งกำลังดำเนินไป
8. เชื่อมต่อพอร์ตอีเทอร์เน็ตบน HMC เข้ากับพอร์ตอีเทอร์เน็ตที่ชื่อ HMC1 บนเซิร์ฟเวอร์ที่จัดการ
9. ถ้าคุณกำลังเชื่อมต่อ HMC ตัวที่สองเข้ากับเซิร์ฟเวอร์ที่จัดการ ให้เชื่อมต่อพอร์ตอีเทอร์เน็ตที่มีเลเบล HMC2 บนเซิร์ฟเวอร์ที่จัดการ
10. เสียบปลั๊กสายไฟสำหรับมอนิเตอร์, HMC และโมเด็มภายนอก HMC เข้ากับจุดจ่ายไฟ

หมายเหตุ: หากคุณกำลังเชื่อมต่อ HMC นี้กับระบบที่จัดการใหม่ ไม่ต้องเชื่อมต่อระบบที่จัดการเข้ากับ แหล่งกำเนิดไฟฟ้าในเวลานี้

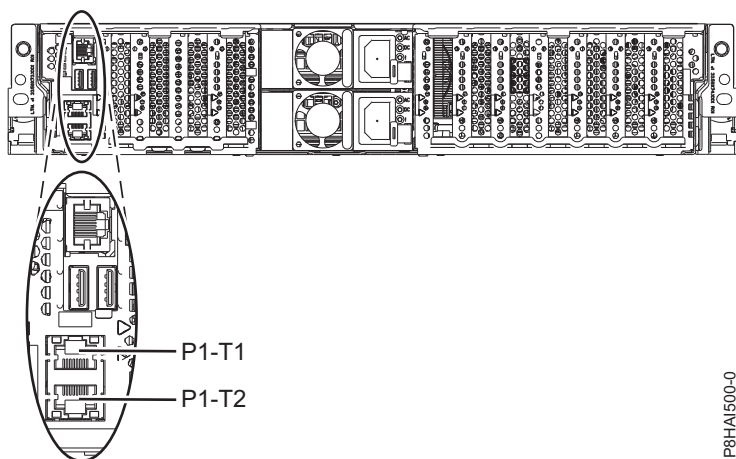
จากนั้น คุณจะต้องตั้งค่าซอฟต์แวร์ HMC ดำเนินการต่อด้วย “การกำหนดคอนฟิก HMC” ในหน้า 100

ตำแหน่งพอร์ตของ HMC

คุณสามารถค้นหาคำแนะนำพอร์ตได้โดยใช้โค้ดตำแหน่ง ใช้ภาพประกอบ ตำแหน่งพอร์ตของ HMC เพื่อแม็พโค้ดตำแหน่งกับตำแหน่งพอร์ตของ HMC บนเซิร์ฟเวอร์

โมเดล 8247-21L, 8247-22L, 8284-21A หรือตำแหน่งพอร์ต 8284-22A HMC

ใช้ไดอะแกรมและตารางนี้เพื่อแม็พพอร์ต HMC บน 8247-21L, 8247-22L, 8284-21A หรือ 8284-22A



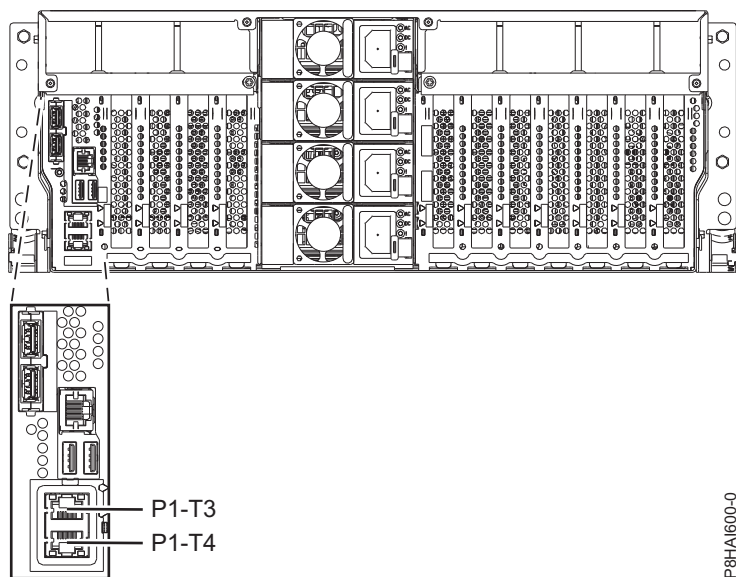
รูปที่ 14. 8247-21L, 8247-22L, 8284-21A หรือตำแหน่งพอร์ต 8284-22A HMC

ตารางที่ 5. 8247-21L, 8247-22L, 8284-21A หรือตำแหน่งพอร์ต 8284-22A HMC

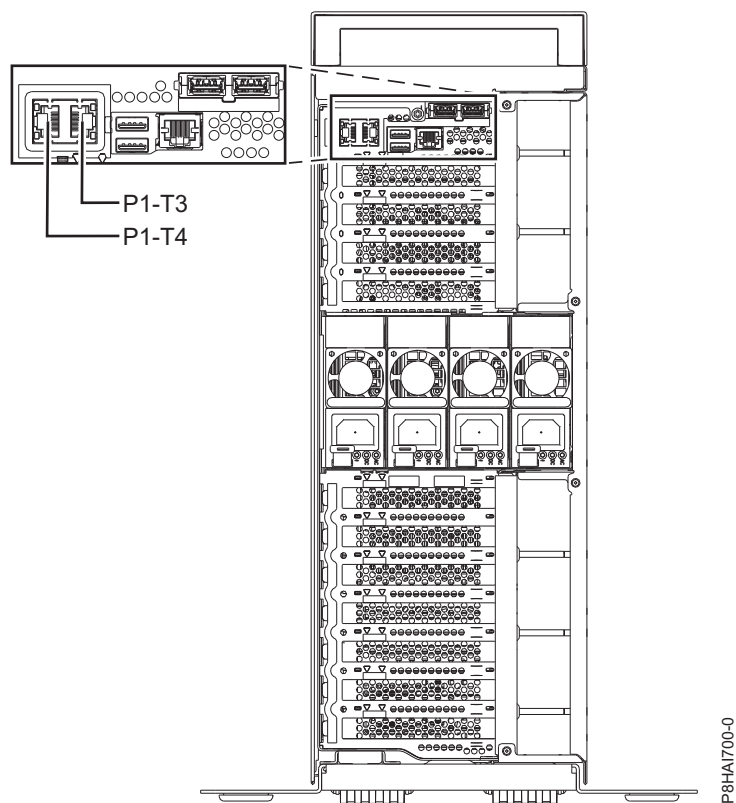
พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T1	ไม่มี
พอร์ต HMC 2	Un-P1-T2	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งของพอร์ต HMC เกี่ยวกับ 8247-21L, 8247-22L, 8284-21A หรือ 8284-22A โปรดดูตำแหน่งของชิ้นส่วนและ รหัสตำแหน่งสำหรับ 8247-21L, 8247-22L หรือ 8284-22A		

ตำแหน่งพอร์ตของโมเดล 8247-42L, 8286-41A, หรือ 8286-42A HMC

ใช้แผนภาพนี้และตารางเพื่อแม็พพอร์ต HMC บน 8247-42L, 8286-41A หรือ 8286-42A



รูปที่ 15. มุมมอง ด้านหลัง - 8247-42L, 8286-41A หรือ 8286-42A ตำแหน่งพอร์ต HMC



รูปที่ 16. ตำแหน่งพอร์ต 8286-41A HMC แบบทาวเวอร์

ตารางที่ 6. ตำแหน่ง 8247-42L, 8286-41A หรือ 8286-42A พอร์ต HMC

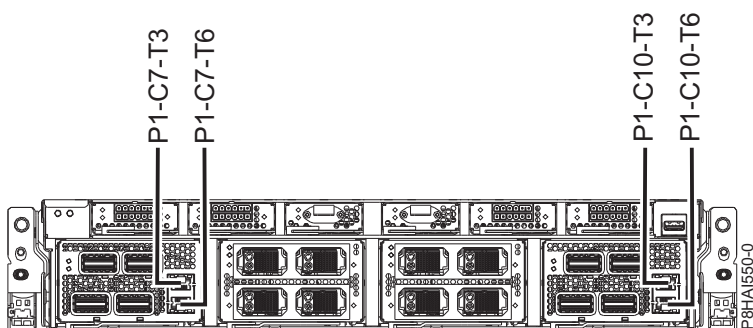
พอร์ต	โค้ดตำแหน่งฟิลิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T3	ไม่มี

ตารางที่ 6. ตำแหน่ง 8247-42L, 8286-41A หรือ 8286-42A พอร์ต HMC (ต่อ)

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 2	Un-P1-T4	ไม่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ต HMC บน 8247-42L, 8286-41A หรือ 8286-42A โปรดดู ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8247-42L, 8286-41A หรือ 8286-42A		

ตำแหน่งพอร์ตของโมเดล 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC

ใช้ไดอะแกรมและตารางนี้เพื่อแม็พพอร์ต HMC บน 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME



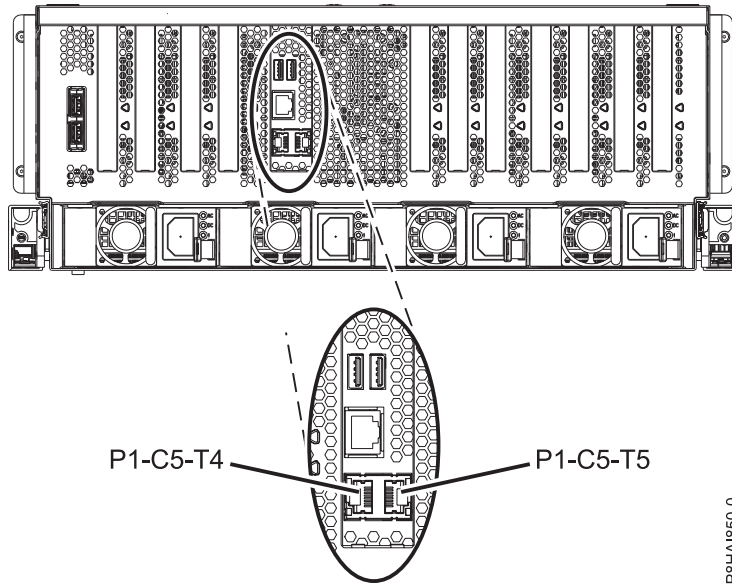
รูปที่ 17. ตำแหน่งพอร์ต 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME HMC

ตารางที่ 7. ตำแหน่งพอร์ต 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME HMC

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
การ์ดตัวประมวลผลเซอร์วิส 1 - พอร์ต HMC 1	Un-P1-C7-T3	ไม่มี
การ์ดตัวประมวลผลเซอร์วิส 1 - พอร์ต HMC 2	Un-P1-C7-T6	ไม่
การ์ดตัวประมวลผลเซอร์วิส 2 - พอร์ต HMC 1	Un-P1-C10-T3	ไม่
การ์ดตัวประมวลผลเซอร์วิส 2 - พอร์ต HMC 2	Un-P1-C10-T6	ไม่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ต HMC บน 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME โปรดดู ตำแหน่งพอร์ตและโค้ดตำแหน่งสำหรับตำแหน่ง 9080-MHE, 9080-MME, 9119-MHE หรือ 9119-MME		

ตำแหน่งพอร์ตของโมเดล 8408-44E และ 8408-E8E HMC

ใช้แผนภาพนี้และตารางเพื่อแม็พพอร์ต HMC บน 8408-44E และ 8408-E8E



รูปที่ 18. ตำแหน่งพอร์ต HMC 8408-44E and 8408-E8E

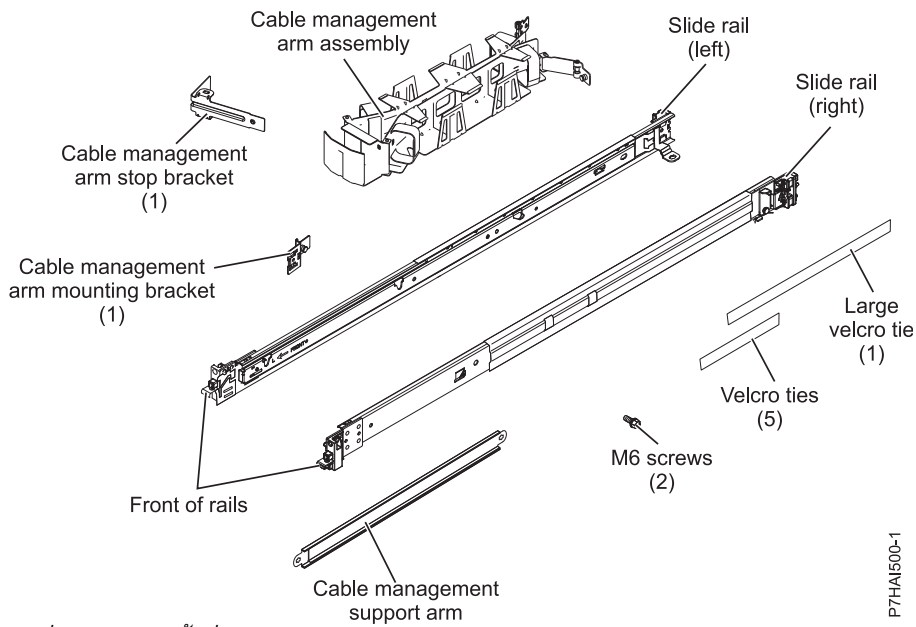
ตารางที่ 8. ตำแหน่งพอร์ต HMC 8408-44E and 8408-E8E

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-C5-T4	ไม่มี
พอร์ต HMC 2	Un-P1-C5-T5	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ต HMC บน 8408-44E และ 8408-E8E โปรดดู ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8404-44E และตำแหน่ง 8408-E8E		

การติดตั้ง 7042-CR5 และ 7042-CR6 ในชั้นวาง

ส่วนนี้อธิบายวิธีติดตั้ง 7042-CR5 และ 7042-CR6 HMC ในชั้นวาง

ทำรายการชิ้นส่วนให้เสร็จสิ้น รูปประกอบต่อไปนี้แสดงรายการที่คุณต้องการติดตั้งเซิร์ฟเวอร์ในตู้ชั้นวาง ถ้ารายการใดๆ หายไปหรือเกิดความเสียหาย โปรดติดต่อสถานที่ที่คุณซื้อ

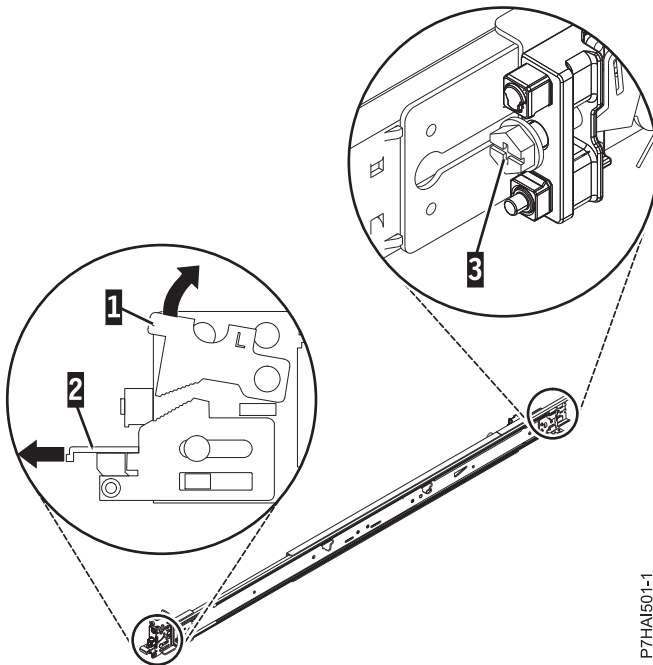


รูปที่ 19. รายการชิ้นส่วน

หมายเหตุ: คุณสามารถใช้สกรูสำหรับการจัดตั้ง หรือเพื่อเพิ่มความแข็งแรงมากขึ้น ในพื้นที่ที่มีการสั่นสะเทือนสูง

เพื่อติดตั้ง 7042-CR6 HMC ลงในชั้นวาง ให้ดำเนินการขั้นตอนต่อไปนี้:

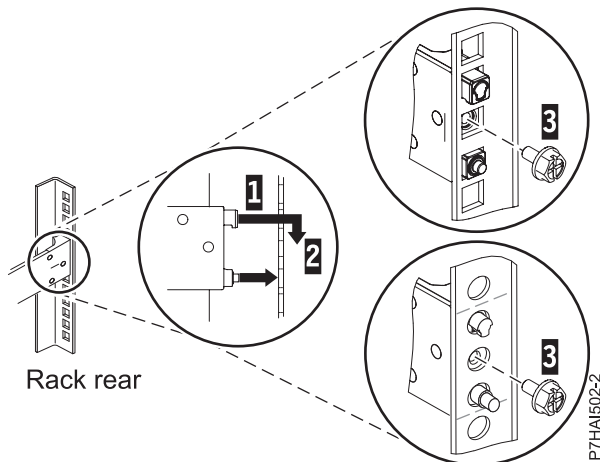
1. วางแบบสไลด์แต่ละรางมีเครื่องหมาย R (ด้านขวา) หรือ L (ด้านซ้าย) อย่างใดอย่างหนึ่ง เลือกหนึ่งในรางแบบสไลด์ และดันขึ้นบนแท็บด้านหน้าที่สามารถเคลื่อนย้ายได้ (1) จากนั้นดึงแลตซ์ด้านหน้า (2) เพื่อเลื่อนรางแบบสไลด์ด้านหน้า ถ้าติดตั้งตะปูควงไว้ในรางแบบสไลด์ (3) ให้ถอดออก



รูปที่ 20. รางแบบสไลด์และแท็บที่สามารถเคลื่อนย้ายได้

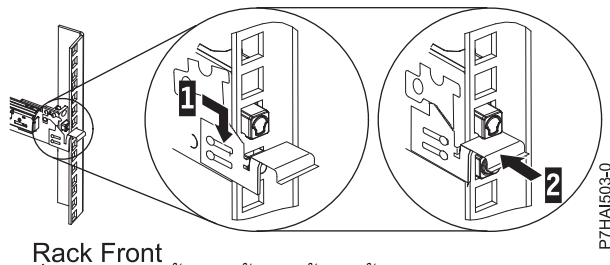
หมายเหตุ: ตรวจสอบให้แน่ใจว่า แท็บที่สามารถเคลื่อนย้ายได้ยังคงขยายได้ และไม่กลับสู่ตำแหน่งเดิม

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



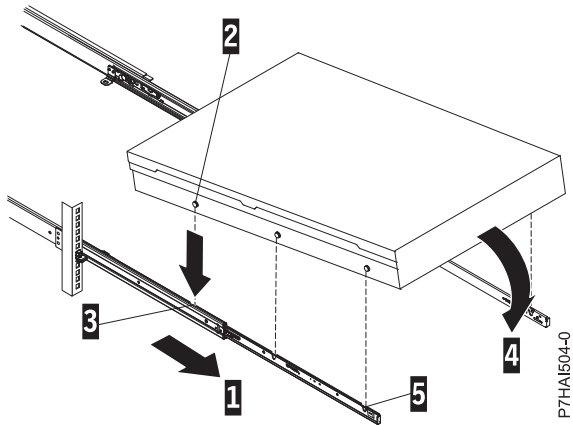
รูปที่ 21. จัดตำแหน่งขั้วภายในรูที่ด้านหลังของชั้นวาง

3. ดึงรางแบบสไลด์ไปข้างหน้าและใส่ขั้วสองขั้ว (1) ที่ด้านหน้าของรางลงในรูที่ต่ำกว่าสองรูใน U บนด้านหน้าของชั้นวาง รางลงในตำแหน่งจนกว่าจะเข้าที่ ผลักแลตซ์ด้านหน้า (2) ในทุกทาง ทำซ้ำขั้นตอนที่ 1 ถึง 3 เพื่อติดตั้งรางอื่นลงในชั้นวาง ตรวจสอบให้แน่ใจว่า แลตซ์ด้านหน้าแต่ละตัวอยู่ในตำแหน่งที่เหมาะสม



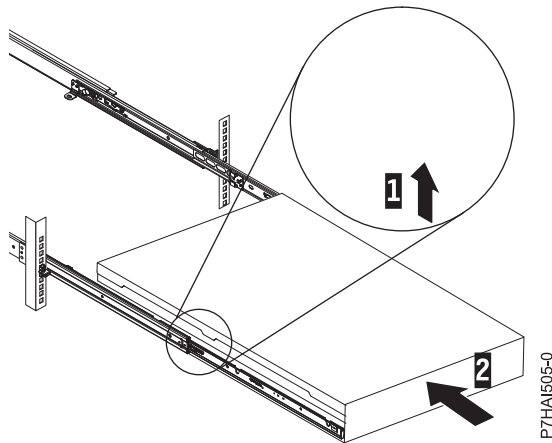
รูปที่ 22. รางและขั้ว ของชั้นวางด้านหน้า

4. ดึงรางแบบสไลด์ไปข้างหน้า (1) จนกว่าจะมาถึงเสียงคลิกสองครั้งในตำแหน่ง ให้ยกเชิฟเวอร์ด้วยความระมัดระวัง และเอียงลงในตำแหน่งที่อยู่เหนือรางแบบสไลด์ ดังนั้น หัวตะปูด้านหลัง (2) บนเชิฟเวอร์อยู่แนวเดียวกับสล็อตด้านหลัง (3) บนรางแบบสไลด์ เลื่อนเชิฟเวอร์ลงจนกว่าหัวตะปูด้านหลังจะเข้าไปอยู่ในสล็อตด้านหลัง สองช่อง จากนั้นลดระดับเชิฟเวอร์ด้านหน้าลง (4) จนกว่าหัวตะปูอื่นเข้าสู่สล็อตอื่นๆ บนรางแบบสไลด์ ตรวจสอบให้แน่ใจว่า แลตซ์ด้านหน้า (5) เลื่อนผ่านหัวตะปู



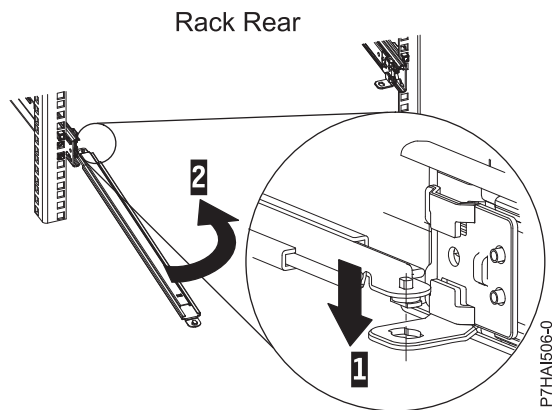
รูปที่ 23. รางแบบสไลด์ที่ขยาย หัวตะปูของเซิร์ฟเวอร์ที่จัดตำแหน่งในแนวเดียวกับสลอตในราง

5. ยกแลตซ์ขึ้น (1) บนรางแบบสไลด์และผลักเซิร์ฟเวอร์ (2) ในทุกทิศทางเข้าไปในชั้นวางจนกว่าจะมีเสียงคลิกเพื่อให้เข้าตำแหน่ง



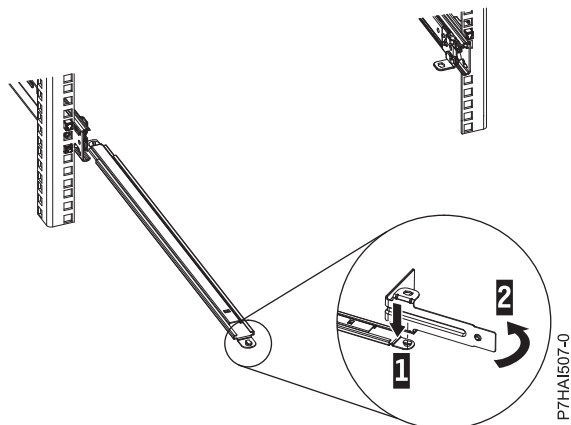
รูปที่ 24. ปลดแลตซ์และเซิร์ฟเวอร์

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



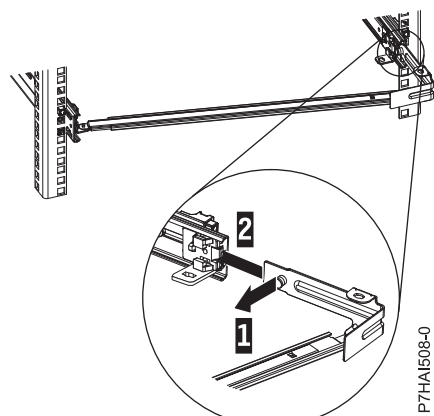
รูปที่ 25. การเชื่อมต่อแขนยึด

7. ติดตั้งแท่นยึดที่หยุดการยืดสายเคเบิลรูปตัว L (1) บนด้านปลายสุดของแขนยึดที่ไม่ได้ถูกยึดไว้เปิดแท่นยึด (2) เพื่อยึดแท่นยึดเข้ากับแขนยึด



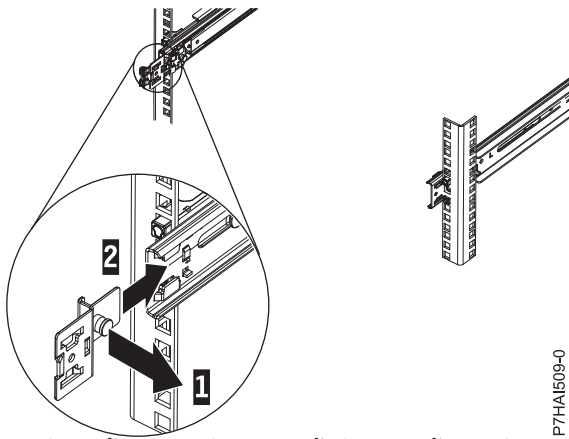
รูปที่ 26. แท่นยึดที่หยุดการยืดสายเคเบิล ซึ่งยึดกับแขนยึด

8. เมื่อต้องการยึดแขนยึดด้านอื่นกับด้านหลังของรางแบบสไลด์ให้ดึงข้อออก (1) จากนั้นเลื่อนแท่นยึด (2) เข้าไปในรางแบบสไลด์



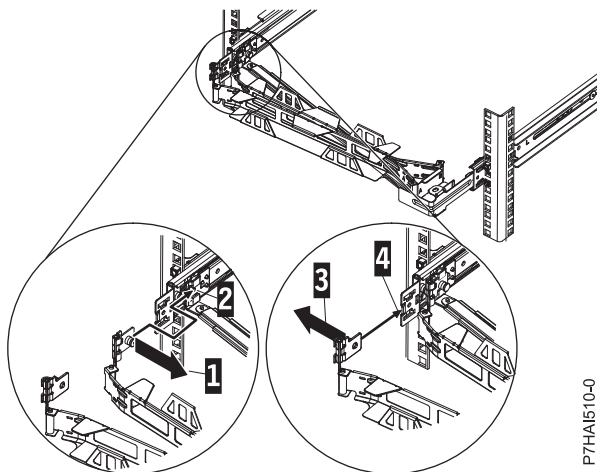
รูปที่ 27. ขั้วที่ขยายแท่นยึดที่ติดตั้งภายในรางแบบสไลด์

9. ดึงหัวของแท่นยึดที่ประกอบเข้าออก (1) และเลื่อนแท่นยึดที่ประกอบเข้า (2) ลงในรางแบบสไลด์ที่คุณกำลังติดตั้ง
แขนยึดสายเคเบิล ผลักแท่นยึด ลงในรางแบบสไลด์จนกว่าหัวสปริงจะเข้าสู่ตำแหน่ง



รูปที่ 28. หัวแท่นยึดที่ประกอบเข้าซึ่งขยายได้และแท่นยึดที่ประกอบเข้าซึ่งติดตั้งในรางแบบสไลด์

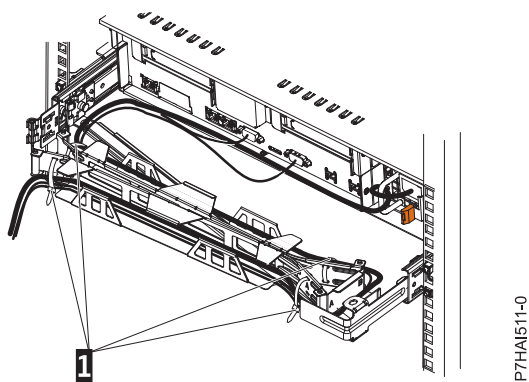
10. วางแขนยึดสายเคเบิลบนแขนยึด ดึงหัวแขนยึดสายเคเบิล ออก (1) จากนั้น เลื่อนแท็บ แขนยึดสายเคเบิล (2) ลง
ในสล๊อตที่ด้านในของรางแบบสไลด์ ผลักแท็บจนกว่า จะเข้าตำแหน่ง ดึงหัวแขนยึดสายเคเบิลด้านอื่นออก (3) จากนั้น
เลื่อนแท็บแขนยึดสายเคเบิลลงในสล๊อต (4) ที่ด้านนอกของรางแบบสไลด์ ผลักแท็บจนกว่าจะเข้าตำแหน่ง



รูปที่ 29. การเชื่อมต่อแขนยึดสายเคเบิล

11. ยึดสายไฟและสายเคเบิลเข้ากับด้านหลังของเซิร์ฟเวอร์ (ซึ่งรวมถึงคีย์บอร์ด จอมอนิเตอร์ และสายเมาส์ ตามต้องการ)
จัดเส้นทางสายเคเบิลและสายไฟบนแขนยึดสายเคเบิล (1) และยึดสายเหล่านั้นด้วยสายผูกเคเบิลหรือรัดด้วยสายรัด

หมายเหตุ: อนุญาตให้ หย่อนสายเคเบิลทั้งหมดเพื่อไม่ให้สายเคเบิลตึงเกินไปตามการย้ายแขนยึด สายเคเบิล



รูปที่ 30. การยึดสายไฟและการจัดเส้นทาง

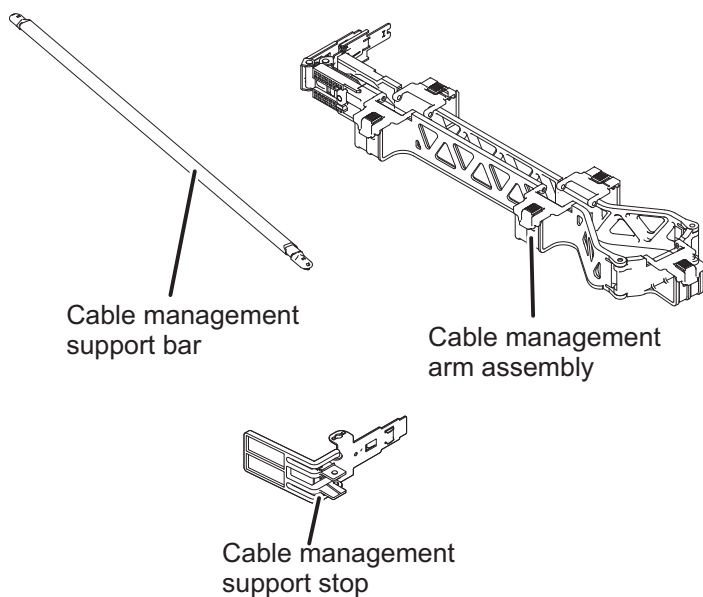
12. เลื่อนเซิร์ฟเวอร์ลงในชั้นวางจนกระทั่งเข้าที่

การติดตั้ง 7042-CR7 และ 7042-CR8 ในชั้นวาง

เรียนรู้วิธีการติดตั้ง 7042-CR7 และ 7042-CR8 Hardware Management Console (HMC) ในชั้นวาง

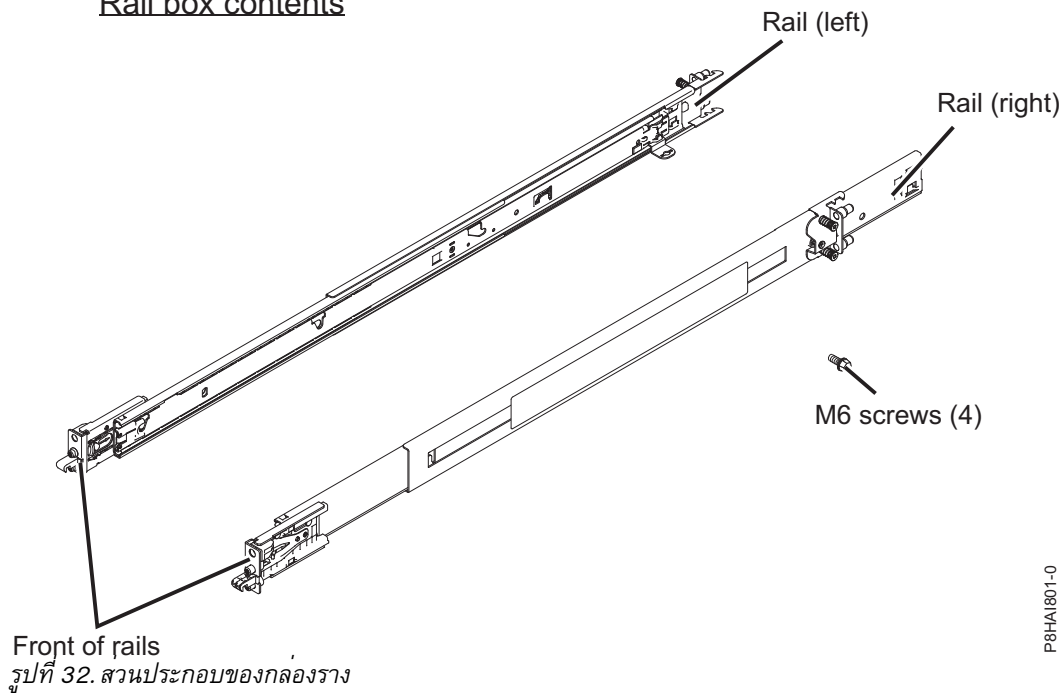
ทำการยกชิ้นส่วนให้เสร็จสิ้น รูปประกอบต่อไปนี้แสดงไอเท็มที่คุณต้องติดตั้งเซิร์ฟเวอร์ในตู้ชั้นวาง ถ้ารายการใดๆ หายไปหรือเกิดความเสียหาย โปรดติดต่อสถานที่ที่คุณซื้อ

Cable Management Arm box contents



รูปที่ 31. ส่วนประกอบของกล่องแขนยึดสายเคเบิล

Rail box contents

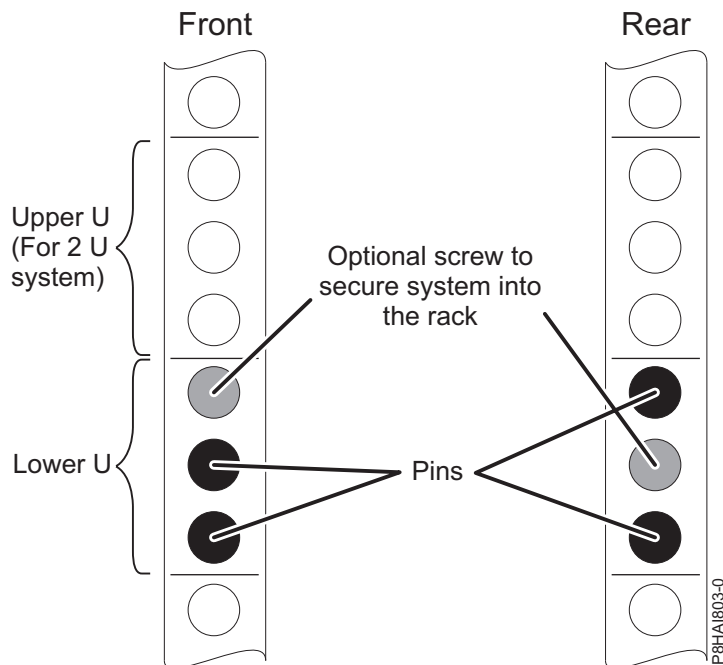


P8HA1801-0

หมายเหตุ: คุณจะต้องใช้ทั้งกล่องรางสไลด์ และกล่อง แชนยัดสายเคเบิลสำหรับการติดตั้งนี้

เมื่อต้องการติดตั้ง 7042-CR7 หรือ 7042-CR8 HMC ในชั้นวาง ให้ทำขั้นตอนต่อไป:

1. เลือก 1 ยูนิตที่พร้อมใช้งาน หรือ 2 ยูนิตพื้นที่ว่าง (ขึ้นอยู่กับ เซิร์ฟเวอร์ซึ่งคุณกำลังติดตั้ง) ในชั้นวางเพื่อติดตั้งเซิร์ฟเวอร์

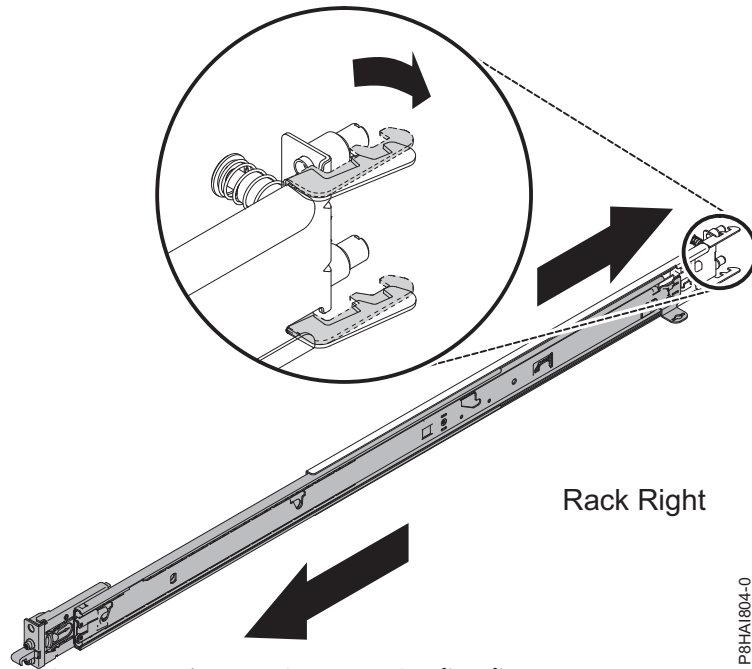


P8HA1803-0

รูปที่ 33. การระบุพื้นที่ว่างของชั้นวาง

หมายเหตุ: เมื่อคุณติดตั้งเซิร์ฟเวอร์แบบ 2 ยูนิต ตรวจสอบให้แน่ใจว่าติดตั้งรางสไลด์ใน U ด้านล่างของพื้นที่ 2 U ในชั้นวาง

2. รางสไลด์แต่ละรางมีการทำเครื่องหมายเป็น หน้า/หลังด้านซ้าย หรือ หน้า/หลังด้านขวา ที่ปลาย เลือกรางสไลด์อย่างใดอย่างหนึ่ง และ ดึงตัวยึดด้านหลังย้อนกลับจนสุด จนกว่าได้ยินเสียงคลิกเข้าที่

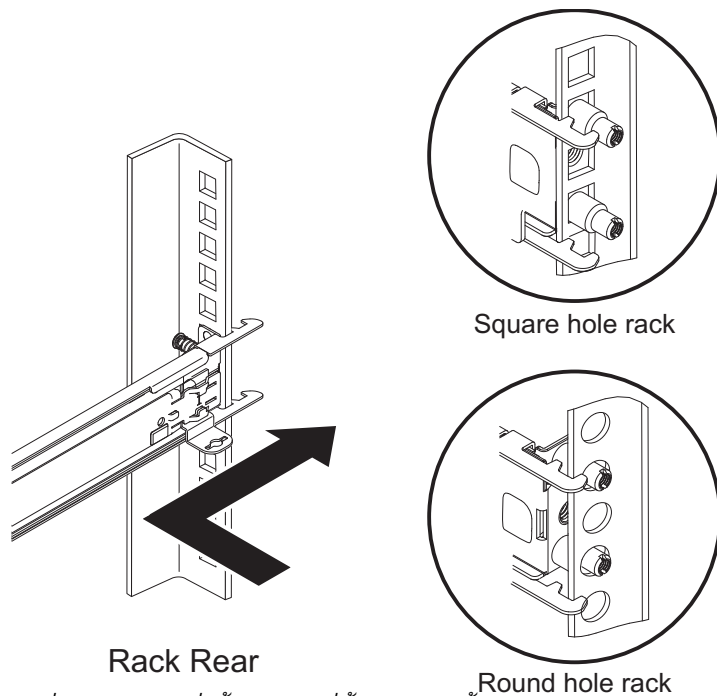


P8HA1804-0

รูปที่ 34. รางสไลด์และแท็บที่สามารถเคลื่อนย้ายได้

หมายเหตุ: ตรวจสอบให้แน่ใจว่าแท็บที่สามารถเคลื่อนย้ายได้ ยังคงขยายอยู่และไม่คลิกกลับเข้าที่

3. จากด้านหน้าของชั้นวาง จัดตำแหน่งข้อต่อข้อต่อที่ ด้านหลังของรางสไลด์ใน U ที่เลือกไว้บนด้านหลังของชั้นวาง กดราง เพื่อให้ข้อเข้าไปอยู่ในรูและสไลด์ราง เข้าในชั้นวางเพื่อล็อคด้านหลังของรางสไลด์เข้าในชั้นวาง

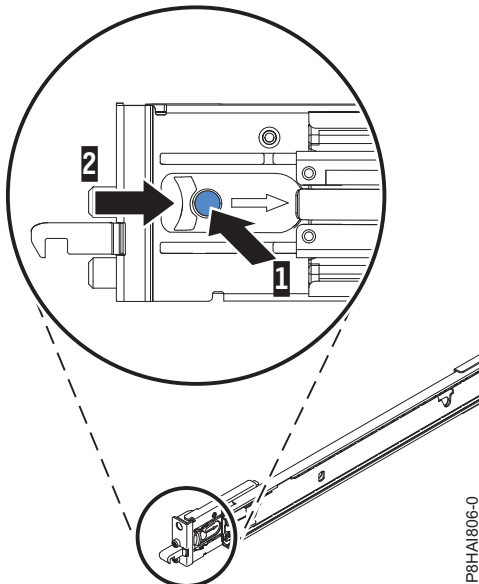


P8HA1805-0

รูปที่ 35. จัดตำแหน่งข้อภายในรูที่ด้านหลังของชั้นวาง

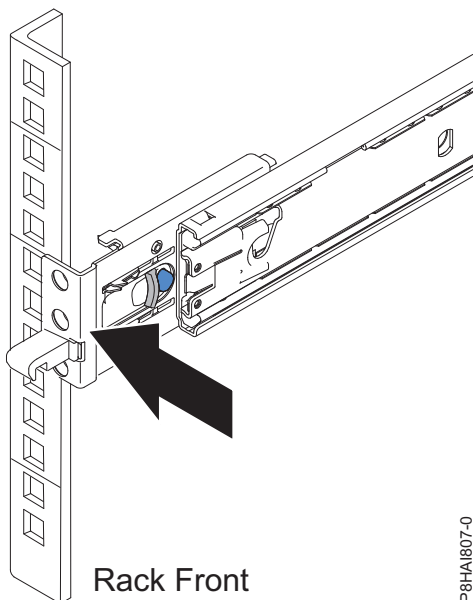
หมายเหตุ: ถ้าคุณกำลังติดตั้งรางสไลด์เข้าไปในพื้นที่ 1 U โดยมีอุปกรณ์ที่ติดตั้งไว้แล้วอยู่ต่อกันทางด้านบนและด้านล่าง พื้นที่ 1 U นี้คุณต้องขยายรางเพื่อสไลด์ด้านหลังของรางสไลด์เข้าไปด้านหลังของชั้นวาง

4. เปิดแลตซ์รางสไลด์ด้านหน้า ถ้าแลตซ์ปิดอยู่เมื่อ คุณได้รับ ให้เปิดแลตซ์โดยกดปุ่มสีน้ำเงินเข้า และ ดันแลตซ์ย้อนกลับ



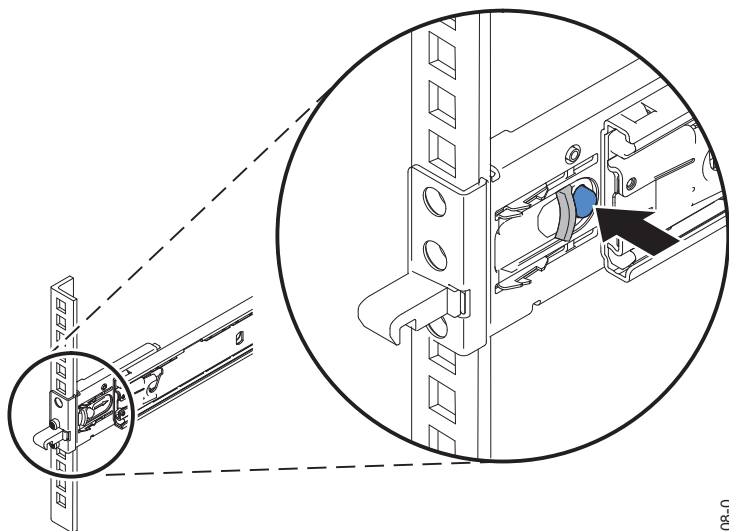
รูปที่ 36. แลตซ์รางสไลด์ด้านหน้า

5. ผลักรางสไลด์ไปข้างหน้า และจัดวางแลตซ์ด้านหน้า ในพื้นที่ U ซึ่งเหมาะสมที่ด้านหน้าของราง EIA ชั้นวาง ปรับ ความยาวของราง ตรวจสอบให้แน่ใจว่าปลายด้านหน้ามีการหมุน พร้อมกับแลตซ์ด้านหน้า ที่ด้านหน้าของราง EIA ของ ชั้นวาง



รูปที่ 37. รางและขั้ว ของชั้นวางด้านหน้า

6. กดปุ่มสีน้ำเงินเพื่อปิดตัวยึดเข้ากับขั้วย้ายรางสไลด์ขึ้นและลงเพื่อให้แน่ใจว่ารางทำงานได้อย่างเต็มที่ ทำซ้ำขั้นตอนที่ 1 - 5 เพื่อติดตั้งรางอื่นเข้าไปในชั้นวาง ตรวจสอบให้แน่ใจว่าแลตซ์ด้านหน้าแต่ละตัวทำงานได้อย่างเต็มที่

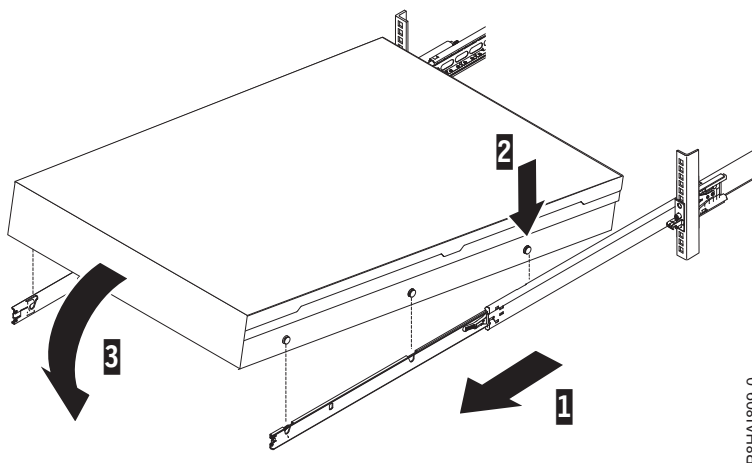


P8HA1808-0

Rack Front

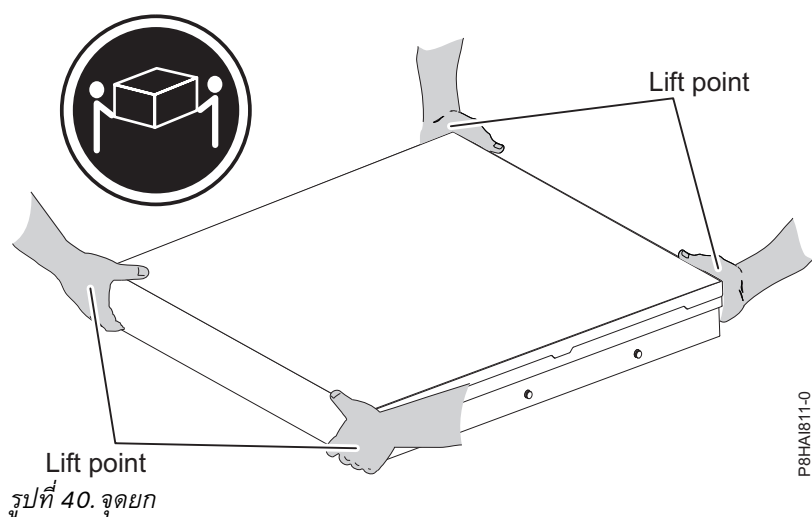
รูปที่ 38. รางและขั้ว ของชั้นวางด้านหน้า

7. ดึงรางแบบสไลด์ไปข้างหน้า (1) จนกว่าจะมาเสียงคลิกสองครั้งในตำแหน่ง ยกเซิร์ฟเวอร์ด้วยความระมัดระวัง และเอียงลงในตำแหน่งที่อยู่เหนือรางสไลด์ เพื่อให้หัวตะปูด้านหลัง (2) บน เซิร์ฟเวอร์อยู่ในแนวเดียวกับสล๊อตด้านหลังบนรางสไลด์ ลดระดับ เซิร์ฟเวอร์ลงจนกว่าหัวตะปูด้านหลังจะเข้าไปอยู่ในสล๊อตด้านหลังสองช่อง จากนั้น ลดระดับด้านหน้าของเซิร์ฟเวอร์ (3) จนกว่า หัวตะปูตัวอื่นจะเข้าไปอยู่ในสล๊อตอื่นบนรางสไลด์ (เมื่อ ได้ยินเสียงคลิกสองครั้ง) ตรวจสอบให้แน่ใจว่าแลตซ์ด้านหน้าปิด หัวตะปูด้านหน้า เพื่อรักษาความปลอดภัยของระบบในรางสไลด์



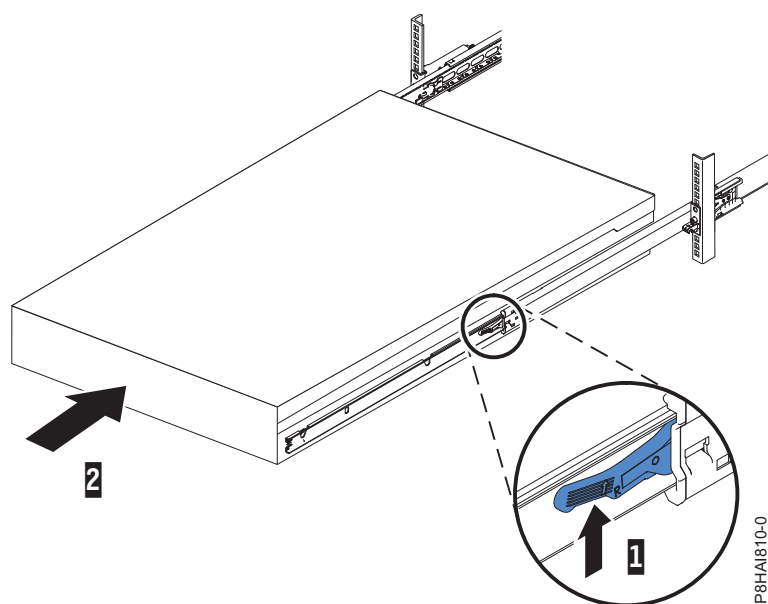
P8HA1809-0

รูปที่ 39. รางแบบสไลด์ที่ขยาย หัวตะปูของเซิร์ฟเวอร์ที่จัดตำแหน่งในแนวเดียวกับสล๊อตในราง

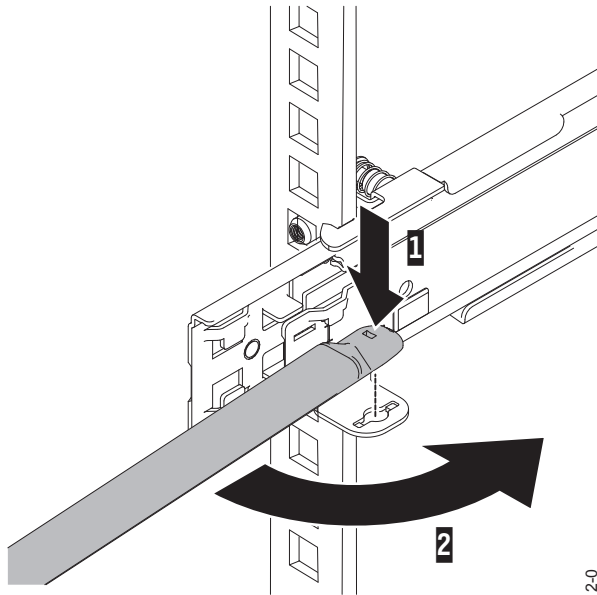


หมายเหตุ: ใช้วิธีปฏิบัติที่ปลอดภัยขณะยก ถ้าคุณกำลัง ติดตั้งเซิร์ฟเวอร์แบบ 2 U ตรวจสอบให้แน่ใจว่าคุณใช้สองคน เมื่อยก เซิร์ฟเวอร์ มือต้องอยู่ในตำแหน่งดังแสดงใน รูปที่ 40

8. ยกคานล้อชั้น (1) บน รางสไลด์ และผลักเซิร์ฟเวอร์ (2) ในทุกทิศทาง เข้าในชั้นวางจนกว่าจะได้ยินเสียงคลิกเข้าที่



9. แขนยึดสายเคเบิลสามารถติดตั้งบนด้านใดด้านหนึ่งของเซิร์ฟเวอร์รูปภาพต่อไปนี้แสดงการติดตั้งแขนยึดสายเคเบิล บนด้านซ้าย เมื่อต้องการติดตั้งแขนยึดสายเคเบิลทางด้านขวา ให้ทำตามคำสั่งและติดตั้งฮาร์ดแวร์ในทิศทางตรงกันข้าม เชื่อมต่อส่วนปลายสุดด้านหนึ่งของแขนยึด (1) เข้ากับรางแบบสไลด์ตัวเดียวกันกับที่คุณวางแผนที่จะยึดแขนยึดสายเคเบิล ดังนั้น คุณสามารถหมุนปลายสุดอีกด้านหนึ่งของแขนยึด (2) ไปทางด้านหน้าของชั้นวาง

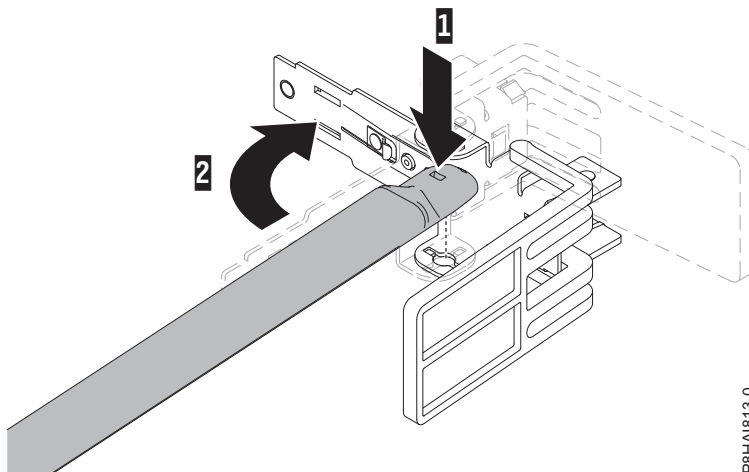


Rack Rear

รูปที่ 42. การเชื่อมต่อแขนยึด

P8HA1812-0

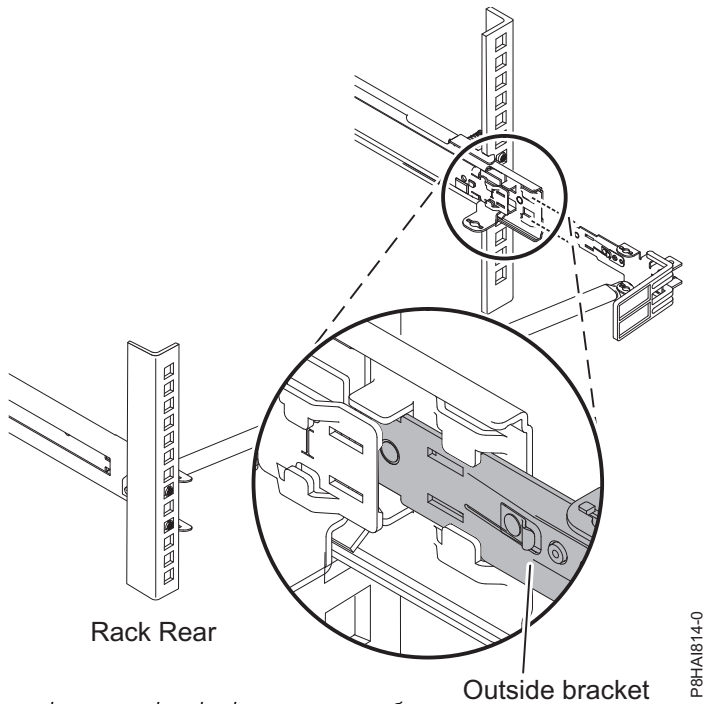
10. เชื่อมต่อปลายอีกด้านหน้าของแขนยึดเข้ากับที่หยุดการจัดการสายเคเบิล (1) เปิดแขนยึด (2) เพื่อยึดแขนยึดเข้ากับแขนยึด



รูปที่ 43. แขนยึดที่หยุดการยึดสายเคเบิล ซึ่งยึดกับแขนยึด

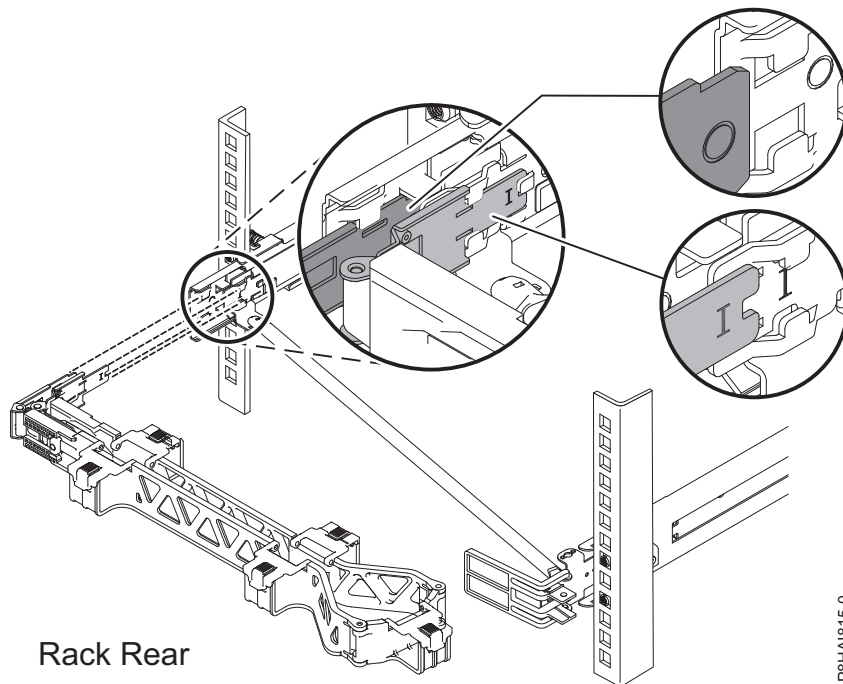
P8HA1813-0

11. มีการพิมพ์ตัวอักษรพิมพ์ใหญ่ I และ O บนหัวแขนยึดสายเคเบิล เพื่อระบุหัวด้านในและ ด้านนอก ติดตั้งที่หยุดการจัดการสายเคเบิล (ที่มีตัวอักษรพิมพ์ใหญ่ O) บนปลายที่ไม่ได้ติดตั้งของแขนยึด ตรวจสอบว่าติดตั้ง แขนยึดแน่นดีแล้ว



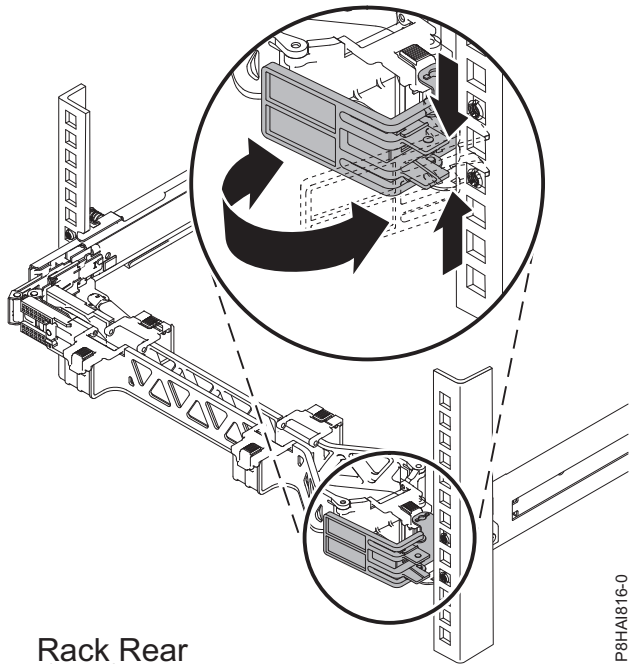
รูปที่ 44. การเชื่อมต่อที่หยุดกับรางสไลด์

12. วางแขนยึดสายเคเบิลบนแขนยึด ดึงข้อทั้งด้านในและด้านนอกของแขนยึดสายเคเบิลออกจากนั้น สไลด์แท็บแขนยึดสายเคเบิลเข้าในสล็อตทั้งด้านใน และด้านนอกของรางสไลด์ ผลักแท็บจนกว่าจะเข้าตำแหน่ง



รูปที่ 45. การเชื่อมต่อแขนยึดสายเคเบิล

13. เพื่อให้หมุนแขนยึดสายเคเบิลเข้าและออกจาก แขนค้ำการจัดการสายเคเบิลได้ง่ายขึ้น คุณสามารถเปิดที่หยุด โดยการ ผลักแท็บให้สูงกว่าและต่ำกว่าที่หยุดเพื่อปิด

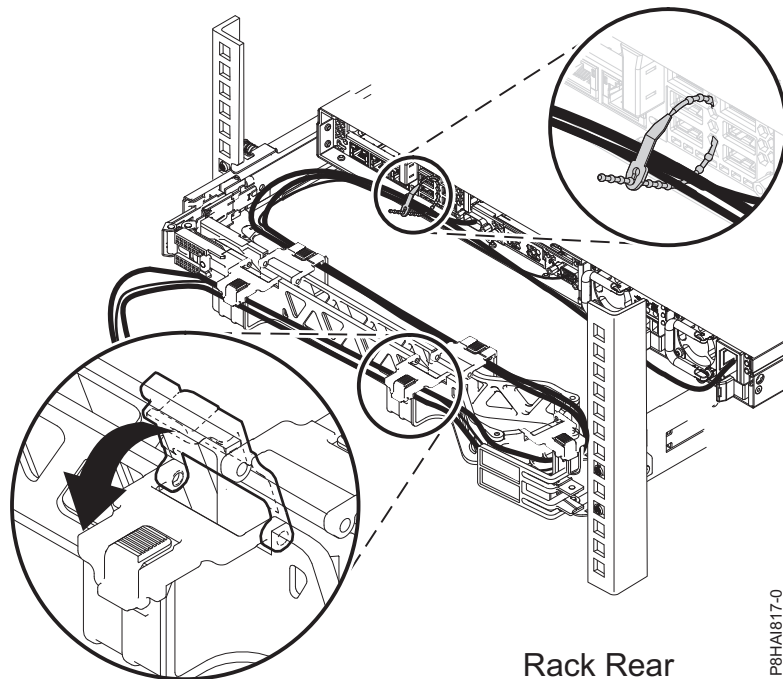


Rack Rear

รูปที่ 46. ที่หยุดแขนยึดสายเคเบิล

14. ยึดสายไฟและสายเคเบิลเข้ากับด้านหลังของเซิร์ฟเวอร์ (ซึ่งรวมถึงคีย์บอร์ด จอมอนิเตอร์ และสายเมาส์ ตามต้องการ) จัดเส้นทางสายเคเบิลและสายไฟบนแขนยึดสายเคเบิล และยึดสายเหล่านั้น ด้วยสายผูกเคเบิล หรือรัดด้วยสายรัด

หมายเหตุ: ตำแหน่ง ของตัวมัดสายเคเบิลอาจแตกต่างกันเล็กน้อยในแต่ละ ระบบ ใช้ตัวมัดสายเคเบิลที่จัดเตรียมไว้ที่ด้านหลังของ ระบบ เพื่อรักษาสายเคเบิลและป้องกันไม่ให้หย่อน

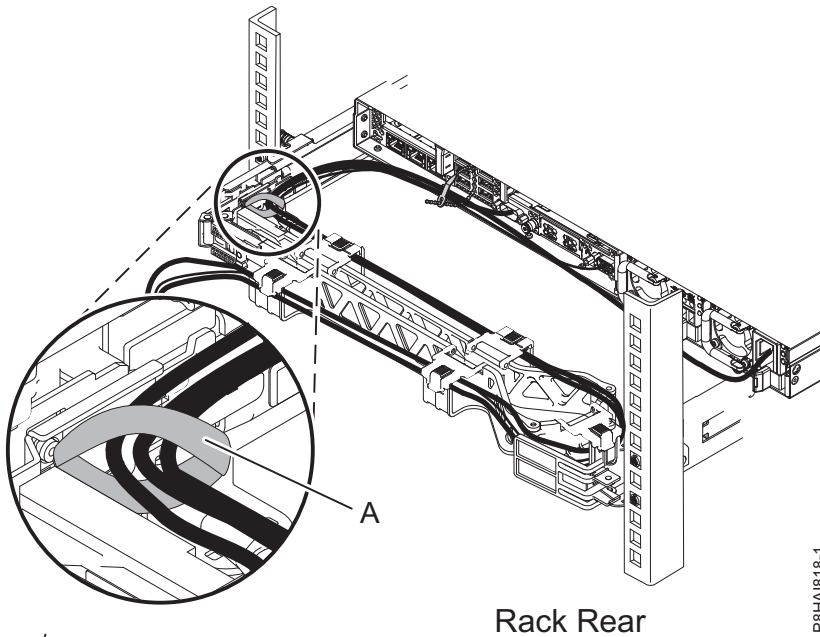


Rack Rear

รูปที่ 47. การยึดสายไฟและการจัดเส้นทางสายเคเบิล

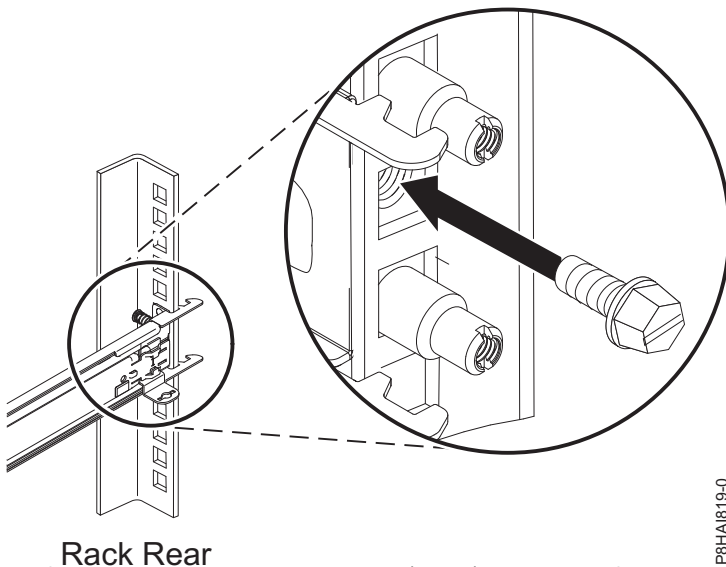
15. ต้มมัดสายเคเบิลโดยใช้ตัวรัดเพื่อให้ แขนยึดสายเคเบิลเคลื่อนย้ายได้อย่างถูกต้อง

หมายเหตุ: ตรวจสอบให้แน่ใจว่าสายเคเบิลไม่หย่อนต่ำกว่าพื้นที่ B เพื่อไม่ให้ไปติดขัด บนระบบที่ต่ำกว่าอนุญาตให้หย่อนสายเคเบิลทั้งหมดเพื่อไม่ให้สายเคเบิลตึงเกินไปตามการย้ายแขนยึดสายเคเบิล



รูปที่ 48. ตัวรัด

16. ถ้าคุณกำลังจัดตั้งชั้นวางที่มีการติดตั้งระบบไว้หรือถ้าคุณอยู่ในพื้นที่ซึ่งเสี่ยงต่อการสั่นสะเทือนให้ใช้สกรู M6 ที่ด้านหลังของสไลด์ใช้ตัวมัดสายเคเบิลเพื่อยึดปลายที่อิสระของ แขนยึดสายเคเบิลเข้ากับชั้นวาง ถ้าจำเป็น



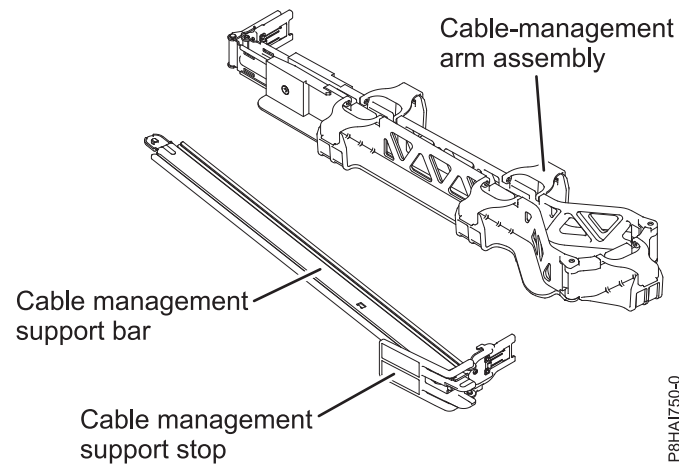
รูปที่ 49. การรักษาความปลอดภัยของ เชีรฟ์เวอร์สำหรับการจัดตั้ง

การติดตั้ง 7042-CR9 HMC ลงในชั้นวาง

ศึกษาเกี่ยวกับวิธีติดตั้ง 7042-CR9 Hardware Management Console (HMC) ลงในชั้นวาง

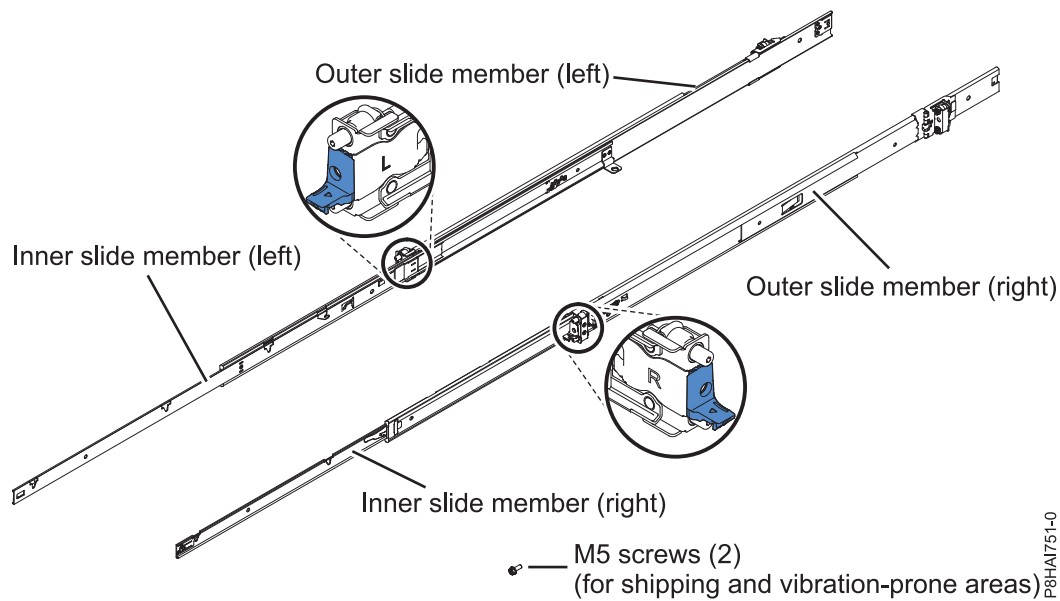
ทำรายการชิ้นส่วนให้เสร็จสิ้น รูปประกอบต่อไปนี้ แสดงไอเท็มที่คุณต้องติดตั้งเซิร์ฟเวอร์ในตู้ชั้นวาง ถ้ารายการใดๆ หายไป หรือเกิดความเสียหาย โปรดติดต่อสถานที่ที่คุณซื้อ

Cable Management Arm box contents



รูปที่ 50. ส่วนประกอบของกล่องแขนยึดสายเคเบิล

Rail box contents

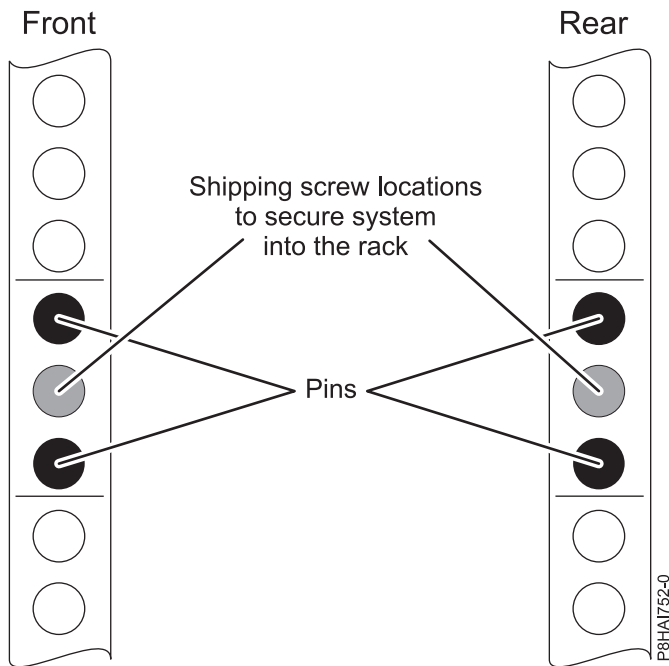


รูปที่ 51. ส่วนประกอบของกล่องราง

หมายเหตุ: คุณต้องใช้ทั้งกล่องรางสไลด์และกล่องแขนยึดสายเคเบิลสำหรับการติดตั้งนี้

เมื่อต้องการติดตั้ง 7042-CR9 HMC ลงในชั้นวาง ให้ทำตามขั้นตอน ต่อไปนี้:

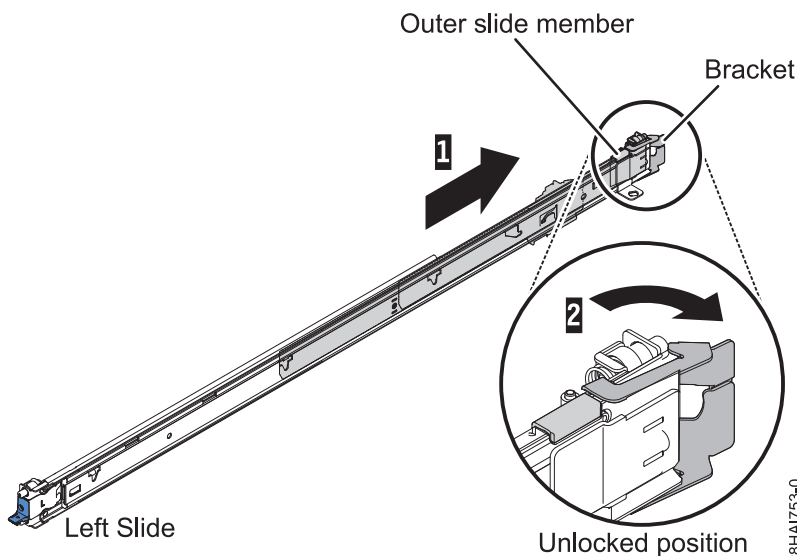
1. เลือกพื้นที่ว่าง (ขึ้นอยู่กับเซิร์ฟเวอร์ที่คุณ กำลังติดตั้ง) ในชั้นวางเพื่อติดตั้งเซิร์ฟเวอร์ของคุณ



รูปที่ 52. การระบุพื้นที่ว่างของชั้นวาง

หมายเหตุ: คุณต้องการ 1 ยูนิต (1 U) ของพื้นที่ว่าง และติดตั้งรางสไลด์ที่ยูนิตด้านล่าง (U) ของยูนิตของพื้นที่ 1

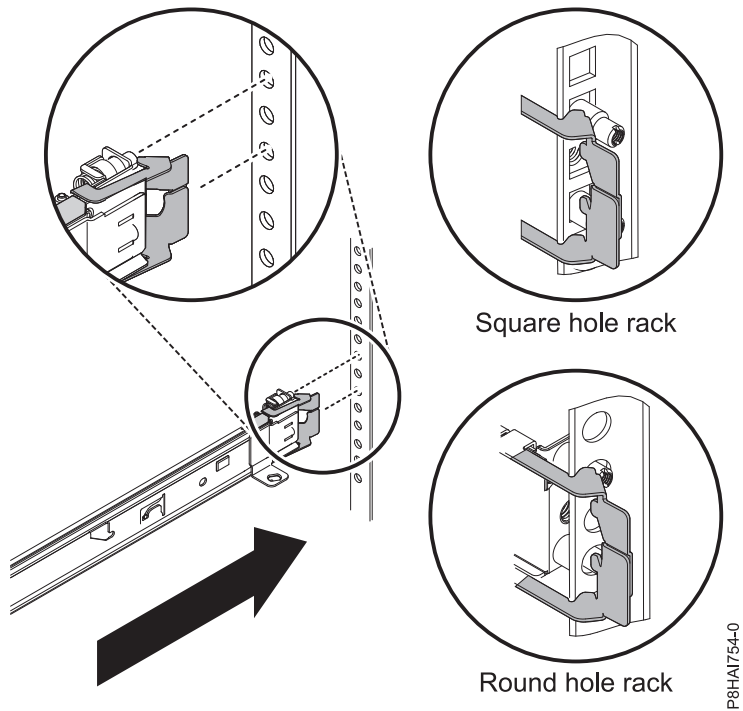
2. ขยายชิ้นส่วนหลักของสไลด์ที่อยู่รอบนอกกลับเข้าที่จนกว่าคุณจะได้ยินเสียงคลิก จากยึดประกอบเข้ากับชั้นวางด้านหลัง จะถูกหมุนไปยังตำแหน่งที่ไม่ได้ล็อก



รูปที่ 53. รางสไลด์และชิ้นส่วนหลักของสไลด์ที่อยู่รอบนอก

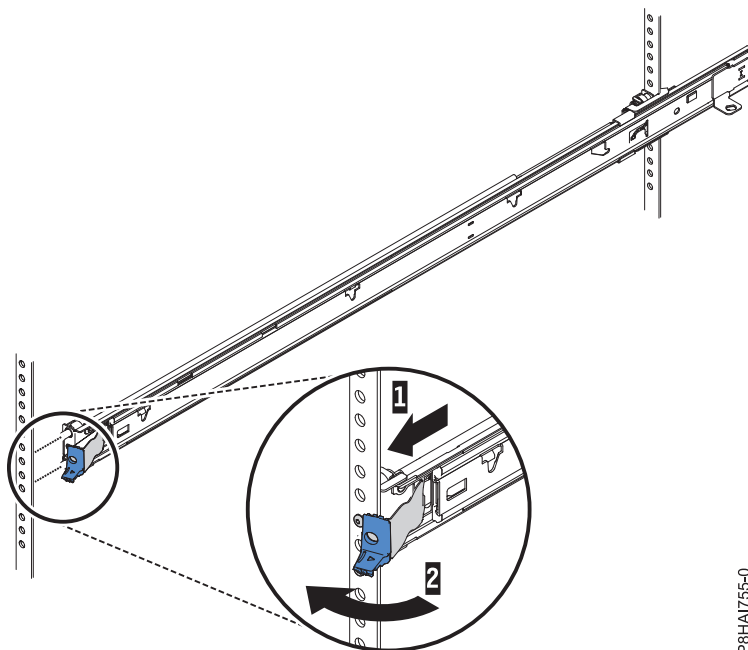
หมายเหตุ: รางสไลด์แต่ละราง มีเครื่องหมาย R (ด้านขวา) หรือ L (ด้านซ้าย) ที่ส่วนปลาย

3. จัดตำแหน่งชิ้นส่วนหลักของสไลด์ที่อยู่รอบนอกให้ชิดกับรูบนชั้นวางด้านหลัง เปรียงหมุดและปลั๊กสไลด์ให้ลงหมุด ดังนั้น หมุดจะลงไปยังรู หมุดสไลด์สองตัวจะยื่นผ่านรูด้านบน และด้านล่างบนปีก EIA ปลั๊กสไลด์ ไปทางด้านหลังของชั้นวางจนกว่าจากยึดประกอบเข้ากับชั้นวางด้านหลัง จะล็อกอยู่ในตำแหน่ง



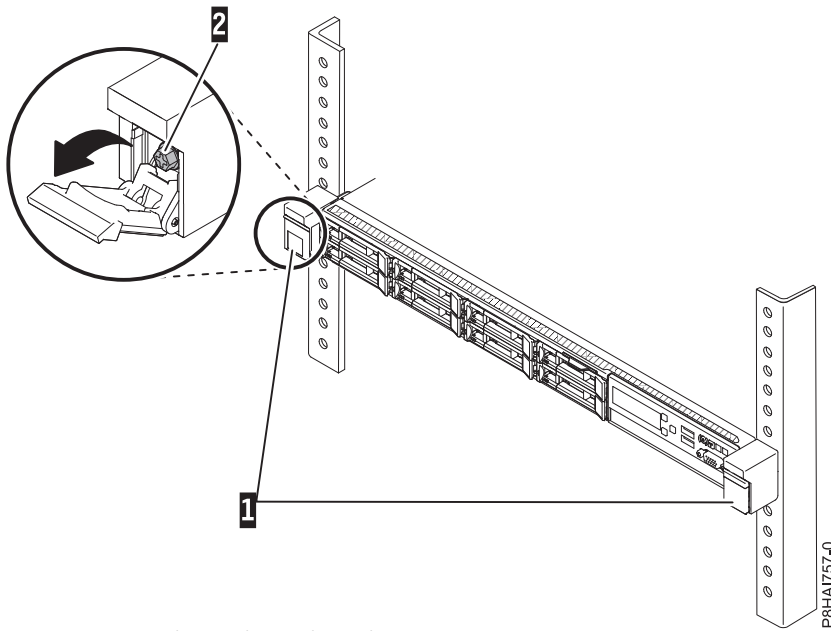
รูปที่ 54. จัดตำแหน่งขั้วภายในรู ที่ด้านหลังของชั้นวาง

4. หมุนสลักด้านหน้าไปยังตำแหน่งเปิด และจัดตำแหน่งส่วนปลายด้านหน้าของชิ้นส่วนหลักของสไลด์ที่อยู่รอบนอกให้ชิดกับรูบนชั้นวางด้านหน้า เรียงหมุดให้อยู่ในระดับเดียวกับรูในปีก EIA และดึงสไลด์ไปข้างหน้า ดังนั้น หมุดจะยื่นผ่านรูล็อกด้านหน้าของสไลด์โดยหมุนสลักด้านหน้า ไปยังตำแหน่งปิด ทำซ้ำขั้นตอนที่ 2-4 สำหรับชิ้นส่วนหลักของสไลด์ที่อยู่รอบนอกอื่นๆ



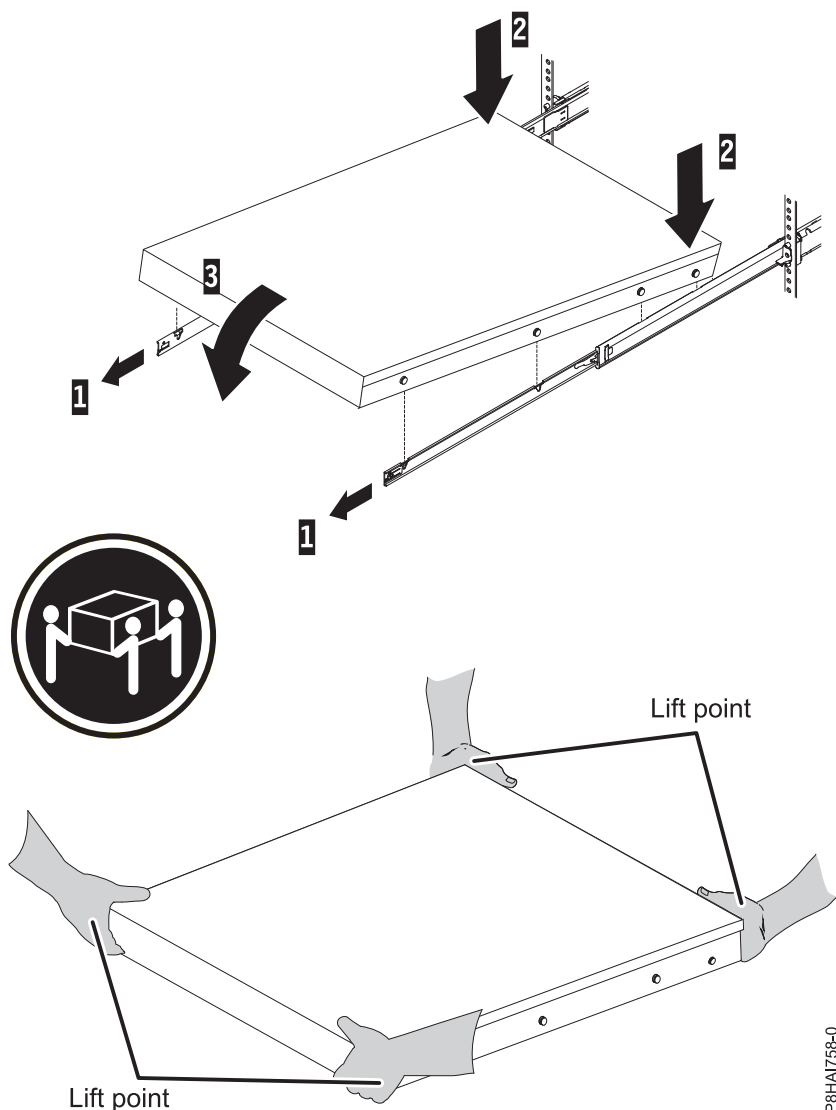
รูปที่ 55. แลตซ์รางสไลด์ด้านหน้า

5. กดปุ่มปลดสลัก (1) เมื่อคุณย้ายตู้ชั้นวาง หรือถ้าคุณติดตั้งตู้ชั้นวางในพื้นที่ที่มีการสั่นสะเทือน ให้ขันสกรู M5 (2) ในด้านหน้าของเซิร์ฟเวอร์



รูปที่ 56. รางและขา ของชั้นวางด้านหน้า

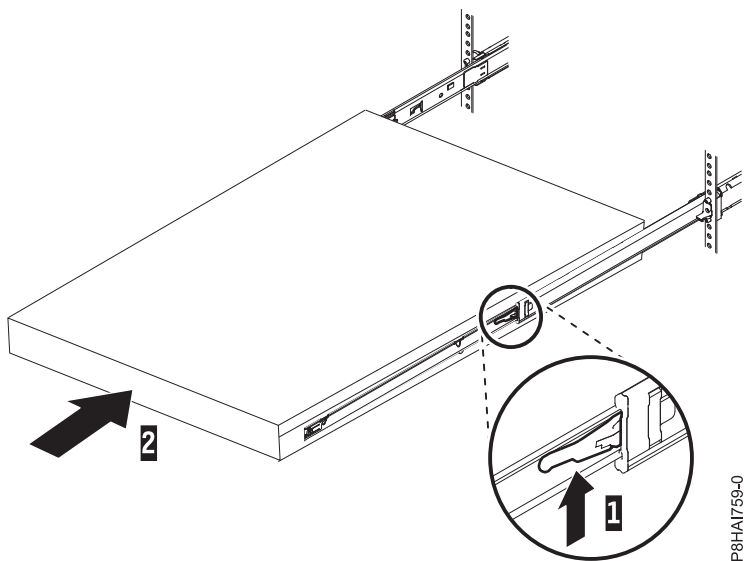
6. ดึงรางแบบสไลด์ไปข้างหน้า (1) จนกว่าจะมาเสียงคลิกสองครั้งในตำแหน่ง ยกเซิร์ฟเวอร์ด้วยความระมัดระวัง และเอียงลงในตำแหน่งที่อยู่เหนือรางสไลด์เพื่อให้หัวตะปูด้านหลัง (2) บนเซิร์ฟเวอร์เรียงตรงตามช่องในรางสไลด์ ยกเซิร์ฟเวอร์ลง จนกว่าหัวตะปูด้านหลังจะเลื่อนสองช่องด้านหลัง จากนั้นค่อยๆ ยกเซิร์ฟเวอร์ด้านหน้าลง (3) จนกว่าหัวตะปูตัวอื่นลงไปยังรูอื่นๆ บนรางสไลด์ ตรวจสอบให้แน่ใจว่า สลักด้านหน้าคลุมหัวตะปูด้านหน้า ดังนั้น ระบบจะถูกยึดอยู่ในรางสไลด์อย่างมั่นคง



รูปที่ 57. รางสไลด์ที่ขยายเพิ่ม หัวตะปูของเซิร์ฟเวอร์ที่จัดตำแหน่งให้ตรงกับช่องในราง และจุดยก

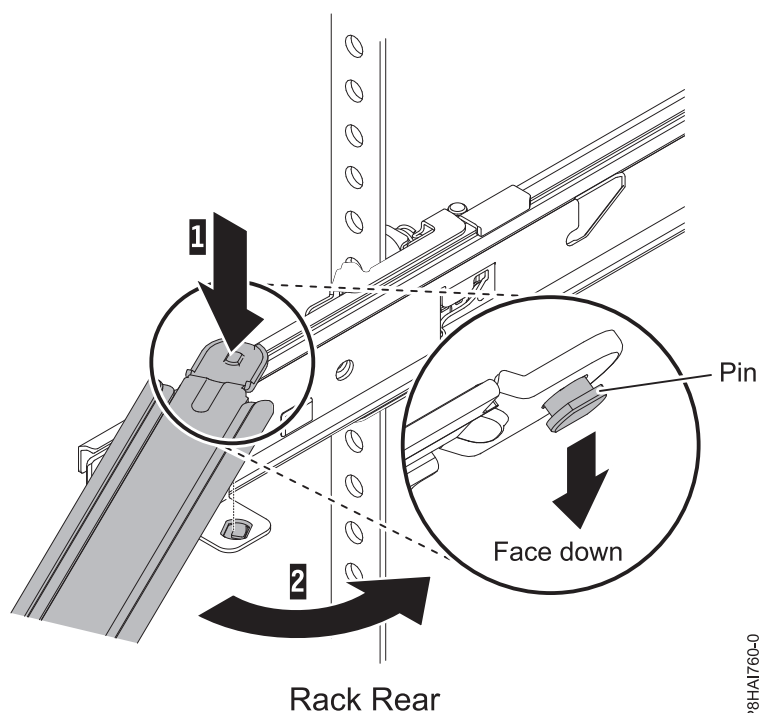
หมายเหตุ: ใช้วิธีปฏิบัติที่ปลอดภัยขณะยก ถ้าคุณกำลังติดตั้งเซิร์ฟเวอร์ 1 U ให้มั่นใจว่า คุณใช้คนสองคนเมื่อคุณยกเซิร์ฟเวอร์ มือต้องอยู่ในตำแหน่งดังแสดงใน รูปที่ 57

7. ยกคานล้อขึ้น (1) บน รางสไลด์ และผลักเซิร์ฟเวอร์ (2) ในทุกทิศทาง เข้าในชั้นวางจนกว่าจะได้ยินเสียงคลิกเข้าที่



รูปที่ 58. ปล่อยแพลตฟอร์มและเชิร์ฟเวอร์

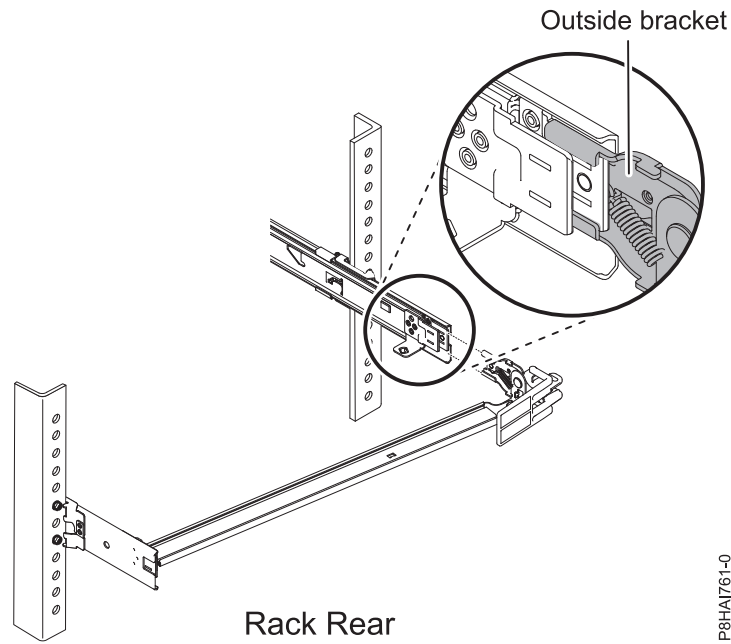
8. แขนยึดสายเคเบิลสามารถติดตั้งบนด้านใดด้านหนึ่งของเชิร์ฟเวอร์รูปที่ 59 แสดงการติดตั้งแขนยึดสายเคเบิลด้านซ้าย วิธีการที่ดีที่สุดคือ การติดตั้งแขนยึดสายเคเบิลเพื่อให้พบไปยังด้านตรงข้ามกับแหล่งจ่ายไฟ เพื่อให้เข้าถึงแหล่งจ่ายไฟ เมื่อต้องการติดตั้งแขนยึดสายเคเบิลทางด้านขวา ให้ทำตามคำสั่งและติดตั้งฮาร์ดแวร์ในทิศทางตรงกันข้าม วางมุม (1) ลงในช่องแนวนอนที่ด้านหลังของรางสไลด์ จากนั้น หมุนส่วนปลายอื่นๆ ของแท่งไปทางขึ้นวาง (2) ไปทางขึ้นวาง



รูปที่ 59. การเชื่อมต่อแขนยึด

หมายเหตุ: แท่งยึดสายเคเบิลต้องอยู่ด้านบนของแผ่นสไลด์ เพื่อให้ทำงานได้อย่างถูกต้อง

9. ติดตั้งที่หยุดการจัดการสายเคเบิล (ที่มีตัวอักษรพิมพ์ใหญ่ O) บนปลายที่ไม่ได้ติดตั้งของแขนยึด ตรวจสอบว่าติดตั้งแขนยึดแน่นดีแล้ว

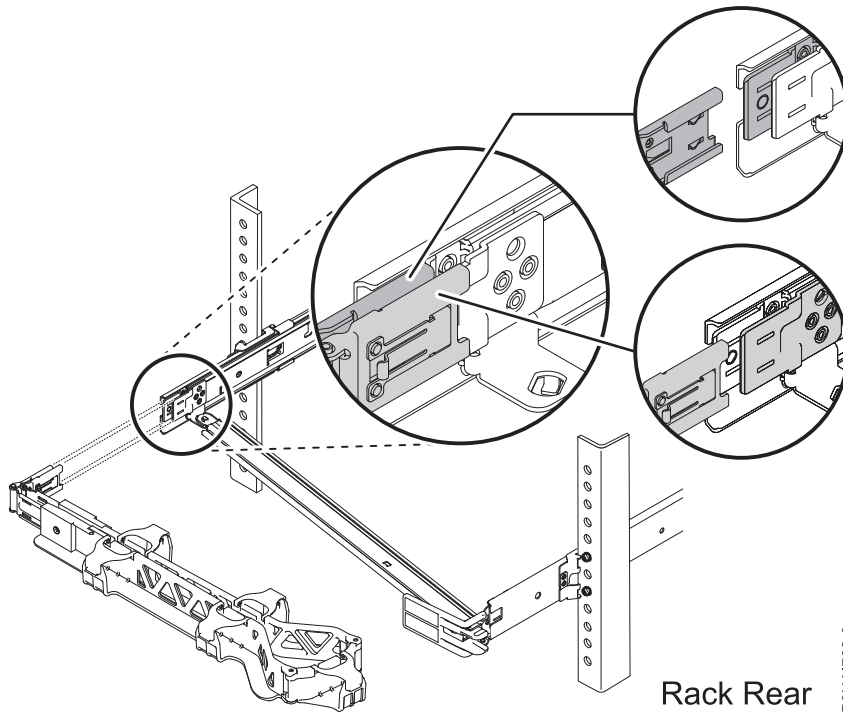


P8HA761-0

รูปที่ 60. การเชื่อมต่อที่หยุดกับรางสไลด์

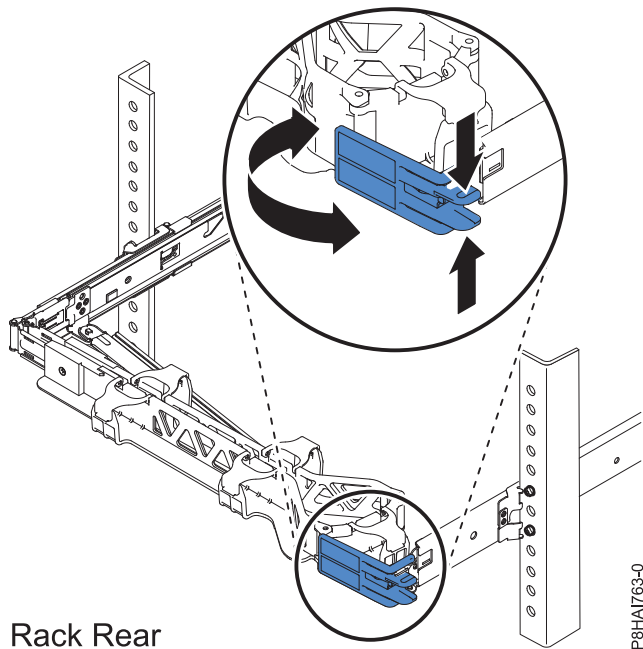
หมายเหตุ: มีตัวอักษรตัวพิมพ์ใหญ่ O อยู่บนหมดแขนยึดสายเคเบิลเพื่อระบุหมุดที่อยู่ด้านนอก

10. วางแขนยึดสายเคเบิลบนแขนยึด สไลด์ แท็บแขนยึดสายเคเบิลไปทางด้านในและนอกของช่อง ของรางสไลด์ ผลักแท็บจนกว่าจะเข้าตำแหน่ง



รูปที่ 61. การเชื่อมต่อแขนยึดสายเคเบิล

11. เพื่อให้ง่ายต่อการหมุนแขนยึดสายเคเบิลเข้าและออกจากแขนค้ำสำหรับชุดสายเคเบิล คุณสามารถเปิดฉากยึดปิด โดยผลักแท็บขึ้นด้านบนและลงด้านล่างแขนยึด

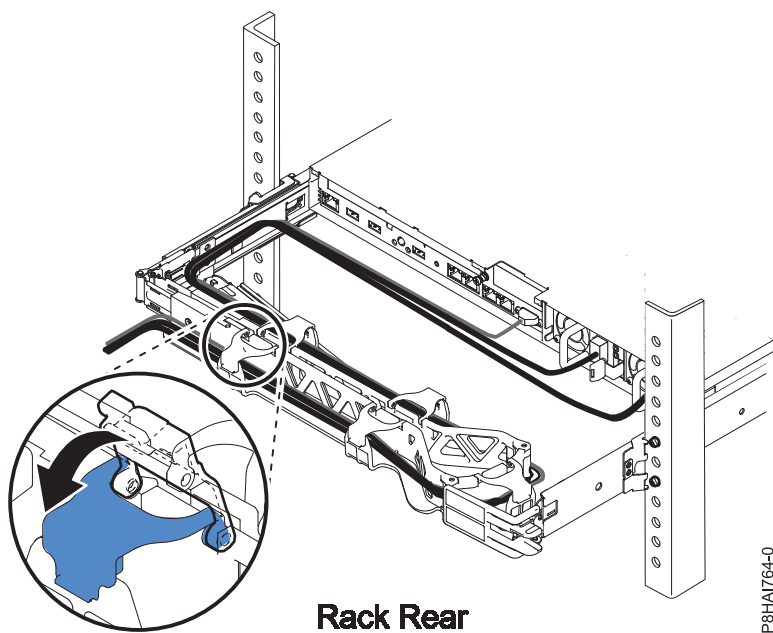


Rack Rear

รูปที่ 62. ที่หยุดแขนยึดสายเคเบิล

12. ยึดสายไฟและสายเคเบิลเข้ากับด้านหลังของเซิร์ฟเวอร์ (ซึ่งรวมถึงคีย์บอร์ด จอมอนิเตอร์ และสายเมาส์ ตามต้องการ) จัดเส้นทางสายเคเบิลและสายไฟบนแขนยึดสายเคเบิล และยึดสายเหล่านั้น ด้วยสายผูกเคเบิล หรือรัดด้วยสายรัด

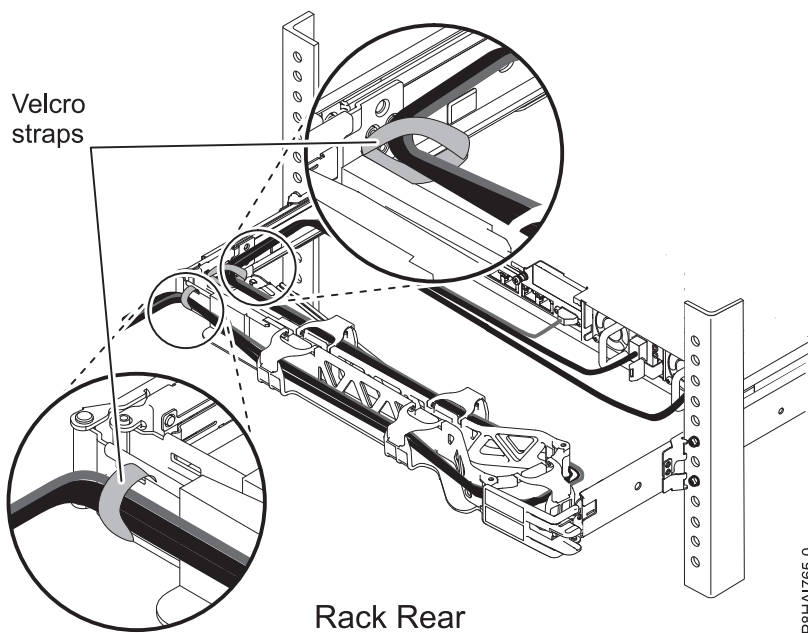
หมายเหตุ: ตำแหน่งของตัวมัดสายเคเบิลอาจแตกต่างกันเล็กน้อยในแต่ละระบบ ใช้ตัวมัดสายเคเบิลที่จัดเตรียมไว้ที่ด้านหลังของระบบ เพื่อรักษาสายเคเบิลและป้องกันไม่ให้หย่อน



รูปที่ 63. การพ่วงต่อสาย Power และการจัดเส้นทางสายเคเบิล

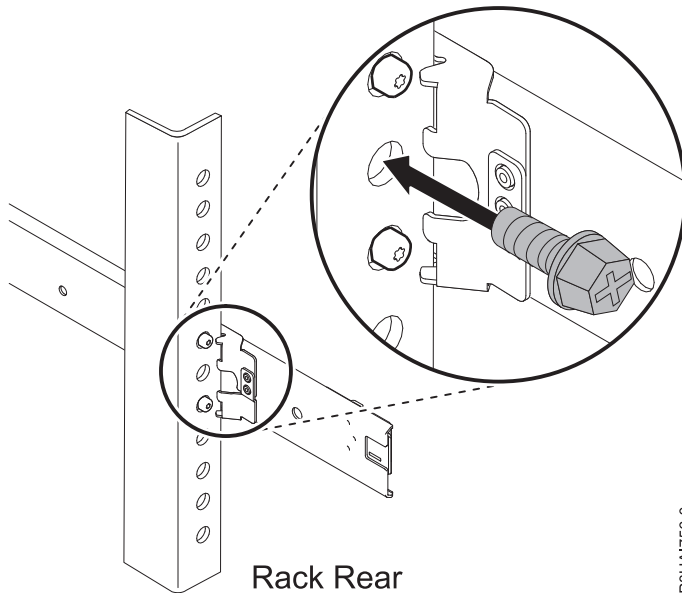
13. สายเคเบิลต้องถูกมัดด้วยตัวรัดสายเคเบิลเพื่อให้การเคลื่อนที่ของ แขนยึดสายเคเบิลเป็นไปอย่างเหมาะสม

หมายเหตุ: ตรวจสอบให้แน่ใจว่าสายเคเบิลไม่หย่อนต่ำกว่าพื้นที่ B เพื่อไม่ให้ไปติดขัด บนระบบที่ต่ำกว่า อนุญาตให้หย่อนสายเคเบิลทั้งหมดเพื่อให้สายเคเบิลตึงเกินไปตามการย้ายแขนยึดสายเคเบิล



รูปที่ 64. ตัวรัด

14. ถ้าคุณกำลังจัดตั้งชั้นวางพร้อมกับการติดตั้งระบบ หรือถ้าคุณอยู่ในพื้นที่ที่มีการสั่นสะเทือน ให้เพิ่มสกรู M5 ที่ด้านหลังของสไลด์ ใช้ตัวมัดสายเคเบิลเพื่อยึดปลายที่อิสระของ แขนยึดสายเคเบิลเข้ากับชั้นวาง ถ้าจำเป็น



รูปที่ 65. การรักษาความปลอดภัยของเซิร์ฟเวอร์สำหรับการจัดตั้ง

การติดตั้ง 7063-CR1 ในชั้นวาง

เรียนรู้วิธีติดตั้ง 7063-CR1 Hardware Management Console (HMC) ในชั้นวาง

สิ่งที่จำเป็นต้องมีสำหรับการติดตั้งระบบ 7063-CR1 บนชั้นวาง

ใช้ข้อมูลเพื่อทำความเข้าใจกับสิ่งที่จำเป็นต้องมีที่จำเป็นสำหรับการติดตั้ง ระบบ

คุณอาจต้องอ่านเอกสารต่อไปนีก่อนคุณ ติดตั้งเซิร์ฟเวอร์:

- เวอร์ชันล่าสุดของเอกสารนี้จะถูกเก็บไว้แบบออนไลน์โปรดดู การติดตั้ง 7063-CR1 ลงในชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER8/p8hai/p8hai_install7063_kickoff.htm)
- เพื่อวางแผนการติดตั้งเซิร์ฟเวอร์ของคุณ โปรดดูที่ การวางแผนสำหรับระบบ (http://www.ibm.com/support/knowledgecenter/POWER8/p8had/p8had_8xx_kickoff.htm)

ตรวจสอบให้แน่ใจว่า คุณมีรายการต่อไปนี้ก่อนที่จะเริ่มต้นการติดตั้ง:

- ไขควง Phillips
- ไขควงหัวแบน
- ที่ตัดกล่อง
- สายรัดข้อมือป้องกันไฟฟ้าสถิต (ESD)
- ชั้นวางที่มียูนิต Electronic Industries Association (EIA) สองชุด (2U) ของพื้นที่

หมายเหตุ: หากคุณไม่ได้ติดตั้งชั้นวาง ให้ติดตั้งชั้นวาง สำหรับคำแนะนำ โปรดดูที่ ชั้นวางและคุณสมบัติชั้นวาง (http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/p8hbf_8xx_kickoff.htm).

การจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ

ใช้ข้อมูลนี้เพื่อจัดทำรายการชิ้นส่วนสำหรับระบบของคุณ

1. ตรวจสอบว่า คุณได้รับกล่องทั้งหมดที่คุณได้สั่งซื้อไว้
2. นำส่วนประกอบของเซิร์ฟเวอร์ออก เท่าที่จำเป็น
3. จัดทำรายการชิ้นส่วนก่อนที่คุณจะติดตั้งส่วนประกอบของชิ้นส่วน แต่ละชิ้นโดยทำตามขั้นตอนต่อไปนี้:
 - a. ทารายการชิ้นส่วนสำหรับเซิร์ฟเวอร์ของคุณ
 - b. ตรวจสอบให้แน่ใจว่า คุณจะได้รับชิ้นส่วนทั้งหมดที่คุณต้องการสั่งซื้อ

หมายเหตุ: ข้อมูลการสั่งซื้อของคุณ มาพร้อมกับผลิตภัณฑ์ของคุณ คุณยังสามารถขอรับข้อมูลการสั่งซื้อได้จากตัวแทนฝ่ายการตลาดของคุณ หรือ IBM Business Partner

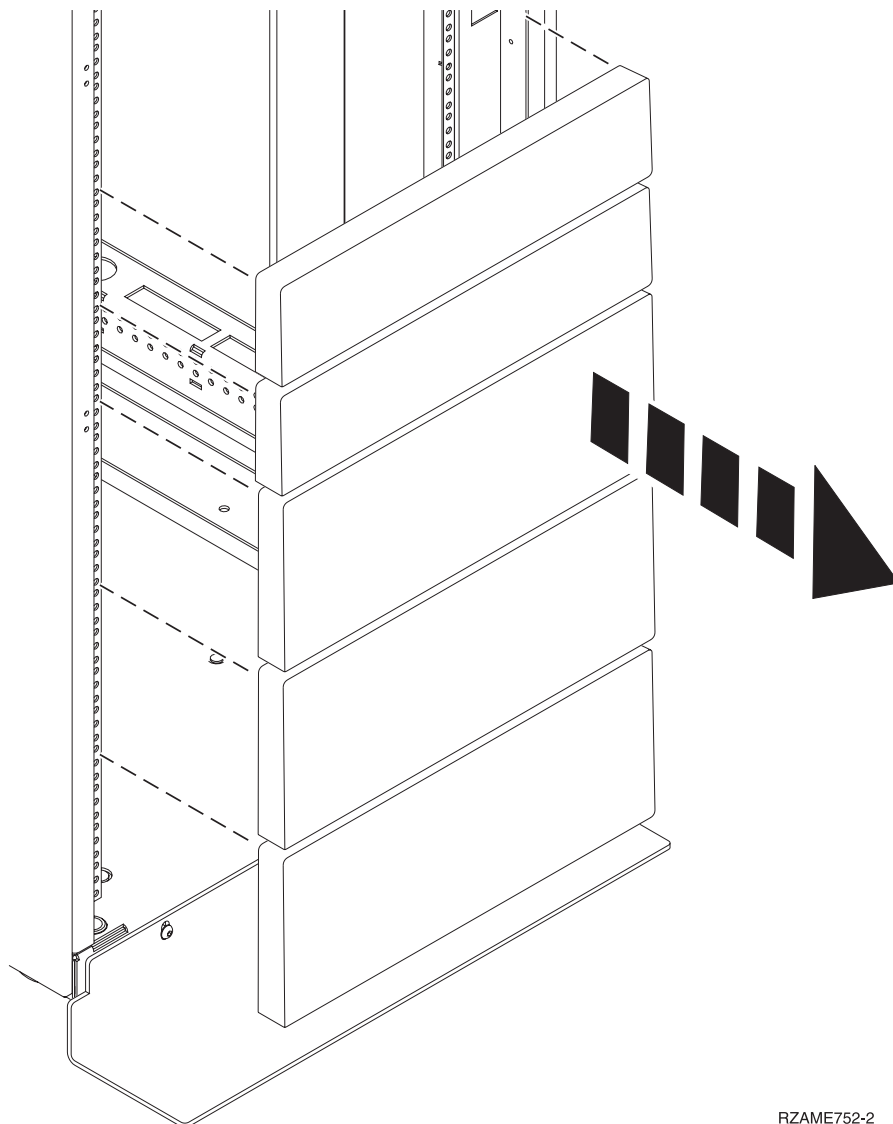
หากคุณได้รับชิ้นส่วนที่ไม่ถูกต้อง ชิ้นส่วนที่หายไป หรือชิ้นส่วนที่เสียหาย ให้ติดต่อรีซอร์สใดๆ ต่อไปนี้:

- ตัวแทนจำหน่าย IBM ของคุณ
- สายข้อมูลอัตโนมัติเกี่ยวกับการผลิต IBM Rochester ที่หมายเลข 1-800-300-8751 (สหรัฐอเมริกาเท่านั้น)
- เว็บไซต์ไคเร็กทอรีของผู้ติดต่อทั่วโลก <http://www.ibm.com/planetwide> เลือกตำแหน่งของคุณเพื่อดูข้อมูลผู้ติดต่อฝ่ายสนับสนุนและบริการ

การกำหนดและทำเครื่องหมายตำแหน่งในชั้นวางสำหรับระบบ 7063-CR1

คุณอาจจำเป็นต้องกำหนดตำแหน่งที่ต้องติดตั้งยูนิตระบบลงในชั้นวาง

1. อ่าน Rack safety notices (<http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/racksafety.htm>).
2. กำหนดตำแหน่งที่ต้องการวาง ยูนิตระบบในชั้นวาง เนื่องจากคุณวางแผนติดตั้งยูนิตระบบในชั้นวาง ให้พิจารณาข้อมูลต่อไปนี้:
 - จัดวางยูนิตที่มีขนาดใหญ่และหนัก ลงในส่วนล่างของชั้นวาง
 - วางแผนการติดตั้งยูนิตลงในส่วนล่างของชั้นวาง เป็นอันดับแรก
 - บันทึกตำแหน่ง Electronic Industries Alliance (EIA) ในแผนงานของคุณ
3. หากจำเป็น ให้ถอดพาเนลฟิลเลอร์เพื่ออนุญาตให้เข้าถึงด้านในกล่องหุ้ม ซึ่งเป็นตำแหน่งที่คุณวางแผนที่จะวางยูนิตตามที่แสดงอยู่ใน รูปที่ 66 ในหน้า 48.



RZAME752-2

รูปที่ 66. การถอดพาเนลฟิลเลอร์

4. กำหนดที่จะวางระบบในชั้นวางบันทึกตำแหน่ง EIA
5. หันหน้าเข้าหาชั้นวางและทำงานจากด้านขวา ใช้เทป ปากกาทำเครื่องหมาย หรือดินสอ เพื่อทำเครื่องหมายที่รูด้านล่างของยูนิต EIA แต่ละตัว
6. ทำซ้ำขั้นตอน 5 สำหรับรูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
7. ไปที่ด้านหลังของชั้นวาง
8. ที่ด้านขวาให้หา ยูนิต EIA ที่ตรงกับยูนิต EIA ด้านล่างซึ่งทำเครื่องหมายอยู่บนด้านหน้าของชั้นวาง
9. ทำเครื่องหมายที่ยูนิต EIA ด้านล่าง
10. ทำเครื่องหมายรูที่สอดคล้องกันซึ่งอยู่ทางด้านซ้ายของชั้นวาง

การติดตั้ง HMC ลงในชั้นวางโดยใช้รางยึด

หากคุณกำลังติดตั้ง 7063-CR1 HMC ในชั้นวางโดยใช้รางติดกับที่ให้ดำเนินการงานต่อไปนี้

48 ระบบพลังงาน: การติดตั้งและตั้งค่า Hardware Management Console

การยึดรางกับโครงเครื่องและยึดกับชั้นวาง:

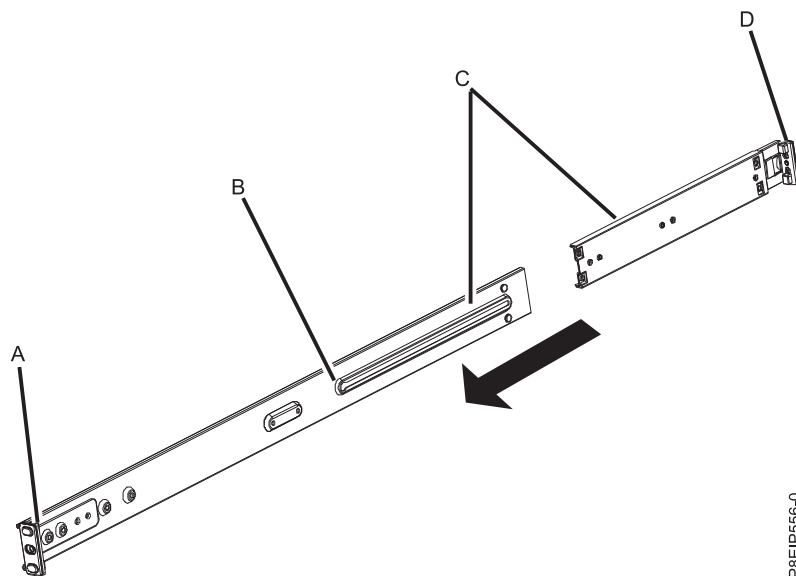
คุณต้องติดตั้งรางบนโครงเครื่องและยึดกับชั้นวาง ใช้วิธีการนี้ เพื่อดำเนินการกับภารกิจนี้

ข้อควรสนใจ: เพื่อหลีกเลี่ยงความล้มเหลวของราง และอันตรายที่จะเกิดขึ้นกับตัวคุณและกับยูนิต ตรวจสอบให้แน่ใจว่า คุณมีรางและอุปกรณ์เชื่อมต่อที่ถูกต้อง สำหรับชั้นวางของคุณ หากชั้นวางของคุณมีช่องหน้าแปลนค้ำรูปสี่เหลี่ยม หรือช่องหน้าแปลนค้ำแบบสกรูเกลียว ตรวจสอบให้แน่ใจว่า รางและอุปกรณ์เชื่อมต่อตรงกับช่องหน้าแปลนค้ำที่ไซบน ชั้นวางของคุณ ห้ามติดตั้งฮาร์ดแวร์ที่ไม่ตรงกันโดยใช้แหวนรอง หรือแผ่นรองกันระยะ หากคุณไม่มีรางและอุปกรณ์ต่อเชื่อม ที่ถูกต้องสำหรับชั้นวางของคุณ ให้ติดต่อตัวแทนจำหน่าย IBM ของคุณ

หมายเหตุ: ระบบต้องการพื้นที่ว่างยูนิตชั้นวาง 1 EIA (1U)

ตรวจสอบว่า คุณมีชิ้นส่วนที่จำเป็นเพื่อติดตั้งราง ชิ้นส่วนต่อไปนี้ ถูกรวมกับชุดของราง:

- สกรูสำหรับรางสไลด์ใช้เพื่อยึดชิ้นส่วนสองชิ้นของรางสไลด์แต่ละชิ้น
 - สกรูสำหรับชั้นวางรางสไลด์ใช้เพื่อยึดรางกับชั้นวาง
 - ราง
 - สกรู 10 - 32 x 0.635 ซม. (0.25 นิ้ว) ใช้เพื่อยึดรางกับโครงเครื่อง
1. ถอดส่วนของรางออกจากแพ็คเกจและวางลงบนพื้นที่งาน
 2. เชื่อมต่อชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวางแต่ละชิ้น เมื่อต้องการเชื่อมต่อชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวาง ให้ดำเนินการดังต่อไปนี้:
 - a. ระบุชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวางด้านซ้าย จัดตำแหน่งชิ้นส่วนที่สั้นและชิ้นส่วนที่ยาว (C) ตรวจสอบให้แน่ใจว่า หมุดสำหรับรางชั้นวางอยู่ในตำแหน่งเดียวกับ (A) และ (D)



- b. ชิ้นส่วนที่สั้นกว่าของรางสไลด์ชั้นวางจะมีหมุดโลหะอยู่ใหมุดลงในช่องที่อยู่ในชิ้นส่วนที่ยาวกว่า ของรางสไลด์ชั้นวาง (B) เลื่อนชิ้นส่วนที่สั้นกว่าของรางชั้นวางเข้าไปในชิ้นส่วนที่ยาวกว่า ของรางชั้นวาง
- c. จัดตำแหน่งช่องโหลในชิ้นส่วนสองชิ้นของรางสไลด์ชั้นวาง ใช้ไขควงหัว Philips ยึดชิ้นส่วนสองชิ้นโดยคลายสกรูรางสองตัวผ่านช่องในรางสไลด์ชั้นวาง

หมายเหตุ: ห้ามขันสกรูรางสไลด์ชั้นวางให้แน่น

- d. ทำซ้ำขั้นตอนเหล่านี้สำหรับรางสไลด์ด้านขวา
3. ยึดรางโครงเครื่องกับโครงเครื่อง เมื่อต้องการยึดรางโครงเครื่องกับโครงเครื่องให้ดำเนินการดังต่อไปนี้:
 - a. ที่ด้านซ้ายของระบบ ให้จัดตำแหน่งแท็บโลหะบนโครงเครื่องด้านซ้ายให้ตรงกับ ช่องสี่เหลี่ยมบนรางสไลด์โครงเครื่องด้านซ้าย เลื่อนรางสไลด์โครงเครื่องไปยังด้านหน้าของชั้นวาง จนกว่ารางสไลด์โครงเครื่องล็อกอยู่ในตำแหน่ง
 - b. ยึดรางสไลด์โครงเครื่องกับโครงเครื่องโดยขันสกรูสองตัวที่จัดเตรียมไว้ในชุดราง
 - c. ทำซ้ำสำหรับรางเลื่อนของโครงเครื่องทางด้านขวาของระบบ
4. ติดตั้งรางสไลด์ชั้นวางลงในชั้นวาง
 - a. ย้ายไปยังด้านหน้าของชั้นวาง
 - b. เลือกรางสไลด์ชั้นวางด้านซ้าย และหาชนิด EIA ที่คุณได้ทำเครื่องหมายไว้ก่อนหน้านี้ รางสไลด์แต่ละด้าน ยังถูกทำเครื่องหมาย Back เพื่อกำหนดด้านหลังของชั้นวาง ตรวจสอบให้แน่ใจ คุณกำลังยึดจุดปลายด้านหน้าของ รางสไลด์ชั้นวาง
 - c. ขยายรางจากด้านหน้าของชั้นวางไปทางด้านหลังของชั้นวาง และจัดตำแหน่งมุมรางสไลด์ชั้นวางให้ตรงกับช่องในหน้าแปลนชั้นวางที่คุณได้ทำเครื่องหมายไว้ก่อนหน้านี้
 - d. ดันมุมรางชั้นวางลงในหน้าแปลนชั้นวางด้านหลังจนกว่าแลตซ์รางชั้นวางด้านหลัง ล็อกอยู่ในตำแหน่ง
 - e. ดึงด้านหน้าของรางชั้นวางไปทางด้านหน้าของหน้าแปลนรางชั้นวาง จัดตำแหน่งมุมรางสไลด์ให้ตรงกับช่องในหน้าแปลนราง และดึงจนกว่าแลตซ์รางสไลด์จะล็อกอยู่ในตำแหน่ง
 - f. ใช้ไขควงเพื่อขันสกรูรางที่คุณติดตั้งในขั้นตอนที่ 2 ให้แน่น
 - g. ทำซ้ำขั้นตอนที่ 4a – 4f สำหรับรางเลื่อนด้านขวา
5. ยึดรางกับชั้นวาง
 - a. ย้ายไปยังด้านหลังของชั้นวาง
 - b. สไลด์แหวนรองแต่ละชิ้นไปทางสกรูที่ยาวกว่าซึ่งรวมอยู่ในชุดราง
 - c. ขันสกรูและแหวนรองผ่านช่องกลางของรางแต่ละชิ้นในแต่ละด้านของด้านหลัง ของชั้นวาง

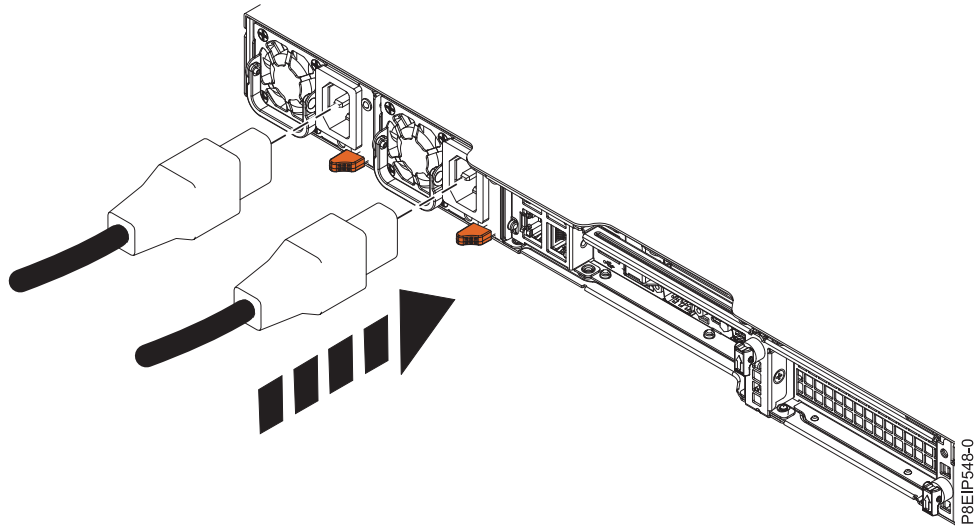
การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ:

หลังจากที่คุณติดตั้งระบบลงในชั้นวางแล้ว ให้เชื่อมต่อและวางสายเคเบิล แหล่งจ่ายไฟ

หมายเหตุ: ระบบนี้ต้องการคนสองคนเพื่อติดตั้งลงในชั้นวาง

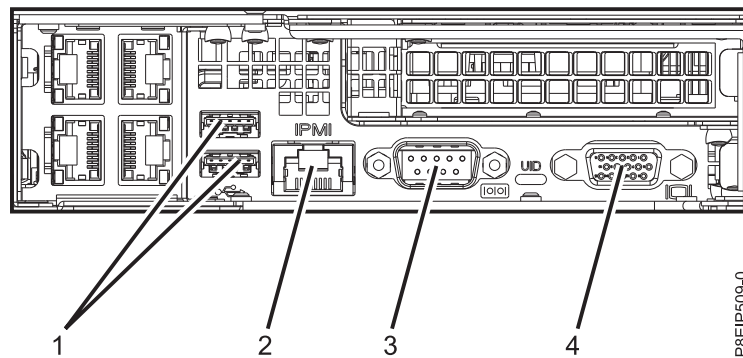
1. ถอดฟิล์มพลาสติกเคลือบออกจากด้านบนโครงเครื่องของระบบ
2. ย้ายไปยังด้านหน้าของชั้นวาง
3. ใช้คนสองคนยกระบบและจัดตำแหน่งรางของโครงเครื่องของระบบบนแต่ละด้านของโครงเครื่องให้ลงรางสไลด์ ของชั้นวาง
4. ขณะที่คนหนึ่งกำลังรับน้ำหนักของระบบอยู่ให้อีกคนหนึ่งค่อยๆ ผลักระบบ ลงในชั้นวาง จนกว่าคุณจะได้ยินเสียงคลิกจากรางสไลด์แต่ละด้านที่ล็อกอยู่ในตำแหน่ง
5. ผลักระบบไปทางด้านหลังของชั้นวางจนกว่าระบบจะอยู่ในตำแหน่ง
6. ยึดระบบกับชั้นวางด้วยการหมุนสกรูผ่านทางด้ามจับบนแต่ละด้าน ของโครงระบบ

7. เสียบสายไฟเข้ากับแหล่งจ่ายไฟ



รูปที่ 67. การเสียบสายไฟเข้ากับแหล่งจ่ายไฟ

8. แนบสายเคเบิลทั้งหมดที่ด้านหลังของเซิร์ฟเวอร์



รูปที่ 68. พอร์ตด้านหลัง

ตารางที่ 9. พอร์ตอินพุตและเอาต์พุต

หมายเลข ID	คำอธิบาย
1	USB 2.0 ใช้สำหรับคีย์บอร์ดและเมาส์
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Serial IPMI
4	Video Graphics Array (VGA) ที่ใช้สำหรับมอนิเตอร์เฉพาะค่าติดตั้ง 1024 x 768 ที่ 60 Hz VGA เท่านั้นที่สนับสนุน สนับสนุนสายเคเบิลสูงสุด 3 เมตรเท่านั้น สนับสนุนความสามารถแบบอิงข้อความเท่านั้น ณ เวลานี้

9. เสียบสายไฟของระบบและสายไฟสำหรับอุปกรณ์พ่วงต่ออื่นๆ เข้ากับแหล่งจ่ายไฟกระแสสลับ (AC)

10. ดำเนินการต่อด้วย “การกำหนดค่า HMC โดยใช้อินเทอร์เฟซ HMC Enhanced+” ในหน้า 133

การติดตั้ง HMC ลงในชั้นวางโดยใช้รางสไลด์

หากคุณกำลังติดตั้ง HMC ลงในชั้นวางโดยใช้รางสไลด์ให้ทำตาม การกิจต่อไปนี้

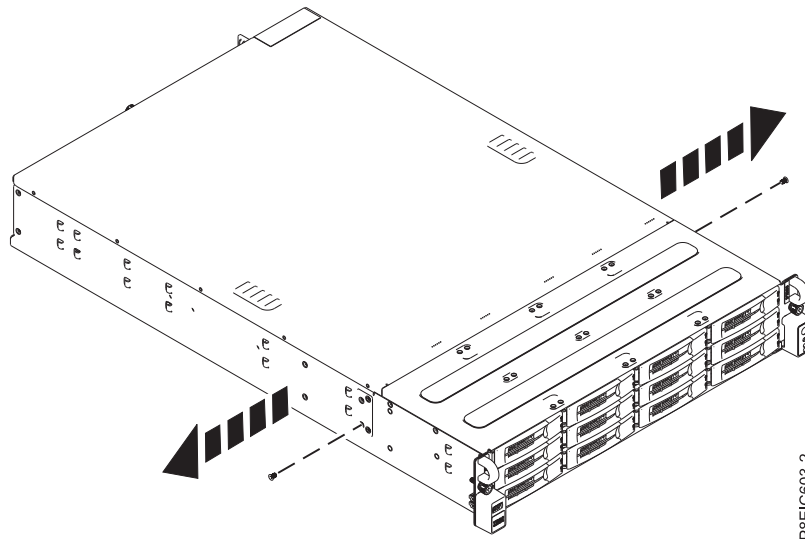
การติดตั้งรางสไลด์กับระบบและชั้นวาง:

ติดตั้งรางสไลด์กับระบบ จากนั้นติดตั้งกับชั้นวาง

ข้อควรสนใจ: เพื่อหลีกเลี่ยงความล้มเหลวของราง และอันตรายที่จะเกิดขึ้นกับตัวคุณและกับยูนิต ตรวจสอบให้แน่ใจว่า คุณมีรางและอุปกรณ์เชื่อมต่อที่ถูกต้อง สำหรับชั้นวางของคุณ หากชั้นวางของคุณมีช่องหน้าแปลนค้ำรูปสี่เหลี่ยม หรือช่องหน้าแปลนค้ำแบบสกรูเกลียว ตรวจสอบให้แน่ใจว่า รางและอุปกรณ์เชื่อมต่อตรงกับช่องหน้าแปลนค้ำที่ใช้น ชั้นวางของคุณ ห้ามติดตั้งฮาร์ดแวร์ที่ไม่ตรงกันโดยใช้แหวนรอง หรือแผ่นรองกันระยะ หากคุณไม่มีรางและอุปกรณ์ต่อเชื่อม ที่ถูกต้องสำหรับชั้นวางของคุณ ให้ติดต่อตัวแทนจำหน่าย IBM ของคุณ

รางสไลด์จะมาพร้อมกับส่วนประกอบที่ประกอบแล้วอย่างครบถ้วน เมื่อต้องการติดตั้งรางสไลด์ลงในชั้นวาง คุณต้องถอดรางสไลด์ออกเป็นสี่ชิ้น

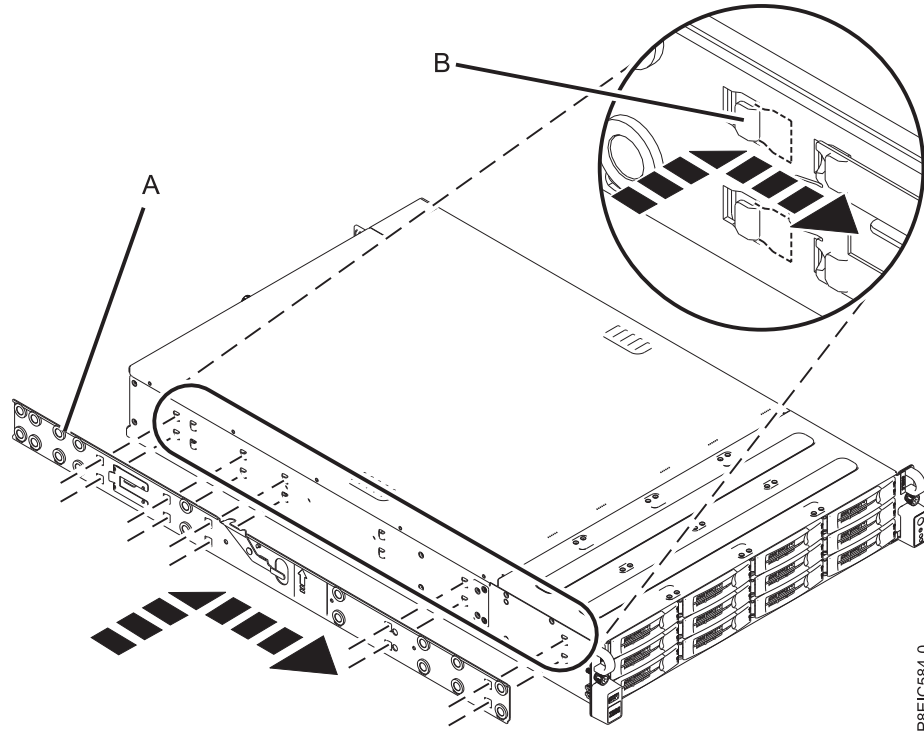
1. ถอดสกรูแบ็คเพลนของ direct-access storage device (DASD) ด้านล่างบนแต่ละด้านออกเพื่อให้คุณ สามารถให้บริการแบ็คเพลนได้ในวันหลังโดยไม่ต้องถอดระบบออกจากชั้นวาง



รูปที่ 69. การถอดสกรูแบ็คเพลน DASD

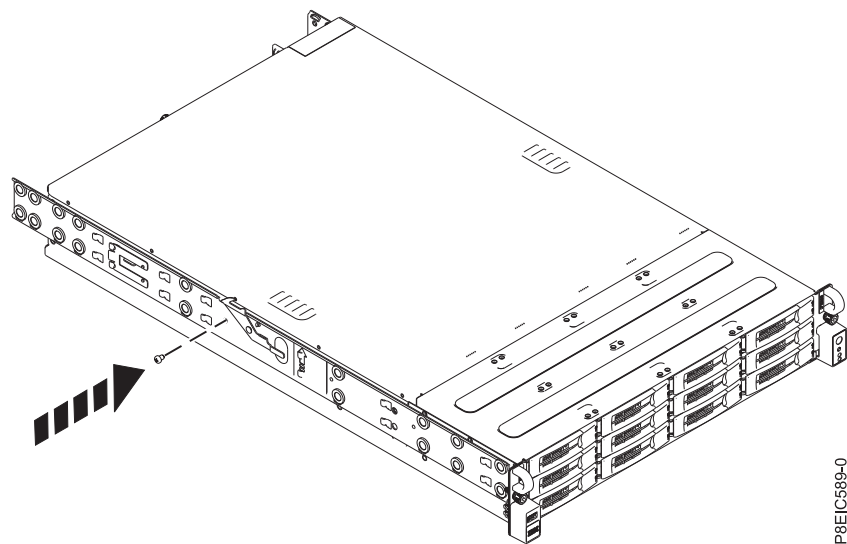
2. ยึดรางสไลด์โครงเครื่องกับโครงเครื่องแต่ละด้าน ที่ด้านหลังของโครงเครื่อง จัดตำแหน่งแท็บบนโครงเครื่อง (B) ให้ตรงกับสล๊อตบนรางสไลด์ (A) กดรางสไลด์ตัวเครื่องไปข้างหน้าเพื่อให้ยึดอยู่ในตำแหน่ง

หมายเหตุ: รางระบบถูกทำเครื่องหมายด้วย L เพื่อกำหนดรางระบบด้านซ้าย และทำเครื่องหมายด้วย R เพื่อกำหนดรางระบบด้านขวาจากด้านหน้าของระบบ



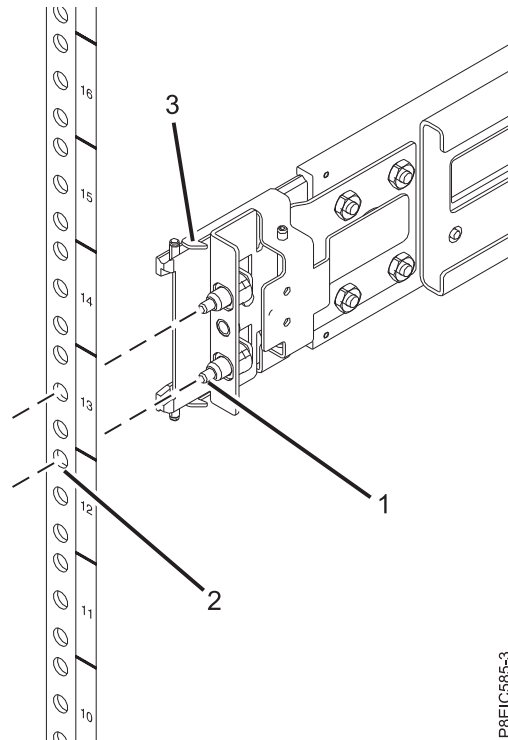
รูปที่ 70. การติดตั้งเส้นเข้ากับโครงเครื่องทางด้านซ้ายของระบบ

3. ติดตั้งสกรูยึดบนรางสไลด์โครงเครื่องแต่ละด้านเพื่อติดตั้งรางสไลด์ กับโครงเครื่องเพิ่มเติม



รูปที่ 71. การติดตั้งสกรูยึดรางเข้ากับโครงเครื่องทางด้านซ้ายของระบบ

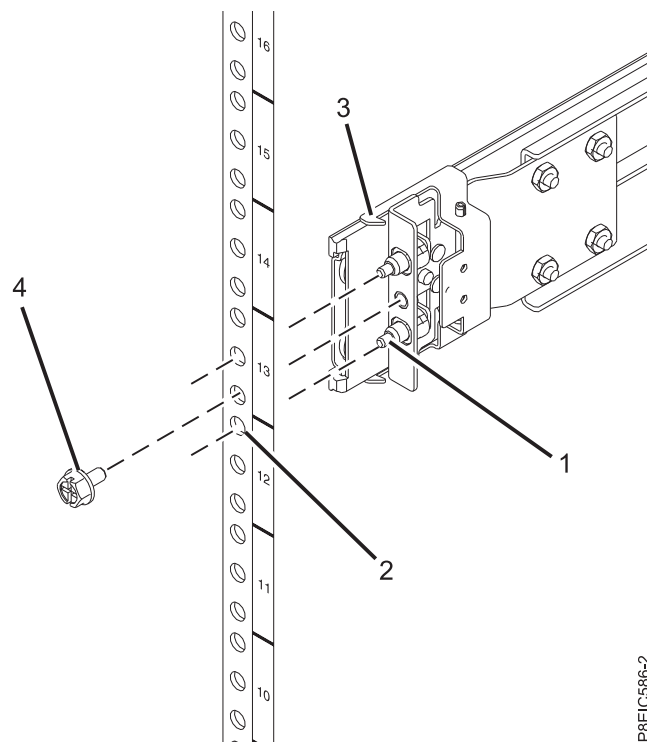
4. ถัดไปให้ติดตั้งรางสไลด์ชั้นวางลงในชั้นวาง รางสไลด์ชั้นวางแต่ละชั้นถูกทำเครื่องหมายด้วย R (ขวา) หรือ L (ซ้าย) เมื่อคุณมองจากด้านหน้า เลือกรางสไลด์ด้านขวา นำรางสไลด์ไปที่ด้านหน้าของชั้นวาง และหาตำแหน่งยูนิต EIA ที่เลือกไว้
5. จากด้านหน้าของชั้นวาง ให้ใส่หมุดที่ด้านหน้าของรางสไลด์ (1) ลงในช่องที่ด้านหน้าของชั้นวางซึ่งคุณได้ทำเครื่องหมาย (2) ไว้ก่อนหน้านี้ ดึงรางสไลด์ไปเพื่อให้คลิปสตรึงราง (3) ยึดกับหน้าแปลนของรางและล็อกอยู่ในตำแหน่ง



P8EIC585-3

รูปที่ 72. การติดตั้งรางสไลด์จากด้านหน้าของชั้นวาง

6. ทำซ้ำขั้นตอนที่ 3 และ 4 สำหรับรางสไลด์ด้านซ้าย
7. ย้ายไปยังด้านหลังของชั้นวาง ดึงรางสไลด์เข้าหาคุณเพื่อใส่หมุด (1) สองตัวลงในช่องของชั้นวาง (2) ดึงรางสไลด์จนกว่าคลิปสตริงของราง (3) ล็อกอยู่ในตำแหน่ง ติดตั้งสกรู (4) เพื่อยึดรางสไลด์กับชั้นวาง



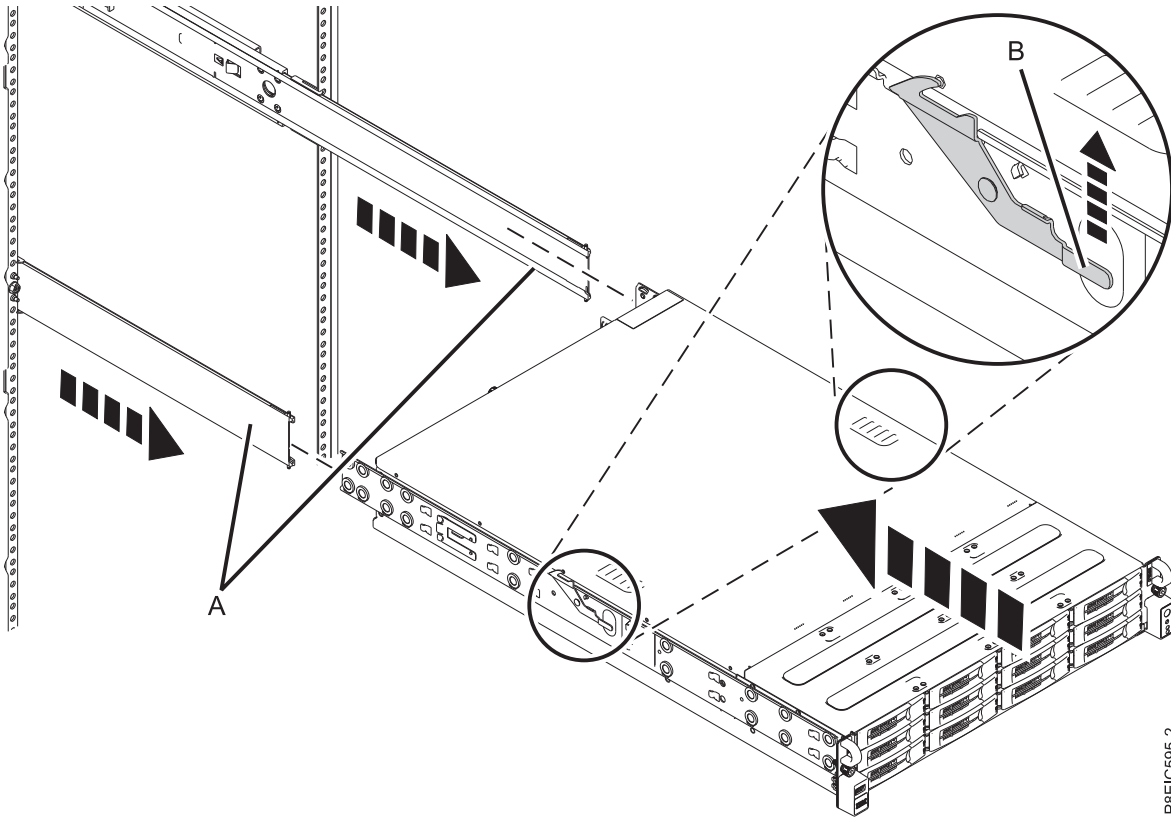
รูปที่ 73. การติดตั้งรางสไลด์ที่ด้านหลังของชั้นวาง

การติดตั้งระบบลงในชั้นวางและเชื่อมต่อและวางสายเคเบิลแหล่งจ่ายไฟ:

หลังจากที่คุณติดตั้งระบบลงในชั้นวางแล้ว ให้เชื่อมต่อและวางสายเคเบิล แหล่งจ่ายไฟ

หมายเหตุ: ระบบนี้ต้องการคนสองคนเพื่อติดตั้งลงในชั้นวาง

1. ให้ต่อรางสไลด์จนกว่ารางจะล็อกลงในตำแหน่งให้บริการ (A)
2. ใช้คนสองคนยกกระบอกและจัดตำแหน่งหมุดล็อกกลิ้งที่อยู่ต่ำกว่าบนรางของตัวเครื่อง ให้ลงร่องในรางสไลด์ของชั้นวางทั้งสองด้าน



P8EIC595-2

รูปที่ 74. จัดตำแหน่งหมุดล็อกที่ต่ำกว่าบนรางของตัวเครื่องให้ลงร่องในรางสไลด์ของชั้นวาง

3. ยกแลตซ์ด้านใดด้านหนึ่งของชั้นวาง (B) ที่มีเครื่องหมาย ลูกศรสีเขียวพร้อมกัน
4. ผลักระบบลงในชั้นวาง
5. ชั้นตะปูควงด้านใดด้านหนึ่งของระบบเพื่อยึดระบบเข้ากับชั้นวาง

การวางสายเคเบิล 7063-CR1 HMC ที่ติดตั้งในชั้นวาง

ศึกษาเกี่ยวกับวิธีการติดตั้ง Hardware Management Console (HMC) ที่ประกอบเข้ากับชั้นวางของคุณ

1. ตรวจสอบให้แน่ใจว่า คุณวาง HMC ไว้ในตำแหน่งที่ถูกต้อง
2. ติดตั้ง HMC ลงในชั้นวาง สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การติดตั้ง 7063-CR1 ในชั้นวาง” ในหน้า 46 หลังจากคุณติดตั้ง HMC ในชั้นวาง ให้ดำเนินการขั้นตอนถัดไป
3. เสียบปลั๊กสายไฟเข้ากับ HMC
4. เชื่อมต่อคีย์บอร์ด มอนิเตอร์ และเมาส์
5. เชื่อมต่อสายเคเบิลอีเทอร์เน็ต (หรือสายครอสโอเวอร์) จาก HMC ไปยังเซิร์ฟเวอร์ที่ถูกจัดการ:

หมายเหตุ: เมื่อต้องการศึกษาเพิ่มเติมเกี่ยวกับการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80

6. หากระบบที่ถูกจัดการได้รับการติดตั้งแล้ว คุณสามารถตรวจสอบว่าการเชื่อมต่อ สายเคเบิลอีเทอร์เน็ตว่าแอ็คทีฟอยู่หรือไม่โดยการสังเกตไฟสัญญาณสีเขียวที่ HMC ทั้ง 2 เครื่อง และที่พอร์ตอีเทอร์เน็ตของระบบที่ถูกจัดการในขณะที่ขั้นตอนติดตั้งกำลังดำเนินไป
7. เชื่อมต่อพอร์ต Ethernet Intelligent Platform Management Interface (IPMI) กับเครือข่าย

หมายเหตุ: การเชื่อมต่อนี้ต้องการเข้าถึง baseboard management controller (BMC) บน HMC การเข้าถึง BMC จำเป็นสำหรับภารกิจบริการและเพื่อจัดการกับเฟิร์มแวร์ HMC สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80

8. เชื่อมต่อพอร์ตอีเทอร์เน็ตบน HMC เข้ากับพอร์ตอีเทอร์เน็ตที่ชื่อ **HMC1** บนเซิร์ฟเวอร์ที่จัดการ
9. ถ้าคุณกำลังเชื่อมต่อ HMC ตัวที่สองเข้ากับเซิร์ฟเวอร์ที่จัดการ ให้เชื่อมต่อพอร์ตอีเทอร์เน็ตที่มีเลเบล **HMC2** บนเซิร์ฟเวอร์ที่จัดการ
10. เสียบปลั๊กสายไฟสำหรับมอนิเตอร์, HMC และโมเด็มภายนอก HMC เข้ากับจุดจ่ายไฟ

หมายเหตุ: หากคุณกำลังเชื่อมต่อ HMC นี้กับระบบที่จัดการระบบใหม่ ห้ามเชื่อมต่อระบบที่จัดการ กับแหล่งจ่ายไฟ

ถัดไป คุณจำเป็นต้องติดตั้งและกำหนดคอนฟิกซอฟต์แวร์ HMC ของคุณ ดำเนินการต่อด้วย “การกำหนดค่า 7063-CR1 HMC”

การกำหนดค่า 7063-CR1 HMC

ศึกษาเกี่ยวกับวิธีการติดตั้งและกำหนดคอนฟิก Hardware Management Console (HMC)

คุณสามารถดาวน์โหลด HMC เวอร์ชันที่คุณต้องการจากเว็บไซต์ Fix Central ใช้สื่อบันทึกแบบถอดออกได้ (เช่น DVD หรือ USB) เพื่อสร้างไฟล์ ISO ที่สามารถบูตได้จากแพ็คเกจ HMC (อิมเมจ ISO)

หมายเหตุ: การติดตั้งต่อไปนี้จะถูกแสดงไว้ตามตัวอย่าง

การติดตั้ง HMC โดยใช้แฟลชไดรฟ์ USB

เมื่อต้องการติดตั้ง HMC โดยใช้แฟลชไดรฟ์ USB ให้ทำตามขั้นตอนต่อไปสำหรับระบบ Linux:

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

หมายเหตุ: ไดรฟ์ USB ต้องมีพื้นที่อย่างน้อย 4 GB

3. เสียบไดรฟ์ USB และเปิดระบบ

การติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตจากวิเวอร์คอนโซล

เมื่อต้องการติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตจากวิเวอร์คอนโซล ให้ทำตามขั้นตอนต่อไปนี้:

1. ล็อกอินเข้าสู่เว็บอินเตอร์เฟซ BMC (<http://<bmc-ip>>)
2. เลือกตัวควบคุมแบบรีโมต
3. เลือกเปลี่ยนทิศทางคอนโซล
4. คลิก เรียกใช้งานคอนโซล.
5. ใน Java™ iKVM Viewer ให้เลือก สื่อบันทึกเสมือน > หน่วยเก็บข้อมูลเสมือน
6. ภายใต้ ประเภทของโลจิคัลไดรฟ์ ให้เลือก ไฟล์ ISO
7. คลิก เปิดอิมเมจ และหาตำแหน่งไฟล์ ISO บนระบบของคุณ

8. กด **Plugin** เพื่อเมาท์ไฟล์ ISO
9. เปิด ระบบ

การติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตจากเว็บอินเตอร์เฟซ BMC

เมื่อต้องการติดตั้ง HMC โดยใช้สื่อบันทึกแบบรีโมตจากเว็บอินเตอร์เฟซ BMC ให้ทำตามขั้นตอน ต่อไปนี้:

1. ล็อกอินเข้าสู่เว็บอินเตอร์เฟซ BMC (<http://<bmc-ip>>)
2. เลือก สื่อบันทึกแบบเสมือน
3. เลือก อิมเมจ CD-ROM
4. กรอกข้อมูลต่อไปนี้:

แบ่งใช้โฮสต์

IP ของโฮสต์ Server Message Block (SMB) หากคุณกำลังใช้ชื่อโฮสต์ให้ตรวจสอบว่า domain name system (DNS) บน BMC ถูกกำหนดค่าอย่างถูกต้อง

พาธไปยังอิมเมจ

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

ผู้ใช้ (ตัวเลือก)

ชื่อผู้ใช้ที่ใช้เพื่อล็อกอินเข้าสู่โฮสต์ SMB

รหัสผ่าน (ตัวเลือก)

รหัสผ่านสำหรับผู้ใช้

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

หมายเหตุ: หากไม่แสดงข้อความ ให้ตรวจสอบข้อมูลอีกครั้งและทำซ้ำขั้นตอนที่ 5 - 7

8. เปิด ระบบ

หมายเหตุ: ไม่สนับสนุน Server Message Block เวอร์ชัน 3 (SMBv3)

ถัดไป คุณจำเป็นต้องกำหนดคอนฟิกซอฟต์แวร์ HMC ของคุณ สำหรับคำแนะนำ โปรดดูที่ “การกำหนดค่า HMC โดยใช้อินเตอร์เฟซ HMC Enhanced+” ในหน้า 133

หลักการที่เกี่ยวข้อง:

“กำหนดค่าการเชื่อมต่อ BMC” ในหน้า 163

คุณสามารถกำหนดค่าหรือดูค่าติดตั้งเครือข่ายบน BMC สำหรับคอนโซลการจัดการ

การติดตั้ง เครื่องมือเสมือน HMC

ศึกษาเกี่ยวกับวิธีติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC)

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

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

ข้อกำหนดต่ำสุดสำหรับการรัน เครื่องมือเสมือน HMC:

- หน่วยความจำ 8 GB
- 4 ตัวประมวลผล
- 1 อินเทอร์เน็ตเครือข่าย (สูงสุด 4 ตัว)
- พื้นที่ดิสก์ 160 GB (แนะนำ: 700 GB เพื่อจัดเก็บข้อมูล Performance and Capacity Monitoring (PCM) ได้อย่างเพียงพอ)

หมายเหตุ:

1. ตัวประมวลผลบนระบบที่โฮสต์ เครื่องมือเสมือน HMC ต้องเป็นตัวประมวลผลที่เปิดใช้งานฮาร์ดแวร์แบบเสมือน Intel VT-x หรือ AMD-V
2. เครื่องมือเสมือน HMC DVD ที่คุณได้รับไม่สามารถบูตได้ คุณต้องเผาที่สื่อบันทึกก่อน จากนั้นคัดลอกไฟล์ .tgz จากสื่อบันทึก วิธีเผา DVD อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการที่คุณใช้
3. ไวยากรณ์คำสั่งที่ใช้ในตัวอย่างต่อไปนี้ อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการที่คุณใช้

ข้อมูลที่เกี่ยวข้อง:

อีเมลการติดตั้งเครือข่าย HMC V8 และวิธีการติดตั้ง

การติดตั้ง เครื่องมือเสมือน HMC บน x86

เรียนรู้วิธีติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) ในสภาวะแวดล้อม x86

การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ KVM:

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

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC บน KVM ให้ทำตามขั้นตอนต่อไปนี้:

หมายเหตุ: ขั้นตอนต่อไปนี้จะใช้อินเตอร์เฟซบรรทัดคำสั่ง และต้องมีสิทธิ์ผู้ใช้ รุท ไวยากรณ์คำสั่ง อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ

1. ตรวจสอบว่า แพ็กเกจเวอร์ชวลไลเซชันถูกติดตั้งบนระบบที่มี Red Hat Enterprise Linux (RHEL) เวอร์ชัน 6.7 หรือใหม่กว่า
2. ดาวน์โหลดไฟล์ <KVM vHMC installation filename>.tar.gz ลงในระบบโฮสต์
3. รันคำสั่งต่อไปนี้: `mkdir -p /var/lib/libvirt/images/vHMC`

4. รันคำสั่งต่อไปนี้: `cd /var/lib/libvirt/images/vHMC`
5. เมื่อต้องการคลายอิมเมจดิสก์เสมือน ให้รันคำสั่งต่อไปนี้: `tar -zxvf <KVM vHMC installation filename>.tgz`

หมายเหตุ: ในคำสั่งนี้ให้ระบุพาธเต็มของไฟล์ เครื่องมือเสมือน HMC .tar ของคุณ

6. ไฟล์ `domain.xml` จะอยู่ในไฟล์ `<KVM vHMC installation filename>.tar.gz` ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. แก้ไขไฟล์ `domain.xml` และตรวจสอบว่า พาธไปยังดิสก์ของคุณถูกต้อง ไฟล์นี้จะมีสตริง `DISK_PATH`
 - b. ตรวจสอบให้แน่ใจว่าใช้ `virtio` ในค่าบัสสำหรับอุปกรณ์ดิสก์ของคุณ
 - c. คุณสามารถเลือกชื่อที่แตกต่างกันสำหรับ VM ของคุณ ชื่อดีฟอลต์ในไฟล์ `domain.xml` คือ `vHMC`
 - d. ตรวจสอบว่าแอดเดรสการควบคุมการเข้าถึงสื่อ (MAC) ถูกกำหนดไว้ในไฟล์ `domain.xml` ไฟล์นี้จะมี สตริง `MAC_ADDRESS`

หมายเหตุ: ลบบรรทัดนี้หาก คุณต้องการให้ MAC แอดเดรสถูกสร้างขึ้นโดยอัตโนมัติสำหรับคุณ

- e. ตรวจสอบว่าบริดจ์ของคุณตรงกับอุปกรณ์อีเทอร์เน็ตของคุณ ไฟล์ `domain.xml` ดีฟอลต์ จะระบุหนึ่งอีเทอร์เน็ต
7. เมื่อต้องการกำหนด VM ให้รันคำสั่งต่อไปนี้: `virsh define <domain>.xml`
8. เมื่อต้องการเริ่มต้น VM ให้รันคำสั่งต่อไปนี้: `virsh start vHMC`
9. เมื่อต้องการกำหนดหมายเลขแสดง Virtual Network Computing (VNC) ของคอนโซลของคุณ ให้รันคำสั่งต่อไปนี้: `virsh vncdisplay vHMC`
10. เมื่อต้องการเชื่อมต่อกับคอนโซลของคุณด้วยวิวเวอร์ VNC ให้รันคำสั่งต่อไปนี้: `vncviewer HOSTNAME:ID` (โดยที่ ID คือ หมายเลขที่แสดง, ตัวอย่างเช่น 0)

หมายเหตุ: หาก คุณต้องการเข้าถึงจากระยะไกล คุณต้องลบ หรือกำหนดคอนฟิกไฟวอลล์ของคุณ เพื่ออนุญาตให้เข้าถึงพอร์ต 5900

การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ Xen:

ศึกษาเกี่ยวกับวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) โดยใช้ไฮเปอร์ไวเซอร์ Xen

เครื่องมือเสมือน HMC สนับสนุน Xen เวอร์ชัน 4.2 หรือสูงกว่า

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC โดยใช้ไฮเปอร์ไวเซอร์ Xen ให้ทำตามขั้นตอนต่อไปนี้:

หมายเหตุ: ขั้นตอนต่อไปนี้จะอินเตอร์เฟซบรรทัดคำสั่ง และต้องมีสิทธิ์แบบผู้ใช้ root ไวยากรณ์คำสั่ง อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ

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

หมายเหตุ: ในคำสั่งนี้ให้ระบุพาธเต็มของไฟล์ เครื่องมือเสมือน HMC .tar ของคุณ

6. ไฟล์ `vhmc.cfg` ถูกจัดเตรียมไว้ในไฟล์ `<XEN vHMC installation filename>.tar.gz` เปิดไฟล์ `vhmc.cfg` ในเท็กซ์เอดิเตอร์ และแก้ไขค่าต่อไปนี้:
 - a. เปลี่ยนชื่อของ HMC เสมือน (ทางเลือก): แก้ไขไฟล์ `vhmc.cfg` และตรวจสอบว่า พารามิเตอร์ของคณุนั้นถูกต้อง ไฟล์นี้จะมีสตริง `DISK_PATH`
 - b. แทนที่ `DISK_PATH` ด้วยพารามิเตอร์สำหรับ `disk1.img`:


```
disk = [ 'file:DISKPATH,hda,w' ]
```
 - c. แทนที่ `ethernet adapter` และเพิ่ม MAC address (ทางเลือก):


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

 MAC Address ทางเลือก:


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

หมายเหตุ: เมื่อ Virtual HMC ระบุตัวแล้ว ไฮเปอร์ไวเซอร์ Xen จะสร้าง MAC address ขึ้นใหม่อีกครั้ง การเพิ่ม MAC Address เพิ่มเติมจะช่วยแก้ปัญหา
 - d. แทนที่ `FLOPPYPATH` (หากคุณกำลังใช้ Activation Engine):


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

การติดตั้ง เครื่องมือเสมือน HMC โดยใช้ VMware ESXi:

ศึกษาเกี่ยวกับวิธีการติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) โดยใช้ VMware ESXi

คุณสามารถติดตั้ง เครื่องมือเสมือน HMC บน VMware ESXi ได้โดยใช้ส่วนติดต่อผู้ใช้แบบกราฟิกบนไคลเอนต์ vSphere เพื่อปรับใช้เทมเพลต Open Virtualization Format (OVF)

หมายเหตุ: คุณสามารถติดตั้ง เครื่องมือเสมือน HMC บน VMware ESXi เวอร์ชัน 5.5 หรือเวอร์ชันถัดมาได้

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC บน VMware ESXi โดยใช้ไคลเอนต์ vSphere ให้ทำตามขั้นตอนต่อไปนี้:

หมายเหตุ: ไวยากรณ์คำสั่ง อาจแตกต่างกันขึ้นอยู่กับระบบปฏิบัติการ

1. ขอรับไฟล์เก็บถาวร Tar: `<VMware vHMC installation file name>.tgz`
2. ใช้คำสั่ง `tar` เพื่อคลายไฟล์ OVA ออกจากไฟล์จัดเก็บถาวร Tar
3. สตาร์ทไคลเอนต์ vSphere และล็อกอินเข้าสู่โฮสต์ ESXi
4. จากเมนู File ให้เลือก **Deploy OVF template**
5. คลิก **Browse** และเลือกไฟล์ OVA
6. คลิก **Next**
7. หลังจากการปรับใช้เสร็จสิ้นแล้วให้คลิก **ปิด** และเลือกไอคอน เครื่องมือเสมือน HMC เพื่อเปิด เครื่องมือเสมือน HMC

การติดตั้ง เครื่องมือเสมือน HMC บน PowerVM (โลจิคัลพาร์ติชัน)

เรียนรู้วิธีติดตั้ง เครื่องมือเสมือน Hardware Management Console (HMC) ในสภาวะแวดล้อม PowerVM®

หมายเหตุ: เมื่อคุณติดตั้ง เครื่องมือเสมือน HMC บนพาร์ติชันโดยใช้อิมเมจไฟล์ HMC ISO คุณจะไม่มีทางเข้าถึงคอนโซลแบบกราฟิกแบบโลคัลเพื่อเข้าถึงส่วนติดต่อผู้ใช้แบบเว็บ

เมื่อต้องการติดตั้ง เครื่องมือเสมือน HMC บน PowerVM ให้ทำตามขั้นตอนต่อไปนี้:

1. ทำตามขั้นตอนปกติสำหรับการติดตั้งอิมเมจ ISO บน PowerVM สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีกำหนดค่า VIOS Media Repository / Virtual Media Library
2. หลังจากการติดตั้งเสร็จสมบูรณ์และระบบเริ่มทำงาน คุณต้องเลือกภาษาจากไดอะล็อกบ็อกซ์ การเลือกภาษา
3. ยอมรับข้อตกลงการอนุญาตให้ใช้งาน

หมายเหตุ: ตรวจสอบให้แน่ใจว่าคอนโทรลเลอร์คำสั่งพร้อมที่จะยอมรับคำสั่ง ก่อนที่คุณจะรันคำสั่งใดๆ เช่น การรันคำสั่ง `lshmc -V` จะกว่าจะสำเร็จ

4. ล็อกอินในฐานะ `hscroot` และใช้คำสั่ง `chhmc` เพื่อกำหนดค่าเครือข่าย
ตัวอย่างต่อไปนี้แสดงลำดับของคำสั่ง `chhmc` ที่สามารถใช้เพื่อกำหนดค่าเครือข่ายและเปิดใช้งานการเข้าถึง ssh และการเข้าถึงรีโมตเว็บบน HMC

```
chhmc -c network -s modify -i eth0 -a <hmc ip address> -nm <hmc network mask> --lparcomm on
chhmc -c network -s modify -h <hmc hostname> -d <hmc domain name> -g <gateway ip>
chhmc -c network -s add -ns <name server> -ds <domain search>
chhmc -c ssh -s enable
chhmc -c ssh.name -s add -a <ip address>
chhmc -c SecureRemoteAccess.name -s add -a <ip address>
hmcshutdown -r -t now
```

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

5. รีสตาร์ทระบบ

การใช้ Activation Engine สำหรับ เครื่องมือเสมือน HMC

ศึกษาเกี่ยวกับวิธีการใช้ Activation Engine สำหรับ เครื่องมือเสมือน Hardware Management Console (HMC)

Activation Engine เป็นเฟรมเวิร์กที่อนุญาตให้กำหนดคอนฟิก คอมโพเนนต์ต่างๆ ภายในเครื่องเสมือนระหว่างการเริ่มต้นระบบ Activation Engine สามารถใช้กับอิมเมจดิสก์ ที่จัดเก็บไว้ล่วงหน้าเท่านั้น ตัวอย่างเช่น หาก เครื่องมือเสมือน HMC ถูกสร้างขึ้นโดยใช้ไฟล์ ISO ของ HMC Recovery แล้ว Activation Engine จะไม่ถูกเปิดใช้งาน เมื่อต้องการใช้ Activation Engine คุณจำเป็นต้องตั้งค่าโปรไฟล์ คอนฟิกูเรชัน XML เพื่ออนุญาตให้ เครื่องมือเสมือน HMC อยู่ในสถานะพร้อมที่จะจัดการในการเริ่มต้นใช้งานในครั้งแรก สำหรับข้อมูลเพิ่มเติม เกี่ยวกับการกำหนดคอนฟิกโปรไฟล์คอนฟิกูเรชัน XML ให้ดูที่ “การตั้งค่าโปรไฟล์คอนฟิกูเรชันสำหรับ Activation Engine” ในหน้า 63 สามารถใช้ไฟล์คอนฟิกูเรชัน เพื่อกำหนดคอนฟิกตัวเลือกต่างๆ ต่อไปนี้:

- ตั้งค่าคีย์บอร์ดดีฟอลต์ (US)
- ภาษาดีฟอลต์ (US)
- ข้อตกลงสิทธิการใช้งาน และรหัสเครื่อง
- ปิดใช้งานวิซาร์ดการติดตั้ง
- ปิดใช้งานวิซาร์ด Call Home
- กำหนดค่าได้ถึง 4 การ์ดอินเตอร์เฟซเครือข่าย
- กำหนดการตั้งค่าไฟลวอลล์สำหรับแต่ละอินเตอร์เฟซ

เมื่อต้องการตั้งค่า Activation Engine ให้ดำเนินการขั้นตอน ต่อไปนี้:

1. สร้างไฟล์ XML ที่ชื่อ **vHMC-Conf.xml** โดยใช้โปรแกรมแก้ไขข้อความ หรือใช้ไฟล์ตัวอย่างที่มีให้ใน แฟ้มเก็บ vHMC install file.tgz
2. สร้างอิมเมจดิสก์เกิด บนระบบที่รันระบบปฏิบัติการ Linux งานนี้สามารถดำเนินการโดยใช้คำสั่ง dd:


```
dd if=/dev/zero of=/Floppy/Path/Floppy.img count=1440 bs=1k
```
3. จัดรูปแบบไฟล์โดยใช้คำสั่ง mkfs.ext2:


```
/sbin/mkfs.ext2 /Floppy/Path/Floppy.img
```
4. คัดลอกไฟล์ **vHMC-Conf.xml** ไปยังอิมเมจ ดิสก์เกิด:


```
mkdir /Path/to/Tempfolder/Temp
mount -o loop,rw /Floppy/Path/Floppy.img /Path/to/Tempfolder/Temp
cp /Path/to/vHMC-Conf.xml /Path/to/Tempfolder/Temp
umount /Path/to/Tempfolder/Temp
```
5. สำหรับไฮเปอร์ไวเซอร์เคียวเอ็ม (KVM) ให้เพิ่ม ตำแหน่งดิสก์เกิดลงในไฟล์ **domain.xml** :


```
<disk type='file' device='floppy'>
  <driver name='qemu' type='raw' cache='default' />
  <source file='Path/to/Floppy' />
  <target dev='fda' bus='fdc' />
  <address type='drive' controller='0' bus='0' target='0' unit='0' />
</disk>
```
6. เมื่อต้องการกำหนด VM ให้รันคำสั่งต่อไปนี้: **virsh define PATH_TO_DOMAIN_XML**
7. เมื่อต้องการเริ่มต้น VM ให้รันคำสั่งต่อไปนี้: **virsh start NAME_OF_VM** (NAME_OF_VM จะอธิบายไว้ในไฟล์ Domain.xml)

การตั้งค่าโปรไฟล์คอนฟิกรูเรชันสำหรับ Activation Engine:

เรียนรู้วิธีการตั้งค่าไฟล์คอนฟิกรูเรชันของ Activation Engine โดยใช้แท็ก XML

แท็ก XML สำหรับไฟล์คอนฟิกรูเรชัน

แท็ก XML จะถูกใช้ในไฟล์คอนฟิกรูเรชัน Activation Engine เพื่อกำหนดค่าเฉพาะ สำหรับแอตทริบิวต์ต่างๆ คุณสามารถกำหนดค่าเหล่านี้ด้วยตัวเองใน ไฟล์คอนฟิกรูเรชัน Activation Engine ใช้ส่วนต่อไปนี้ เพื่อดูรายละเอียดของแต่ละแท็ก และค่าที่อนุญาต:

- “แท็ก HMC” ในหน้า 64

- “แท็ก Ethernet” ในหน้า 65
- “แท็ก Firewall” ในหน้า 66
- “แท็ก NTPServers” ในหน้า 68

หมายเหตุ: การตั้งค่าเซิร์ฟเวอร์ Dynamic Host Configuration Profile daemon (DHCPD) ไม่ได้กำหนดโดย Activation Engine

ใช้ส่วนต่อไปเพื่อดูคอนฟิกูเรชันตัวอย่างของไฟล์คอนฟิกูเรชัน:

- “ตัวอย่างไฟล์คอนฟิกูเรชัน XML ของ Activation Engine ที่ไม่มี NTPServer” ในหน้า 69
- “ตัวอย่างของไฟล์คอนฟิกูเรชัน XML ของ Activation Engine ที่มี NTPServers” ในหน้า 70

แท็ก HMC

แท็ก HMC จะเก็บค่าสำหรับ คอนฟิกูเรชันการตั้งค่า HMC ตัวอย่างต่อไปนี้จะแสดง แท็ก HMC ที่สามารถใช้งานได้:

HMC License Agreement Tag:

```

TAG: <AcceptLicense></AcceptLicense>
Acceptable Values:
Yes -> Will Accept HMC License Agreement
No  -> Will Prompt User to Accept HMC License Agreement

```

HMC Locale Tag:

```

TAG: <Locale></Locale>
Acceptable Values:
en_US.UTF-8

```

HMC Setup Wizard Tag:

```

TAG: <SetupWizard></SetupWizard>
Acceptable Values:
Yes  -> Will Display HMC Setup Wizard
No   -> Will Disable HMC Setup Wizard

```

HMC Setup Call Home Wizard Tag:

```

TAG: <SetupCallHomeWizard></SetupCallHomeWizard>
Acceptable Values:
Yes  -> Will Display HMC Call Home Wizard
No   -> Will Disable HMC Call Home Wizard

```

HMC Setup Keyboard Tag:

```

TAG: <SetupKeyboard></SetupKeyboard>
Acceptable Values:
Yes  -> Will Prompt User for Keyboard Configuration:wq
No   -> Will Accept Default keyboard setup (U.S.)

```

แท็ก Ethernet

แท็ก Ethernet จะเก็บค่าสำหรับการตั้งค่าอะแดปเตอร์เน็ต Activation Engine สามารถกำหนดค่าอะแดปเตอร์เน็ตได้สูงสุด 4 อะแดปเตอร์ตัวอย่างต่อไปนี้แสดงแท็ก Ethernet ที่สามารถใช้งานได้:

Ethernet Enable Tag:

```
TAG: <Enable></Enable>
Acceptable Values:
Yes ->   Configure this adapter
No  ->   Do not Configure this adapter
```

Ethernet MACAddr Tag:

```
TAG: <MACAddr></MACAddr>
Acceptable Values:
XX:XX:XX:XX:XX:XX -> Where X is a 0-F Value
XX-XX-XX-XX-XX-XX -> Where X is a 0-F Value
```

Ethernet IPVersion Tag:

```
TAG: <IPVersion></IPVersion>
Acceptable Values:
IPV4 ->   Use IPV4 configuration
IPV6 ->   Use IPV6 configuration
MIX  ->   Use Both IPV4 and IPV6 configuration
```

Ethernet IPV4 Network Type Tag:

```
TAG: <IPv4NetworkType></IPv4NetworkType>
Acceptable Values:
Static ->   Configure Adapter using Static Configuration
Dhcp   ->   Configure Adapter using DHCP Configuration
```

Ethernet IPV4 Address Tag:

```
TAG:   <IPv4Address></IPv4Address>
Acceptable Values:
Any valid IPV4 Address Value
```

Ethernet IPV4 Netmask Tag:

```
TAG:   <IPv4Netmask></IPv4Netmask>
Acceptable Values:
Any valid IPV4 Netmask Value
```

Ethernet IPV4 Gateway Tag:

```
TAG:   <IPv4Gateway></IPv4Gateway>
Acceptable Values:
Any valid IPV4 Address Value
```

Ethernet IPV6 Network Type Tag:

TAG: <IPv6NetworkType></IPv6NetworkType>
Acceptable Values:
Static -> Configure Adapter using Static Configuration
Dhcp -> Configure Adapter using DHCP Configuration

Ethernet IPV6 Address Tag:

TAG: <IPv6Address></IPv6Address>
Acceptable Values:
Any valid IPV6 Address Value

Ethernet IPV6 Gateway Tag:

TAG: <IPv6Gateway></IPv6Gateway>
Acceptable Values:
Any valid IPV6 Address Value

Ethernet Hostname Tag:

TAG: <Hostname></Hostname>
Acceptable Values:
Valid String

Ethernet Domain Tag:

TAG: <Domain></Domain>
Acceptable Values:
Any Valid Domain Value
Ex. austin.ibm.com

Ethernet DNS Servers Tag:

TAG: <DNSServers></DNSServers>
Acceptable Values:
Up to 3 Valid IPV4 or IPV6 Addresses seperated by a coma
It is acceptable to have an Empty DNS Server Value.
Ex.1 IPV4: 9.3.2.1 IPV6: 2001:4860:4860::8888
Ex.2 IPV4: 9.3.2.1,9.5.4.1 IPV6: 2001:4860:4860::8888,2001:4860:4860::8844
Ex.3 IPV4: 9.3.2.1,9.5.4.1,9.4.3.2 IPV6: 2001:4860:4860::8888,2001:4860:4860::8844,
::ffff:903:201

แท็ก Firewall

แท็ก Firewall จะเก็บค่าไฟลล์วอลล์ที่เกี่ยวข้องสำหรับอะแดปเตอร์เน็ตที่สอดคล้องกัน ตัวอย่างต่อไปนี้แสดงแท็ก HMC ที่สามารถใช้งานได้:

หมายเหตุ: แท็กทั้งหมดจะต้องมีค่าที่เปิด หรือปิดใช้งาน

Firewall PEGASUS Tag:

TAG: <PEGASUS></PEGASUS>
Acceptable Values:
Enabled -> Will Allow PEGASUS Ports to be open

Disabled -> Will Disable PAGASUS Ports

Firewall RPD Tag:

TAG: <RPD></RPD>

Acceptable Values:

Enabled -> Will Allow RMC Ports to be open

Disabled -> Will Disable RMC Ports

Firewall FCS Tag:

TAG: <FCS></FCS>

Acceptable Values:

Enabled -> Will Allow FCS Ports to be open

Disabled -> Will Disable FCS Ports

Firewall I5250 Tag:

TAG: <I5250></I5250>

Acceptable Values:

Enabled -> Will Allow 5250 Ports to be open

Disabled -> Will Disable 5250 Ports

Firewall PING Tag:

TAG: <PING></PING>

Acceptable Values:

Enabled -> Will Allow PING Port to be open

Disabled -> Will Disable PING Port

Firewall L2TP Tag:

TAG: <L2TP></L2TP>

Acceptable Values:

Enabled -> Will Allow L2TP Ports to be open

Disabled -> Will Disable L2TP Ports

Firewall SLP Tag:

TAG: <SLP></SLP>

Acceptable Values:

Enabled -> Will Allow SLP Ports to be open

Disabled -> Will Disable SLP Ports

Firewall RSCT Tag:

TAG: <RSCT></RSCT>

Acceptable Values:

Enabled -> Will Allow RSCT Ports to be open

Disabled -> Will Disable RSCT Ports

Firewall SECUREREMOTEACCESS Tag:

TAG: <SECUREREMOTEACCESS></SECUREREMOTEACCESS>

Acceptable Values:

Enabled -> Will Allow Secure Remote Access Ports to be open
Disabled -> Will Disable Secure Remote Access Ports

Firewall SSH Tag:

TAG: <SSH></SSH>
Acceptable Values:
Enabled -> Will Allow SSH Port to be open
Disabled -> Will Disable SSH Port

Firewall VTTY Tag:

TAG: <VTTY></VTTY>
Acceptable Values:
Enabled -> Will Allow VTTY Ports to be open
Disabled -> Will Disable VTTY Ports

Firewall NTP Tag:

TAG: <NTP></NTP>
Acceptable Values:
Enabled -> Will Allow NTP Ports to be open
Disabled -> Will Disable NTP Ports

Firewall SNMPTraps Tag:

TAG: <SNMPTraps></SNMPTraps>
Acceptable Values:
Enabled -> Will Allow SNMP Traps Ports to be open
Disabled -> Will Disable SNMP Traps Ports

Firewall SNMPAgents Tag:

TAG: <SNMPAgents></SNMPAgents>
Acceptable Values:
Enabled -> Will Allow SNMP Agents Ports to be open
Disabled -> Will Disable SNMP Agents Ports

แท็ก NTPServers

แท็ก NTPServers จำเป็นต้องมีหากคุณต้องการกำหนดคอนฟิกสูงสุดสำหรับ NTP เซิร์ฟเวอร์ใน เครื่องมือเสมือน HMC สามารถเพิ่มเซิร์ฟเวอร์ NTP โดยใช้แท็ก <ntpparam ntpserver="server" ntpversion="1-4"/> พารามิเตอร์เซิร์ฟเวอร์ ยอมรับค่า IPv4 หรือ IPv6 หรือชื่อโดเมน ตัวอย่างต่อไปนี้ แสดงแท็ก NTPServers ที่สามารถใช้ได้:

NTPServers Tag:

TAG: <NTPServers></NTPServers>
Accepts <ntpparam ntpserver="server" ntpversion="1-4"/>

Ex.1 <NTPServers>
<ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
</NTPServers>

Ex.2 <NTPServers>
<ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>

```

<ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
<ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>

```

ntpparam Tag

```

TAG: <ntpparam ntpserver="" ntpverion="" />
Attribute Values:

```

```

ntpserver: will accept IPv4/IPv6 values and valid nostnames
ntpversion: will accept a 1-4 numeric value

```

ตัวอย่างไฟล์คอนฟิกูเรชัน XML ของ Activation Engine ที่ไม่มี NTPServer

ตัวอย่างต่อไปนี้แสดงไฟล์คอนฟิกูเรชัน XML ของ Activation Engine ที่ไม่มี NTPServers:

```

<vHMC-Configuration>
  <LicenseAgreement>
  </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
</Ethernet>
  <Enable>No</Enable>
  <MACAddr></MACAddr>
  <IPVersion></IPVersion>
  <IPv4NetworkType></IPv4NetworkType>
  <IPv4Address></IPv4Address>
  <IPv4Netmask></IPv4Netmask>
  <IPv4Gateway></IPv4Gateway>
  <IPv6NetworkType></IPv6NetworkType>
  <IPv6Address></IPv6Address>
  <IPv6Gateway></IPv6Gateway>
  <Hostname></Hostname>
  <Domain></Domain>
</DNSServers></DNSServers>
<Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <VTTY>Disabled</VTTY>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>

```

```

    <SNMPAgents>Disabled</SNMPAgents>
  </Firewall>
</Ethernet>
</vHMC-Configuration>

```

ตัวอย่างของไฟล์คอนฟิกูเรชัน XML ของ Activation Engine ที่มี NTPServers

ตัวอย่างต่อไปนี้แสดงไฟล์คอนฟิกูเรชัน XML ของ Activation Engine XML ที่มี NTPServers

```

<vHMC-Configuration>
  <LicenseAgreement>
  </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
<Ethernet>
  <Enable>No</Enable>
  <MACAddr></MACAddr>
  <IPVersion></IPVersion>
  <IPv4NetworkType></IPv4NetworkType>
  <IPv4Address></IPv4Address>
  <IPv4Netmask></IPv4Netmask>
  <IPv4Gateway></IPv4Gateway>
  <IPv6NetworkType></IPv6NetworkType>
  <IPv6Address></IPv6Address>
  <IPv6Gateway></IPv6Gateway>
  <Hostname></Hostname>
  <Domain></Domain>
  <DNSServers></DNSServers>
<Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <VTTY>Disabled</VTTY>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>
  <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
<NTPServers>
  <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
  <ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
  <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>
</vHMC-Configuration>

```

การติดตั้งหน้าจอและคีย์บอร์ด

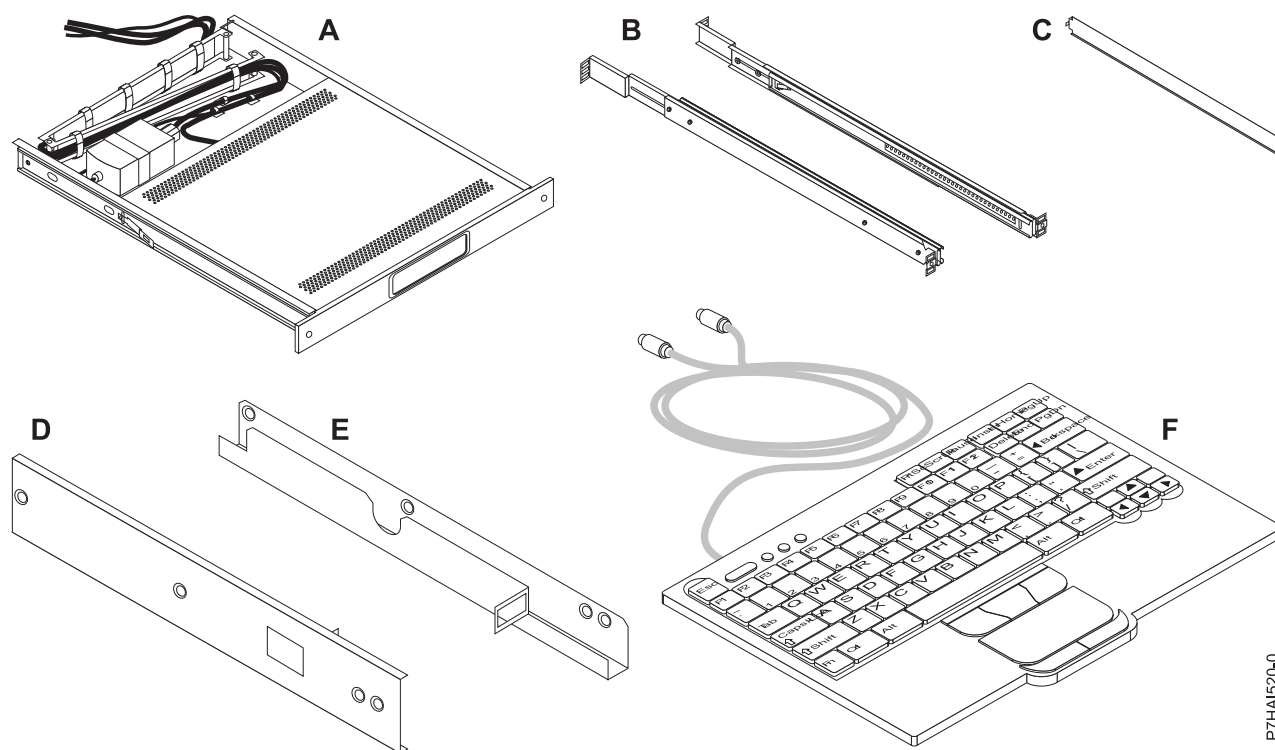
ศึกษาวิธีการติดตั้งหน้าจอและคีย์บอร์ด ซึ่ง มาพร้อมกับ 7042-CR6 HMC เข้ากับชั้นวาง นี้คืองานของลูกค้า

ถ้า HMC ถูกใช้เพื่อจัดการระบบแบบอิงตัวประมวลผล POWER8 แล้ว HMC ต้องอยู่ที่ CR3 หรือเวอร์ชันถัดมา ซึ่งต้องเป็นโมเดล HMC ที่ประกอบเข้ากับชั้นวาง IBM eserver 7316-TF3 มีขนาด 17 นิ้ว เป็นพาเนลแบบระนาบ และมอนิเตอร์ที่ประกอบเข้ากับชั้นวางและมีถาดคีย์บอร์ด คีย์บอร์ดพิเศษซึ่งพร้อมใช้งานสำหรับหลายภาษาวางอยู่ที่ด้านหน้าของถาดคีย์บอร์ดได้พอดี ถาดคีย์บอร์ดและหน้าจอจะใช้พื้นที่ขนาด 1 ยูนิต Electronics Industries Association (EIA) ในตู้ชั้นวาง คุณสามารถติดตั้งสวิตช์คอนโซลด้านหลังถาดเพื่อต่อคีย์บอร์ดและหน้าจอแบบจอแบน เข้ากับเซิร์ฟเวอร์มากกว่าหนึ่งตัว

เพื่อติดตั้ง 7042-CR6 HMC ลงในชั้นวาง ให้ดำเนินการขั้นตอนต่อไปนี้:

ข้อควรสนใจ: การติดตั้งรางในชั้นวางเป็นโปรซีเจอร์ที่ซับซ้อน เมื่อต้องการติดตั้งรางอย่างถูกต้อง คุณต้องปฏิบัติงานแต่ละงานตามลำดับดังนี้

1. ทำรายการชิ้นส่วนให้เสร็จสิ้น สำหรับคำแนะนำ โปรดดูที่ “การทำให้รายการชิ้นส่วนให้เสร็จสิ้น” ในหน้า 72 การทำรายการชิ้นส่วนให้เสร็จสิ้น
2. ค้นหาตำแหน่งชุดฮาร์ดแวร์ที่ประกอบเข้ากับชั้นวาง และชุดรางของระบบ ซึ่งประกอบด้วยยูนิตระบบของคุณ



รูปที่ 75. ชิ้นส่วนของชุดการติดตั้ง

P7HA520-0

ตารางที่ 10. เนื้อหาชิ้นส่วนของชุดการติดตั้ง

ชุดการติดตั้ง	เนื้อหาชิ้นส่วน
A	หนึ่งถาดคีย์บอร์ดที่มีหน้าจอพาเนลระนาบในตัว
B	รางด้านนอก (2)
C	สเปเซอร์การจัดตำแหน่งราง (1)
D	ฉากยึดที่ประกอบเข้ากับสวิตช์คอนโซลด้านขวา (1)
E	ฉากยึดที่ประกอบเข้ากับสวิตช์คอนโซลด้านซ้าย (1)
F	คีย์บอร์ดพร้อมด้วยอุปกรณ์ชี้ในตัว (1)
G	ชุดฮาร์ดแวร์เบ็ดเตล็ด: นีต U ยึดอุปกรณ์ 12 ตัว คลิปนีต 12 ตัว สกรูหัวร่องสี่แฉก 10 ตัว สกรู (8-32) 4 ตัว และสกรูทางปลา 2 ตัว
H	สายไฟยาว 1.8 ม. (6 ฟุต) (1)
I	2.4 ม. (8 ฟุต) ขั้วต่อสายไฟ International Electrotechnical Commission (IEC) (1)
J	สายต่อคีย์บอร์ด (1)
K	สายต่อเมาส์ (1)
L	แผ่น CD ที่มีไดรเวอร์คีย์บอร์ดและเมาส์ที่ทำงานบนระบบ Windows (ไม่ได้ใช้กับระบบ Eserver pSeries หรือระบบ AIX®, Linux หรือระบบที่อิง OS/400 ใดๆ)
สำคัญ: ใช้เครื่องมือต่อไปนี้เพื่อติดตั้งคีย์บอร์ดและหน้าจอแบบจอแบนที่ประกอบเข้ากับชั้นวาง: • กรรไกร • ไขควง Phillips • ไขควงแบบแบน	

การทำให้รายการชิ้นส่วนให้เสร็จสิ้น

คุณอาจต้องการทำรายการชิ้นส่วนให้เสร็จสิ้น

ถ้าคุณยังไม่ได้ทำให้ทำรายการชิ้นส่วนให้เสร็จสิ้น ก่อนที่จะดำเนินการติดตั้ง:

1. หาตำแหน่งรายงานชุดเครื่องมือในกล่องอุปกรณ์
2. ตรวจสอบให้แน่ใจว่า คุณได้รับชิ้นส่วนทุกชิ้นที่คุณได้สั่งซื้อ

ถ้าชิ้นส่วนไม่ถูกต้อง หายไป หรือเสียหาย ให้ติดต่อผู้ขายของ IBM หรือฝ่ายขายและสนับสนุนของ IBM

การทำเครื่องหมายตำแหน่งโดยไม่ใช่แท้มเพลตประกอบเข้ากับชั้นวาง

คุณสามารถทำเครื่องหมายตำแหน่งโดยไม่ใช่แท้มเพลต

แท้มเพลตที่ประกอบเข้ากับชั้นวางไม่ได้ประกอบเข้ากับระบบนี้ ระบบเหล่านี้คือยูนิต 1 EIA แบบสูง

เมื่อต้องการกำหนดตำแหน่งการประกอบเข้า ให้ปฏิบัติตามขั้นตอนเหล่านี้:

1. กำหนดที่จะวางระบบในชั้นวาง บันทึกตำแหน่ง EIA

หมายเหตุ: ยูนิต EIA บนชั้นวางของคุณประกอบด้วยกลุ่มของรูสามรู

2. หันด้านหน้าของชั้นวางและทำงานจากด้านขวา จุดยึดเหนี่ยวที่อยู่ถัดจากรูด้านบนสุดของยูนิต EIA

หมายเหตุ: จุดยึดเหนี่ยวจะถูกใช้เพื่อวัตถุประสงค์ในการระบุตำแหน่งบนชั้นวาง ถ้าคุณไม่มีจุดใดๆ ให้ใช้รูปแบบอื่นๆ ของเครื่องมือที่ใช้ทำเครื่องหมาย เพื่อวัตถุประสงค์ในการระบุตำแหน่งรู (ตัวอย่างเช่น เทป ตัวทำเครื่องหมาย หรือดินสอ) ถ้าคุณกำลังติดตั้งรางแบบสไลด์ให้วางเครื่องหมายหรือจุดยึดเหนี่ยวที่ตำแหน่งด้านล่างและกึ่งกลางรูของยูนิต EIA แต่ละยูนิต

3. วางจุดยึดเหนี่ยวอื่นๆ ถัดจากรูด้านล่างของ ยูนิต EIA ข้างต้น

หมายเหตุ: ถ้าคุณกำลังนับรูให้เริ่มต้นด้วยรูที่ระบุโดยจุดแรกและนับไปอีกสองรู วางจุดที่สองให้อยู่ถัดจากรูที่สาม

4. ทำซ้ำขั้นตอน 1 ในหน้า 9 สำหรับรูที่ตั้งอยู่ทางด้านซ้ายของชั้นวาง
5. ไปที่ด้านหลังของชั้นวาง
6. ที่ด้านขวาให้หา ยูนิต 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) ใน ตู้ชั้นวาง คุณสามารถใช้สายยึดที่มีให้ในชุดนี้ เพื่อติดตั้งสวิตช์คอนโซลในพื้นที่การติดตั้งบนชั้นวาง เดียวกับชุดคอนโซลหน้าจอ

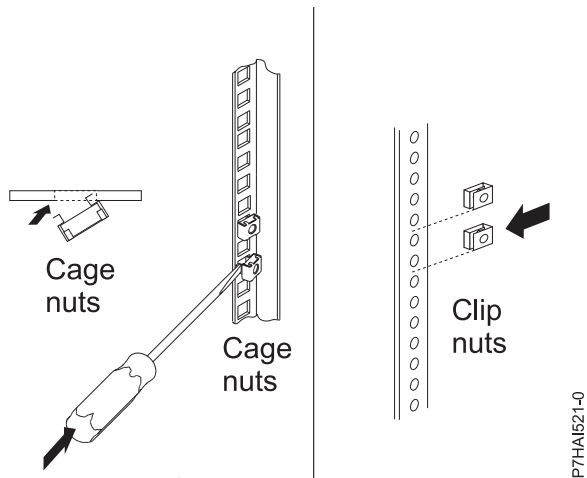
เพื่อติดตั้งหน้าจอและคีย์บอร์ดของ 7042-CR6 HMC ลงในชั้นวาง ให้ดำเนินการขั้นตอนต่อไป:

ข้อควรสนใจ: ถอดประตูลังชั้นวางและแผงด้านข้างออกเพื่อให้การ เข้าถึงสำหรับการติดตั้งได้ง่ายขึ้น

ดำเนินการขั้นตอนต่อไปเพื่อติดตั้งหน้าจอและคีย์บอร์ด ลงในชั้นวาง:

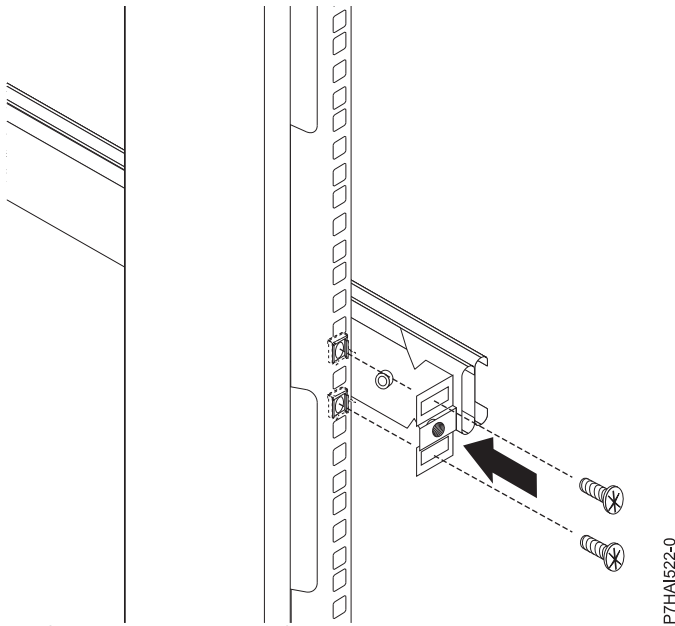
1. เลือกตำแหน่งในชั้นวางสำหรับถาดวางหน้าจอและคีย์บอร์ด สำหรับข้อมูลเพิ่มเติม โปรดดูที่ การทำเครื่องหมาย ตำแหน่ง.
2. ติดตั้งน็อต U ยึดอุปกรณ์ 4 ตัว (รูสล็อตเปลี่ยนหน้าแปลนชั้นวาง) หรือน็อตคัลป 4 ตัว (รูวงกลมบนหน้าแปลนชั้นวาง) ในตำแหน่ง EIA เดียวกันที่ด้านหน้า และด้านหลังของชั้นวาง

หมายเหตุ: หากคุณวางแผนที่จะติดตั้งสวิตช์คอนโซล ให้ติดตั้งน็อต U ยึดอุปกรณ์ หรือน็อตคัลปในตำแหน่งด้านหลัง ตรงกลาง ตามที่แสดงในรูปภาพต่อไปนี้



รูปที่ 76. การติดตั้ง น็อต U ยึดอุปกรณ์

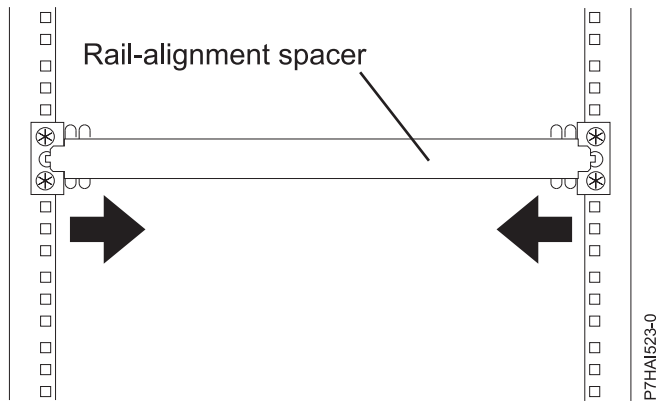
3. คลายสกรูปรับรางสองตัวที่อยู่บน รางเลื่อนด้านนอกแต่ละตัวออก ดึงรางออกไปยังการปรับด้านนอก สูงสุด
4. ปรับขยับรางเลื่อนด้านนอกให้พอดีกับความลึกของ ตู้ชั้นวาง จากนั้น ติดตั้งขยับรางเลื่อนให้พอดีกับ ความลึกของตู้ชั้นวางโดยใช้สกรูสี่ตัวจากชุดฮาร์ดแวร์ เบ็ดเตล็ด สกรูควรแน่นด้วยแรงนิ้วเพื่อให้สามารถปรับ ราง



รูปที่ 77. การปรับขยับรางเลื่อน

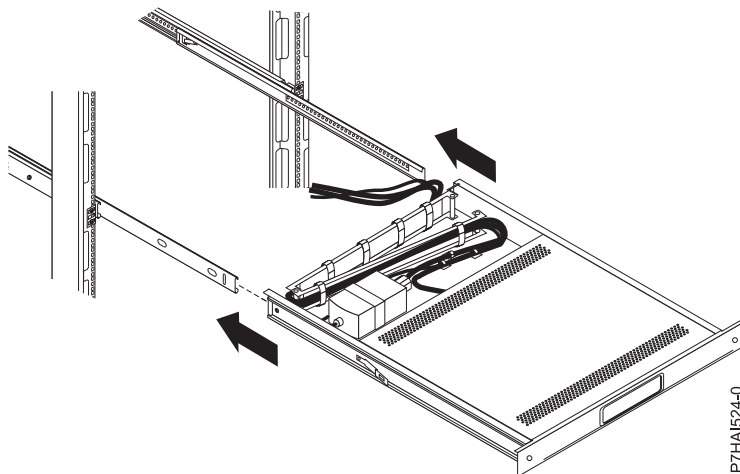
หมายเหตุ: ตรวจสอบให้แน่ใจว่าขยับรางเลื่อนขยายออกไปด้านนอกของหน้าแปลนการยึดตู้ชั้นวาง อย่าติดตั้ง สกรูในรูตรงกลางทางด้านหน้าหรือด้านหลังของขยับ รางเลื่อน รูเหล่านี้จะใช้เพื่อติดตั้งสกรูทางปลา หรือขยับ การติดตั้ง สวิตช์คอนโซลตามลำดับต่อไปในขั้นตอนนี้

5. ใช้สกรูสี่ตัวจาก ชุดฮาร์ดแวร์เบ็ดเตล็ด และหมุนให้แน่นด้วยมือจากด้านข้างของ slide-rail brackets ถึง rack cabinet. ตรวจสอบให้แน่ใจว่าขยับรางเลื่อน ขยายออกด้านนอกของหน้าแปลนการยึดตู้ชั้นวาง
6. ชันสกรูการปรับรางสองตัวบนรางด้านนอกแต่ละตัว ที่คุณคลายไว้ในขั้นตอน 5 ให้แน่น
7. ใส่สเปเซอร์จัดตำแหน่งรางลงในช่องตรงกลางรางเลื่อน ตรวจสอบให้แน่ใจว่าสเปเซอร์การจัดตำแหน่งรางหุ้มรอบรางชั้น สกรูสี่ตัวด้านหน้า จากนั้นถอดสเปเซอร์ออก



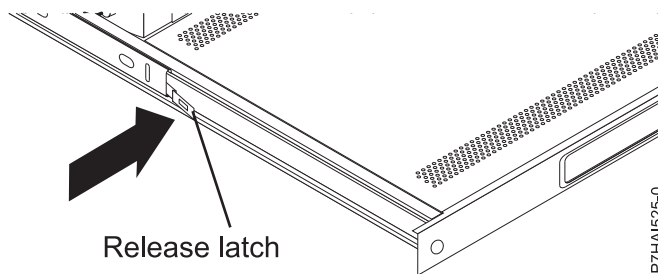
รูปที่ 78. การใส่สเปเซอร์การปรับราง

8. ดึงชิ้นส่วนด้านในของรางที่ยึดกับชั้นวางให้ยืดออก จากนั้น เลื่อนชุดล้อเลื่อนมาทางด้านหน้าของราง
9. เลื่อนถาดวางคีย์บอร์ดและหน้าจอแบบจอบแบนไปยังชุดล้อเลื่อน ในราง



รูปที่ 79. การเลื่อนหน้าจอและคีย์บอร์ด

10. กดสลักปลดล็อก และดันถาดวางคีย์บอร์ดและหน้าจอลงในชั้นวางให้สนิท คุณอาจพบแรงต้านทานบางอย่างในตอนเริ่มต้น เนื่องจากชุดล้อเลื่อนวางอยู่ระหว่างรางด้านในและด้านนอก ดึงถาดออกมาครึ่งทาง จากนั้นดันกลับไปเพื่อให้ถาดอยู่ในราง ทำเช่นนี้สองสามครั้งเพื่อให้แน่ใจว่า สามารถเลื่อนถาดในรางได้อย่างราบรื่น



รูปที่ 80. การใช้สลัก ปลดล็อก

หมายเหตุ:

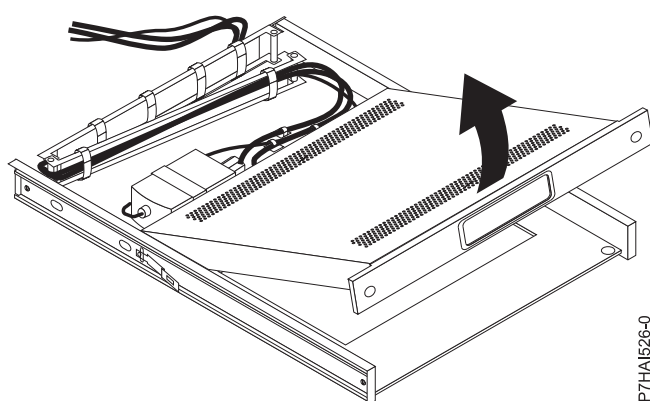
สายวิดีโอจะเชื่อมต่อกับหน้าจอแบบจอแบน เมื่อคุณติดตั้งการ์ดลงในตู้ชั้นวาง ตรวจสอบให้แน่ใจว่าคุณไม่ได้พับหรือตัดสายวิดีโอ

11. วางการ์ดลงในราง และขันสกรูยึดขายึดรางเลื่อนด้านหลัง สี่ตัวให้แน่น
12. วางคีย์บอร์ดบนพื้นผิวเรียบที่มั่นคง และถอดแผ่นยาง ที่ปลายด้านล่างของคีย์บอร์ดใหม่ แต่ละด้านออก อย่างป้อนแผ่นยางไว้บนคีย์บอร์ด เนื่องจาก แผ่นยางอาจขยายไปยังพื้นที่ด้านล่างการ์ด

หมายเหตุ:

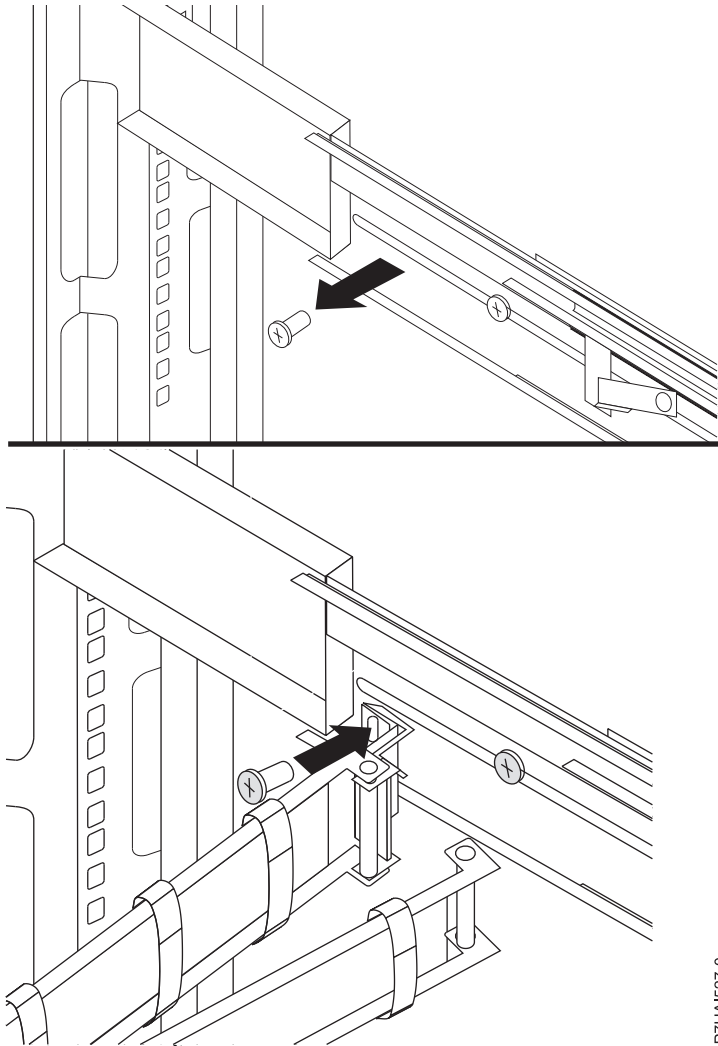
อย่า ดึงขาตั้งคีย์บอร์ดออก หน้าจอแบบจอแบนอาจ เกิดความเสียหายหากขาตั้งถูกดึงออกเมื่ออยู่ใกล้หน้าจอ

13. ดึงการ์ดออกจากชั้นวางจนสุด ราง
14. ยกด้านหน้าของหน้าจอแบบจอแบนขึ้น จากนั้นยกหน้าจอ ในตำแหน่งที่ยกสูงขึ้น



รูปที่ 81. การยกหน้าจอใน ตำแหน่งที่ยกสูงขึ้น

15. วางคีย์บอร์ดลงในถาด จากนั้นสอดสายเคเบิลของคีย์บอร์ดและ เมาส์ผ่านคลิปรัดสายทางด้านล่างของถาดผ่านช่องทางด้านขวาของถาด และไปยังแขนการจัด สายเคเบิล ดึงสายเคเบิลทั้งหมดผ่านช่อง
16. วางสายคีย์บอร์ดและเมาส์บนถาดด้านหลังหน้าจอ ตรวจสอบให้แน่ใจว่าสายเคเบิลขวางกับอุปกรณ์ต่างๆ ในชั้นวางเมื่อ ดันถาด กลับเข้าที่ในชั้นตอนต่อไป นี้ คุณต้อง สอดสายผ่านแขนการจัดสายเคเบิล
17. ลดหน้าจอให้ต่ำลง จากนั้นดันถาด กลับเข้าไปในชั้นวางจนสุด ใช้สกรูหางปลาเพื่อยึดด้านหน้าของถาด เข้ากับชั้นวาง
18. จากด้านหลังของชั้นวาง ให้ถอดแถบรัดสำหรับการขนส่งที่ยึด แขนการจัดสายเคเบิลเข้ากับถาดออก
19. สอดสายคีย์บอร์ดและเมาส์ผ่านแขนการจัด สายเคเบิล ใช้แถบรัดสายที่มีอยู่เพื่อยึดสายเคเบิล
20. ถอดสกรูการปรับรางที่อยู่ใกล้กับ ด้านหลังของชั้นวางออกจากรางเลื่อนด้านซ้าย ใช้สกรูเพื่อติดตั้ง แขนการจัดสายเคเบิลเข้ากับราง



PTHAI527-0

รูปที่ 82. การติดตั้งแขนการจัดสาย เคเบิล

21. เชื่อมต่อขั้วต่อวีดีโอ, คีย์บอร์ด และเมาส์เข้ากับ เซิร์ฟเวอร์หรือสวิตช์คอนโซลในตู้ชั้นวาง หาก ติดตั้งสวิตช์คอนโซล โปรดดูที่ การติดตั้ง Optional Console Switch และดำเนินขั้นตอนตามที่อธิบายไว้ หากไม่ได้ติดตั้ง ให้ปฏิบัติตาม ขั้นตอนจากขั้นตอน 21 เพื่อดำเนินการติดตั้งถาดวางหน้าจอและคีย์บอร์ด ของคุณ
22. เชื่อมต่อสายไฟ เข้ากับสายจัมเปอร์แบบสั้นบนแขนการจัดสายเคเบิล
23. ต่อสายเคเบิลและขั้วต่อสัญญาณทั้งหมดเข้ากับขั้วต่อหรือ อุปกรณ์ที่ถูกต้อง
24. ตรวจสอบให้แน่ใจว่าสวิตช์ไฟถูกปิดอยู่ ต่อสายไฟ เข้ากับปลั๊กเสียบไฟฟ้าที่มีกราวด์ หรือ Power Distribution Unit (PDU)

หมายเหตุ: ตรวจสอบให้แน่ใจว่า แรงดันไฟฟ้าของแหล่งจ่ายไฟในท้องถิ่นอยู่ในช่วงไฟกระแสสลับ 100 – 240 โวลต์ ก่อนที่คุณจะเชื่อมต่อสายไฟเข้ากับหัวแปลงปลั๊กไฟ กระแสตรง

25. ดึงถาดออกจากด้านหน้าของตู้ชั้นวาง สอดสายเคเบิล ภายในตู้ชั้นวาง และยึดด้วยแถบรัดสาย

การติดตั้งสวิตช์คอนโซล (ตัวเลือก)

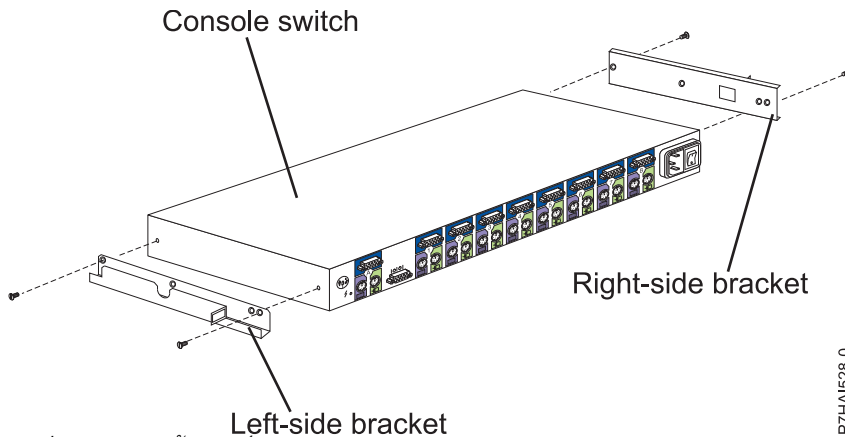
ศึกษาเกี่ยวกับวิธีการติดตั้งสวิตช์คอนโซลที่เป็นตัวเลือก

คุณสามารถใช้สวิตช์คอนโซลเพื่อเชื่อมต่อมากกว่าหนึ่งเซิร์ฟเวอร์ กับคีย์บอร์ดและหน้าจอเดียว ออฟชั่นของสวิตช์คอนโซลสามารถแยกออกจากกัน แต่ขายึดที่กำหนดเองสำหรับสวิตช์จะมีอยู่ในชุดการติดตั้ง

โดยการติดตั้งสวิตช์คอนโซลที่ด้านหลังถาดวางหน้าจอและถาดวางคีย์บอร์ด ทั้งถาดวางหน้าจอและคีย์บอร์ดสามารถใช้พื้นที่ด้วยกัน ในชั้นวาง เพื่อติดตั้งสวิตช์คอนโซลหลังถาดให้ใช้ขายึด ที่มาพร้อมกับชุดการติดตั้ง

ดำเนินการขั้นตอนต่อไปเพื่อติดตั้งสวิตช์คอนโซลด้านหลัง ถาด:

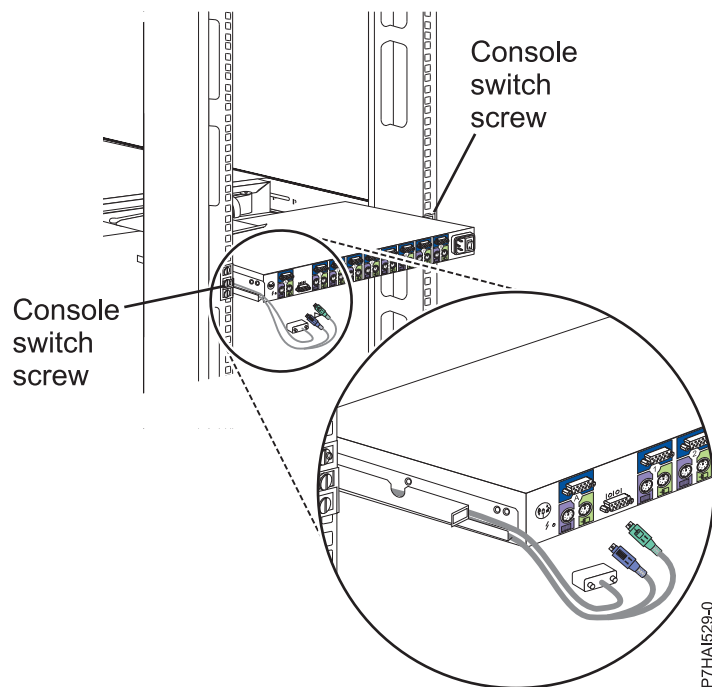
1. ใช้สกรู 8-32 ตัวเพื่อยึดขายึดด้านขวาและซ้าย เข้ากับด้านขวาและด้านซ้ายของสวิตช์คอนโซลตามลำดับ



รูปที่ 83. การติดตั้งสวิตช์คอนโซล

หมายเหตุ: ขายึด ด้านซ้าย จะมีช่องเพื่อสอดสายไฟ, วิดีโอ, คีย์บอร์ด และเมาส์ ตรวจสอบให้แน่ใจว่าคุณติดตั้งขายึดเข้ากับสวิตช์คอนโซล โดยให้ช่องทางด้านซ้ายของขายึดหันขึ้น

2. ติดตั้งสวิตช์คอนโซลด้านหลังถาดวางคีย์บอร์ดและหน้าจอแบน โดยใช้สกรูสี่ตัว (ด้านละสองตัว) ที่มาพร้อมกับชุดฮาร์ดแวร์ต่างๆ
3. สอดสายไฟ, วิดีโอ, คีย์บอร์ด และเมาส์ผ่าน ช่องในขายึดทางด้านซ้ายบนสวิตช์คอนโซล จากนั้น เชื่อมต่อหัวต่อวิดีโอ, คีย์บอร์ด และเมาส์เข้ากับสวิตช์คอนโซล



รูปที่ 84. การกำหนดเส้นทางสาย

4. เชื่อมต่อสายไฟ, การกำหนดเส้นทางสายเคเบิลต่างๆ และการรัดสายเคเบิล สำหรับ คำแนะนำ โปรดดูที่ การเชื่อมต่อ สายไฟเข้ากับสายจัมเปอร์แบบสันบนแผนการจัดการสาย

การกำหนดค่า HMC โดยใช้อินเทอร์เฟซ HMC Classic หรือ HMC Enhanced

ศึกษาเกี่ยวกับวิธีตั้งค่าการเชื่อมต่อเครือข่าย กำหนดค่า HMC ของคุณ ดำเนินการขั้นตอนหลังการกำหนดค่า และอัปเดต และอัปเดต HMC ของคุณโดยใช้อินเทอร์เฟซ HMC Classic หรือ HMC Enhanced

หมายเหตุ:

1. อินเทอร์เฟซ HMC Classic ไม่มีอยู่บน Hardware Management Console (HMC) เวอร์ชัน 8.7.0 หรือเวอร์ชันถัดมาอีกต่อไป ฟังก์ชันที่พร้อมใช้งานกับอินเทอร์เฟซ HMC Classic ก่อนหน้านี้พร้อมใช้งานกับ อินเทอร์เฟซ HMC Enhanced+ แล้ว ในตอนนี้
2. HMC Enhanced GUI มีอยู่บน HMC เวอร์ชัน 8.1.0.1 หรือ 8.2.0 โดยการเลือกอัปเดต HMC Enhanced ขณะที่คุณเลือกเข้าสู่ HMC ตั้งแต่ HMC เวอร์ชัน 8.3.0 โปรดดูและฟังก์ชันของอินเทอร์เฟซ HMC Enhanced ตอนนี้จะเป็นส่วนของ อินเทอร์เฟซ HMC Enhanced+
3. ขึ้นอยู่กับระดับของการปรับแต่งค่าเองที่คุณต้องการกำหนดให้กับคอนฟิกูเรชัน HMC ของคุณ คุณมีตัวเลือกหลายตัวเลือก สำหรับการตั้งค่า HMC เพื่อให้เหมาะสมกับความต้องการของคุณ ตัวช่วยสร้างการติดตั้งที่แนะนำ คือเครื่องมือใน HMC ซึ่งได้รับการออกแบบมาเพื่อช่วยให้การตั้งค่า HMC เป็นไปอย่างง่ายตาย คุณสามารถเลือกใช้วิธีลัดผ่านทางวิซาร์ด เพื่อสร้างสภาวะแวดล้อมของ HMC ตามที่แนะนำได้อย่างรวดเร็ว หรือคุณสามารถเลือกที่จะสำรวจการกำหนดค่าทั้งหมดที่วิซาร์ดแนะนำ คุณยังสามารถดำเนินขั้นตอนกำหนดคอนฟิกโดยใช้ความช่วยเหลือจากวิซาร์ด การกำหนดคอนฟิก HMC โดยใช้เมนู HMC

การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC

เรียนรู้เกี่ยวกับค่าติดตั้งเน็ตเวิร์กที่คุณสามารถใช้บน HMC

การเชื่อมต่อเน็ตเวิร์ก HMC

คุณสามารถใช้การเชื่อมต่อเน็ตเวิร์กประเภทต่างๆ เพื่อเชื่อมต่อ HMC ของคุณกับระบบที่ถูกจัดการสำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีตั้งค่า HMC เพื่อเชื่อมต่อกับเน็ตเวิร์ก โปรดดูที่ “การกำหนดคอนฟิก HMC” ในหน้า 100 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ HMC บนเน็ตเวิร์ก โปรดดูดังต่อไปนี้:

ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC:

เรียนรู้วิธีใช้ฟังก์ชันการจัดการและการให้บริการแบบรีโมต HMC โดยใช้เครือข่ายของคุณ

HMC สนับสนุนการสื่อสารโลจิคัลในประเภทดังต่อไปนี้:

HMC to managed system

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

HMC to logical partition

ใช้เพื่อรวบรวมข้อมูลที่เกี่ยวข้องกับแพลตฟอร์ม (เหตุการณ์ข้อผิดพลาดแพลตฟอร์ม การทำรายการฮาร์ดแวร์) จากระบบปฏิบัติการที่รันอยู่บนโลจิคัลพาร์ติชัน และเพื่อประสานกิจกรรมบางอย่างของแพลตฟอร์ม (LPAR แบบไดนามิก, การซ่อมพร้อมกัน) กับระบบปฏิบัติการเหล่านั้น หากคุณต้องการใช้บริการและคุณลักษณะการแจ้งข้อผิดพลาด คุณต้องสร้างการเชื่อมต่อนี้

HMC กับ BMC

หมายเหตุ: การเชื่อมต่อ baseboard management controller (BMC) ใช้ได้เฉพาะกับโมเดล HMC 7063-CR1 ใช้เพื่อดำเนินการงานการให้บริการและซ่อมบำรุง การเชื่อมต่อ BMC ใช้เพื่อโหลดและดูแลรักษาเฟิร์มแวร์ HMC บนระบบ การเชื่อมต่อนี้จำเป็นสำหรับการเข้าถึง BMC บน HMC

HMC to remote users

ช่วยให้ผู้ใช้รีโมตสามารถเข้าถึงฟังก์ชัน HMC ผู้ใช้รีโมตสามารถ เข้าถึง HMC โดยวิธีดังต่อไปนี้:

- โดยการใช้อยู่ที่เบราว์เซอร์เพื่อเข้าถึงฟังก์ชัน HMC GUI ทั้งหมดแบบรีโมต
- โดยการใช้อยู่ที่ Secure Socket Shell (SSH) เพื่อเข้าถึงฟังก์ชันบรรทัดรับคำสั่ง HMC แบบรีโมต

HMC เพื่อให้บริการ และสนับสนุน

ใช้เพื่อส่งข้อมูล เช่น รายงานความผิดพลาดฮาร์ดแวร์ ข้อมูลคลัง และการอัปเดตไมโครโค้ด ไปยังและจากผู้ให้บริการของคุณ คุณสามารถใช้พารามิเตอร์นี้เพื่อเรียกการให้บริการโดยอัตโนมัติ

HMC ของคุณสามารถสนับสนุนฟิสิกส์อีเทอร์เน็ตอินเทอร์เฟซได้มากถึงสี่อินเทอร์เฟซขึ้นอยู่กับแต่ละรุ่น เวอร์ชันสแตนด์อะโลนของ HMC สนับสนุนอินเทอร์เฟซ HMC สามอินเทอร์เฟซเท่านั้น โดยใช้อีเทอร์เน็ตอะแดปเตอร์รวมหนึ่งอะแดปเตอร์และจนถึงสองอะแดปเตอร์ปลั๊กอิน ใช้อินเทอร์เฟซ แต่ละตัวเหล่านี้ในวิธีดังต่อไปนี้:

- เน็ตเวิร์กอินเทอร์เน็ตเฟสตั้งแต่หนึ่งชั้นไปสามารถใช้เฉพาะสำหรับการสื่อสารแบบ HMC-ไปที่-ระบบที่ถูกจัดการเท่านั้น ซึ่งหมายความว่า เฉพาะ HMC และเซิร์ฟเวอร์เซสเซอร์ของระบบที่ถูกจัดการเท่านั้นที่จะอยู่บนเน็ตเวิร์กนั้น แม้ว่าอินเทอร์เน็ตเฟส เครือข่ายที่อยู่ในตัวประมวลผลเซิร์ฟเวอร์มีการเข้ารหัสโปรโตคอล Secure Sockets Layer (SSL) และมีการป้องกันด้วยรหัสผ่าน การมีเครือข่าย เฉพาะงานที่แยกต่างหากสามารถช่วยให้อินเทอร์เน็ตเฟสเหล่านี้มีระดับความปลอดภัย สูงขึ้น
- โดยทั่วไปแล้ว อินเทอร์เน็ตเฟสเน็ตเวิร์กแบบเปิดใช้กับการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC และโลจิสติกส์พาร์ติชันบนระบบที่ถูกจัดการ สำหรับการสื่อสารแบบ HMC-ไปที่-โลจิสติกส์พาร์ติชัน คุณยังสามารถใช้เน็ตเวิร์กอินเทอร์เน็ตเฟสแบบเปิดนี้เพื่อจัดการกับ HMC จากระยะไกล
- หรือคุณอาจใช้อินเทอร์เน็ตเฟสอื่นเพื่อเชื่อมต่อกับโลจิสติกส์พาร์ติชัน และจัดการ HMC จากระยะไกล อินเทอร์เน็ตเฟสนี้ยังสามารถใช้ในการเชื่อมต่อ HMC แยกต่างหากไปยังกลุ่มโลจิสติกส์พาร์ติชันอื่น ตัวอย่างเช่น คุณอาจต้องการให้มี LAN การจัดการที่แยกต่างหากจาก LAN ซึ่งธุรกรรมทางธุรกิจปกติทั้งหมดกำลัง รันอยู่ ผู้ดูแลระบบจากระยะไกลสามารถเข้าถึง HMC และหน่วยที่ได้รับการจัดการอื่นๆโดยใช้วิธีนี้ ในบางครั้งโลจิสติกส์พาร์ติชันจะอยู่ใน โดเมนความปลอดภัยเครือข่ายอื่น อาจจะเป็นด้านหลังไฟร์วอลล์ และคุณอาจต้องการมี การเชื่อมต่อเครือข่าย HMC ที่แตกต่างกันสำหรับสองโดเมนเหล่านั้น

ข้อกำหนดเว็บเบราว์เซอร์สำหรับ HMC

Hardware Management Console (HMC) เวอร์ชัน 8.7.0 ได้รับการสนับสนุนโดย Google Chrome เวอร์ชัน 57, Microsoft Internet Explorer (IE) เวอร์ชัน 11.0, Mozilla Firefox เวอร์ชัน 45 และ 52 Extended Support Release (ESR) และ Safari เวอร์ชัน 10.1

ถ้า เบราวเซอร์ของคุณมีการกำหนดคอนฟิกเพื่อใช้อินเทอร์เน็ตพรีอ็อกซี โคลด์ IP แอดเดรส ควรมีการรวมไว้ในรายการข้อยกเว้น โพรตปรักษาผู้ดูแลระบบเครือข่าย ของคุณสำหรับข้อมูลเพิ่มเติมเกี่ยวกับรายการข้อยกเว้น ถ้าคุณยังคงจำเป็นต้องใช้พรีอ็อกซีเพื่อเรียกใช้ HMC ให้เปิดใช้งาน การใช้ HTTP 1.1 ผ่านทาง การเชื่อมต่อพรีอ็อกซี ภายใต้แท็บขั้นสูง ในหน้าต่าง อ็อพชันอินเทอร์เน็ต

ต้องเปิดใช้งานเซสชันคุกกีเพื่อให้ ASMI สามารถทำงานได้เมื่อเชื่อมต่อกับ HMC แบบรีโมตรหัสพรีอ็อกซี asm บันทึกและใช้ข้อมูลเซสชัน ปฏิบัติตามขั้นตอนต่อไปเพื่อเปิดใช้งาน เซสชันคุกกี

การเปิดใช้งานเซสชันคุกกีใน Internet Explorer

1. เลือก เครื่องมือ และคลิก อ็อพชันอินเทอร์เน็ต
2. เลือก ความเป็นส่วนตัว และคลิก ขั้นสูง
3. ตรวจสอบให้แน่ใจว่าได้เลือก อนุญาตเซสชันคุกกีเสมอ ถ้ายังไม่ได้เลือก ให้เลือก ยกเลิกการจัดการคุกกีอัตโนมัติ และเลือก อนุญาต เซสชันคุกกีเสมอ
4. เลือก พรอมต์ภายใต้คุกกีของบุคคลที่หนึ่งและคุกกีของบุคคลที่สาม
5. คลิก ตกลง

การเปิดใช้งานเซสชันคุกกีใน Firefox

1. เลือก เครื่องมือ และคลิก อ็อพชัน
2. คลิก คุกกี
3. เลือก อนุญาตให้ไซต์ตั้งค่าคุกกี
4. เลือก ข้อยกเว้น และเพิ่ม HMC
5. คลิก ตกลง

เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC:

HMC สามารถกำหนดคอนฟิกเพื่อใช้เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดได้ เน็ตเวิร์กส่วนตัวอนุญาตให้ใช้ช่วงที่เลือกของ IP-address ที่เราต์ไม่ได้ เน็ตเวิร์กแบบ **พับลิค** หรือแบบ **"เปิด"** หมายถึงการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC กับโลจิสติกส์พาร์ติชันและระบบอื่นๆ 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 อ็อพชัน dual-FSP ในสถานการณ์นี้ FSP ตัวที่สองทำหน้าที่เป็นอุปกรณ์ "สำรอง" โดยหลักๆ แล้ว ข้อกำหนดการติดตั้งระดับต้นสำหรับระบบที่มี 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

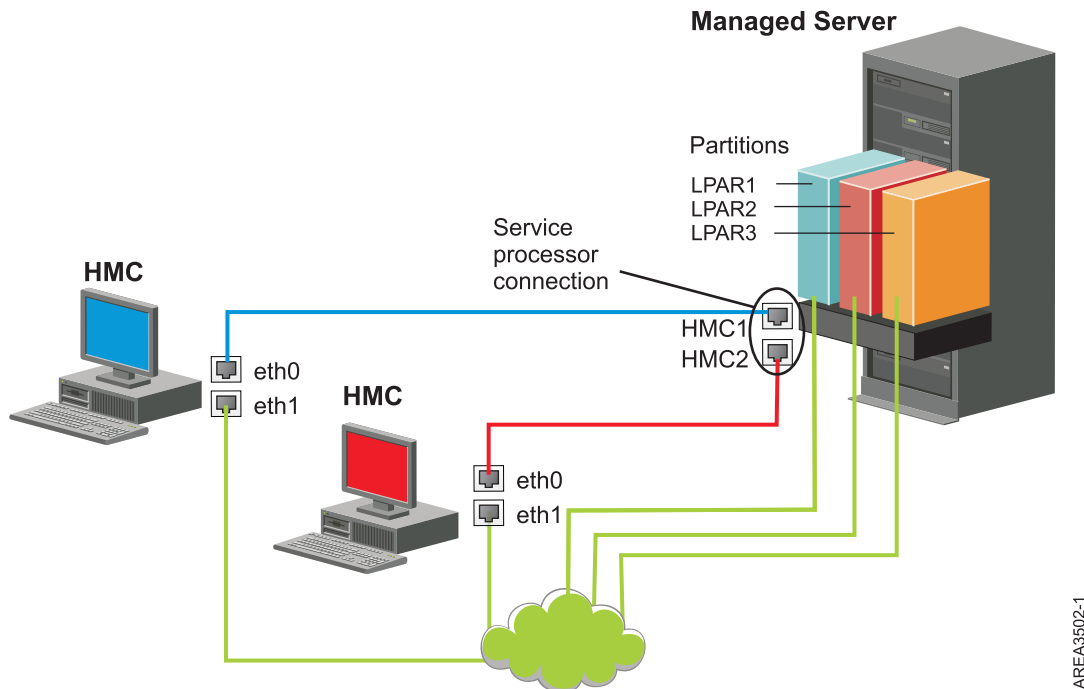
HMC ประกอบด้วยไฟร์วอลล์บนแต่ละ เน็ตเวิร์กอินเตอร์เฟซ ไฟร์วอลล์ระดับต้นจะถูกตั้งค่าโดยอัตโนมัติเมื่อคุณรันวิชาร์ด HMC Guided Setup แต่คุณควรปรับการตั้งค่าไฟร์วอลล์หลังจากการติดตั้งและการคอนฟิก HMC เบื้องต้น

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 109



AREA3502-1

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

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ “การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 109

การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home:

ศึกษาเพิ่มเติมเกี่ยวกับข้อพจน์ของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

คุณสามารถกำหนดคอนฟิก HMC เพื่อส่งข้อมูลที่เกี่ยวข้องกับเซอร์วิส ไปยัง IBM โดยใช้ การเชื่อมต่ออินเทอร์เน็ตแบบใช้ LAN หรือการเชื่อมต่อผ่านโมเด็ม

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

คุณมีตัวเลือกด้านการสื่อสารสองตัวเลือกเมื่อคุณกำหนดคอนฟิกการเชื่อมต่ออินเทอร์เน็ต แบบใช้ LAN ทางเลือกแรกคือใช้ Secure Sockets Layer (SSL) มาตรฐาน สามารถเปิดใช้การสื่อสาร SSL เพื่อเชื่อมต่อ อินเทอร์เน็ตผ่านพรีอซีเซิร์ฟเวอร์ การเชื่อมต่อ SSL มีแนวโน้มว่า จะสอดคล้องกับแนวทางความปลอดภัยขององค์กร ทางเลือกที่สองคือ การใช้การเชื่อมต่อ VPN

หมายเหตุ: หากการเชื่อมต่ออินเทอร์เน็ตเฟสแบบเปิดของคุณใช้เฉพาะ Internet Protocol Version 6 (IPv6) เท่านั้น คุณจะไม่สามารถใช้ Internet VPN ในการเชื่อมต่อเพื่อการสนับสนุนได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรโตคอล ที่ใช้โปรดดู “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 87

ข้อดีของการใช้การเชื่อมต่ออินเทอร์เน็ตอาจได้แก่:

- ความเร็วในการรับส่งข้อมูลที่เร็วกว่า
- ลดค่าใช้จ่ายสำหรับลูกค้า (เช่น ค่าสายโทรศัพท์ท่อน้ำลึก ที่จัดเตรียมไว้โดยเฉพาะ)
- ความเชื่อถือได้สูงกว่า

ลักษณะความปลอดภัยต่อไปนี้มีผลบังคับใช้ไม่ว่าคุณจะใช้วิธีการเชื่อมต่อแบบใดก็ตาม:

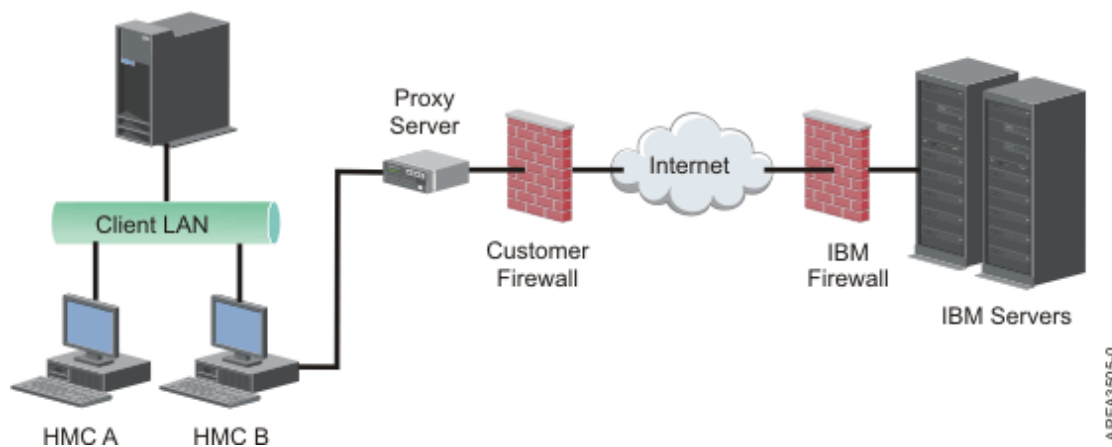
- คำร้องขอของระบบสนับสนุนแบบรีโมตเริ่มต้นจาก HMC ไปยัง IBM การเชื่อมต่อเข้าไม่ได้เริ่มจาก IBM Service Support System
- ข้อมูลทั้งหมดที่โอนระหว่าง HMC และ IBM Service Support System จะถูกเข้ารหัสโดยใช้การเข้ารหัสระดับสูงขึ้นอยู่กับเมธอดของภาวะเชื่อมต่อที่เลือก ซึ่งจะเข้ารหัสโดยใช้ SSL หรือ IPSec Encapsulating Security Payload (ESP)
- เมื่อคุณเริ่มต้นทำงานกับการเชื่อมต่อแบบเข้ารหัส HMC จะพิสูจน์ตัวตน ปลายทางเป้าหมาย นั่นคือ IBM Service Support System

ข้อมูลที่ส่งไปยัง IBM Service Support System ประกอบด้วยข้อมูลเกี่ยวกับปัญหาของฮาร์ดแวร์ และคอนฟิกูเรชัน ไม่มีแอ็พพลิเคชันหรือข้อมูลลูกค้าถูกส่งไปยัง IBM

การใช้การเชื่อมต่ออินเทอร์เน็ตทางอ้อมด้วย พร็อกซีเซิร์ฟเวอร์

หากการติดตั้งของคุณต้องการให้ HMC อยู่บนเครือข่ายแบบไพรเวต คุณต้องเปิดการเชื่อมต่อทางอ้อมผ่านอินเทอร์เน็ต โดยใช้พร็อกซี SSL ซึ่งสามารถส่งคำร้องขอผ่านอินเทอร์เน็ตได้ หนึ่งในข้อดีอีกประการหนึ่งของการใช้พร็อกซี SSL คือ พร็อกซีสามารถสนับสนุนการจัดทำบันทึกและอำนวยความสะดวกด้านการตรวจสอบ

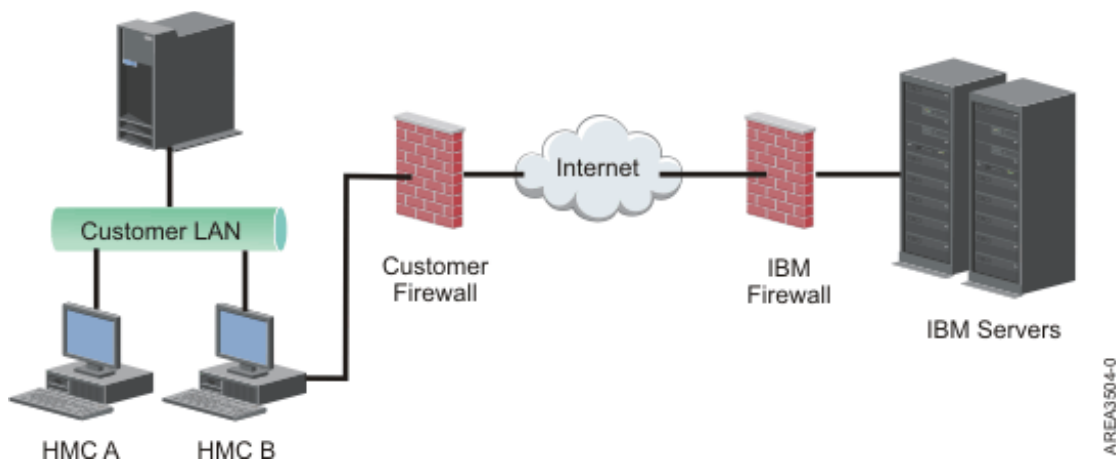
เมื่อต้องการส่งต่อข้อบกพร่อง SSL พร็อกซีเซิร์ฟเวอร์จะต้องสนับสนุนฟังก์ชันส่วนหัวพร็อกซีระดับต้น (ตามที่ระบุไว้ใน RFC 2616) และเมธอด CONNECT หรือ การพิสูจน์ตัวตนพร็อกซีระดับต้น (RFC 2617) สามารถกำหนดคอนฟิก เพื่อให้ HMC พิสูจน์ตัวตนก่อนที่จะพยายามส่งต่อข้อบกพร่องผ่าน พร็อกซีเซิร์ฟเวอร์



เพื่อให้ HMC สื่อสารได้สำเร็จ พร็อกซีเซิร์ฟเวอร์ของลูกค้าจะต้องอนุญาตให้เชื่อมต่อกับพอร์ต 443 คุณสามารถกำหนดคอนฟิกพร็อกซีเซิร์ฟเวอร์ของคุณเพื่อจำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ โปรดดูที่ “รายการแอตเตรส Internet SSL” ในหน้า 87 สำหรับ รายการ IP แอดเดรส

การใช้การเชื่อมต่อ SSL อินเทอร์เน็ตโดยตรง

ถ้า HMC ของคุณ สามารถเชื่อมต่ออินเทอร์เน็ต และสามารถตั้งค่าไฟร์วอลล์ภายนอก เพ่อนุญาตให้ส่งแพ็กเก็ต TCP ไปยังปลายทางที่ระบุไว้ใน “รายการแอตเดรส Internet SSL” ในหน้า 87 คุณจะสามารถใช้ การเชื่อมต่ออินเทอร์เน็ตโดยตรงได้



ภาวะเชื่อมต่อแบบง่าย:

ศึกษาเกี่ยวกับ IP address ที่ HMC ใช้เมื่อกำลังใช้ ภาวะเชื่อมต่อแบบง่าย

สภาวะแวดล้อมของเซิร์ฟเวอร์ call-home แบบใหม่มีให้พร้อมใช้แล้ว ซึ่งได้จัดเตรียมพรีอ็อกซีแบบ front-end ให้กับโครงสร้างพื้นฐาน call-home ในปัจจุบัน สภาวะแวดล้อมนี้ช่วยจัดหาข้อมูลด้านเทคโนโลยีที่จำเป็นต้องมีได้ง่ายขึ้นโดยลดจำนวนเซิร์ฟเวอร์ของ IBM ลง เปิดใช้งานภาวะเชื่อมต่อ IPv6 และจัดเตรียมการรักษาความปลอดภัยที่ได้รับการพัฒนาแล้วโดยสนับสนุน NIST 800-131A คุณมี IBM IP address เพียงไม่กี่หมายเลขที่เปิดอยู่บนไฟร์วอลล์ของคุณ อินเทอร์เน็ตทราฟฟิก call-home ทั้งหมด จะไหลผ่านพรีอ็อกซี call-home

หมายเหตุ: ภาวะเชื่อมต่อแบบง่ายพร้อมใช้งานบน HMC เวอร์ชัน 8.3.0 หรือ เวอร์ชันถัดมา

HMC ใช้ IPv4 address ต่อไปนี้เพื่อติดต่อกับฝ่ายสนับสนุนและฝ่ายบริการของ IBM เมื่อกำหนดคอนฟิก เพื่อใช้ภาวะเชื่อมต่อแบบง่าย:

- 129.42.56.189
- 129.42.60.189
- 129.42.54.189

HMC ใช้ IPv6 address ต่อไปนี้เพื่อติดต่อกับฝ่ายสนับสนุนและฝ่ายบริการของ IBM เมื่อกำหนดคอนฟิก เพื่อใช้ภาวะเชื่อมต่อแบบง่าย:

- 2620:0:6c0:200:129:42:56:189
- 2620:0:6c2:200:129:42:60:189
- 2620:0:6c4:200:129:42:54:189

การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต:

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

หมายเหตุ: พอร์ต HTTPS มาตรฐาน 443 ใช้สำหรับการสื่อสารทั้งหมด

HMC สามารถเปิดใช้งานเพื่อเชื่อมต่อโดยตรงกับอินเทอร์เน็ต หรือเพื่อเชื่อมต่อทางอ้อมจากฟร็อกซีเซิร์ฟเวอร์ที่ถูกตั้งค่าให้ การตัดสินใจเกี่ยวกับแนวทางที่เหมาะสมที่สุดสำหรับการติดตั้งของคุณขึ้นอยู่กับข้อกำหนดความปลอดภัยและระบบเน็ตเวิร์กของ 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 110 และ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 110

รายการแอดเดรส Internet SSL:

ศึกษาเกี่ยวกับแอดเดรสที่ HMC ใช้เมื่อใช้ภาวะเชื่อมต่อ Internet SSL

HMC จะใช้แอดเดรส IPv4 ต่อไปนี้เพื่อติดต่อส่วนบริการ และส่วนสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้การเชื่อมต่ออินเทอร์เน็ตแบบ SSL

แอดเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่:

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

แอดเดรส IPv4 ต่อไปนี้สำหรับทวีปอเมริกา:

- 129.42.160.48
- 129.42.160.49

- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

แอดเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่ที่ไม่ใช่อเมริกา:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

หมายเหตุ: เมื่อตั้งค่าไฟร์วอลล์เพื่่อนุญาตให้ HMC สามารถเชื่อมต่อกับเซิร์ฟเวอร์เหล่านี้จะต้องใช้ IP แอดเดรสที่เฉพาะเจาะจงสำหรับภูมิภาคดังกล่าวเท่านั้น

HMC จะใช้แอดเดรส IPv6 ต่อไปนี้เพื่อติดต่อส่วนบริการและส่วนสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้การเชื่อมต่ออินเทอร์เน็ตแบบ SSL:

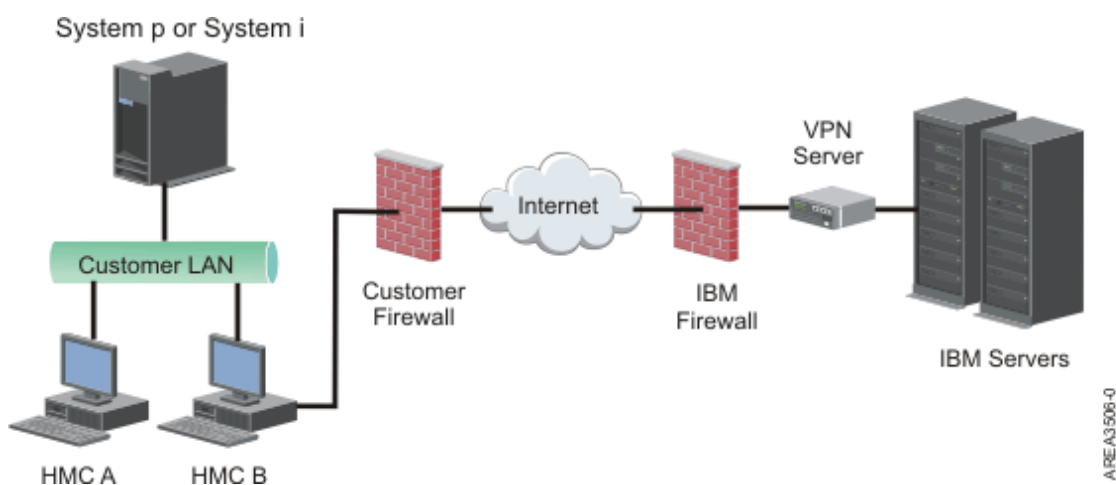
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล:

virtual private network (VPN) จัดเตรียมความปลอดภัย เมื่อคุณเชื่อมต่อกับส่วนสนับสนุนแบบรีโมต

หมายเหตุ: การเชื่อมต่อชนิดนี้พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือเวอร์ชันก่อนหน้านี้นี้เท่านั้น

VPN ช่วยรักษาความเป็นส่วนตัวของเน็ตเวิร์กที่แยกต่างหากบนสายสาธารณะโดยทดแทนการเข้ารหัสและมาตรการความปลอดภัยอื่นๆ สำหรับสายเน็ตเวิร์ก ที่แยกออกจากกันในทางกายภาพของเน็ตเวิร์กส่วนตัวแบบเก่า นอกจากนี้ยังสามารถใช้สำหรับการเชื่อมต่อขาออกแล้ว การเชื่อมต่อ VPN ยังสามารถกำหนดคอนฟิกได้ตามต้องการ เพื่อสนับสนุน service request แบบรีโมต



เป็นความรับผิดชอบของผู้ดูแลระบบในการเตรียมการเชื่อมต่ออินเทอร์เน็ต ไฟร์วอลล์ยังสามารถจำกัด IP address ที่ระบุเฉพาะเพื่อให้ HMC สามารถเชื่อมต่อได้ ถ้าคุณต้องการกำหนดคอนฟิกไฟร์วอลล์ของคุณ เพื่อจำกัด IP แอดเดรสโปรโตคอลที่ “รายการแอดเดรสเซิร์ฟเวอร์ VPN” สำหรับ รายการแอดเดรสที่คุณสามารถใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการเชื่อมต่อกับอินเทอร์เน็ตโดยใช้ LAN-based VPN โปรดดู “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104

รายการแอดเดรสเซิร์ฟเวอร์ VPN:

แสดงรายการเซิร์ฟเวอร์ที่ถูกใช้โดย HMC เมื่อกำหนดคอนฟิก HMC ให้ใช้ภาวะเชื่อมต่อกับอินเทอร์เน็ตโดยใช้ VPN

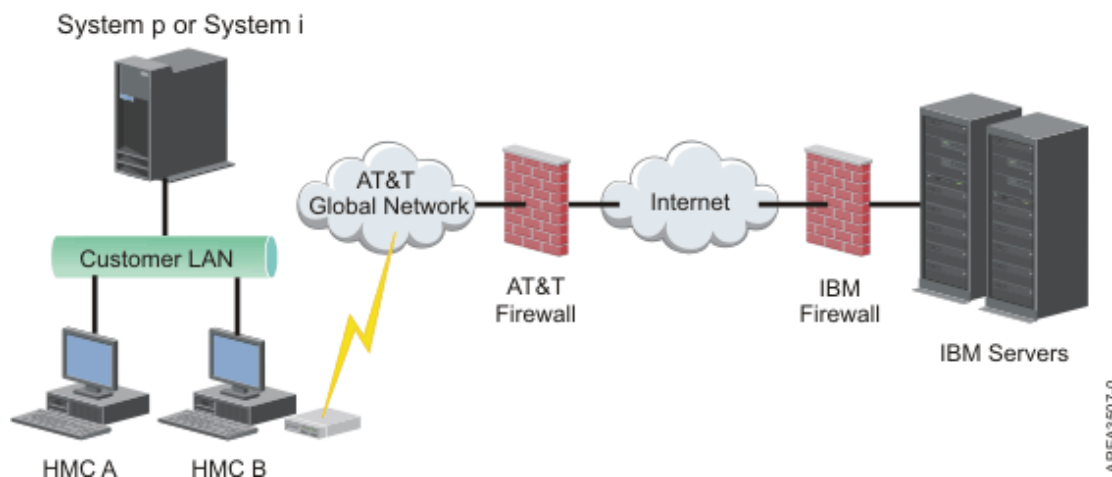
เซิร์ฟเวอร์ต่อไปนี้ใช้โดย HMC เมื่อถูกกำหนดคอนฟิกให้ใช้การเชื่อมต่อ VPN อินเทอร์เน็ต การเชื่อมต่อทั้งหมดใช้ ESP และ UDP บนพอร์ต 500 และพอร์ต 4500 เมื่อกำลังใช้ไฟร์วอลล์ Network Address Translation (NAT)

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต:

ถ้าคุณต้องการใช้โมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต คุณจะต้องจัดหาสายอะนาล็อกแบบเฉพาะงานเพื่อเชื่อมต่อกับโมเด็ม HMC HMC ใช้โมเด็มเพื่อต่อเลขหมายไกลบอลเน็ตเวิร์กและเพื่อเชื่อมต่อกับฝ่ายสนับสนุนแลฝ่ายบริการของ IBM

หมายเหตุ: ประเภทการเชื่อมต่อนี้พร้อมใช้งานบน HMC เวอร์ชัน 8.2.0 หรือเวอร์ชันก่อนหน้านี้นี้เท่านั้น



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเชื่อมต่อฝ่ายสนับสนุนแบบรีโมตโดยใช้โทรศัพท์และโมเด็ม โปรดดู “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104

การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์:

หัวข้อนี้จะอธิบายถึงสิ่งที่คุณจำเป็นต้องทราบเมื่อตัดสินใจใช้เซิร์ฟเวอร์ Call-Home มากกว่าหนึ่งเครื่อง

เมื่อต้องการหลีกเลี่ยงไม่ให้ความล้มเหลวแม้แต่จุดเดียวให้คอนฟิก HMC ให้ใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานเซิร์ฟเวอร์แรก จะพยายามจัดการเหตุการณ์เซอร์วิสแต่ละเหตุการณ์ หากการเชื่อมต่อ หรือการส่งข้อมูลล้มเหลว กับเซิร์ฟเวอร์ Call-Home นี้ จะมีการพยายามร้องขอเซอร์วิสอีกครั้งโดยใช้ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานอื่นจนกว่าจะประสบความสำเร็จหรือได้พยายามกับ ทุกเซิร์ฟเวอร์แล้ว

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

- HMC หลักถูกกำหนดคอนฟิกให้ใช้เซิร์ฟเวอร์ Call-Home ที่ "ค้นพบ" โดยเซิร์ฟเวอร์ Call-Home จะอยู่บนซับเน็ตเดียวกันกับ HMC หลัก หรือจัดการระบบเดียวกัน
- มีการเพิ่มเซิร์ฟเวอร์ Call-Home ด้วยตนเองลงในรายการ คอนโซลเซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานสำหรับการเชื่อมต่อภายนอก

การจัดเตรียมสำหรับการตั้งค่าของ HMC

ใช้ส่วนนี้เพื่อรวบรวมการตั้งค่าการตั้งค่าที่จำเป็นที่คุณต้องทราบก่อนเริ่มขั้นตอนการตั้งค่า

เมื่อต้องการกำหนดคอนฟิก HMC คุณต้องเข้าใจ แนวคิดที่เกี่ยวข้อง ดำเนินการตัดสินใจ และจัดเตรียมการติดตั้ง

ส่วนนี้อธิบายข้อมูลที่คุณจะต้องใช้เพื่อเชื่อมต่อ HMC กับรายการต่อไปนี้:

- เซอร์วิสโพรเซสเซอร์ในระบบที่ถูกจัดการของคุณ
- โลจิคัลพาร์ติชันในระบบที่ถูกจัดการเหล่านั้น
- รีโมตเวิร์กสเตชัน
- IBM Service เพื่อนำฟังก์ชัน “call-home” ไปใช้

หมายเหตุ: มีข้อมูลการเชื่อมต่อและความปลอดภัยเพิ่มเติมพร้อมให้ใช้งาน สำหรับข้อมูลเพิ่มเติม ให้อ่านที่ ESA for HMC Connectivity Security สำหรับ IBM POWER6®, POWER7 และ POWER8 Processor-Based Systems และรายงานอย่างเป็นทางการของ IBM Storage Systems DS8000® จะมีอยู่ที่: IBM Electronic Service Agent™ (<http://www-01.ibm.com/support/esa/security.htm>)

เมื่อต้องการจัดเตรียมสำหรับการตั้งค่า HMC ให้ดำเนินการขั้นตอน ต่อไปนี้:

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 “เน็ตเวิร์กส่วนตัว และเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 82

5. หากคุณใช้เน็ตเวิร์กเปิดเพื่อจัดการกับ FSP คุณต้องตั้งค่าแอตเตอร์สของ FSP ผ่านเมนู Advanced System Management Interface ด้วยตนเอง ขอแนะนำให้คุณใช้เน็ตเวิร์กส่วนตัวที่ไม่สามารถกำหนดเรตได้
6. หากคุณมีสอง HMC ให้กำหนด HMC หลักและรอง HMC หลักควรมีตำแหน่งที่ใกล้กับเครื่องมากกว่า และควรเป็น HMC ที่คอนฟิกร์ให้ติดต่อผู้ให้บริการ
7. กำหนดการตั้งค่าเน็ตเวิร์กที่คุณจะต้องใช้เพื่อเชื่อมต่อ HMC กับรีโมตเวิร์กสเตชัน โลจิคัลพาร์ติชัน และอุปกรณ์เน็ตเวิร์ก
8. กำหนดวิธีที่ HMC จะ “call home” อ็อพชัน Call home รวมถึง การเชื่อมต่ออินเทอร์เน็ตแบบ Secure Socket Layer (SSL) ขาออกเท่านั้น โหมด หรือการเชื่อมต่อ Virtual Private Network (VPN)
9. กำหนดผู้ใช้ HMC ที่คุณจะใช้สร้าง พร้อมทั้งรหัสผ่าน และบทบาทของผู้ใช้เหล่านั้น คุณต้องระบุรหัสผ่านให้กับผู้ใช้ hscroot และ hscope
10. จัดทำเอกสารแสดงข้อมูลติดต่อบริษัทดังต่อไปนี้ ซึ่งจะต้องใช้เมื่อกำหนดคอนฟิกร์ call home:
 - ชื่อบริษัท
 - การติดต่อผู้ดูแลระบบ
 - อีเมลแอตเตอร์ส
 - หมายเลขโทรศัพท์
 - หมายเลขแฟกซ์
 - แอตเตอร์สของที่ตั้งทางกายภาพของ HMC
11. หากคุณวางแผนที่จะใช้อีเมลเพื่อแจ้งเตือนโอเพอเรเตอร์ หรือผู้ดูแลระบบ เมื่อข้อมูลถูกส่งไปยัง IBM Service ผ่าน call-home, ให้ระบุเซิร์ฟเวอร์ Simple Mail Transfer Protocol (SMTP) และแอตเตอร์สอีเมลที่คุณจะใช้
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 “เวิร์กชิตเตรียมการติดตั้งและการคอนฟิกร์สำหรับ HMC”

เวิร์กชิตเตรียมการติดตั้งและการคอนฟิกร์สำหรับ HMC

ใช้เวิร์กชิตนี้เพื่อดูข้อมูลการติดตั้งที่คุณต้องเตรียมพร้อมสำหรับการติดตั้ง

ค่ากำหนดเน็ตเวิร์ก

อินเทอร์เน็ตเฟส LAN: เลือกอะแดปเตอร์ที่มี (เช่น eth0, eth1) ซึ่งจะใช้โดย HMC นี้เพื่อเชื่อมต่อกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน บริการและการสนับสนุน รวมถึงผู้ใช้รีโมต โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80 สำหรับข้อมูลเพิ่มเติม การเชื่อมต่อจาก HMC สามารถอยู่บนเน็ตเวิร์กส่วนตัวหรือเน็ตเวิร์กแบบเปิด

ความเร็วของอีเทอร์เน็ตอะแดปเตอร์และ Duplex

ป้อนความเร็วของอีเทอร์เน็ตอะแดปเตอร์ที่ต้องการและโหมด duplex อ็อพชัน autodetection จะระบุว่าคุณใช้อ็อพชันใดเหมาะสมที่สุด ถ้าคุณไม่แน่ใจว่าความเร็ว และ duplex ใดจะก่อให้เกิดผลลัพธ์ที่ดีที่สุดสำหรับฮาร์ดแวร์ของคุณ

ดีฟอลต์ = Autodetection ความเร็วของสื่อบันทึกที่ระบุความเร็วในโหมด duplex ของอีเทอร์เน็ตอะแดปเตอร์เลือก Autodetection ยกเว้นว่าคุณมีข้อกำหนดในการระบุความเร็วสื่อบันทึกแบบคงที่อุปกรณ์ใดๆ ที่เชื่อมต่อกับ FSP (สวิตช์/HMC) ต้องมีการตั้งค่าเป็นโหมด อัตโนมัต (ความเร็ว) / อัตโนมัต (ดูเพล็กซ์) เนื่องจากเป็นค่าติดตั้ง FSP ดีฟอลต์และไม่สามารถเปลี่ยนได้

ตารางที่ 11. ความเร็วของอีเทอร์เน็ตอะแดปเตอร์และ Duplex

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

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเน็ตเวิร์กแบบเปิดและเน็ตเวิร์กส่วนตัว โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC” ในหน้า 82

ตารางที่ 12. เครือข่ายแบบไพรเวตและเครือข่ายแบบเปิด

	eth0	eth1	eth2	eth3
ระบุเน็ตเวิร์กแบบ ส่วน ตัว หรือ เปิด สำหรับแอด อะแดปเตอร์				

Dynamic Host Configuration Protocol (DHCP) มีวิธีอัตโนมัติสำหรับการตั้งค่าคอนฟิกไคลเอ็นต์แบบไดนามิก คุณสามารถระบุ HMC นี้เป็นเซิร์ฟเวอร์ DHCP ถ้าเป็น HMC เครื่องแรกหรือเครื่องเดียวบนเน็ตเวิร์กส่วนตัว ให้เปิดใช้งาน HMC เป็นเซิร์ฟเวอร์ DHCP เมื่อคุณทำสิ่งนี้ระบบที่ถูกจัดการบนเน็ตเวิร์ก จะถูกตั้งค่าและค้นพบโดย HMC โดยอัตโนมัติ

สำหรับอีเทอร์เน็ตอะแดปเตอร์ที่ระบุ เป็นเน็ตเวิร์กส่วนตัว ให้ดำเนินการตามตารางต่อไปนี้:

ตารางที่ 13. เน็ตเวิร์กส่วนตัว

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

หากคุณกำลังใช้ 7063-CR1 HMC คุณ ต้องเชื่อมต่อพอร์ต Ethernet IPMI กับเครือข่ายเพื่อเข้าถึง baseboard management controller (BMC) บน HMC สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “กำหนดค่าการเชื่อมต่อ BMC” ในหน้า 163 กรอกข้อมูลในตารางต่อไปนี้สำหรับการเชื่อมต่อ BMC ของคุณ

ตารางที่ 14. การเชื่อมต่อ BMC

	IPMI
คุณต้องการกำหนดค่าการเชื่อมต่อโดยใช้โหมด DHCP หรือไม่ (ใช่/ไม่ใช่)	
หากไม่ แสดงรายการสแตติกแอดเดรสที่ระบุด้านล่าง:	
IP แอดเดรส:	
Subnet mask:	
เกตเวย์:	

สำหรับฮาร์ดแวร์แต่ละรุ่นที่ระบุเป็นเน็ตเวิร์ก เปิดให้ดำเนินการตามตารางต่อไปนี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ อินเทอร์เน็ตโปรโตคอลเวอร์ชันอื่น โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 87

การใช้ IPv6

หากคุณกำลังใช้ IPv6 ให้ปรึกษากับผู้บริหารเน็ตเวิร์กของคุณ แล้วเลือกวิธีที่คุณต้องการใช้รับ IP แอดเดรส หลังจากนั้นให้ดำเนินการตาม ตารางต่อไปนี้:

ตารางที่ 15. การใช้ IPv6

	eth0	eth1	eth2	eth3
คุณกำลังใช้ IP แอดเดรสที่มีการกำหนดไว้อย่างคงที่ใช่หรือไม่? หากใช่ให้บันทึกแอดเดรสนั้นไว้ที่นี่				

ตารางที่ 16. การใช้ IPv6

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

ตารางที่ 17. การใช้ IPv6

	eth0	eth1	eth2	eth3
คุณกำลังรับ IP แอดเดรสจากเราเตอร์ IPv6 ใช่หรือไม่?				

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า IPv6 address โปรดดูที่ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 110 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ IPv6 แอดเดรสเท่านั้น โปรดดูที่ “การใช้ IPv6 แอดเดรสเท่านั้น” ในหน้า 110

การใช้ IPv4

ดำเนินการตามตารางต่อไปนี้สำหรับอีเทอร์เน็ตอะแดปเตอร์ที่ระบุเป็น เน็ตเวิร์กเปิดโดยใช้ IPv4

ตารางที่ 18. การใช้ IPv4

	eth0	eth1	eth2	eth3
คุณต้องการรับ IP แอดเดรสโดยอัตโนมัติหรือไม่? (ใช่/ไม่ใช่)				
ถ้า ไม่ แสดงรายการแอดเดรสที่ระบุด้านล่าง:				
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 ตามค่าดีฟอลต์สำหรับ LAN ส่วนตัวแบบโลคัล ถ้า โหนดจะถูกเชื่อมต่อกับเน็ตเวิร์กขนาดใหญ่ที่มีแอดเดรส TCP/IP ที่ถูกจัดการ คุณสามารถระบุแอดเดรส TCP/IP ที่จะใช้ ระบบจะสร้าง ค่าดีฟอลต์

ค่าติดตั้งไฟร์วอลล์

ค่าติดตั้งไฟร์วอลล์ HMC จะสร้างเครื่องกีดกันด้านความปลอดภัยที่อนุญาตหรือปฏิเสธ การเข้าถึงเน็ตเวิร์กแอปพลิเคชันที่เฉพาะเจาะจงบน HMC คุณสามารถระบุ ค่าติดตั้งการควบคุมเหล่านี้สำหรับฟิสิคัลเน็ตเวิร์กอินเตอร์เฟซแต่ละชุด ซึ่งทำให้ คุณสามารถควบคุมว่าเน็ตเวิร์กอินเตอร์เฟซ HMC ใดจะสามารถเข้าถึงไดบนแต่ละเน็ตเวิร์ก

ถ้าคุณได้ตั้งค่าอย่างน้อยหนึ่งอะแดปเตอร์เป็น เน็ตเวิร์กอะแดปเตอร์แบบเปิด คุณจะต้องจัดหาข้อมูลเพิ่มเติมต่อไปนี้ เพื่อให้ HMC ของคุณสามารถเข้าถึง LAN:

ตารางที่ 19. ข้อมูลโฮสต์แบบโลคัล

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

ข้อมูลโฮสต์แบบโลคัล

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

ข้อมูลเกตเวย์

เมื่อต้องการกำหนดเกตเวย์ดีฟอลต์ให้ใส่แอดเดรส TCP/IP ที่จะใช้สำหรับการเร้าต์แพ็กเก็ต IP แอดเดรสเกตเวย์จะแจ้งคอมพิวเตอร์แต่ละเครื่องหรืออุปกรณ์ เน็ตเวิร์กแต่ละอุปกรณ์ว่าจะส่งข้อมูลเมื่อใด ถ้าสถานะเป้าหมายไม่ได้ระบุให้ เน็ตเวิร์กย่อยเป็นต้นทาง

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 สำหรับการแม็ปชื่อโฮสต์ และ IP แอดเดรส ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

ลำดับการค้นหาโดเมนซัพฟิ็กซ์

ป้อนโดเมนซัพฟิ็กซ์ที่คุณกำลังใช้ HMC จะใช้โดเมนซัพฟิ็กซ์ เพื่อผนวกเข้ากับชื่อที่ไม่ถูกต้องสำหรับการค้นหา DNS ซัพฟิ็กซ์จะถูกค้นหาตามลำดับที่แสดงอยู่ในรายการ ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

การแจ้งเตือนทางอีเมล

ลิสต์ข้อมูลติดต่อทางอีเมล ถ้าคุณต้องการได้รับแจ้งทางอีเมล เมื่อเกิดปัญหาเกี่ยวกับฮาร์ดแวร์กับระบบของคุณ

ตารางที่ 20. การแจ้งเตือนทางอีเมล

ฟิลด์	
อีเมลแอดเดรส:	
เซิร์ฟเวอร์ SMTP:	
พอร์ต:	
ข้อผิดพลาดที่จะแจ้ง:	
เฉพาะปัญหา call-home เท่านั้น	
ปัญหาทั้งหมด	

เซิร์ฟเวอร์ SMTP

พิมพ์แอดเดรส simple mail transfer Protocol (SMTP) ของเซิร์ฟเวอร์ที่จะได้รับแจ้งเกี่ยวกับเหตุการณ์ของระบบ ตัวอย่างของชื่อเซิร์ฟเวอร์ SMTP คือ relay.us.ibm.com

SMTP เป็นโปรโตคอลที่ใช้ในการส่งอีเมล เมื่อใช้ SMTP โคลเอ็นต์จะส่งข้อความและสื่อสาร กับเซิร์ฟเวอร์ SMTP โดยใช้โปรโตคอล SMTP

ถ้าคุณไม่ทราบแอดเดรส SMTP ของเซิร์ฟเวอร์ของคุณ หรือไม่แน่ใจให้ติดต่อ 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

ตารางที่ 21. ข้อมูลติดต่อฝ่ายบริการ

ข้อมูลติดต่อฝ่ายบริการ	
ชื่อบริษัท	

ตารางที่ 21. ข้อมูลติดต่อฝ่ายบริการ (ต่อ)

ข้อมูลติดต่อฝ่ายบริการ	
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 84

ตารางที่ 22. ชนิดของการเชื่อมต่อ

ชนิดของการเชื่อมต่อ	
	Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต

ตารางที่ 22. ชนิดของการเชื่อมต่อ (ต่อ)

ชนิดของการเชื่อมต่อ	
	เรียกเลขหมายจาก HMC แบบโลคัล
	Virtual private network (VPN) ผ่านอินเทอร์เน็ต

Secure Sockets Layer (SSL) ผ่านอินเทอร์เน็ต:

ถ้าคุณมีการเชื่อมต่ออินเทอร์เน็ตจาก HMC ของคุณ คุณสามารถใช้การเชื่อมต่อดังกล่าวเพื่อติดต่อผู้ให้บริการ คุณสามารถเชื่อมต่อโดยตรงกับผู้ให้บริการของคุณโดยใช้ Secure Sockets Layer (SSL) แบบเข้ารหัส ซึ่งใช้การเชื่อมต่ออินเทอร์เน็ตที่มีอยู่ เลือกใช้พร็อกซี SSL ถ้าคุณต้องการกำหนดคอนฟิกการใช้ SSL ที่เข้ารหัสโดยใช้การเชื่อมต่อทางอ้อมซึ่งใช้พร็อกซี SSL

ตารางที่ 23. Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต

Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต	
ใช้พร็อกซี SSL? (ใช่/ไม่ใช่)	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
แอดเดรส:	
พอร์ต:	
พิสูจน์ตัวตนด้วยพร็อกซี SSL?	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
ผู้ใช้:	
รหัสผ่าน:	

โปรโตคอลการเชื่อมต่ออินเทอร์เน็ตที่ใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอินเทอร์เน็ตโปรโตคอลอื่น โปรดดูที่ “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 87

___ IPv4

___ IPv6

___ IPv4 และ IPv6

เรียกเลขหมายจาก HMC แบบโลคัล

ป้อนข้อมูลเรียกเลขหมายเพื่อตั้งค่าโลคัลโมเด็มของคุณ ระบุหมายเลขโทรศัพท์ที่ใช้ในการต่อเลขหมายไปยังผู้ให้บริการ เมื่อคุณกำลังเชื่อมต่อ หมายเลขโทรศัพท์จะถูกต่อเลขหมายตามลำดับที่แสดงในรายการ

ตารางที่ 24. เรียกเลขหมายจาก HMC แบบโลคัล

ฟิลด์	
คำแนะนำสำหรับต่อเลขหมาย:	

ตารางที่ 24. เรียกเลขหมายจาก HMC แบบโลคัล (ต่อ)

ฟิลด์	
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 89

___ HMC นี้

___ HMC อื่น

หากคุณได้ตรวจสอบ HMC อื่น ให้แสดงรายการ HMC อื่นที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home ที่นี้:

ตารางที่ 25. HMC อื่นที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home

รายชื่อโฮสต์ HMC หรือ IP แอดเดรส ที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home

คุณสมบัติเพิ่มเติมสำหรับการสนับสนุน

My Systems และ Premium Search

ฟิลด์	
แสดงรายการ IBM ID ของคุณ	
แสดงรายการ IBM ID ของคุณ	

เพื่อเข้าถึงข้อมูลการสนับสนุนที่มีคุณค่าและกำหนดเอง ในส่วนระบบของเงินและการค้นหาแบบพิเศษของเว็บไซต์ 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 เพื่อข้อมูลการสนับสนุนที่มีประโยชน์ซึ่งพร้อมใช้งานสำหรับลูกค้าที่ลงทะเบียน IBM ID ไว้กับระบบ

การกำหนดคอนฟิก HMC

กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก ความปลอดภัย เซอร์วิสแอปพลิเคชัน และความต้องการส่วนตัวบางอย่างของผู้ใช้

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

ก่อนที่จะเริ่มต้น ให้รวบรวมข้อมูลการตั้งค่าที่ต้องการ ซึ่งคุณจำเป็นต้องปฏิบัติตามขั้นตอนต่างๆ ให้เสร็จสิ้นอย่างสมบูรณ์ โปรดดูที่ “การเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90 สำหรับ รายการของข้อมูลที่ต้องการ เมื่อคุณเตรียมการเสร็จสิ้น ตรวจสอบให้แน่ใจว่าคุณเสร็จสิ้น “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91 และกลับไปสู่ส่วนนี้

การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ผ่านทางวิซาร์ดเซตอัพที่แนะนำ

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

เริ่มต้น HMC และปฏิบัติตามขั้นตอนในวิซาร์ดเซตอัพที่แนะนำ:

ล็อกอินเข้าสู่อินเตอร์เฟซ HMC และตั้งค่า HMC ของคุณโดยใช้วิซาร์ด Guided Setup

หมายเหตุ: หากเป็นการติดตั้งใหม่ ตรวจสอบให้แน่ใจว่าระบบที่ถูกจัดการ ไม่ได้เชื่อมต่อกับแหล่งกำเนิดไฟฟ้า สำหรับ HMC ที่ติดตั้งในชั้นวาง หมายความว่าเฉพาะอุปกรณ์ที่เสียบกับบัสกระจายกำลังไฟฟ้า (PDB) ก่อนที่คุณ จะเสียบแหล่งจ่ายไฟหลัก คือ HMC ถ้านี้เป็น HMC เครื่องที่สองที่เชื่อมต่อกับระบบที่ถูกจัดการระบบเดียวกัน ก็จะสามารถเชื่อมต่อกับระบบที่ถูกจัดการเข้ากับแหล่งกำเนิดไฟฟ้า

1. เปิด HMC โดยกดปุ่มเปิด/ปิด.
2. โปรดรอให้ HMC เลือกภาษาดีฟอลต์และค่าติดตั้งโลแคล ประมาณ 30 วินาที
3. ยอมรับข้อตกลงไลเซนส์ของ คอนโซลการจัดการฮาร์ดแวร์ หากคุณไม่ยอมรับข้อตกลงไลเซนส์ของ คอนโซลการจัดการฮาร์ดแวร์ คุณก็จะไม่สามารถกำหนดคอนฟิกของ HMC ให้เสร็จสิ้นได้
4. คลิก ล็อกคอนและเรียกใช้เว็บแอปพลิเคชัน **Hardware Management Console**
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: หาก ตัวช่วยสร้างการติดตั้งที่แนะนำ ไม่ปรากฏขึ้นเมื่อคุณเริ่มต้น HMC ให้คลิก **Guided Setup Wizard** ในพื้นที่การนำทางของเพจต้อนรับเข้าสู่ HMC

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

ตรวจทานคอนฟิกเรชั่นของคุณ:

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

การกำหนดคอนฟิก HMC โดยใช้เมนู HMC

ส่วนนี้มีรายการที่ครบถ้วนของงานคอนฟิกเรชั่น HMC ทั้งหมด ซึ่งช่วยแนะแนวทางตลอดกระบวนการกำหนดคอนฟิก HMC ของคุณ เลือก อีพชั่นนี้ถ้าคุณไม่ต้องการใช้ ตัวช่วยสร้างการติดตั้งที่แนะนำ

คุณต้องรีสตาร์ท HMC เพื่อให้ค่าติดตั้งคอนฟิกเรชั่นมีผลใช้งาน ดังนั้น คุณอาจต้องการพิมพ์รายการตรวจสอบนี้ และเก็บไว้กับคุณเมื่อทำการกำหนดคอนฟิก HMC

ข้อมูลนี้ประกอบด้วยภาษาอังกฤษถึงงานที่ไม่รวมอยู่ใน PDF นี้ คุณสามารถเข้าถึงสื่อประกอบเพิ่มเติม ที่สนับสนุนได้โดยอ้างอิงถึง ส่วนของ **Additional Resources** บนหน้า HMC Welcome

สิ่งที่ต้องการก่อน

ก่อนที่คุณจะเริ่มกำหนดคอนฟิก HMC โดยใช้เมนู HMC ตรวจสอบให้แน่ใจว่าได้ทำงานจัดเตรียมคอนฟิกูเรชัน ตามที่อธิบายใน “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90 แล้ว

ตารางที่ 27. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่ที่สามารถหาข้อมูลที่เกี่ยวข้องได้

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. สตาร์ท HMC	“การเริ่มต้น HMC” ในหน้า 103
2. ตั้งค่าวันที่และเวลา	
3. เปลี่ยนรหัสผ่านที่กำหนดไว้ล่วงหน้า	
4. สร้างผู้ใช้เพิ่มเติม และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
5. กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก	“การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104
6. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิด และ IP แอดเดรสแบบฟิกซ์ ตั้งข้อมูล identification	
7. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิดและ IP แอดเดรสแบบฟิกซ์ ให้ตั้งค่า entry การเร้าเป็นดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าเป็นดีฟอลต์เกตเวย์” ในหน้า 112
8. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิด และ IP แอดเดรสแบบฟิกซ์ ให้ตั้งค่าบริการโดเมนเนม	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
9. หากคุณกำลังใช้ IP แอดเดรสแบบฟิกซ์ และมีการใช้งาน DNS ให้ตั้งค่าโดเมนซัพฟิกซ์	“การตั้งค่าคอนฟิกโดเมนซัพฟิกซ์” ในหน้า 112
10. กำหนดคอนฟิกเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการ และสนับสนุน IBM และส่งคืนรายการตรวจสอบนี้ เมื่อคุณได้ทำขั้นตอนนี้เสร็จสิ้นแล้ว	“การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้” ในหน้า 114
11. ตั้งค่าฐานข้อมูล Events สำหรับการจัดทำเวอร์ชัน	“การกำหนดคอนฟิก Events Manager for Call Home” ในหน้า 120
12. เชื่อมต่อระบบที่ถูกจัดการเข้ากับแหล่งจ่ายไฟ	
13. ตั้งค่ารหัสผ่านให้กับระบบที่ถูกจัดการ และรหัสผ่านของ ASMI แต่ละรายการ (general และ admin)	“การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ” ในหน้า 121
14. เข้าใช้ ASMI เพื่อตั้งวันที่และเวลาบนระบบที่ถูกจัดการ	
15. สตาร์ทระบบที่ถูกจัดการ และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
16. ตรวจสอบว่า คุณมีหนึ่งโลจิสติกส์พาร์ติชันบนระบบที่ถูกจัดการ	
17. ทางเลือก: เพิ่มระบบที่ถูกจัดการอีก และกลับไปสู่รายการตรวจสอบเมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	

ตารางที่ 27. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่สามารถหาข้อมูลที่เกี่ยวข้องได้ (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
18. ทางเลือก: หากคุณกำลังติดตั้งเซิร์ฟเวอร์ใหม่ด้วย HMC ของคุณ ให้ตั้งค่าโลจิสติกส์พาร์ติชันและติดตั้งระบบปฏิบัติการ	
19. หากคุณไม่ได้กำลังติดตั้งเซิร์ฟเวอร์ใหม่ในเวลานี้ให้ทำงาน postconfiguration ซึ่งเลือกดำเนินการได้ เพื่อปรับค่าคอนฟิกูเรชันของคุณต่อไปอีก	“ขั้นตอน Postconfiguration” ในหน้า 122

การเริ่มต้น HMC:

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

เมื่อต้องการเริ่มต้น HMC ให้ทำโปรซีเจอร์ต่อไปนี้:

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

หมายเหตุ: ข้อความแจ้งเตือนนี้จะปรากฏอยู่เป็นเวลา 30 นาทีหาก你不ดำเนินการใดๆ

3. เลือกโลแคลที่คุณต้องการแสดงจากรายการ ในหน้าต่าง การเลือกโลแคล และคลิก ตกลง โลแคลจะระบุภาษาที่อิน
เตอร์เฟซ HMC ใช้
4. คลิก **Log on and launch the Hardware Management Console web application**
5. ล็อกอินเข้าสู่ HMC โดยใช้ ID ผู้ใช้และรหัสผ่านดีฟอลต์ต่อไปนี้:

ID: hscroot

รหัสผ่าน: abc123

หมายเหตุ: บน HMC เวอร์ชัน 8.1.0.1 คุณสามารถเลือกจากอ็อปชันล็อกอินต่อไปนี้:

ล็อกอิน: Last Login, HMC Classic หรือ HMC Enhanced

เลือกซอฟต์แวร์อินเทอร์เฟซที่จะใช้เมื่อคุณล็อกอินเข้าสู่ HMC อินเทอร์เฟซ HMC Classic ช่วยให้เข้าถึงฟังก์ชันแบบ
ดั้งเดิมทั้งหมดของ HMC และอินเทอร์เฟซ HMC Enhanced จัดเตรียมทั้งภารกิจและฟังก์ชันที่ออกแบบใหม่และการทำ
เสมือนใหม่

ล็อกอินล่าสุด

แสดงส่วนติดต่อผู้ใช้แบบกราฟิก (GUI) ที่คุณเลือก จากเซสชันล็อกอินก่อนหน้านี้

HMC Enhanced

แสดง GUI ที่ปรับปรุงใหม่ซึ่งมีคุณลักษณะ PowerVM ที่ปรับปรุง

HMC Classic

แสดง GUI มาตรฐานซึ่งไม่มีคุณลักษณะ PowerVM ที่ปรับปรุง

หมายเหตุ: เมื่อ HMC ทำงานเป็นเซิร์ฟเวอร์ DHCP, HMC จะใช้รหัสผ่านดีฟอลต์ เมื่อเชื่อมต่อกับตัวประมวลผลเซิร์ฟเวอร์ในครั้งแรก

6. และกด Enter

การเปลี่ยนวันที่และเวลา:

นาฬิกาแบบใช้แบตเตอรี่จะบันทึกวันที่และเวลาไว้สำหรับ HMC คุณอาจต้องรีเซ็ตวันที่และเวลาของคอนโซลหากเปลี่ยนแบตเตอรี่หรือย้ายระบบของคุณไปยังเซตเวลาที่แตกต่าง ศึกษาเกี่ยวกับวิธีการเปลี่ยนวันที่และเวลาสำหรับ HMC

หากคุณเปลี่ยนข้อมูลของวันที่ และเวลา, การเปลี่ยนแปลงนั้นจะไม่ส่งผลกระทบต่อระบบ และโลจิคัลพาร์ติชันที่ HMC จัดการอยู่

ถ้าต้องการเปลี่ยนวันที่และเวลาสำหรับ HMC ให้ทำตามต่อไปนี้:

1. ตรวจสอบให้แน่ใจว่าคุณมีหนึ่งในบทบาทต่อไปนี้:
 - ผู้ดูแลระบบพิเศษ
 - ตัวแทนบริการ
 - ผู้ควบคุมเครื่อง
 - ผู้ชม
2. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
3. ในหน้าต่างย่อยเนื้อหา ให้คลิก **เปลี่ยน วันที่และเวลา**
4. ถ้าคุณเลือก UTC ในฟิลด์ Clock การตั้งค่าเวลาจะมีการปรับโดยอัตโนมัติ เมื่อมีการเลื่อนเวลาใน เซตเวลาที่เลือกไว้ในวันที่ เวลา และเซตเวลา แล้วคลิก **OK**

การตั้งค่าชนิดเน็ตเวิร์ก HMC:

ตั้งค่า HMC ของคุณ เพื่อให้สามารถสื่อสารกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน ผู้ใช้ระยะไกล และบริการและการสนับสนุนได้

การตั้งค่า HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ:

ตั้งค่า HMC เพื่อให้สามารถเชื่อมต่อกับและจัดการระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำตามนี้:

ตารางที่ 28. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ ขอแนะนำให้ใช้ eth0	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุอินเตอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุอินเตอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิกอินเตอร์เน็ตอะแดปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสื่อบันทึก	“การตั้งค่าความเร็วของสื่อบันทึก” ในหน้า 109

ตารางที่ 28. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109
c. ตั้งค่าสแตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 110
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 111
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าต์เป็นดีฟอลต์เกตเวย์” ในหน้า 112
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 122

การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ:

กำหนดคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับ และจัดการระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กส่วนตัว

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับระบบที่ถูกจัดการโดยใช้เน็ตเวิร์กส่วนตัวให้ทำต่อไปนี้:

ตารางที่ 29. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุไอเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุไอเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP	“การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 109
4. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 122

การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับ โลจิคัลพาร์ติชัน:

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ โลจิคัลพาร์ติชันได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 30. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุไอเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุไอเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 107

ตารางที่ 30. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
3. กำหนดคอนฟิกอีเทอร์เน็ตอะแดปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อต	“การตั้งค่าความเร็วของสล็อต” ในหน้า 109
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109
c. ตั้งค่าสแตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 110
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 111
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าต์เป็นดีฟอลต์เกตเวย์” ในหน้า 112
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกรจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกรจัดการ” ในหน้า 122

การกำหนดคอนฟิกค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับ ผู้ใช้ระยะไกล:

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ ผู้ใช้ระยะไกลได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 31. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกรจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุอีเทอร์เน็ตพอร์ตให้กับ HMC ของคุณ	“การระบุอีเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิกอีเทอร์เน็ตอะแดปเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อต	“การตั้งค่าความเร็วของสล็อต” ในหน้า 109
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109
c. ตั้งค่าสแตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 110
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 111
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าต์เป็นดีฟอลต์เกตเวย์” ในหน้า 112
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
g. ตั้งค่าซัพฟิกส์	“การตั้งค่าคอนฟิกโดเมนซัพฟิกส์” ในหน้า 112
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	

การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC:

เมื่อต้องการคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC เพื่อให้สามารถรายงานปัญหาได้ให้ปฏิบัติตามดังต่อไปนี้:

ตารางที่ 32. การกำหนดคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ตรวจสอบให้แน่ใจว่าคุณมีข้อมูลลูกค้าที่จำเป็นทั้งหมด	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. กำหนดคอนฟิก HMC นี้เพื่อรายงานข้อผิดพลาด หรือเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่เพื่อรายงานความผิดพลาด	“การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน” ในหน้า 115 “การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้” ในหน้า 118
3. ตรวจสอบว่าคอนฟิกูเรชัน Call-Home ของคุณใช้งานได้	“การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่” ในหน้า 119
4. ให้อิทธิพลใช้ในการดูข้อมูลระบบที่เก็บรวบรวม	“การให้อิทธิพลใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” ในหน้า 119
5. จัดกำหนดการการส่งข้อมูลของข้อมูลระบบ	“ข้อมูลการบริการส่งข้อมูล” ในหน้า 119

การระบุอีเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0:

การเชื่อมต่ออีเทอร์เน็ตกับเซิร์ฟเวอร์ที่จัดการต้องกระทำโดยใช้อีเทอร์เน็ตพอร์ตที่กำหนดเป็น eth0 บน HMC ของคุณ

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

หากคุณติดตั้งอีเทอร์เน็ตอะแดปเตอร์เสริมไว้ในสล็อต PCI พอร์ตที่กำหนดเป็น eth0 จะขึ้นกับตำแหน่งและประเภทของอีเทอร์เน็ตอะแดปเตอร์ที่คุณติดตั้ง

หมายเหตุ: กฎเหล่านี้เป็นกฎทั่วไป และอาจไม่มีผลกับ configuration ทั้งหมด

ตารางต่อไปนี้แสดงกฎของการติดตั้งอีเทอร์เน็ตตามประเภท HMC

ตารางที่ 33. 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: - หากมีอีเทอร์เน็ตอะแดปเตอร์เดี่ยวติดตั้งไว้ 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 ใดที่คุณต้องการต่อเข้ากับสายเคเบิลอีเทอร์เน็ตด้วย ศึกษาเพิ่มเติมเกี่ยวกับการพิจารณาว่าตัวเชื่อมต่อ NIC ใดที่ HMC ระบุเป็น eth0 และ eth1

เมื่อต้องการพิจารณาชื่อที่ HMC กำหนดให้กับอีเทอร์เน็ตอะแดปเตอร์ ให้ปฏิบัติตามนี้:

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

5. พิมพ์ Ctrl+C เพื่อหยุดคำสั่ง tail

การตั้งค่าความเร็วของสื่อบันทึก:

ศึกษาเกี่ยวกับวิธีการระบุความเร็วของสื่อบันทึก ซึ่งรวมถึง ความเร็วและโหมด duplex ของอะแดปเตอร์อีเทอร์เน็ต

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

1. ในพื้นที่การนำทาง ให้คลิก **HMCการจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้ทำงาน 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 และยังคงครอบคลุมถึงอุปกรณ์เน็ตเวิร์กย่อย และเน็ตเวิร์ก

เมื่อต้องการเลือกเน็ตเวิร์กส่วนบุคคลหรือพับลิคเน็ตเวิร์ก ให้ปฏิบัติตามนี้:

1. ในพื้นที่การนำทาง ให้คลิก **HMCการจัดการ**
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. ในพื้นที่การนำทาง ให้คลิก **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 คุณไม่มีตัวเลือกในการเลือก เปิดใช้งาน DHCP

6. เลือกช่วงแอดเดรสของเซิร์ฟเวอร์ DHCP
7. คลิก OK

ถ้าคุณได้ตั้งค่า HMC ของคุณไปเป็นเซิร์ฟเวอร์ DHCP บนเน็ตเวิร์กส่วนตัวแล้ว คุณต้องตรวจสอบว่า คุณได้ตั้งค่าเน็ตเวิร์กส่วนตัว HMC DHCP อย่างถูกต้อง สำหรับข้อมูลเกี่ยวกับการเชื่อมต่อ HMC เข้ากับเน็ตเวิร์กส่วนตัว, โปรดดูที่ “การเลือกเน็ตเวิร์กส่วนตัวบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 82

การตั้งค่า IPv4 address:

ศึกษาถึงวิธีการตั้งค่า IPv4 address ของคุณบน HMC

1. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
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:

ศึกษาวิธีเชื่อมต่อ IPv6 address on the HMC.

1. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
2. คลิก **Change network settings**
3. คลิกแท็บ **LAN Adapters**
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก **Details**
5. คลิกแท็บ **IPv6 Settings**
6. เลือกตัวเลือก 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. ในพื้นที่การนำทางให้คลิก **HMCการจัดการ**
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:

ในเน็ตเวิร์กแบบเปิดไฟร์วอลล์จะถูกใช้เพื่อควบคุมการเข้าสู่เน็ตเวิร์กภายในบริษัทจากภายนอก HMC ก็มีไฟร์วอลล์ในอะแดปเตอร์เน็ตแต่ละตัว เมื่อต้องการควบคุม HMC จากระยะไกล หรือให้รีโมตแอ็กเซสแก่บุคคลอื่น แกไขการตั้งค่าคอนฟิกไฟร์วอลล์ของอีเทอร์เน็ตอะแดปเตอร์บน HMC ซึ่งเชื่อมต่อกับเน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิกไฟร์วอลล์, ให้ใช้ขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก HMCการจัดการ
2. คลิก Change network settings
3. คลิกแท็บ LAN Adapters
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก Details
5. คลิกแท็บ Firewall
6. โดยการใช้วิธีใดวิธีหนึ่งต่อไปนี้ คุณสามารถอนุญาตให้ IP แอดเดรสใดๆ ใช้แอปพลิเคชันเฉพาะผ่านไฟร์วอลล์ หรือคุณสามารถระบุ IP แอดเดรสมากกว่าหนึ่งได้:
 - อนุญาตให้ IP แอดเดรสใดๆ ที่ใช้แอปพลิเคชันเฉพาะผ่านไฟร์วอลล์ได้:
 - a. จากช่องด้านบน, ให้เลือกแอปพลิเคชัน
 - b. คลิก Allow Incoming แอปพลิเคชันจะไปปรากฏอยู่ในช่องด้านล่างเพื่อแสดงว่าถูกเลือกแล้ว
 - ระบุ IP แอดเดรสเพื่ออนุญาตให้ผ่านไฟร์วอลล์ได้:
 - a. จากช่องด้านบน ให้เลือกแอปพลิเคชัน
 - 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. ใน พื้นที่การนำทาง ให้คลิก การจัดการ HMC
2. คลิก Remote Command Execution
3. เลือก เปิดใช้งานการเรียกใช้งานคำสั่งรีโมต โดยใช้ ssh จากนั้นคลิก OK

ถึงตอนนี้ การเข้าถึงเซลล์ที่จำกัดแบบรีโมตถูกเปิดใช้งานแล้ว

การเปิดใช้งาน การเข้าถึงเว็บแบบรีโมต:

คุณสามารถเปิดใช้งานการเข้าถึงเว็บแบบรีโมตด้วย HMC ของคุณ

เมื่อต้องการเปิดใช้งานการเข้าถึงเว็บแบบรีโมตให้ทำดังนี้:

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

ถึงตอนนี้ การเข้าถึงเว็บแบบรีโมตถูกเปิดใช้งานแล้ว

การกำหนดคอนฟิก entry การเร้าเป็นดีฟอลต์เกตเวย์:

ศึกษาเกี่ยวกับวิธีการตั้งค่าการเร้า entry ตามดีฟอลต์เกตเวย์ งานนี้สามารถใช้ได้กับการตั้งค่าที่ใช้เน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิก entry การเร้าเป็นดีฟอลต์เกตเวย์ให้ปฏิบัติตามดังนี้:

1. ในพื้นที่การนำทางให้คลิก HMCการจัดการ
2. ในพื้นที่ใช้งาน ให้คลิก **Change network settings** หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ **Routing**
4. ในส่วนข้อมูลดีฟอลต์เกตเวย์ ป้อนเกตเวย์แอดเดรสและอุปกรณ์เกตเวย์ของ entry การเร้าที่คุณต้องการกำหนดเป็นดีฟอลต์เกตเวย์
5. คลิก OK

การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส:

ถ้าคุณวางแผนที่จะติดตั้งเน็ตเวิร์กแบบเปิดให้ตั้งค่าโดเมนเนมเซอร์วิส

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

1. ในพื้นที่การนำทางให้คลิก 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 และโดเมนซัพพลิคันทา แล้วคลิก **Add**
6. คลิก OK

การตั้งค่าคอนฟิกโดเมนซัพพลิคันทา:

รายการโดเมนซัพพลิคันทาใช้สำหรับ resolve IP แอดเดรสโดยเริ่มจาก entry แรกที่พบในรายการ

โดเมนซัพพลิคคือสตริงที่ต่อท้ายด้วยชื่อโฮสต์ซึ่งช่วยในการแปลงค่า IP แอดเดรสของรายการ ตัวอย่างเช่น ชื่อโฮสต์ของ myname อาจแปลงไม่ได้ อย่างไรก็ตาม หากสตริง myloc.mycompany.com เป็นสมาชิกของตารางโดเมนซัพพลิค เครื่องจะพยายามแปลง myname.mloc.mycompany.com ด้วยเช่นกัน

เมื่อต้องการ กำหนดคอนฟิกของรายการโดเมนซัพพลิค ให้ใช้ขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก การจัดการ HMC
2. ในพื้นที่ใช้งาน ให้คลิก **Change network settings** หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ Name Services
4. ป้อนสตริงที่จะใช้เป็น entry ของโดเมนซัพพลิค
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 104

เมื่อต้องการกำหนดค่า HMC เพื่อให้ใช้การพิสูจน์ตัวตน LDAP ให้ดำเนินการตามขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก การจัดการ HMC
2. ในพื้นที่เนื้อหา ให้คลิก **Configure LDAP**. หน้าต่าง **LDAP Server Definition** จะเปิดขึ้น
3. เลือก **เปิดใช้งาน LDAP**
4. กำหนดเซิร์ฟเวอร์ LDAP เพื่อใช้สำหรับการพิสูจน์ตัวตน (ตัวอย่างเช่น Microsoft Active Directory, Tivoli® และ Open LDAP)
5. กำหนดแอตทริบิวต์ LDAP ที่ใช้เพื่อระบุ ผู้ใช้ที่พิสูจน์ตัวตน ค่าดีฟอลต์คือ uid แต่คุณสามารถ ใช้แอตทริบิวต์ของคุณเองได้ สำหรับ Microsoft Active Directory, ใช้ sAMAccountName เป็นแอตทริบิวต์
6. กำหนดรหัสชื่อที่แตกต่าง ซึ่งเป็นฐานการค้นหสำหรับเซิร์ฟเวอร์ LDAP
7. คลิก **OK**
8. หากผู้ใช้ต้องการใช้การพิสูจน์ตัวตน LDAP ผู้ใช้ต้อง กำหนดค่าโปรไฟล์เพื่อให้ใช้การพิสูจน์ตัวตน LDAP จากระยะไกล แทนการพิสูจน์ตัวตนแบบโลคัล

การกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ Key Distribution Center สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos:

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

เมื่อผู้ใช้ลงชื่อเข้าใช้ HMC ระบบจะดำเนินการพิสูจน์ตัวตนของไฟล์รหัสผ่านภายในก่อน หากไม่พบไฟล์รหัสผ่านภายใน HMC สามารถติดต่อเซิร์ฟเวอร์ Kerberos ระยะไกลสำหรับการพิสูจน์ตัวตนได้ คุณต้องกำหนดคอนฟิก HMC ของคุณเพื่อให้อาศัยการพิสูจน์ตัวตนระยะไกลด้วย Kerberos

หมายเหตุ: ก่อนที่คุณจะกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตนระยะไกลด้วย Kerberos คุณต้องตรวจสอบให้แน่ใจว่ามีการเชื่อมต่อเน็ตเวิร์กการทำงาน ระหว่าง HMC และเซิร์ฟเวอร์ KDC สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104

เมื่อต้องการกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตนระยะไกล ด้วย Kerberos ปฏิบัติดังต่อไปนี้:

1. เปิดใช้งานเซิร์ฟเวอร์ Network Time Protocol (NTP) บน HMC และตั้งค่าเซิร์ฟเวอร์ HMC และ KDC ให้ซิงโครไนซ์โดยใช้เซิร์ฟเวอร์ NTP เดียวกัน เมื่อต้องการเปิดใช้งานเซิร์ฟเวอร์ NTP บน HMC ให้ปฏิบัติตามดังต่อไปนี้:
 - a. ในพื้นที่การนำทาง ให้เลือก **HMC Management**
 - b. ในพื้นที่เนื้อหา ให้เลือก **เปลี่ยนวันที่ และเวลา**
 - c. เลือกแท็บ **คอนฟิกูเรชัน NTP**
 - d. เลือก **เปิดใช้งานเซิร์ฟเวอร์ NTP บน HMC นี้**
 - e. คลิก **OK**
2. คอนฟิกแต่ละโปรไฟล์ผู้ใช้ของ HMC ระยะไกลเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย Kerberos แทนที่จะใช้การพิสูจน์ตัวตนภายใน
3. ทางเลือก: คุณสามารถอิมพอร์ตไฟล์คีย์เซิร์ฟเวอร์ลงใน HMC นี้ได้ ไฟล์คีย์เซิร์ฟเวอร์จะมีบัญชีโฮสต์ที่ระบุ HMC ให้แก่เซิร์ฟเวอร์ไฟล์คีย์เซิร์ฟเวอร์รู้จักกันในชื่อของ **คีย์แท็บ** เมื่อต้องการอิมพอร์ตไฟล์คีย์เซิร์ฟเวอร์ลงใน HMC นี้ ให้ปฏิบัติตามดังต่อไปนี้:
 - a. ในพื้นที่การนำทาง ให้เลือก **HMC Management**
 - b. ในพื้นที่เนื้อหา ให้เลือก **กำหนดคอนฟิก KDC** หน้าต่างคอนฟิกูเรชัน Key Distribution Center จะปรากฏขึ้น
 - c. เลือก **การดำเนินการ > อิมพอร์ตเซิร์ฟเวอร์คีย์** หน้าต่าง อิมพอร์ตคีย์เซิร์ฟเวอร์ จะปรากฏขึ้น
 - d. พิมพ์ตำแหน่งของไฟล์คีย์เซิร์ฟเวอร์
 - 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 อิมพอร์ตคีย์เซิร์ฟเวอร์ จะปรากฏขึ้น
 - d. พิมพ์ชื่อกลุ่มระบบเครือข่ายและชื่อโฮสต์ หรือ IP แอดเดรสของเซิร์ฟเวอร์ KDC
 - e. คลิก **OK**

การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้:

คอนฟิก HMC ของคุณเพื่อให้สามารถแจ้งให้คุณทราบเมื่อเกิดปัญหานั้น

การคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับฝ่ายบริการและสนับสนุนได้โดยใช้ชาร์ตการติดตั้ง Call-Home:

คอนฟิก HMC เพื่อให้เป็นเซิร์ฟเวอร์ Call-Home โดยใช้ชาร์ต Call-Home

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

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- ถ้า คุณกำหนดคอนฟิกการสนับสนุนอินเทอร์เน็ตผ่านทางพรีอ็อกซีเซิร์ฟเวอร์ คุณยังต้องมีสิ่งต่อไปนี้ด้วย:
 - IP แอดเดรสและพอร์ตของพรีอ็อกซีเซิร์ฟเวอร์
 - ข้อมูลการพิสูจน์ตัวตนสำหรับพรีอ็อกซี
- มีการใส่แอดเดรสที่กำหนดเป็น eth1 (ซึ่งกำหนดเป็นเน็ตเวิร์กแบบเปิด) สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC” ในหน้า 80
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

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

1. ในพื้นที่การนำทางให้เลือก การจัดการเซอร์วิส
2. ในพื้นที่เนื้อหาให้เลือก วิซาร์ดเซตอัพ Call-Home วิซาร์ดการเชื่อมต่อและเซิร์ฟเวอร์ Call-Home จะเปิดขึ้น ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อกำหนดคอนฟิก Call-Home

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน:

คอนฟิก HMC นี้เพื่อให้สามารถติดต่อผู้ให้บริการเกี่ยวกับความผิดพลาดได้โดยใช้การเชื่อมต่อทาง LAN โพรซีจหรือโมเด็ม หรือ VPN

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

การคอนฟิก HMC เพื่อติดต่อบริการและสนับสนุนโดยใช้อินเทอร์เน็ต ทาง LAN และ SSL:

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

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว ตรวจสอบค่านี้โดยไปที่อินเทอร์เน็ตเฟส HMC และคลิก **Service Management > Manage Customer Information**
- ถ้าคุณกำหนดคอนฟิกการสนับสนุนอินเทอร์เน็ตผ่านทางพรีอ็อกซีเซิร์ฟเวอร์ คุณจะต้อง มีสิ่งต่างๆ ต่อไปนี้เช่นกัน:
 - IP แอดเดรสและพอร์ตของพรีอ็อกซีเซิร์ฟเวอร์
 - ข้อมูลการพิสูจน์ตัวตนสำหรับพรีอ็อกซี
- คุณจำเป็นต้องคอนฟิกอย่างน้อยหนึ่งเน็ตเวิร์กอินเทอร์เน็ตที่เปิดอยู่ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 82

- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

ในการตั้งค่า HMC เป็นเซิร์ฟเวอร์ Call Home โดยใช้อินเทอร์เน็ตทาง LAN และ SSL ให้ทำดังนี้:

1. ในพื้นที่การนำทางให้คลิก **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 ให้เลือก **เพจ Internet**
7. ทำเครื่องหมายในกล่อง **Allow an existing internet connections for service**
8. ถ้าคุณกำลังใช้พรีอ็อกซี SSL ให้เลือก **Use SSL proxy**
9. ถ้าคุณใช้พรีอ็อกซี SSL ให้ใส่แอดเดรสและพอร์ตของพรีอ็อกซี ขอรับข้อมูลนี้ได้จากผู้บริหรเน็ตเวิร์ก
10. ถ้าคุณเลือก **Use SSL proxy** และพรีอ็อกซีต้องใช้การพิสูจน์ตัวตนด้วย user ID และรหัสผ่าน ให้เลือก **Authenticate with the SSL proxy** พิมพ์ userid และรหัสผ่าน ขอรับข้อมูล user ID และรหัสผ่านได้จากผู้บริหรเน็ตเวิร์ก
11. เลือก **โปรโตคอลของอินเทอร์เน็ต ที่คุณต้องการใช้**
12. บนเพจ อินเทอร์เน็ต ให้คลิก **ทดสอบ**
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

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- คุณมีสายโทรศัพท์นาล็อกที่จัดเตรียมไว้โดยเฉพาะ
- คุณมีข้อมูลที่เป็นสำหรับการตั้งค่าโมเด็ม สำหรับ ข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว คุณอาจตรวจสอบ โดยการไปที่อินเทอร์เน็ตเฟส HMC และคลิก **Service Management > Manage Customer Information**
- ตรวจสอบว่าคุณมีข้อมูลต่อไปนี้:
 - ประเภทของสายนาฬิกา กล่าวคือ เป็น tone หรือ pulse สายส่วนใหญ่เป็นประเภท tone แต่บางสายยังคงเป็นประเภท rotary หรือ pulse แบบเดิม
 - เมื่อยกหูโทรศัพท์แล้ว สายโทรศัพท์มีเสียงสัญญาณ หรือไม่ สายโทรศัพท์ส่วนใหญ่มีเสียง แต่บางสายอาจไม่มีเสียง

- ต้องใช้หมายเลขนำหน้าสำหรับการหมุนโทรศัพท์หรือไม่ หมายเลขนำหน้าสำหรับการหมุนโทรศัพท์คือหมายเลขหรือชุดหมายเลขที่ช่วยให้โทรออกได้

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

1. ในพื้นที่การนำทางให้คลิก **Service Management**
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity**
3. คลิก **Configure**
4. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้เลือก เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ call-home
5. ยอมรับข้อตกลง
6. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้คลิกแท็บ โลคัล โมเด็ม
7. บนหน้าโลคัลโมเด็มให้เลือกเช็kb็อกซ์อนุญาตให้ใช้ การหมุนโลคัลโมเด็มสำหรับเซอร์วิส
8. บนหน้าโลคัลโมเด็มให้เลือกเช็kb็อกซ์โมเด็มคอนฟิगरชัน
9. ในหน้าต่าง Customize Modem Settings ให้คลิก **Dial type, Tone or Pulse** ถ้าสายโทรศัพท์ที่มีเสียงสัญญาณ เมื่อยกหูโทรศัพท์ให้เลือกเช็kb็อกซ์ รอสัญญาณหมุน กรอกหมายเลขนำหน้าสำหรับการหมุนโทรศัพท์เพื่อให้คุณสามารถโทรออกได้
10. คลิก **OK**
11. บนหน้าโลคัลโมเด็มให้คลิก **เพิ่ม**
12. เลือกหมายเลขจากรายการ
13. ถ้าเป็นหมายเลขในท้องถิ่นให้ลบรหัสพื้นที่ออกจากฟิลด์ **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) ระบบจะลองหมุนหมายเลขตามลำดับที่กำหนดคอนฟิกไว้ เมื่อต้องการเพิ่ม หมายเลขเพิ่มเติมลงในรายการที่สามารถโทรได้ให้ทำซ้ำขั้นตอนต่างๆ ในกระบวนการนี้
20. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้คลิก **OK**

การเชื่อมต่อระบบให้บริการและสนับสนุนโดยใช้ VPN บน LAN:

ตั้งค่าเซิร์ฟเวอร์ call-home โดยใช้ VPN

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- มีการใช้เซิร์ฟเวอร์ที่กำหนดเป็น eth1 (ซึ่งกำหนดเป็นเน็ตเวิร์กแบบเปิด) สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC” ในหน้า 80
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว ตรวจสอบค่านี้โดยคลิก **Service Management > Manage Customer Information** บนอินเทอร์เน็ตเฟส HMC

เมื่อต้องการกำหนดคอนฟิกเซิร์ฟเวอร์ call-home โดยใช้ VPN ให้ทำตามต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิก **Service Management**
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity**
3. คลิก **Configure**
4. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้เลือก **เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ call-home**
5. ยอมรับข้อตกลง
6. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้คลิกแท็บ **Internet VPN**
7. บนหน้าอินเทอร์เน็ต VPN ให้เลือก **อนุญาตให้ใช้ VPN และการเชื่อมต่ออินเทอร์เน็ตที่มีอยู่สำหรับเซอร์วิส**
8. บนหน้าอินเทอร์เน็ต VPN ให้คลิก **เช็กล่องข้อทดสอบ**
9. ในหน้าต่าง Test Internet VPN ให้คลิก **Start**
10. ตรวจสอบว่าการทดสอบเสร็จสิ้นสมบูรณ์
11. ในหน้าต่าง Test Internet VPN ให้คลิก **Cancel**
12. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้คลิก **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 นี้รายงานข้อผิดพลาดให้ปฏิบัติตามต่อไปนี้:

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

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

การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่:

ทดสอบการรายงานปัญหาเพื่อตรวจสอบให้แน่ใจว่า การเชื่อมต่อไปยังส่วนบริการ และสนับสนุนกำลังทำงานอยู่

เมื่อต้องการตรวจสอบว่าคอนฟิगरชัน 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. ตรวจสอบว่ามีการกำหนดเหตุการณ์ PMH และหมายเลขให้กับหมายเลขปัญหา ที่คุณเปิด
8. เลือกเหตุการณ์ และเลือก ปิด
9. บนหน้าต่าง ปิด ให้พิมพ์ชื่อของคุณและความคิดเห็นสั้นๆ

การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม:

คุณต้องให้สิทธิ์แก่ผู้ใช้ในการดูข้อมูลเกี่ยวกับระบบของคุณ

ก่อนที่คุณจะให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวมมา คุณต้องขอรับ IBM ID ก่อน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการขอรับ IBM ID โปรดดูที่ “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91

เมื่อต้องการให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม ให้ปฏิบัติตามต่อไปนี้:

1. ในพื้นที่การนำทาง ให้เลือก การจัดการเซอร์วิส
2. ในพื้นที่เนื้อหา ให้เลือก ผู้ใช้ที่ได้รับสิทธิ
3. ป้อน IBM ID ของคุณ
4. คลิก **OK**

ข้อมูลการบริการส่งข้อมูล:

ส่งข้อมูลเซอร์วิส ดังนั้น จึงสามารถใช้เพื่อกำหนดปัญหาได้

IBM จัดเตรียมฟังก์ชันสำหรับเว็บที่ทำให้เป็นส่วนตัว ซึ่งใช้ข้อมูลที่เก็บรวบรวมโดย IBM Electronic Service Agent เพื่อใช้ฟังก์ชันเหล่านี้ คุณต้องลงทะเบียนบนเว็บไซต์ IBM Registration ก่อนที่ <http://www.ibm.com/account/profile> เมื่อต้องการอนุญาตให้ผู้ใช้งานข้อมูล 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. คลิกหนึ่งในแท็บต่อไปนี้:

- ส่งใช้นี้เพื่อกำหนดตารางเวลาที่ต้องการส่งข้อมูลเซิร์ฟเวอร์ไปยังตัวแทนบริการของคุณ (ระบุความถี่ในรูปของวันและเวลา) และวิธีที่คุณต้องการส่งเซิร์ฟเวอร์และข้อมูลการจัดการกับผลการทำงาน
- **FTP** ใช้นี้เพื่อกำหนดคอนฟิกข้อมูล File Transfer Protocol (FTP) สำหรับเซิร์ฟเวอร์ FTP ที่มีหรือไม่มีไฟร์วอลล์สำหรับปิดการไหลข้อมูลเซิร์ฟเวอร์ ข้อมูลเซิร์ฟเวอร์นี้เป็นข้อมูล แสดงข้อผิดพลาดเพิ่มเติม ซึ่งประกอบด้วยปัญหาที่เกี่ยวข้องกับข้อมูลที่เป็นปัญหบน Hardware Management Console (HMC) สำหรับ HMC หรือระบบที่ถูกจัดการ
- ส่งข้อมูลเซิร์ฟเวอร์ไปยัง **IBM** ใช้นี้เพื่อจัดเตรียมความสามารถในการส่งข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ HMC ซึ่งสามารถใช้เพื่อกำหนดปัญหา ข้อมูลอาจเป็นข้อมูลเกี่ยวกับการติดตาม บันทึกการทำงาน หรือดัมพ์ และปลายทางของข้อมูลอาจเป็น IBM Service Support System แผ่นดิสก์ ไดรฟ์หน่วยความจำแฟลชแบบ USB หรือทีวีดีแรม ก่อนที่คุณจะสามารถส่งข้อมูลไปยัง IBM Service Support System ได้นั้น คุณต้องเปิดใช้งาน Phone Server และ Remote Service

4. ดำเนินงานให้เสร็จสมบูรณ์ในหน้าต่างรายละเอียดเซิร์ฟเวอร์การกระจายสัญญาณ แล้วคลิก **OK**.

การกำหนดคอนฟิก Events Manager for Call Home:

เรียนรู้วิธีการกำหนดคอนฟิกภารกิจ Events Manager for Call Home คุณสามารถมอนิเตอร์และอนุมัติข้อมูลใดๆที่กำลังส่งผ่านจาก HMC ไปยัง IBM ผ่านภารกิจนี้

โหมด Events Manager for Call Home (เปิดใช้งานหรือปิดใช้งาน) มีการตั้งค่าโดยใช้อินเตอร์เฟซบรรทัดรับคำสั่ง HMC การเปิดใช้งานภารกิจ Events Manager for Call Home จะบล็อก HMC ไม่ให้เรียกเหตุการณ์โฮมโดยอัตโนมัติเมื่อเกิดขึ้นเพื่อป้องกันการเรียกเหตุการณ์โฮมโดยไม่มี การอนุมัติ, HMCs ทั้งหมดที่รันอยู่ในสถานะแวดล้อมนี้ต้องมีการเปิดใช้งาน Events Manager for Call Home

เมื่อต้องการเปิดใช้งาน หรือปิดใช้งานภารกิจ Events Manager for Call Home ให้รัน คำสั่งต่อไปนี้:

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

หมายเหตุ: การเปิดใช้งานงาน Events Manager for Call Home จะพักเหตุการณ์ call home ไว้จนกว่าจะได้รับการอนุมัติสำหรับงาน call home หากคุณปิดใช้งานงาน Events Manager for Call Home จะไม่เปิดใช้งานคุณลักษณะ call home โดยอัตโนมัติ เชื้อต่อพื้นที่ ป้องกันการเรียกโฮมโดยไม่ได้ตั้งใจของข้อมูลกลับไปยัง IBM เลือกจากอ็อปชันคำสั่งต่อไปนี้ เพื่อกำหนดคอนฟิกเรชันที่ต้องการ:

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

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

คุณสามารถลงทะเบียน HMC กับ Events Manager for Call Home หลังจากคุณลงทะเบียน HMC, events manager จะเคียวรี HMC ที่ลงทะเบียนสำหรับเหตุการณ์ใดๆ ซึ่งกำลังรอถูกเรียกโฮมไปยัง IBM Events Manager แสดงข้อมูลที่กำลังถูกส่งกลับไปยัง IBM และอนุมัติเหตุการณ์เหล่านี้ หลังจากอนุมัติแล้ว Event Manager จะแจ้ง HMC ที่ลงทะเบียนว่า สามารถดำเนินการเรียกโฮมต่อไปได้

ภารกิจ Events Manager for Call Home สามารถรันจาก HMC ใดๆ หรือจากหลาย HMCs เมื่อต้องการลงทะเบียนคอนโซลการจัดการที่มีภารกิจ Events Manager for Call Home ให้ทำขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทาง ให้เลือก การจัดการเซอวิส
2. ในพื้นที่เนื้อหา เลือก Events Manager for Call Home
3. จากหน้าต่าง Events Manager for Call Home คลิก จัดการคอนโซล
4. จากหน้าต่าง จัดการคอนโซลที่ลงทะเบียน คลิก เพิ่มคอนโซล เพื่อป้อนข้อมูลเพื่อลงทะเบียน คอนโซลการจัดการที่มีภารกิจ Events Manager for Call Home
5. คลิก ตกลง เพื่อ commit การเปลี่ยนแปลงในรายการ ของคอนโซลการจัดการที่ลงทะเบียน

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

การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ:

คุณต้องตั้งรหัสผ่านสำหรับเซิร์ฟเวอร์และ Advanced System Management (ASM) ของคุณ อ่านเพิ่มเติมเกี่ยวกับวิธีการใช้อินเทอร์เฟซ HMC เพื่อตั้งรหัสผ่านเหล่านี้

หากคุณได้รับข้อความ Authentication Pending HMC จะเตือนให้คุณตั้งรหัสผ่านสำหรับระบบที่ถูกจัดการ

หากคุณไม่ได้รับข้อความ Authentication Pending ให้ทำขั้นตอนต่อไปให้เสร็จสิ้น เพื่อตั้งรหัสผ่านสำหรับระบบที่ถูกจัดการ

การอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณ:

เมื่อต้องการอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณ ให้ทำดังนี้:

1. ในพื้นที่การนำทาง ให้เลือก ระบบที่ถูกจัดการ
2. ในพื้นที่งาน ให้คลิก Operations
3. คลิก Change Password หน้าต่าง อัปเดตรหัสผ่าน จะเปิด
4. พิมพ์ข้อมูลที่จำเป็น และคลิก OK

การอัปเดตรหัสผ่านทั่วไปสำหรับ Advanced System Management (ASM):

หมายเหตุ: ค่าดีฟอลต์ของรหัสผ่านสำหรับ ID ผู้ใช้ทั่วไปคือ general และค่าดีฟอลต์ของรหัสผ่านสำหรับ ID ผู้ดูแลระบบคือ admin

เมื่อต้องการ อัปเดตรหัสผ่านทั่วไปของ ASM ให้ทำดังนี้:

1. ในพื้นที่การนำทางของ HMC ให้เลือกกระบวนที่ถูกรจัดการ
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 และ คลิก **Log In**
6. ในพื้นที่การนำทางให้ขยาย ล็อกอินโปรไฟล์
7. เลือก **Change Password**
8. ระบุข้อมูลที่จำเป็น และคลิก **Continue**

การรีเซ็ตรหัสผ่านผู้ดูแลระบบ *Advanced System Management (ASM)*:
เมื่อต้องการรีเซ็ตรหัสผ่านของผู้ดูแลระบบ ให้ติดต่อผู้ให้บริการ ที่ได้รับสิทธิ

การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกรจัดการ:

ข้อพหานี้ช่วยคุณตรวจสอบว่า คุณได้เชื่อมต่อกับเน็ตเวิร์ก อย่างถูกต้องหรือไม่

เมื่อต้องการทดสอบภาวะเชื่อมต่อเน็ตเวิร์ก, คุณต้องมีบทบาทใดบทบาทหนึ่ง ดังต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ตัวแทนบริการ

เมื่อต้องการทดสอบการเชื่อมต่อระหว่าง HMC และระบบที่ถูกรจัดการ ให้ปฏิบัติตามนี้:

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

หากคุณยังไม่ได้สร้างโลจิคัลพาร์ติชันอื่นใด คุณจะไม่สามารถ ping แอดเดรสได้ คุณสามารถใช้ HMC เพื่อสร้าง โลจิคัลพาร์ติชันบนเซิร์ฟเวอร์ของคุณ – สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ Logical partitioning.

เมื่อต้องการทำความเข้าใจ กับวิธีการใช้ HMC ในเน็ตเวิร์ก โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ การกำหนดค่า HMC เพื่อเชื่อมต่อกับ เครือข่าย โปรดดูที่ “การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 101

ขั้นตอน Postconfiguration

เมื่อคุณติดตั้งและตั้งค่าคอนฟิก HMC แล้ว ให้สำรองข้อมูล HMC ตามที่จำเป็น

การสำรองข้อมูล HMC ที่สำคัญ

คุณสามารถสำรองข้อมูลคอนโซลที่สำคัญลงในอุปกรณ์หน่วยความจำแฟลชีชแบบ 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)
- รีโมตไคลเอนต์ผ่านทาง FTP

สำรองข้อมูล HMC หลังจากที่คุณทำการเปลี่ยนแปลงใน HMC หรือในข้อมูลที่เกี่ยวข้องกับโลจิสติกส์พาร์ติชัน

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

ถ้าต้องการสำรองข้อมูล HMC คุณต้องมีบทบาทใดบทบาทหนึ่ง ดังต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ผู้ควบคุมเครื่อง
- ตัวแทนบริการ

หากต้องการสำรองข้อมูลที่สำคัญของ HMC ให้ทำสิ่งต่อไปนี้:

1. ในพื้นที่การนำทาง ให้คลิก **การจัดการ HMC**
2. เลือก **Back up HMC Data**
3. เลือกอ็อปชันการเก็บถาวร คุณสามารถสำรองข้อมูลลงในสื่อบันทึกบนระบบภายในเครื่อง ระบบระยะไกลที่เชื่อมต่อ หรือส่งข้อมูลสำรองไปยังไซต์ระยะไกล
4. ปฏิบัติตามคำสั่งบนหน้าต่างเพื่อสำรองข้อมูล

การสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ทั้งหมดไว้บนระบบรีโมต

คุณสามารถใช้ HMC เพื่อสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ทั้งหมด ของ HMC ไว้บน ระบบรีโมต

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

เมื่อต้องการสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ไว้บนระบบรีโมต คุณต้องเป็นสมาชิกของบทบาทอย่างใดอย่างหนึ่ง ต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ผู้ควบคุมเครื่อง
- ตัวแทนบริการ

เมื่อต้องการสำรองข้อมูลฮาร์ดไดรฟ์ HMC ให้กับระบบรีโมต 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 โดยมีสื่อบันทึกการบูต HMC ในไดรฟ์ DVD หากต้องการเริ่มต้นอินเตอร์เฟซ HMC จากเน็ตเวิร์กบูตเซิร์ฟเวอร์ที่กำหนดคอนฟิกไว้ให้แน่ใจว่าเน็ตเวิร์กอินเตอร์เฟซคือหนึ่งในอุปกรณ์ต่อไปนี้ในลำดับการเริ่มทำงาน เมื่อต้องการดูรายการของอุปกรณ์สตาร์ทอัพ ให้กด F12 เมื่อเปิด HMC และเลือกเน็ตเวิร์กอินเตอร์เฟซที่คุณต้องการบูต
4. เลือกอีพซันสำรองข้อมูล และคลิก Next
5. เลือกเน็ตเวิร์กอินเตอร์เฟซเพื่อใช้สำหรับสื่อสารกับ รัมโบตเซิร์ฟเวอร์ หากคุณกำลังเริ่มต้น HMC โดยติดต่อกับเน็ตเวิร์กบูตเซิร์ฟเวอร์ และเซิร์ฟเวอร์นี้ยังเป็นรัมโบตเซิร์ฟเวอร์ที่คุณต้องการสำรองข้อมูล ให้เลือกค่ากำหนดดีฟอลต์ จากนั้นให้คลิก ถัดไป และไปยังขั้นตอนที่ 7 ถ้าคุณไม่ได้เลือกค่ากำหนดดีฟอลต์ไว้ให้ดำเนินการต่อด้วยขั้นตอนถัดไป

หมายเหตุ: หมายเลขอินเตอร์เฟซ (eth0, eth1) อาจไม่ตรงกับหมายเลขที่บันทึกในขั้นตอนที่ 1 สามารถใช้ MAC address ที่แสดงรายการไว้เพื่อระบุอินเตอร์เฟซที่ต้องการได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การระบุไอทีเอ็นเน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 107

6. ถ้าคุณไม่ได้เลือกค่าติดตั้งดีฟอลต์ คุณต้องเลือก โพรโตคอลเครือข่ายเพื่อใช้กับอินเตอร์เฟซที่เลือกไว้ คุณสามารถเลือกที่จะรับ IP แอดเดรสจากเซิร์ฟเวอร์ DHCP ในเน็ตเวิร์กของคุณ หรือกำหนด IP แอดเดรส แบบคงที่ให้กับเน็ตเวิร์กอินเตอร์เฟซที่เลือก ทำการเลือก และคลิก Next
7. หากคุณไม่ได้เลือกค่าติดตั้งดีฟอลต์ ให้พิมพ์ IP แอดเดรสหรือชื่อโฮสต์ของรัมโบตเซิร์ฟเวอร์ของคุณ ไฟล์สำรองข้อมูลจะถูกสร้างขึ้นโดยใช้ยูลิซิปบีบอัด gzip และคำสั่ง tar ระบุไฟล์ด้วยนามสกุล .tgz ในฟิลด์ **File on remote host** หากคุณสามารถเลือกค่ากำหนดดีฟอลต์เน็ตเวิร์กไว้ คุณต้องใช้ เซิร์ฟเวอร์ไต่เรือทอรีในการกำหนดคอนฟิกเน็ตเวิร์กบูตของคุณ ข้อมูลนี้จะถูกแสดงในฟิลด์ **File on remote host** หลังจากที่คุณ บ้อนข้อมูลที่ต้องการทั้งหมดเสร็จสิ้นแล้ว ให้คลิก Next
8. เลือกวิธีที่คุณต้องการใช้เพื่อถ่ายโอนข้อมูลจาก HMC ของคุณ ให้กับรัมโบตเซิร์ฟเวอร์ หากคุณเลือกการเข้ารหัสข้อมูล รัมโบตโฮสต์ของคุณจะต้องมีเซิร์ฟเวอร์ Secure Shell (SSH) ที่กำลังรันอยู่ หากคุณเลือก การถ่ายโอนข้อมูลโดยไม่มีการเข้ารหัส รัมโบตโฮสต์ของคุณต้องมี Network File Server (NFS) ที่กำลังรันอยู่ และไต่เรือทอรีที่คุณต้องการ สำรองข้อมูล ต้องถูกเอ็กซ์พอร์ตเพื่อทำการบันทึก ทำการเลือก และคลิก Next
9. ถ้าคุณเลือกถ่ายโอนข้อมูลโดยใช้การเข้ารหัส คุณต้องพิมพ์ ID ผู้ใช้และรหัสผ่านของรัมโบตเซิร์ฟเวอร์
10. ตรวจสอบข้อมูลที่คุณป้อนให้ถูกต้อง และคลิก **Finish** เมื่อการสำรองข้อมูลเสร็จสมบูรณ์ อินเตอร์เฟซ HMC จะปรากฏขึ้น

ถ้าคุณปรับเปลี่ยนลำดับของการเริ่มทำงานโดยกด F1 เมื่อคุณเปิด HMC คุณต้องบูต HMC และเปลี่ยนค่าติดตั้งอีกครั้ง เมื่อคุณเปลี่ยนลำดับการเริ่มทำงาน ให้แน่ใจว่าฮาร์ดดิสก์ของคุณจะถูกแสดงก่อนเน็ตเวิร์กอินเตอร์เฟซ ในลำดับการเริ่มทำงาน

การอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ

การอัปเดตและอัปเดตควรดำเนินการเป็นระยะๆ เพื่อให้ HMC สามารถเพิ่มคุณสมบัติการทำงานใหม่ๆ และปรับปรุงคุณลักษณะที่มีอยู่ ศึกษาเพิ่มเติมเกี่ยวกับความแตกต่างระหว่างการอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ รวมทั้งศึกษาวิธีการดำเนินการอัปเดต อัปเดต หรือโอนย้ายรหัสเครื่อง HMC

เมื่อคุณทำงานแต่ละงานเหล่านี้เสร็จสิ้น HMC จะรีบูต แต่พาร์ติชันไม่รีบูต

การอัปเดตรหัส HMC

ใช้การบำรุงรักษาที่ระดับ HMC ที่มีอยู่

คุณไม่จำเป็นต้องทำงาน **Save upgrade data**

การอัปเดตรหัส HMC

แทนที่ซอฟต์แวร์ HMC ด้วยรหัสใหม่หรือระดับโปรแกรมฟิร์มแวร์ของโปรแกรมเดียวกัน

คุณต้องบูตจากสื่อบันทึกที่ถูกต้อง

การโอนย้ายรหัส HMC

ย้ายข้อมูล HMC จาก HMC เวอร์ชันหนึ่งเป็นเวอร์ชันอื่น

การโอนย้ายระบบเป็นการอัปเดตชนิดหนึ่ง

การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ

เรียนรู้วิธีการดูเวอร์ชันและรหัสของรหัสเครื่อง HMC

ระดับของรหัสเครื่องบน HMC จะกำหนดคุณลักษณะที่มีอยู่ รวมถึงการบำรุงรักษาเซิร์ฟเวอร์เฟิร์มแวร์และการปรับปรุงสำหรับการอัปเดตเป็นรหัสใหม่

เมื่อต้องการดูเวอร์ชันและรหัสของรหัสเครื่อง HMC ให้ทำดังนี้:

1. ในพื้นที่การนำทาง ให้คลิก **อัปเดต**
2. ในพื้นที่ใช้งาน ให้ดูและบันทึกข้อมูลที่ปรากฏภายใต้หัวข้อ **HMC Code Level** รวมทั้งเวอร์ชันของ HMC, รหัส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน

การขอรับและการใช้การอัปเดตรหัสเครื่องสำหรับ HMC เมื่อมีการเชื่อมต่ออินเทอร์เน็ต

ศึกษาวิธีขอรับอัปเดตรหัสเครื่องสำหรับ HMC เมื่อ HMC มีการเชื่อมต่ออินเทอร์เน็ต

เมื่อต้องการขอรับอัปเดตรหัสเครื่องสำหรับ HMC ให้ปฏิบัติตามขั้นตอนที่ 1 ถึง 5

ขั้นตอนที่ 1. ตรวจสอบให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต:

เมื่อต้องการดาวน์โหลดอัปเดตจากระบบส่วนบริการ และสนับสนุนหรือเว็บไซต์ไปยัง HMC หรือเซิร์ฟเวอร์ของคุณ คุณต้องมีอย่างน้อยอย่างหนึ่งต่อไปนี้:

- การเชื่อมต่อ SSL โดยมีหรือไม่มีพรีอ็อกซี 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

- ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์ ถ้าการทดสอบไม่เสร็จสมบูรณ์ ให้แก้ปัญหาการเชื่อมต่อและแก้ไข ปัญหา ก่อนที่จะดำเนินการต่อตามขั้นตอนนี้อีกทางหนึ่ง คุณสามารถ ขอรับอัปเดตบนทีวีดี
- ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

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

ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอน ต่อไปนี้:

- จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ตให้ไปที่ <http://www.ibm.com/eserver/support/fixes>
- เลือกตระกูลที่เหมาะสมในรายการตระกูล ผลิตภัณฑ์
- เลือก Hardware Management Console ใน รายการชนิดผลิตภัณฑ์หรือโปรแกรมฟิกซ์
- คลิก ทำต่อไป ไซด์ Hardware Management Console จะปรากฏขึ้น
- เลื่อนลงไปยังระดับเวอร์ชัน HMC ของคุณ เพื่อ ดูระดับ HMC ที่มีอยู่

หมายเหตุ: ถ้าคุณต้องการ คุณสามารถติดต่อ ส่วนบริการและสนับสนุน

- ดำเนินการต่อด้วย “ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC”

ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC:

เมื่อต้องการใช้การอัปเดตรหัสเครื่อง HMC ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

- ก่อนที่คุณจะติดตั้งอัปเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูลคอนโซลที่สำคัญบน HMC ของคุณ สำหรับคำแนะนำ โปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 122 จากนั้น ให้ดำเนินการขั้นตอนถัดไป
- ในพื้นที่การนำทาง ให้คลิก อัปเดต
- คลิก Update HMC วิซาร์ด Install Corrective Service จะเปิดขึ้น
- ปฏิบัติตามคำแนะนำในวิซาร์ดเพื่อติดตั้งอัปเดต
- ปิดเครื่อง แล้วรีสตาร์ท HMC เพื่อให้ อัปเดตมีผล
- คลิก Log on and launch the Hardware Management Console web application
- ล็อกอินเข้าสู่อินเทอร์เน็ตเฟส HMC

ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์:

เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งอย่างถูกต้องแล้ว ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

- ในพื้นที่การนำทาง ให้คลิก อัปเดต
- ในพื้นที่ใช้งาน เวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน จะแสดงอยู่ภายใต้ หัวข้อ HMC Code Level
- ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง

4. หากระดับของโค้ดที่แสดงไม่ใช่ระดับที่คุณติดตั้งให้ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. เลือกการเชื่อมต่อเครือข่ายบน HMC
 - b. ลองทำการอัปเดตเฟิร์มแวร์อีกครั้ง โดยใช้ที่เก็บอื่น
 - c. ถ้ายังคงมีปัญหาอยู่ให้ติดต่อระดับของการสนับสนุนถัดไป

การขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP

เรียนรู้วิธีการขอรับอัปเดตรหัสเครื่องสำหรับ HMC โดยใช้ DVD หรือเซิร์ฟเวอร์ FTP

เมื่อต้องการขอรับส่วนอัปเดตรหัสเครื่องของ HMC ให้ปฏิบัติตามขั้นตอนที่ 1-5

ขั้นตอนที่ 1. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

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 ที่มีอยู่ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

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

หมายเหตุ: หากคุณต้องการ 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

เมื่อเสร็จเรียบร้อยแล้ว ให้ดำเนินการต่อด้วย “ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC”

ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC:

เมื่อต้องการใช้การอัปเดตรหัสเครื่อง HMC ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ก่อนที่คุณจะติดตั้งอัปเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูล HMC ของคุณ สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 122
2. ถ้าคุณได้รับหรือสร้างอัปเดตบนดีวีดีแรม ให้ใส่แผ่นดิสก์ดังกล่าวในไดรฟ์ดีวีดีบน HMC ถ้าคุณได้รับหรือสร้างอัปเดตบนอุปกรณ์หน่วยความจำแบบ USB ให้เสียบอุปกรณ์หน่วยความจำนั้น
3. ในพื้นที่การนำทาง ให้คลิก 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. ในพื้นที่การนำทาง ให้คลิก อัปเดต ในพื้นที่ใช้งาน เวอร์ชันของ HMC, รีลีส, ระดับการบำรุงรักษา, ระดับบิลด์ และเวอร์ชันพื้นฐาน จะแสดงอยู่ภายใต้ หัวข้อ HMC Code Level
2. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
3. หากระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. ลองอัปเดตรหัสเครื่องอีกครั้ง ถ้าคุณสร้างดีวีดีในขั้นตอนนี้ ให้ใช้สื่อบันทึกใหม่
 - b. ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การอัปเดตซอฟต์แวร์ HMC ของคุณ

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากรีลีสหนึ่งเป็นรีลีสถัดไป ในขณะที่ยังคงรักษาข้อมูลคอนฟิกูเรชัน HMC ของคุณ

เมื่อต้องการอัปเดตรหัสเครื่องบน HMC ให้ปฏิบัติตามขั้นตอนที่ 1–9

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 เพื่อสั่งซื้อการอัปเดตบนดิสก์

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

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการกำหนดระดับรหัสเครื่องที่มีอยู่บน HMC ให้ปฏิบัติตาม ขั้นตอนเหล่านี้:

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 เพื่อให้สามารถเรียกคืนระดับก่อนหน้านั้นในกรณีที่เกิดปัญหา 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. ในพื้นที่การนำทางให้เลือก **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”

ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล:

เมื่อต้องการบันทึกสถานะคำสั่งระยะไกลให้ทำดังนี้:

1. ในพื้นที่การนำทางให้เลือก **HMC Management**
2. ในรายการงานให้คลิก **Remote Command Execution**.
3. บันทึกว่าเช็kb็อกซ์ **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 ให้บันทึกข้อมูลอัปเดตในทันทีก่อนที่จะอัปเดตซอฟต์แวร์ HMC ของคุณให้เป็นรีลีสใหม่ แอ็คชันนี้อินนุญาติให้คุณเรียกคืนคอนฟิกูเรชัน HMC ได้หลังจากการอัปเดต

หมายเหตุ: อินนุญาติให้มีข้อมูลสำรองได้เพียงระดับเดียวเท่านั้น แต่ครั้งที่คุณบันทึกข้อมูลอัปเดต ระดับก่อนหน้านี้จะถูกเขียนทับ

เมื่อต้องการ บันทึกข้อมูลอัปเดตให้ทำดังนี้:

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

หมายเหตุ: ถ้างานบันทึกข้อมูลอัปเดตล้มเหลว ห้ามดำเนินกระบวนการอัปเดต

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 และ ข้อมูลระบบจะเลื่อนอยู่บนหน้าต่าง
6. เลือก **Upgrade** และคลิก **Next**
7. เลือกจากอ็อปชันต่อไปนี้:
 - ถ้าคุณบันทึกข้อมูลอัปเดตที่บันทึกไว้ในระหว่างงานก่อนหน้านี้ ให้ทำขั้นตอนถัดไป
 - ถ้าคุณไม่ได้บันทึกข้อมูลอัปเดตก่อนหน้านี้ในขั้นตอนนี้ คุณจะ ต้อง บันทึกข้อมูลอัปเดตในตอนนี้ ก่อนที่คุณจะดำเนินการต่อ

8. เลือก Upgrade from media และคลิก Next
9. ยืนยันค่าติดตั้ง และคลิก Finish
10. ปฏิบัติตามพร้อมท์

หมายเหตุ:

- ถ้าน้ำจ้วว่างเปล่า ให้กด space bar เพื่อดูข้อมูล
- ดีวีดีแผ่นแรกอาจใช้เวลาประมาณ 20 ในการติดตั้ง

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

ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์:

เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับ HMC ได้รับการติดตั้งเสร็จสมบูรณ์แล้ว ให้ทำดังนี้:

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

การอัปเดต HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตบนเครือข่าย

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตเครือข่าย

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตเครือข่าย ใช้ขั้นตอนต่อไปนี้อัปเกรด 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:
 - img2a
 - img3a
 - base.img
 - disk1.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 alt diskboot -s enable --mode upgrade` เพื่อรีบูต HMC

7. รีบูต HMC และเริ่มต้นการอัปเดต รันคำสั่ง `hmcshutdown -r -t now` เพื่อเริ่มต้นการอัปเดต

การกำหนดค่า HMC โดยใช้อินเทอร์เฟซ HMC Enhanced+

ศึกษาเกี่ยวกับวิธีตั้งค่าการเชื่อมต่อเครือข่าย กำหนดค่า HMC ของคุณ ดำเนินการขั้นตอนหลังการกำหนดค่า และอัปเดต และอัปเดต HMC ของคุณโดยใช้อินเทอร์เฟซ HMC Enhanced+

หมายเหตุ: โปรซีเดอร์และฟังก์ชันของอินเทอร์เฟซ HMC Enhanced + Tech Preview (Pre-GA) ซึ่งเป็นอ็อปชันที่ถูกจัดเตรียมไว้พร้อมกับ HMC เวอร์ชัน 8.20 เหมือนกับอินเทอร์เฟซ HMC Enhanced+ ที่จัดเตรียมไว้พร้อมกับ HMC เวอร์ชัน 8.30 เฉพาะ HMC Enhanced+ เท่านั้นที่อ้างถึงในเอกสารคู่มือนี้ แต่เนื้อหาในนี้ยังใช้กับอินเทอร์เฟซ HMC Enhanced + Tech Preview (Pre-GA) ได้

การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC

เรียนรู้เกี่ยวกับค่าติดตั้งเน็ตเวิร์กที่คุณสามารถใช้นบน HMC

การเชื่อมต่อเน็ตเวิร์ก HMC

คุณสามารถใช้การเชื่อมต่อเน็ตเวิร์กประเภทต่างๆ เพื่อเชื่อมต่อ HMC ของคุณกับระบบที่ถูกจัดการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีตั้งค่า HMC เพื่อเชื่อมต่อกับเน็ตเวิร์ก โปรดดูที่ “การกำหนดคอนฟิก HMC” ในหน้า 100 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ HMC บนเน็ตเวิร์ก โปรดดูดังต่อไปนี้:

ประเภทของการเชื่อมต่อเน็ตเวิร์ก HMC:

เรียนรู้วิธีใช้ฟังก์ชันการจัดการและการให้บริการแบบรีโมต HMC โดยใช้เครือข่ายของคุณ

HMC สนับสนุนการสื่อสารโลจิคัลในประเภทดังต่อไปนี้:

HMC to managed system

ใช้เพื่อดำเนินฟังก์ชันการจัดการฮาร์ดแวร์โดยส่วนใหญ่ ซึ่ง HMC ออกคำขอฟังก์ชันควบคุมผ่านทางเซอร์วิสโปรเซสเซอร์ของระบบที่ถูกจัดการ บางครั้ง การเชื่อมต่อระหว่าง HMC และเซอร์วิสโปรเซสเซอร์เรียกว่าเป็น **เน็ตเวิร์กบริกา** การเชื่อมต่อนี้ต้องใช้สำหรับการจัดการระบบที่ถูกจัดการ

HMC to logical partition

ใช้เพื่อรวบรวมข้อมูลที่เกี่ยวข้องกับแพลตฟอร์ม (เหตุการณ์ข้อผิดพลาดแพลตฟอร์ม การทำรายการฮาร์ดแวร์) จากระบบปฏิบัติการที่รันอยู่บนโลจิคัลพาร์ติชัน และเพื่อประสานกิจกรรมบางอย่างของแพลตฟอร์ม (LPAR แบบไดนามิก, การซ่อมพร้อมกัน) กับระบบปฏิบัติการเหล่านั้น หากต้องการใช้บริการและคุณลักษณะการแจ้งข้อผิดพลาด คุณต้องสร้างการเชื่อมต่อ

HMC กับ BMC

หมายเหตุ: การเชื่อมต่อ baseboard management controller (BMC) ใช้ได้เฉพาะกับโมเดล HMC 7063-CR1 ใช้เพื่อดำเนินการงานการให้บริการและซ่อมบำรุง การเชื่อมต่อ BMC ใช้เพื่อโหลดและดูแลรักษาเฟิร์มแวร์ HMC บนระบบ การเชื่อมต่อจำเป็นสำหรับการเข้าถึง BMC บน HMC

HMC to remote users

ช่วยให้ผู้ใช้โมสามารถเข้าถึงฟังก์ชัน HMC ผู้ใช้โมสามารถเข้าถึง HMC โดยวิธีดังต่อไปนี้:

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

HMC เพื่อให้บริการ และสนับสนุน

ใช้เพื่อส่งข้อมูล เช่น รายงานความผิดพลาดฮาร์ดแวร์ ข้อมูลคลัง และการอัปเดตไมโครโค้ด ไปยังและจากผู้ให้บริการของคุณ คุณสามารถใช้พาดการสื่อสารนี้เพื่อเรียกการให้บริการโดยอัตโนมัติ

HMC ของคุณสามารถสนับสนุนฟิสิกส์อินเทอร์เนตอินเทอร์เฟซได้มากถึงสี่อินเทอร์เฟซขึ้นอยู่กับแต่ละรุ่น เวอร์ชันสแตนด์อะโลนของ HMC สนับสนุนอินเทอร์เฟซ HMC สามอินเทอร์เฟซเท่านั้น โดยใช้อินเทอร์เฟซอะแดปเตอร์รวมหนึ่งอะแดปเตอร์และจนถึงสองอะแดปเตอร์บล็อกอิน อินเทอร์เฟซ แต่ละตัวเหล่านี้ในวิธีดังต่อไปนี้:

- เน็ตเวิร์กอินเทอร์เฟซตั้งแต่หนึ่งขึ้นไปสามารถใช้เฉพาะสำหรับการสื่อสารแบบ HMC-ไปที่-ระบบที่ถูกจัดการเท่านั้น ซึ่งหมายความว่า เฉพาะ HMC และเซิร์ฟเวอร์โฮสต์ของระบบที่ถูกจัดการเท่านั้นที่จะอยู่บนเน็ตเวิร์กนั้น แม้ว่าอินเทอร์เฟซ เครือข่ายที่อยู่ในตัวประมวลผลเซิร์ฟเวอร์มีการเข้ารหัสโปรโตคอล Secure Sockets Layer (SSL) และมีการป้องกันด้วยรหัสผ่าน การมีเครือข่าย เฉพาะงานที่แยกต่างหากสามารถช่วยให้อินเทอร์เฟซเหล่านี้มีระดับความปลอดภัย สูงขึ้น
- โดยทั่วไปแล้ว อินเทอร์เฟซเน็ตเวิร์กแบบเปิดใช้กับการเชื่อมต่อเน็ตเวิร์กระหว่าง HMC และโลจิคัลพาร์ติชันบนระบบที่ถูกจัดการ สำหรับการสื่อสารแบบ HMC-ไปที่-โลจิคัลพาร์ติชัน คุณยังสามารถใช้เน็ตเวิร์กอินเทอร์เฟซแบบเปิดนี้เพื่อจัดการกับ HMC จากระยะไกล
- หรือคุณอาจใช้อินเทอร์เฟซอื่นเพื่อเชื่อมต่อกับโลจิคัลพาร์ติชัน และจัดการ HMC จากระยะไกล อินเทอร์เฟซนี้ยังสามารถใช้เป็นการเชื่อมต่อ HMC แยกต่างหากไปยังกลุ่มโลจิคัลพาร์ติชันอื่น ตัวอย่างเช่น คุณอาจต้องการให้มี LAN การจัดการที่แยกต่างหากจาก LAN ซึ่งธุรกรรมทางธุรกิจปกติทั้งหมดกำลัง รันอยู่ ผู้ดูแลระบบจากระยะไกลสามารถเข้าถึง HMC และหน่วยที่ได้รับการจัดการอื่นๆโดยวิธีนี้ ในบางครั้งโลจิคัลพาร์ติชันจะอยู่ใน โดเมนความปลอดภัยเครือข่ายอื่น อาจจะเป็นด้านหลังไฟร์วอลล์ และคุณอาจต้องการมี การเชื่อมต่อเครือข่าย HMC ที่แตกต่างกันสำหรับสองโดเมนเหล่านั้น

ข้อกำหนดเว็บเบราว์เซอร์สำหรับ HMC

Hardware Management Console (HMC) เวอร์ชัน 8.7.0 ได้รับการสนับสนุนโดย Google Chrome เวอร์ชัน 57, Microsoft Internet Explorer (IE) เวอร์ชัน 11.0, Mozilla Firefox เวอร์ชัน 45 และ 52 Extended Support Release (ESR) และ Safari เวอร์ชัน 10.1

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

ต้องเปิดใช้งานเซสชันคุกกี้เพื่อให้ ASMI สามารถทำงานได้เมื่อเชื่อมต่อกับ HMC แบบรีโมต รหัสพรีอ็อกซี asm บันทึกและใช้ข้อมูลเซสชัน ปฏิบัติตามขั้นตอนต่อไปเพื่อเปิดใช้งาน เซสชันคุกกี้

การเปิดใช้งานเซสชันคุกกี้ใน Internet Explorer

1. เลือก เครื่องมือ และคลิก อีพชันอินเทอร์เน็ต
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 อีพชัน
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" หมายถึงการเชื่อมต่อเน็ตเวิร์กกระหว่าง HMC กับโลจิสติกส์พาร์ตชันและ 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 อีพชัน 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

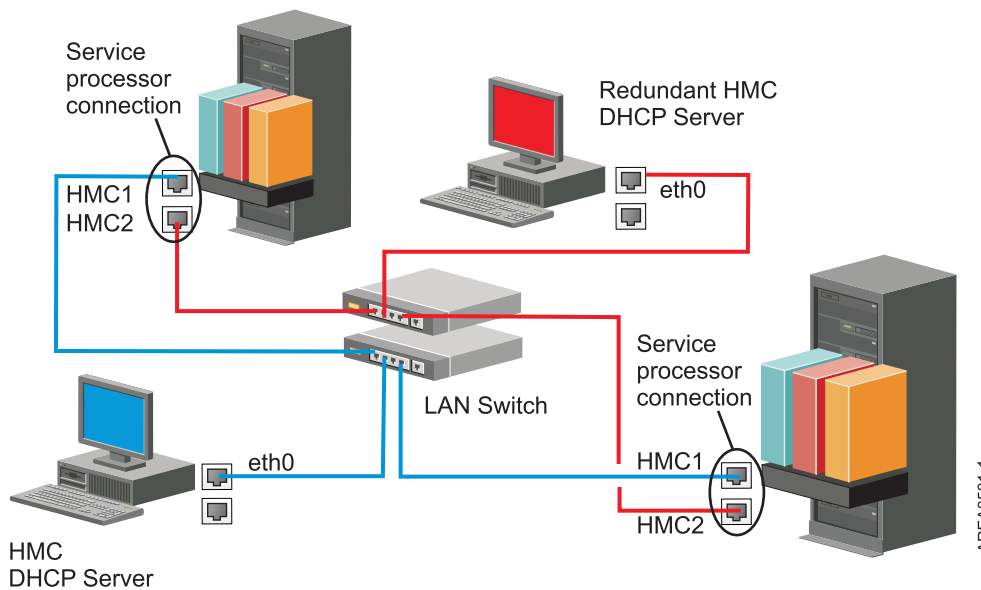
HMC ประกอบด้วยไฟร์วอลล์บนแต่ละ เน็ตเวิร์กอินเตอร์เฟซ ไฟร์วอลล์ระดับต้นจะถูกตั้งค่าโดยอัตโนมัติเมื่อคุณรันวิซาร์ด HMC Guided Setup แต่คุณควรปรับการตั้งค่าไฟร์วอลล์หลังจากการติดตั้งและการคอนฟิก HMC เบื้องต้น

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 109

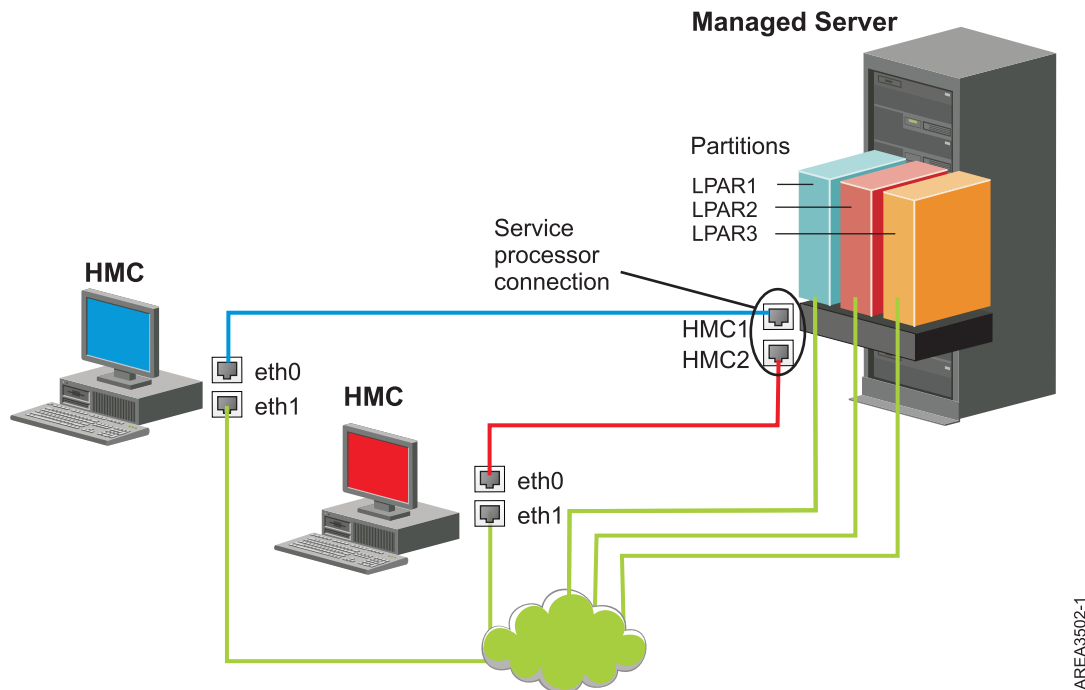


รูปภาพนี้แสดงสภาวะแวดล้อม HMC สำรอง พร้อมด้วยระบบที่ถูกจัดการ 2 ระบบ HMC เครื่องแรกเชื่อมต่อกับพอร์ตแรกบนแต่ละ FSP และ HMC สำรองเชื่อมต่อกับพอร์ตที่สองบน HMC แต่ละเครื่อง HMC แต่ละเครื่องถูกตั้งค่าเป็นเซิร์ฟเวอร์ DHCP โดยใช้ช่วง IP แอดเดรสที่แตกต่างกัน การเชื่อมต่ออยู่บนเน็ตเวิร์กส่วนตัวที่แยกต่างหาก 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 สองเครื่องที่เชื่อมต่อกับเซิร์ฟเวอร์ที่จัดการเดียวกันบนเน็ตเวิร์กส่วนตัว และกับโลจิคัลพาร์ติชัน 3 พาร์ติชัน บนเน็ตเวิร์กสาธารณะ คุณสามารถมีอีเทอร์เนตอะแดปเตอร์เพิ่มเติมเพื่อให้ HMC มี เน็ตเวิร์กอินเตอร์เฟซ 3 ชุด คุณสามารถใช้เน็ตเวิร์กที่สามนี้เป็นเน็ตเวิร์กการจัดการ หรือเชื่อมต่อกับ CSM (Cluster Systems Manager) Management Server

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ DHCP โปรดดูที่ “การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 109

การกำหนดวิธีการเชื่อมต่อที่จะใช้กับเซิร์ฟเวอร์ call-home:

ศึกษาเพิ่มเติมเกี่ยวกับข้อพจน์ของการเชื่อมต่อที่คุณมีอยู่เมื่อคุณใช้เซิร์ฟเวอร์ call-home

คุณสามารถกำหนดคอนฟิก HMC เพื่อส่งข้อมูลที่เกี่ยวข้องกับเซอร์วิส ไปยัง IBM โดยใช้ การเชื่อมต่ออินเทอร์เน็ตแบบใช้ LAN หรือการเชื่อมต่อผ่านโมเด็ม

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

คุณมีตัวเลือกด้านการสื่อสารสองตัวเลือกเมื่อคุณกำหนดคอนฟิกการเชื่อมต่ออินเทอร์เน็ต แบบใช้ LAN ทางเลือกแรกคือใช้ Secure Sockets Layer (SSL) มาตรฐาน สามารถเปิดใช้การสื่อสาร SSL เพื่อเชื่อมต่อ อินเทอร์เน็ตผ่านพรีอซีเซิร์ฟเวอร์ การเชื่อมต่อ SSL มีแนวโน้มว่าจะสอดคล้องกับแนวทางความปลอดภัยขององค์กร ทางเลือกที่สองคือ การใช้การเชื่อมต่อ VPN

หมายเหตุ: หากการเชื่อมต่อเน็ตเวิร์กอินเทอร์เน็ตแบบเปิดของคุณใช้เฉพาะ Internet Protocol Version 6 (IPv6) เท่านั้น คุณจะไม่สามารถใช้ Internet VPN ในการเชื่อมต่อเพื่อการสนับสนุนได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรโตคอลที่ใช้โปรดดู “การเลือก อินเทอร์เน็ตโปรโตคอล” ในหน้า 87

ข้อดีของการใช้การเชื่อมต่ออินเทอร์เน็ตอาจได้แก่:

- ความเร็วในการรับส่งข้อมูลที่เร็วกว่า
- ลดค่าใช้จ่ายสำหรับลูกค้า (เช่น ค่าสายโทรศัพท์ท่อนาล็อก ที่จัดเตรียมไว้โดยเฉพาะ)
- ความเชื่อถือได้สูงกว่า

ลักษณะความปลอดภัยต่อไปนี้มีผลบังคับใช้ไม่ว่าคุณ会选择ใช้วิธีการเชื่อมต่อแบบใดก็ตาม:

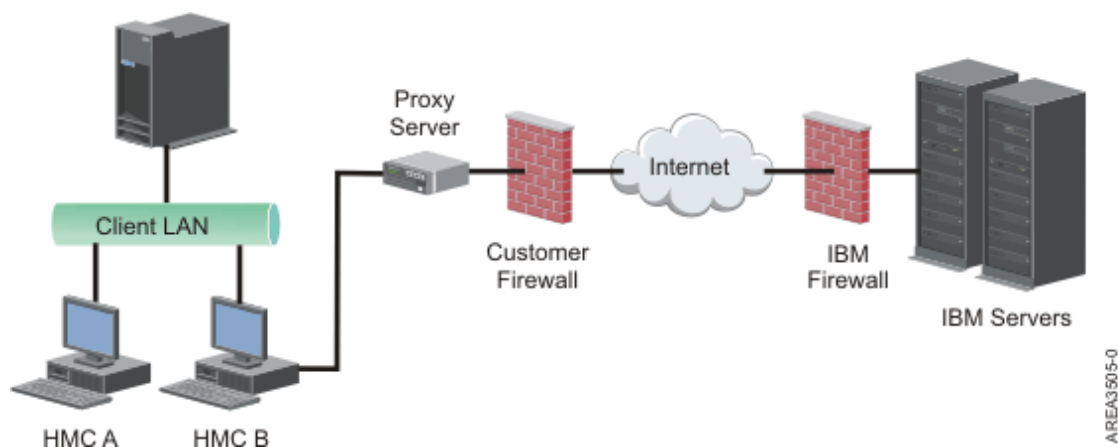
- คำร้องขอของระบบสนับสนุนแบบรีโมตเริ่มต้นจาก HMC ไปยัง IBM การเชื่อมต่อเข้าไม่ได้เริ่มจาก IBM Service Support System
- ข้อมูลทั้งหมดที่โอนระหว่าง HMC และ IBM Service Support System จะถูกเข้ารหัสโดยใช้การเข้ารหัสระดับสูงขึ้นอยู่กับเมธอดของภาวะเชื่อมต่อที่เลือก ซึ่งจะเข้ารหัสโดยใช้ SSL หรือ IPSec Encapsulating Security Payload (ESP)
- เมื่อคุณเริ่มต้นทำงานกับการเชื่อมต่อแบบเข้ารหัส HMC จะพิสูจน์ตัวตน ปลายทางเป้าหมาย นั่นคือ IBM Service Support System

ข้อมูลที่ส่งไปยัง IBM Service Support System ประกอบด้วยข้อมูลเกี่ยวกับปัญหาของฮาร์ดแวร์ และคอนฟิกรุ่น ไม่มีแอฟพลิเคชั่นหรือข้อมูลลูกค้าถูกส่งไปยัง IBM

การใช้การเชื่อมต่ออินเทอร์เน็ตทางอ้อมด้วย พรีอซีเซิร์ฟเวอร์

หากการติดตั้งของคุณต้องการให้ HMC อยู่บนเครือข่ายแบบไพรเวต คุณต้องเปิดการเชื่อมต่อทางอ้อมผ่านอินเทอร์เน็ต โดยใช้พรีอซี SSL ซึ่งสามารถส่งคำร้องขอผ่านอินเทอร์เน็ตได้ หนึ่งในข้อดีอีกประการหนึ่งของการใช้พรีอซี SSL คือ พรีอซีสามารถสนับสนุนการจัดทำบันทึกและอำนวยความสะดวกด้านการตรวจสอบ

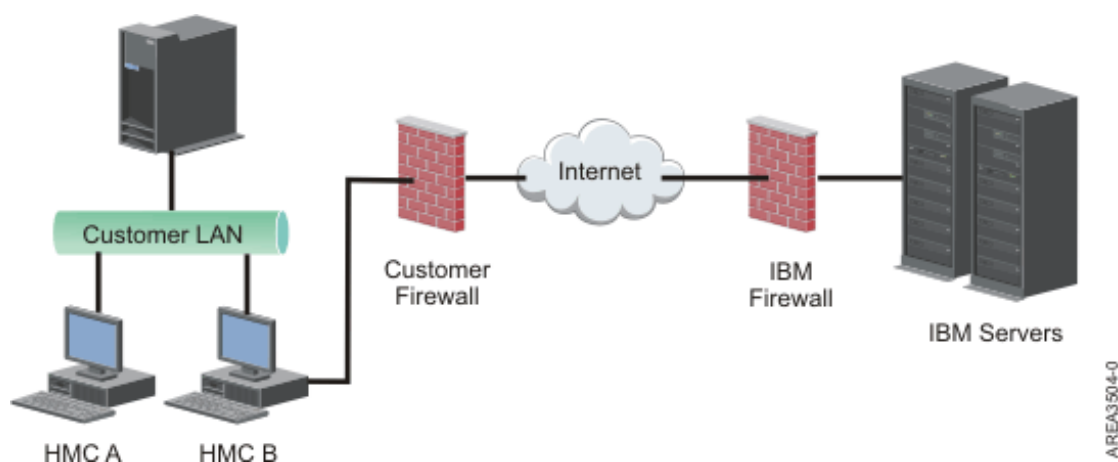
เมื่อต้องการส่งต่อข้อผิดพลาด SSL พรีอซีเซิร์ฟเวอร์จะต้องสนับสนุนฟังก์ชันส่วนหัวพรีอซีระดับต้น (ตามที่ระบุไว้ใน RFC 2616) และเมธอด CONNECT หรือ การพิสูจน์ตัวตนพรีอซีระดับต้น (RFC 2617) สามารถกำหนดคอนฟิก เพื่อให้ HMC พิสูจน์ตัวตนก่อนที่จะพยายามส่งต่อข้อผิดพลาดผ่าน พรีอซีเซิร์ฟเวอร์



เพื่อให้ HMC สื่อสารได้สำเร็จ พร็อกซีเซิร์ฟเวอร์ของลูกค้าจะต้องอนุญาตให้เชื่อมต่อกับพอร์ต 443 คุณสามารถกำหนดคอนฟิกพร็อกซีเซิร์ฟเวอร์ของคุณเพื่อจำกัด IP แอดเดรสที่เฉพาะเจาะจง ซึ่ง HMC สามารถเชื่อมต่อได้ โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 87 สำหรับ รายการ IP แอดเดรส

การใช้การเชื่อมต่อ SSL อินเทอร์เน็ตโดยตรง

ถ้า HMC ของคุณ สามารถเชื่อมต่ออินเทอร์เน็ต และสามารถตั้งค่าไฟร์วอลล์ภายนอก เพื่ออนุญาตให้ส่งแพ็กเก็ต TCP ไปยังปลายทางที่ระบุไว้ใน “รายการแอดเดรส Internet SSL” ในหน้า 87 คุณจะสามารถใช้ การเชื่อมต่ออินเทอร์เน็ตโดยตรงได้



การใช้ Internet SSL เพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต:

การสื่อสารทั้งหมดถูกจัดการผ่านซ็อกเก็ต TCP ซึ่งเริ่มโดย HMC และใช้ SSL ระดับสูง เพื่อเข้ารหัสข้อมูลที่ส่งผ่าน แอดเดรส TCP/IP ปลายทางถูกเผยแพร่ (โปรดดูที่ “รายการแอดเดรส Internet SSL” ในหน้า 87) เพื่อที่ว่าไฟร์วอลล์ภายนอก จะสามารถตั้งค่าเพื่ออนุญาตการเชื่อมต่อเหล่านี้

หมายเหตุ: พอร์ต HTTPS มาตรฐาน 443 ใช้สำหรับการสื่อสารทั้งหมด

HMC สามารถเปิดใช้งานเพื่อเชื่อมต่อโดยตรงกับอินเทอร์เน็ต หรือเพื่อเชื่อมต่อทางอ้อมจากพร็อกซีเซิร์ฟเวอร์ที่ถูกตั้งค่าให้ การตัดสินใจเกี่ยวกับแนวทางที่เหมาะสมที่สุดสำหรับการติดตั้งของคุณขึ้นอยู่กับข้อกำหนดความปลอดภัยและระบบเน็ตเวิร์กของ องค์กรของคุณ HMC (โดยตรง หรือผ่านพร็อกซี SSL) ใช้แอตเดรสต่อไปนี้ เมื่อถูกตั้งค่าให้ใช้การเชื่อมต่อ Internet SSL

การเลือก อินเทอร์เน็ตโปรโตคอล:

ระบุเวอร์ชันของ IP แอตเดรสที่จะใช้เมื่อ HMC เชื่อมต่อไปยังผู้ให้บริการของคุณ

ผู้ใช้งานมากจะใช้ Internet Protocol Version 4 (IPv4) เพื่อเชื่อมต่อไปยังผู้ให้บริการ IPv4 แอตเดรสปรากฏขึ้นในรูปแบบที่แสดงถึง ไบต์สี่ไบต์ของ IPv4 แอตเดรส 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 110 และ “การตั้งค่า IPv6 แอตเดรส” ในหน้า 110

รายการแอตเดรส Internet SSL:

ศึกษาเกี่ยวกับแอตเดรสที่ HMC ใช้เมื่อใช้ภาวะเชื่อมต่อ Internet SSL

HMC จะใช้แอตเดรส IPv4 ต่อไปนี้เพื่อติดต่อส่วนบริการ และส่วนสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้การเชื่อมต่ออินเทอร์เน็ตแบบ SSL

แอตเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่:

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

แอตเดรส IPv4 ต่อไปนี้สำหรับทวีปอเมริกา:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

แอตเดรส IPv4 ต่อไปนี้สำหรับทุกสถานที่ที่ไม่ใช่อเมริกา:

- 129.42.160.48
- 129.42.160.50

- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

หมายเหตุ: เมื่อตั้งค่าไฟร์วอลล์เพื่ออนุญาตให้ HMC สามารถเชื่อมต่อกับเซิร์ฟเวอร์เหล่านี้จะต้องใช้ IP แอดเดรสที่เฉพาะเจาะจงสำหรับภูมิภาคดังกล่าวเท่านั้น

HMC จะใช้แอดเดรส IPv6 ต่อไปนี้เพื่อติดต่อส่วนบริการและส่วนสนับสนุนของ IBM เมื่อมีการตั้งค่าให้ใช้การเชื่อมต่ออินเทอร์เน็ตแบบ SSL:

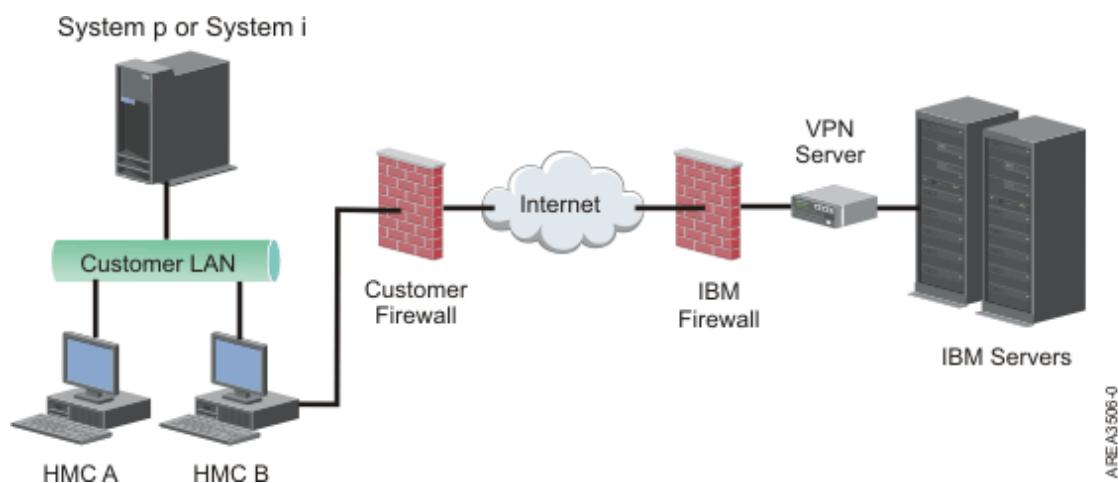
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

การใช้ Virtual Private Network เพื่อเชื่อมต่อระบบสนับสนุนระยะไกล:

virtual private network (VPN) จัดเตรียมความปลอดภัย เมื่อคุณเชื่อมต่อกับส่วนสนับสนุนแบบรีโมต

หมายเหตุ: การเชื่อมต่อชนิดนี้พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือเวอร์ชันก่อนหน้านี้นี้เท่านั้น

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



เป็นความรับผิดชอบของผู้ดูแลระบบในการจัดเตรียมการเชื่อมต่ออินเทอร์เน็ต ไฟร์วอลล์ยังสามารถจำกัด IP address ที่ระบุเฉพาะเพื่อให้ HMC สามารถเชื่อมต่อได้ ถ้าคุณต้องการกำหนดคอนฟิกไฟร์วอลล์ของคุณเพื่อจำกัด IP แอดเดรส โปรดดูที่ “รายการแอดเดรสเซิร์ฟเวอร์ VPN” ในหน้า 89 สำหรับ รายการแอดเดรสที่คุณสามารถใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการเชื่อมต่อกับอินเทอร์เน็ตโดยใช้ LAN-based VPN โปรดดู “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104

รายการแอตเดรสเซิร์ฟเวอร์ VPN:

แสดงรายการเซิร์ฟเวอร์ที่ถูกใช้โดย HMC เมื่อกำหนดคอนฟิก HMC ให้ใช้ภาวะเชื่อมต่อกับอินเทอร์เน็ตโดยใช้ VPN

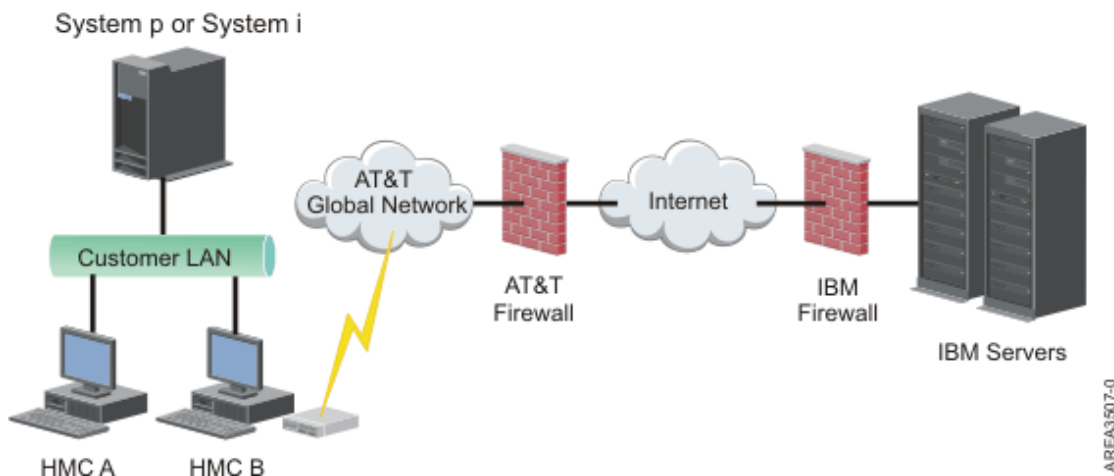
เซิร์ฟเวอร์ต่อไปนี้ใช้โดย HMC เมื่อถูกกำหนดคอนฟิกให้ใช้การเชื่อมต่อ VPN อินเทอร์เน็ต การเชื่อมต่อทั้งหมดใช้ ESP และ UDP บนพอร์ต 500 และพอร์ต 4500 เมื่อกำลังใช้ไฟร์วอลล์ Network Address Translation (NAT)

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

การใช้โทรศัพท์และโมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต:

ถ้าคุณต้องการใช้โมเด็มเพื่อเชื่อมต่อระบบสนับสนุนแบบรีโมต คุณจะต้องจัดหาสายอะนาล็อกแบบเฉพาะงานเพื่อเชื่อมต่อกับโมเด็ม HMC HMC ใช้โมเด็มเพื่อต่อเลขหมายโกลบอลเน็ตเวิร์กและเพื่อเชื่อมต่อกับฝ่ายสนับสนุนแลฝ่ายบริการของ IBM

หมายเหตุ: ประเภทการเชื่อมต่อนี้พร้อมใช้งานบน HMC เวอร์ชัน 8.2.0 หรือเวอร์ชันก่อนหน้านี้นี้เท่านั้น



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเชื่อมต่อฝ่ายสนับสนุนแบบรีโมตโดยใช้โทรศัพท์และโมเด็ม โปรดดู “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104

การใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์:

หัวข้อนี้จะอธิบายถึงสิ่งที่คุณจำเป็นต้องทราบเมื่อตัดสินใจใช้เซิร์ฟเวอร์ Call-Home มากกว่าหนึ่งเครื่อง

เมื่อต้องการหลีกเลี่ยงไม่ให้เกิดความล้มเหลวแม้แต่จุดเดียวให้คอนฟิก HMC ให้ใช้เซิร์ฟเวอร์ Call-Home หลายเซิร์ฟเวอร์ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานเซิร์ฟเวอร์แรก จะพยายามจัดการเหตุการณ์เซอร์วิสแต่ละเหตุการณ์ หากการเชื่อมต่อหรือการส่งข้อมูลล้มเหลว กับเซิร์ฟเวอร์ Call-Home นี้ จะมีการพยายามร้องขอเซอร์วิสอีกครั้งโดยใช้ เซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานอื่นจนกว่าจะประสบความสำเร็จหรือได้พยายามกับ ทุกเซิร์ฟเวอร์แล้ว

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

- HMC หลักถูกกำหนดคอนฟิกให้ใช้เซิร์ฟเวอร์ Call-Home ที่ "ค้นพบ" โดยเซิร์ฟเวอร์ Call-Home จะอยู่บนซับเน็ตเดียวกันกับ HMC หลัก หรือจัดการระบบเดียวกัน
- มีการเพิ่มเซิร์ฟเวอร์ Call-Home ด้วยตนเองลงในรายการ คอนโซลเซิร์ฟเวอร์ Call-Home ที่พร้อมใช้งานสำหรับการเชื่อมต่อภายนอก

การจัดเตรียมสำหรับการตั้งค่าของ HMC

ใช้ส่วนนี้เพื่อรวบรวมการตั้งค่าการตั้งค่าที่จำเป็นที่คุณต้องทราบก่อนเริ่มขั้นตอนการตั้งค่า

เมื่อต้องการกำหนดคอนฟิก HMC คุณต้องเข้าใจ แนวคิดที่เกี่ยวข้อง ดำเนินการตัดสินใจ และจัดเตรียมการติดตั้ง

ส่วนนี้อธิบายข้อมูลที่คุณจะต้องใช้เพื่อเชื่อมต่อ HMC กับรายการต่อไปนี้:

- เซอร์วิสโปรเซสเซอร์ในระบบที่ถูกจัดการของคุณ
- โลจิคัลพาร์ติชันในระบบที่ถูกจัดการเหล่านั้น
- รีโมตเวิร์กสเตชัน
- IBM Service เพื่อนำฟังก์ชัน "call-home" ไปใช้

หมายเหตุ: มีข้อมูลการเชื่อมต่อและความปลอดภัยเพิ่มเติมพร้อมให้ใช้งาน สำหรับข้อมูลเพิ่มเติม ให้ดูที่ **ESA for HMC Connectivity Security** สำหรับ IBM POWER6, POWER7 และ POWER8 Processor-Based Systems และรายงานอย่างเป็นทางการของ IBM Storage Systems DS8000 จะมีอยู่ที่: IBM Electronic Service Agent (<http://www-01.ibm.com/support/esa/security.htm>)

เมื่อต้องการจัดเตรียมสำหรับการตั้งค่า HMC ให้ดำเนินการขั้นตอน ต่อไปนี้:

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 82
5. หากคุณใช้เน็ตเวิร์กเปิดเพื่อจัดการกับ FSP คุณต้องตั้งค่าแอตเดรสของ FSP ผ่านเมนู Advanced System Management Interface ด้วยตนเอง ขอแนะนำให้ใช้เน็ตเวิร์กส่วนตัวที่ไม่สามารถกำหนดเราต์ได้
6. หากคุณมีสอง HMC ให้กำหนด HMC หลักและรอง HMC หลักควรมีตำแหน่งที่ใกล้กับเครื่องมากกว่า และควรเป็น HMC ที่คอนฟิกให้ติดต่อผู้ให้บริการ
7. กำหนดการตั้งค่าเน็ตเวิร์กที่คุณจะต้องใช้เพื่อเชื่อมต่อ HMC กับรีโมตเวิร์กสเตชัน โลจิคัลพาร์ติชัน และอุปกรณ์เน็ตเวิร์ก

8. กำหนดวิธีที่ HMC จะ “call home” อีพซัน Call home รวมถึง การเชื่อมต่ออินเทอร์เน็ตแบบ Secure Socket Layer (SSL) ขาออกเท่านั้น โมเด็ม หรือการเชื่อมต่อ Virtual Private Network (VPN)
9. กำหนดผู้ใช้ HMC ที่คุณจะสร้าง พร้อมทั้งรหัสผ่าน และบทบาทของผู้ใช้เหล่านั้น คุณต้องระบุรหัสผ่านให้กับผู้ใช้ hscroot และ hscope
10. จัดทำเอกสารแสดงข้อมูลติดต่อบริษัทดังต่อไปนี้ ซึ่งจะต้องใช้เมื่อกำหนดคอนฟิก call home:
 - ชื่อบริษัท
 - การติดต่อผู้ดูแลระบบ
 - อีเมลแอดเดรส
 - หมายเลขโทรศัพท์
 - หมายเลขแฟกซ์
 - แอดเดรสของที่ตั้งทางกายภาพของ HMC
11. หากคุณวางแผนที่จะใช้อีเมลเพื่อแจ้งเตือนโอเปอเรเตอร์ หรือผู้ดูแลระบบ เมื่อข้อมูลถูกส่งไปยัง IBM Service ผ่าน call-home, ให้ระบุเซิร์ฟเวอร์ Simple Mail Transfer Protocol (SMTP) และแอดเดรสอีเมลที่คุณจะใช้
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 และเตรียมบ่อนค่า เมื่อเชื่อมต่อกับ FSP ของเซิร์ฟเวอร์ที่ถูกจัดการในครั้งแรก

เมื่อคุณดำเนินขั้นตอนเตรียมการเหล่านี้เสร็จสิ้น ให้ป้อนข้อมูลใน “เวิร์กชิตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91

เวิร์กชิตเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC

ใช้เวิร์กชิตนี้เพื่อดูข้อมูลการติดตั้งที่คุณต้องเตรียมพร้อมสำหรับการติดตั้ง

ค่ากำหนดเน็ตเวิร์ก

อินเทอร์เน็ตเฟส LAN: เลือกอะแดปเตอร์ที่มี (เช่น eth0, eth1) ซึ่งจะใช้โดย HMC นี้เพื่อเชื่อมต่อกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน บริการและการสนับสนุน รวมถึงผู้ใช้โมด โปรดักต์ที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80 สำหรับข้อมูลเพิ่มเติม การเชื่อมต่อจาก HMC สามารถอยู่บนเน็ตเวิร์กส่วนตัวหรือเน็ตเวิร์กแบบเปิด

ความเร็วของอีเทอร์เน็ตอะแดปเตอร์และ Duplex

บ่อนความเร็วของอีเทอร์เน็ตอะแดปเตอร์ที่ต้องการและโหมด duplex อีพซัน autodetection จะระบุออีพซันใดเหมาะสมที่สุด 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

ตารางที่ 34. ความเร็วของอีเทอร์เน็ตอะแดปเตอร์และ Duplex

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

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเน็ตเวิร์กแบบเปิดและเน็ตเวิร์กส่วนตัว โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสถานะแวดล้อม HMC” ในหน้า 82

ตารางที่ 35. เครือข่ายแบบไพรเวตและเครือข่ายแบบเปิด

	eth0	eth1	eth2	eth3
ระบุเน็ตเวิร์กแบบ ส่วน ตัว หรือ เปิด สำหรับแต่ ละอะแดปเตอร์				

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

สำหรับอีเทอร์เน็ตอะแดปเตอร์ที่ระบุ เป็นเน็ตเวิร์กส่วนตัว ให้ดำเนินการตามตารางต่อไปนี้:

ตารางที่ 36. เน็ตเวิร์กส่วนตัว

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

หากคุณกำลังใช้ 7063-CR1 HMC คุณต้องเชื่อมต่อพอร์ต Ethernet IPMI กับเครือข่ายเพื่อเข้าถึง baseboard management controller (BMC) บน HMC สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “กำหนดค่าการเชื่อมต่อ BMC” ในหน้า 163 กรอกรหัสข้อมูลในตารางต่อไปนี้สำหรับการเชื่อมต่อ BMC ของคุณ

ตารางที่ 37. การเชื่อมต่อ BMC

	IPMI
คุณต้องการกำหนดค่าการเชื่อมต่อนี้โดยใช้โหมด DHCP หรือไม่ (ใช่/ไม่ใช่)	
หากไม่ แสดงรายการสแตติกแอดเดรสที่ระบุด้านล่าง:	
IP แอดเดรส:	

ตารางที่ 37. การเชื่อมต่อ BMC (ต่อ)

	IPMI
Subnet mask:	
เกตเวย์:	

สำหรับฮาร์ดแวร์เน็ตเวิร์กที่ระบุเป็นเน็ตเวิร์ก เปิดให้ดำเนินการตามตารางต่อไปนี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ อินเทอร์เน็ตโปรโตคอลเวอร์ชันอื่น โปรดดูที่ “การเลือกอินเทอร์เน็ตโปรโตคอล” ในหน้า 87

การใช้ IPv6

หากคุณกำลังใช้ IPv6 ให้ปรึกษากับผู้บริหารเน็ตเวิร์กของคุณ แล้วเลือกวิธีที่คุณต้องการใช้รับ IP แอดเดรส หลังจากนั้นให้ดำเนินการตาม ตารางต่อไปนี้:

ตารางที่ 38. การใช้ IPv6

	eth0	eth1	eth2	eth3
คุณกำลังใช้ IP แอดเดรสที่มีการกำหนดไว้อย่างคงที่ใช่หรือไม่? หากใช่ให้บันทึกแอดเดรสนั้นไว้ที่นี่				

ตารางที่ 39. การใช้ IPv6

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

ตารางที่ 40. การใช้ IPv6

	eth0	eth1	eth2	eth3
คุณกำลังรับ IP แอดเดรสจากเราเตอร์ IPv6 ใช่หรือไม่?				

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า IPv6 address โปรดดูที่ “การตั้งค่า IPv6 แอดเดรส” ในหน้า 110 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ IPv6 แอดเดรสเท่านั้น โปรดดูที่ “การใช้ IPv6 แอดเดรสเท่านั้น” ในหน้า 110

การใช้ IPv4

ดำเนินการตามตารางต่อไปนี้สำหรับฮาร์ดแวร์เน็ตเวิร์กที่ระบุเป็น เน็ตเวิร์กเปิดโดยใช้ IPv4

ตารางที่ 41. การใช้ 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 ค่าติดตั้งการควบคุมเหล่านี้สำหรับฟิสิคัลเน็ตเวิร์กอินเตอร์เฟซแต่ละชุด ซึ่งทำให้ คุณสามารถควบคุมว่าเน็ตเวิร์กอินเตอร์เฟซ HMC ใดจะสามารถเข้าถึงไดบนแต่ละเน็ตเวิร์ก

ถ้าคุณได้ตั้งค่าอย่างน้อยหนึ่งอะแดปเตอร์เป็น เน็ตเวิร์กอะแดปเตอร์แบบเปิด คุณจะต้องจัดหาข้อมูลเพิ่มเติมต่อไป เพื่อให้ HMC ของคุณสามารถเข้าถึง LAN:

ตารางที่ 42. ข้อมูลโฮสต์แบบโลคัล

ข้อมูลโฮสต์แบบโลคัล	
ชื่อโฮสต์ HMC:	
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 ให้ป้อน ชื่อโฮสต์และโดเมนเนมของ HMC นอกจากนี้คุณยังระบุชื่อโฮสต์แบบย่อ บนเน็ตเวิร์กของคุณเท่านั้น ให้ป้อนชื่อโฮสต์แบบเต็ม ตัวอย่างโดเมนเนม: name.yourcompany.com

ข้อมูลเกตเวย์

เมื่อต้องการกำหนดเกตเวย์ดีฟอลต์ให้ใส่แอดเดรส TCP/IP ที่จะใช้สำหรับการเร้าต์แพ็กเก็ต IP แอดเดรสเกตเวย์จะแจ้งคอมพิวเตอร์แต่ละเครื่องหรืออุปกรณ์ เน็ตเวิร์กแต่ละอุปกรณ์ว่าจะส่งข้อมูลเมื่อใด ถ้าสถานีเป้าหมายไม่ได้ระบุให้ เน็ตเวิร์กย่อยเป็นต้นทาง

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 สำหรับการแม็ปชื่อโฮสต์ และ IP แอดเดรส ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

ลำดับการค้นหาโดเมนซัพฟิ็กซ์

ป้อนโดเมนซัพฟิ็กซ์ที่คุณกำลังใช้ HMC จะใช้โดเมนซัพฟิ็กซ์ เพื่อผนวกเข้ากับชื่อที่ไม่ถูกต้องสำหรับการค้นหา DNS ซัพฟิ็กซ์จะถูกค้นหาตามลำดับที่แสดงอยู่ในรายการ ลำดับการค้นหานี้จะใช้ได้เฉพาะในกรณีที่ DNS ถูกเปิดใช้งานเท่านั้น

การแจ้งเตือนทางอีเมล

ลิสต์ข้อมูลติดต่อทางอีเมล ถ้าคุณต้องการได้รับแจ้งทางอีเมล เมื่อเกิดปัญหาเกี่ยวกับฮาร์ดแวร์กับระบบของคุณ

ตารางที่ 43. การแจ้งเตือนทางอีเมล

ฟิลด์	
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 โคลเอ็นต์จะส่งข้อความและสื่อสาร 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

ตารางที่ 44. ข้อมูลติดต่อฝ่ายบริการ

ข้อมูลติดต่อฝ่ายบริการ	
ชื่อบริษัท	

ตารางที่ 44. ข้อมูลติดต่อฝ่ายบริการ (ต่อ)

ข้อมูลติดต่อฝ่ายบริการ	
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 84

ตารางที่ 45. ชนิดของการเชื่อมต่อ

ชนิดของการเชื่อมต่อ	
	Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต

ตารางที่ 45. ชนิดของการเชื่อมต่อ (ต่อ)

ชนิดของการเชื่อมต่อ	
	เรียกเลขหมายจาก HMC แบบโลคัล
	Virtual private network (VPN) ผ่านอินเทอร์เน็ต

Secure Sockets Layer (SSL) ผ่านอินเทอร์เน็ต:

ถ้าคุณมีการเชื่อมต่ออินเทอร์เน็ตจาก HMC ของคุณ คุณสามารถใช้การเชื่อมต่อดังกล่าวเพื่อติดต่อผู้ให้บริการ คุณสามารถเชื่อมต่อโดยตรงกับผู้ให้บริการของคุณโดยใช้ Secure Sockets Layer (SSL) แบบเข้ารหัส ซึ่งใช้การเชื่อมต่ออินเทอร์เน็ตที่มีอยู่ เลือกใช้พรีอ็อกซี SSL ถ้าคุณต้องการกำหนดคอนฟิกการใช้ SSL ที่เข้ารหัสโดยใช้การเชื่อมต่อทางอ้อมซึ่งใช้พรีอ็อกซี SSL

ตารางที่ 46. Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต

Secure Sockets Layer (SSL) ผ่าน อินเทอร์เน็ต	
ใช้พรีอ็อกซี SSL? (ใช่/ไม่ใช่)	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
แอดเดรส:	
พอร์ต:	
พิสูจน์ตัวตนด้วยพรีอ็อกซี SSL?	
ถ้า ใช่ แสดงรายการข้อมูลด้านล่าง:	
ผู้ใช้:	
รหัสผ่าน:	

โปรโตคอลการเชื่อมต่ออินเทอร์เน็ตที่ใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอินเทอร์เน็ตโปรโตคอลอื่น โปรดดูที่ “การเลือกอินเทอร์เน็ตโปรโตคอล” ในหน้า 87

___ IPv4

___ IPv6

___ IPv4 และ IPv6

เรียกเลขหมายจาก HMC แบบโลคัล

ป้อนข้อมูลเรียกเลขหมายเพื่อตั้งค่าโลคัลโมเด็มของคุณ ระบุหมายเลขโทรศัพท์ที่ใช้ในการต่อเลขหมายไปยังผู้ให้บริการ เมื่อคุณกำลังเชื่อมต่อ หมายเลขโทรศัพท์จะถูกต่อเลขหมายตามลำดับที่แสดงในรายการ

ตารางที่ 47. เรียกเลขหมายจาก HMC แบบโลคัล

ฟิลด์	
คำแนะนำสำหรับต่อเลขหมาย:	

ตารางที่ 47. เรียกเลขหมายจาก HMC แบบโลคัล (ต่อ)

ฟิลด์	
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 89

___ HMC นี้

___ HMC อื่น

หากคุณได้ตรวจสอบ HMC อื่น ให้แสดงรายการ HMC อื่นที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home ที่นี้:

ตารางที่ 48. HMC อื่นที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home

รายชื่อโฮสต์ HMC หรือ IP แอดเดรส ที่ถูกคอนฟิกเป็นเซิร์ฟเวอร์ Call-Home

คุณสมบัติเพิ่มเติมสำหรับการสนับสนุน

My Systems และ Premium Search

ฟิลด์	
แสดงรายการ IBM ID ของคุณ	
แสดงรายการ IBM ID ของคุณ	

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 เพื่อกำหนดเว็บฟังก์ชันเป็นส่วนบุคคลให้ป้อน IBM ID ที่คุณได้ลงทะเบียนไว้บนเว็บไซต์ IBM Registration ไปที่ <http://www.ibm.com/support/electronic> the valuable เพื่อดูข้อมูลการสนับสนุนที่มีประโยชน์ ซึ่งพร้อมใช้งานสำหรับลูกค้าที่ลงทะเบียน IBM ID ไว้กับระบบ

การกำหนดคอนฟิก HMC

กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก ความปลอดภัย เซอร์วิสแอปพลิเคชัน และความต้องการส่วนตัวบางอย่างของผู้ใช้

ขึ้นอยู่กับระดับของการปรับแต่งค่าเองที่คุณต้องการกำหนดให้กับคอนฟิกูเรชัน HMC ของคุณ คุณมีตัวเลือกหลายตัวเลือกสำหรับการตั้งค่า HMC เพื่อให้เหมาะสมกับความต้องการของคุณ ตัวช่วยสร้างการติดตั้งที่แนะนำ คือเครื่องมือใน HMC ซึ่งได้รับการออกแบบมาเพื่อช่วยให้การตั้งค่า HMC เป็นไปอย่างง่ายดาย คุณสามารถเลือกใช้วิธีลัดผ่านทางวิซาร์ดเพื่อสร้างสภาวะแวดล้อมของ HMC ตามที่แนะนำได้อย่างรวดเร็ว หรือคุณสามารถเลือกที่จะสำรวจการกำหนดค่าทั้งหมดที่วิซาร์ดแนะนำ คุณยังสามารถดำเนินขั้นตอนกำหนดคอนฟิกโดยต้องใช้ความช่วยเหลือจากวิซาร์ด การกำหนดคอนฟิก HMC โดยใช้เมนู HMC

ก่อนที่จะเริ่มต้น ให้รวบรวมข้อมูลการตั้งค่าที่ต้องการ ซึ่งคุณจำเป็นต้องปฏิบัติตามขั้นตอนต่างๆ ให้เสร็จสิ้นอย่างสมบูรณ์ โปรดดูที่ “การเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90 สำหรับรายการของข้อมูลที่ต้องการ เมื่อคุณเตรียมการเสร็จสิ้น ตรวจสอบให้แน่ใจว่าคุณเสร็จสิ้น “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91 และกลับไปสู่ส่วนนี้

การกำหนดคอนฟิก HMC โดยใช้พารามิเตอร์ผ่านทางวิซาร์ดเซตอัพที่แนะนำ

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 ตรวจสอบให้แน่ใจว่าระบบที่ถูกจัดการ ไม่ได้เชื่อมต่อกับแหล่งกำเนิดไฟฟ้า สำหรับ HMC ที่ติดตั้งในชั้นวาง หมายความว่าเฉพาะอุปกรณ์ที่เสียบกับบัลลูนกระจายกำลังไฟฟ้า (PDB) ก่อนที่คุณ จะเสียบแหล่งจ่ายไฟหลัก คือ HMC ถ้านี้เป็น HMC เครื่องที่สองที่เชื่อมต่อกับระบบที่ถูกจัดการระบบเดียวกัน ก็จะสามารถเชื่อมต่อกับระบบที่ถูกจัดการเข้ากับแหล่งกำเนิดไฟฟ้า

1. เปิด HMC โดยกดปุ่มเปิด/ปิด.
2. โปรดรอให้ HMC เลือกภาษาดีฟอลต์และค่าติดตั้งโลแคล ประมาณ 30 วินาที
3. ยอมรับข้อตกลงไลเซนส์ของ คอนโซลการจัดการฮาร์ดแวร์ หากคุณไม่ยอมรับข้อตกลงไลเซนส์ของ คอนโซลการจัดการฮาร์ดแวร์ คุณก็จะไม่สามารถกำหนดคอนฟิกของ HMC ให้เสร็จสิ้นได้
4. คลิก ล็อกคอนและเรียกใช้เว็บแอปพลิเคชัน **Hardware Management Console**
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: หาก ตัวช่วยสร้างการติดตั้งที่แนะนำ ไม่ปรากฏขึ้นเมื่อคุณเริ่มต้น HMC ให้คลิก **Guided Setup Wizard** ในพื้นที่การนำทางของเพจต้อนรับเข้าสู่ HMC

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

ตรวจทานคอนฟิกเรชั่นของคุณ:

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

การกำหนดคอนฟิก HMC โดยใช้เมนู HMC

ส่วนนี้มีรายการที่ครบถ้วนของงานคอนฟิกเรชั่น HMC ทั้งหมด ซึ่งช่วยแนะแนวทางตลอดกระบวนการกำหนดคอนฟิก HMC ของคุณ เลือก อีพชั่นนี้ถ้าคุณไม่ต้องการใช้ ตัวช่วยสร้างการติดตั้งที่แนะนำ

คุณต้องรีสตาร์ท HMC เพื่อให้ค่าติดตั้งคอนฟิกเรชั่นมีผลใช้งาน ดังนั้น คุณอาจต้องการพิมพ์รายการตรวจสอบนี้ และเก็บไว้กับคุณเมื่อทำการกำหนดคอนฟิก HMC

ข้อมูลนี้ประกอบด้วยภาษาอังกฤษถึงงานที่ไม่รวมอยู่ใน PDF นี้ คุณสามารถเข้าถึงสื่อประกอบเพิ่มเติม ที่สนับสนุนได้โดยอ้างอิงถึง ส่วนของ **Additional Resources** บนหน้า HMC Welcome

สิ่งที่ต้องการก่อน

ก่อนที่คุณจะเริ่มกำหนดคอนฟิก HMC โดยใช้เมนู HMC ตรวจสอบให้แน่ใจว่าได้ทำงานจัดเตรียมคอนฟิกูเรชัน ตามที่อธิบายใน “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90 แล้ว

ตารางที่ 50. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่สามารถหาข้อมูลที่เกี่ยวข้องได้

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. สตาร์ท HMC	“การเริ่มต้น HMC” ในหน้า 103
2. ตั้งค่าวันที่และเวลา	
3. เปลี่ยนรหัสผ่านที่กำหนดไว้ล่วงหน้า	
4. สร้างผู้ใช้เพิ่มเติม และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
5. กำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก	“การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104
6. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิด และ IP แอดเดรสแบบฟิกซ์ ตั้งข้อมูล identification	
7. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิดและ IP แอดเดรสแบบฟิกซ์ ให้ตั้งค่า entry การเร้าเป็นดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าเป็นดีฟอลต์เกตเวย์” ในหน้า 112
8. หากคุณกำลังใช้เน็ตเวิร์กแบบเปิด และ IP แอดเดรสแบบฟิกซ์ ให้ตั้งค่าบริการโดเมนเนม	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
9. หากคุณกำลังใช้ IP แอดเดรสแบบฟิกซ์ และมีการใช้งาน DNS ให้ตั้งค่าโดเมนซัพฟิกซ์	“การตั้งค่าคอนฟิกโดเมนซัพฟิกซ์” ในหน้า 112
10. กำหนดคอนฟิกเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการ และสนับสนุน IBM และส่งคืนรายการตรวจสอบนี้ เมื่อคุณได้ทำขั้นตอนนี้เสร็จสิ้นแล้ว	“การคอนฟิก HMC เพื่อให้สามารถติดต่อบริการและการสนับสนุนได้” ในหน้า 114
11. ตั้งค่าฐานข้อมูล Events สำหรับการจัดทำเวอร์ชัน	“การกำหนดคอนฟิก Events Manager for Call Home” ในหน้า 120
12. เชื่อมต่อระบบที่ถูกจัดการเข้ากับแหล่งจ่ายไฟ	
13. ตั้งค่ารหัสผ่านให้กับระบบที่ถูกจัดการ และรหัสผ่านของ ASMI แต่ละรายการ (general และ admin)	“การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ” ในหน้า 121
14. เข้าใช้ ASMI เพื่อตั้งวันที่และเวลาบนระบบที่ถูกจัดการ	
15. สตาร์ทระบบที่ถูกจัดการ และกลับไปสู่รายการตรวจสอบนี้เมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	
16. ตรวจสอบว่า คุณมีหนึ่งโลจิสติกส์พาร์ติชันบนระบบที่ถูกจัดการ	
17. ทางเลือก: เพิ่มระบบที่ถูกจัดการอีก และกลับไปสู่รายการตรวจสอบเมื่อคุณดำเนินการขั้นตอนนี้เสร็จสิ้น	

ตารางที่ 50. งานคอนฟิกูเรชัน HMC ด้วยตนเอง และที่สามารถหาข้อมูลที่เกี่ยวข้องได้ (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
18. ทางเลือก: หากคุณกำลังติดตั้งเซิร์ฟเวอร์ใหม่ด้วย HMC ของคุณ ให้ตั้งค่าโลจิสติกส์พาร์ติชันและติดตั้งระบบปฏิบัติการ	
19. หากคุณไม่ได้กำลังติดตั้งเซิร์ฟเวอร์ใหม่ในเวลานี้ให้ทำงาน postconfiguration ซึ่งเลือกดำเนินการได้ เพื่อปรับค่าคอนฟิกูเรชันของคุณต่อไปอีก	“ขั้นตอน Postconfiguration” ในหน้า 122

การเริ่มต้น HMC:

คุณสามารถล็อกอินเข้าสู่ Hardware Management Console (HMC) และเลือกภาษาที่คุณต้องการแสดง ในอินเทอร์เน็ตเฟส ใช้ UserID hscroot ที่เป็นค่าดีฟอลต์และรหัสผ่าน abc123 เพื่อล็อกอินเข้าสู่ HMC ในครั้งแรก

เมื่อต้องการเริ่มต้น HMC ให้ทำตามขั้นตอนต่อไปนี้:

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

หมายเหตุ: ข้อความแจ้งเตือนนี้จะปรากฏอยู่เป็นเวลา 30 นาที่หาก你不ดำเนินการใดๆ

3. เลือกโลแคลที่คุณต้องการแสดงจากรายการ ในหน้าต่าง การเลือกโลแคล และคลิก ตกลง โลแคลจะระบุภาษาที่อินเทอร์เน็ตเฟส HMC ใช้
4. ล็อกอินเข้าสู่ HMC โดยใช้ ID ผู้ใช้และรหัสผ่านดีฟอลต์ต่อไปนี้:

ชื่อผู้ใช้: hscroot

รหัสผ่าน: abc123

บนเพจล็อกอิน คุณสามารถดูสถานะของระบบ พาร์ติชัน และเซิร์ฟเวอร์ I/O แบบเสมือน คุณยังสามารถดูจำนวนของ Attention LEDs และเหตุการณ์ที่สามารถให้บริการได้ คุณสามารถศึกษาเพิ่มเติมเกี่ยวกับ HMC และคุณลักษณะที่พร้อมใช้งานได้โดยคลิกสื่อบันทึกทางสังคมและลิงก์ IBM developerWorks® จากเพจล็อกอิน

หมายเหตุ: บน HMC เวอร์ชัน 8.6.0.1 คุณสามารถเลือกได้จากอ็อปชันล็อกอินต่อไปนี้:

ล็อกอิน: HMC Classic หรือ HMC Enhanced+

เลือกอินเทอร์เน็ตเฟส HMC Enhanced+ เพื่อดำเนินการต่อ อินเทอร์เน็ตเฟส HMC Classic จัดเตรียมการเข้าถึงฟังก์ชันเดิมทั้งหมดของ HMC และอินเทอร์เน็ตเฟส HMC Enhanced+ จัดเตรียมมุมมองเชิงกราฟิกของระบบ พาร์ติชัน และเซิร์ฟเวอร์ I/O แบบเสมือน และการนำทางแบบเรียบง่าย

HMC Classic

แสดง GUI มาตรฐานซึ่งไม่มีคุณลักษณะ PowerVM ที่ปรับปรุง

HMC Enhanced+

แสดงมุมมองใหม่ของอินเทอร์เฟซการจัดการ HMC ที่ออกแบบใหม่ทั้งหมดซึ่งจัดเตรียมสภาวะแวดล้อม การทำงานอินเทอร์เฟซที่ใช้งานง่ายด้วยมุมมองเชิงกราฟิกของระบบ พาร์ติชัน และเซิร์ฟเวอร์ I/O แบบเสมือน และการนำทางแบบเรียบง่าย

หมายเหตุ: เมื่อ HMC ทำงานเป็นเซิร์ฟเวอร์ DHCP, HMC จะใช้รหัสผ่านดีฟอลต์ เมื่อเชื่อมต่อกับตัวประมวลผลเซิร์ฟเวอร์ในครั้งแรก

5. คลิก ลงชื่อเข้าใช้

การเปลี่ยนวันที่และเวลา:

นาฬิกาแบบใช้แบตเตอรี่จะบันทึกวันที่และเวลาไว้สำหรับ HMC คุณอาจต้องรีเซ็ตวันที่และเวลาของคอนโซลหากเปลี่ยนแบตเตอรี่หรือย้ายระบบของคุณไปยังเขตเวลาที่แตกต่าง ศึกษาเกี่ยวกับวิธีการเปลี่ยนวันที่และเวลาสำหรับ HMC

หากคุณเปลี่ยนข้อมูลของวันที่ และเวลา, การเปลี่ยนแปลงนั้นจะไม่ส่งผลกระทบต่อระบบ และโลจิคัลพาร์ติชันที่ HMC จัดการอยู่

เมื่อต้องการเปลี่ยน วันที่และเวลาสำหรับ HMC ให้ดำเนินการ ตามขั้นตอนต่อไปนี้:

1. ตรวจสอบให้แน่ใจว่าคุณมีหนึ่งในบทบาทต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ตัวแทนบริการ
- ผู้ควบคุมเครื่อง
- ผู้ดูแล

2. ในพื้นที่การนำทางให้คลิกไอคอน HMC Management จากนั้นเลือก ค่าติดตั้งคอนโซล

3. ในหน้าต่างย่อยเนื้อหาให้คลิก เปลี่ยน วันที่และเวลา

4. ถ้าคุณเลือก UTC ในฟิลด์ Clock การตั้งค่าเวลาจะมีการปรับโดยอัตโนมัติ เมื่อมีการเลื่อนเวลาใน เขตเวลาที่คุณเลือกไว้ ใส่วันที่ เวลา และเขตเวลา แล้วคลิก OK

การตั้งค่าชนิดเน็ตเวิร์ก HMC:

ตั้งค่า HMC ของคุณ เพื่อให้สามารถสื่อสารกับระบบที่ถูกจัดการ โลจิคัลพาร์ติชัน ผู้ใช้ระยะไกล และบริการและการสนับสนุนได้

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ:

ตั้งค่า HMC เพื่อให้สามารถเชื่อมต่อกับและจัดการระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับระบบที่ถูกจัดการได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 51. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ ขอแนะนำให้ใช้ eth0	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุอ็อบเจกต์เน็ตเวิร์กให้กับ HMC ของคุณ	“การระบุอ็อบเจกต์เน็ตเวิร์กที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิกอ็อบเจกต์เน็ตเวิร์กต่อแต่ละเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อตบนทีก	“การตั้งค่าความเร็วของสล็อตบนทีก” ในหน้า 109
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109
c. ตั้งค่าสแตตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 110
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 111
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเราต์เป็นดีฟอลต์เกตเวย์” ในหน้า 112
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 122

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ:

กำหนดคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับ และจัดการระบบที่ถูกจัดการ ได้โดยใช้เน็ตเวิร์กส่วนตัว

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อ กับระบบที่ถูกจัดการโดยใช้เน็ตเวิร์กส่วนตัวให้ทำต่อไปนี้:

ตารางที่ 52. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กส่วนตัวที่จะเชื่อมต่อกับระบบที่ถูกจัดการ

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุอ็อบเจกต์เน็ตเวิร์กให้กับ HMC ของคุณ	“การระบุอ็อบเจกต์เน็ตเวิร์กที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP	“การตั้งค่าคอนฟิก HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 109
4. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 122

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน:

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ โลจิคัลพาร์ติชันได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 53. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับโลจิคัลพาร์ติชัน

งาน	ที่ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุอ็อบเจกต์เน็ตเวิร์กให้กับ HMC ของคุณ	“การระบุอ็อบเจกต์เน็ตเวิร์กที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิกอ็อบเจกต์เน็ตเวิร์กต่อแต่ละเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อตบนทีก	“การตั้งค่าความเร็วของสล็อตบนทีก” ในหน้า 109
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109
c. ตั้งค่าสแตตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 110
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 111
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าต์เป็นดีฟอลต์เกตเวย์” ในหน้า 112
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	
5. ทดสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์ที่ถูกจัดการและ HMC	“การทดสอบการเชื่อมต่อจาก HMC ไปยังระบบที่ถูกจัดการ” ในหน้า 122

การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล:

เมื่อต้องการกำหนดคอนฟิกค่าติดตั้งเน็ตเวิร์ก HMC เพื่อให้สามารถเชื่อมต่อกับ ผู้ใช้ระยะไกลได้โดยใช้เน็ตเวิร์กแบบเปิดให้ทำต่อไปนี้:

ตารางที่ 54. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล

งาน	ที่ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. กำหนดอินเตอร์เฟซที่คุณต้องการใช้กับระบบที่ถูกจัดการของคุณ	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. ระบุอ็อบเจกต์เน็ตเวิร์กให้กับ HMC ของคุณ	“การระบุอ็อบเจกต์เน็ตเวิร์กที่จะถูกกำหนดเป็น eth0” ในหน้า 107
3. กำหนดคอนฟิกอ็อบเจกต์เน็ตเวิร์กต่อแต่ละเตอร์โดยการทำงานต่อไปนี้:	
a. ตั้งความเร็วสล็อตบนทีก	“การตั้งค่าความเร็วของสล็อตบนทีก” ในหน้า 109
b. เลือกชนิดเน็ตเวิร์กแบบเปิด	“การเลือกเน็ตเวิร์กส่วนบุคคลหรือ เน็ตเวิร์กแบบเปิด” ในหน้า 109
c. ตั้งค่าสแตตติกแอตเดรส	“การตั้งค่า IPv4 address” ในหน้า 110
d. ตั้งไฟร์วอลล์	“การเปลี่ยนการตั้งค่าไฟร์วอลล์ HMC” ในหน้า 111
e. ตั้งค่าดีฟอลต์เกตเวย์	“การกำหนดคอนฟิก entry การเร้าต์เป็นดีฟอลต์เกตเวย์” ในหน้า 112
f. ตั้งค่า DNS	“การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส” ในหน้า 112

ตารางที่ 54. การกำหนดคอนฟิก ค่าติดตั้ง HMC เพื่อใช้เน็ตเวิร์กแบบเปิดที่จะเชื่อมต่อกับผู้ใช้ระยะไกล (ต่อ)

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
g. ตั้งค่าซีฟิกส์	“การตั้งค่าคอนฟิกโดเมนซีฟิกส์” ในหน้า 112
4. ตั้งค่าอะแดปเตอร์เพิ่มเติม หากมี	

การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC:

เมื่อต้องการคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC เพื่อให้สามารถ รายงานปัญหาได้ ให้ปฏิบัติตามต่อไปนี้:

ตารางที่ 55. การคอนฟิกค่าติดตั้งเซิร์ฟเวอร์ Call-Home ของ HMC

งาน	ที่สามารถหาข้อมูลที่เกี่ยวข้องได้
1. ตรวจสอบให้แน่ใจว่าคุณมีข้อมูลลูกค้าที่จำเป็นทั้งหมด	“เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91
2. กำหนดคอนฟิก HMC นี้เพื่อรายงานข้อผิดพลาด หรือเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่เพื่อรายงานความผิดพลาด	“การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน” ในหน้า 115 “การเลือกเซิร์ฟเวอร์ Call-Home ที่มีอยู่แล้วเพื่อเชื่อมต่อไปยังบริการและการสนับสนุนสำหรับ HMC นี้” ในหน้า 118
3. ตรวจสอบว่าคอนฟิกูเรชัน Call-Home ของคุณใช้งานได้	“การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่” ในหน้า 119
4. ให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม	“การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” ในหน้า 119
5. จัดกำหนดการการส่งข้อมูลของข้อมูลระบบ	“ข้อมูลการบริการส่งข้อมูล” ในหน้า 119

การระบุไอพีแอดเดรสที่ระบุไว้จะถูกระบุเป็น eth0:

การเชื่อมต่อไอพีแอดเดรสกับเซิร์ฟเวอร์ที่จัดการต้องกระทำโดยใช้ไอพีแอดเดรสที่กำหนดเป็น eth0 บน HMC ของคุณ

หากคุณยังไม่ได้ติดตั้งไอพีแอดเดรสบนการ์ดเครือข่าย PCI บน HMC ของคุณ ไอพีแอดเดรสหลักภายในจะถูกกำหนดเป็น eth0 หรือ eth1 บน HMC ของคุณทุกครั้ง หากต้องการใช้ HMC เป็นเซิร์ฟเวอร์ DHCP สำหรับระบบที่ถูกจัดการ

หากคุณติดตั้งไอพีแอดเดรสบนการ์ดเครือข่าย PCI พอร์ตที่กำหนดเป็น eth0 จะขึ้นกับตำแหน่งและประเภทของไอพีแอดเดรสบนการ์ดเครือข่ายที่คุณติดตั้ง

หมายเหตุ: กฎเหล่านี้เป็นกฎทั่วไป และอาจไม่มีผลกับ configuration ทั้งหมด

ตารางต่อไปนี้จะแสดงกฎของการติดตั้งไอพีแอดเดรสตามประเภท HMC

ตารางที่ 56. 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: - หากมีอีเทอร์เน็ตอะแดปเตอร์เดี่ยวติดตั้งไว้ อะแดปเตอร์นั้นจะถูกกำหนดเป็น eth0 - หากอีเทอร์เน็ตอะแดปเตอร์เป็นอีเทอร์เน็ตอะแดปเตอร์พอร์ตคู่ พอร์ตที่ติดเลเบล Act/link A จะเป็น eth0 พอร์ตที่ติดเลเบล Act/link B จะเป็น eth1 ในกรณีนี้ อีเทอร์เน็ตพอร์ตภายในหลักจะถูกกำหนดเป็น eth2 - หากไม่มีอะแดปเตอร์ติดตั้งอยู่ อีเทอร์เน็ตพอร์ตภายในจะถูกกำหนดเป็น eth0 - หากมีอีเทอร์เน็ตอะแดปเตอร์ติดตั้งอยู่หลายตัว โปรดดูที่ “การพิจารณาชื่ออินเตอร์เฟซของอีเทอร์เน็ตอะแดปเตอร์” ในหน้า 108

การพิจารณาชื่ออินเตอร์เฟซของอีเทอร์เน็ตอะแดปเตอร์:

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

เมื่อต้องการพิจารณาชื่อที่ HMC กำหนดให้กับอีเทอร์เน็ตอะแดปเตอร์ ให้ปฏิบัติตามนี้:

1. เปิดเชลล์เทอร์มินัลที่จำกัด เลือก **HMC Management > Open Restricted Shell Terminal**
2. พิมพ์ข้อความต่อไปนี้ที่บรรทัดรับคำสั่ง: `tail -f /var/log/messages` ไฟล์ล็อกข้อความจะเลื่อนไปเมื่อมีเหตุการณ์ใหม่เกิดขึ้น
3. ต่อสายเคเบิลอีเทอร์เน็ตของคุณ ถ้ามีการต่อสายเคเบิลนั้นแล้ว ให้ถอดออก รอประมาณ 5 วินาที แล้วต่อสายอีกครั้ง เชลล์ที่จำกัดจะเลื่อนไปเพื่อแสดงข้อความเมื่อคุณต่อสายเคเบิล entry ตัวอย่างต่อไปนี้แสดงว่าอีเทอร์เน็ตพอร์ตนี้ถูกระบุเป็น 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 ถ้าอะแดปเตอร์นี้ถูกเชื่อมต่อ กับสวิตช์ LAN คุณต้องจับคู่ค่าติดตั้งพอร์ตของสวิตช์ เมื่อต้องการตั้งค่า ความเร็วสื่อบันทึกและดูเฟล็กซ์ให้ดำเนินการตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน HMC Management จากนั้นเลือก ค่าติดตั้งคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก เปลี่ยนค่าติดตั้งเครือข่าย
3. คลิกแท็บ LAN Adapters
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้ทำงาน 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 และยังคงครอบคลุมถึงอุปกรณ์เน็ตเวิร์กย่อย และเน็ตเวิร์ก

เมื่อต้องการเลือกเน็ตเวิร์กส่วนบุคคลหรือพับลิคเน็ตเวิร์ก ให้ปฏิบัติตามนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน HMC Management จากนั้นเลือก ค่าติดตั้งคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก เปลี่ยนค่าติดตั้งเครือข่าย
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. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหาคลิก **เปลี่ยนค่าติดตั้งเครือข่าย** 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 อีพซันในการเลือก 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 109

สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “HMC เป็นเซิร์ฟเวอร์ DHCP” ในหน้า 82

กำหนดค่าการเชื่อมต่อ BMC:

คุณสามารถกำหนดค่าหรือดูค่าติดตั้งเครือข่ายบน BMC สำหรับคอนโซลการจัดการ

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

เมื่อต้องการกำหนดค่าการเชื่อมต่อ BMC ให้ทำตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหาคลิก **เปลี่ยนค่าติดตั้งเครือข่าย BMC/IPMI**
3. เลือกโหมดการเชื่อมต่อ (DHCP หรือ Static)
หาก คุณเลือกโหมด Static ให้ระบุแอดเดรสต่อไปนี้:
 - IP แอดเดรส
 - Subnet mask
 - Gateway
4. คลิกตกลง

คุณยังสามารถกำหนดค่าการเชื่อมต่อเครือข่าย BMC ได้โดยใช้อินเทอร์เฟซ Petitboot bootloader สำหรับข้อมูลเพิ่มเติม โปรดดู การกำหนดค่า IP แอดเดรสเฟิร์มแวร์

การตั้งค่า IPv4 address:

ศึกษาถึงวิธีการตั้งค่า IPv4 address ของคุณบน HMC



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหาคลิก **เปลี่ยนค่าติดตั้งเครือข่าย**
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:

ศึกษาวิธีเซตอัป IPv6 address on the HMC.



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหาคลิก **เปลี่ยนค่าติดตั้งเครือข่าย**
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. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหาคลิก **เปลี่ยนค่าติดตั้งเครือข่าย**
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:

ในเน็ตเวิร์กแบบเปิดไฟร์วอลล์จะถูกใช้เพื่อควบคุมการเข้าสู่เน็ตเวิร์กภายในบริษัทจากภายนอก HMC ก็มีไฟร์วอลล์ในอะแดปเตอร์อีเทอร์เน็ตแต่ละตัว เมื่อต้องการควบคุม HMC จากระยะไกล หรือให้รีโมตแอ็กเซสแก่บุคคลอื่น แกะไขการตั้งค่าคอนฟิกไฟร์วอลล์ของอีเทอร์เน็ตอะแดปเตอร์บน HMC ซึ่งเชื่อมต่อกับเน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิกไฟร์วอลล์, ให้ใช้ขั้นตอนต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management**  จากนั้นเลือก ค่าติดตั้งคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก เปลี่ยนค่าติดตั้งเครือข่าย
3. คลิกแท็บ LAN Adapters
4. เลือกอะแดปเตอร์ LAN ที่คุณต้องการใช้งาน และคลิก Details
5. คลิกแท็บ Firewall
6. โดยการใช้วิธีใดวิธีหนึ่งต่อไปนี้ คุณสามารถอนุญาตให้ IP แอดเดรสใดๆ ใช้แอปพลิเคชันเฉพาะผ่านไฟร์วอลล์หรือคุณสามารถระบุ IP แอดเดรสมากกว่าหนึ่งได้:
 - อนุญาตให้ IP แอดเดรสใดๆ ที่ใช้แอปพลิเคชันเฉพาะผ่านไฟร์วอลล์ได้:
 - a. จากช่องด้านบน, ให้เลือกแอปพลิเคชัน
 - b. คลิก **Allow Incoming** แอปพลิเคชันจะไปปรากฏอยู่ในช่องด้านล่างเพื่อแสดงว่าถูกเลือกแล้ว
 - ระบุ IP แอดเดรสเพื่ออนุญาตให้ผ่านไฟร์วอลล์ได้:
 - a. จากช่องด้านบน ให้เลือกแอปพลิเคชัน
 - 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:

คุณสามารถเปิดใช้การเข้าถึงเซลล์ที่จำกัดแบบรีโมตได้เมื่อตั้งค่าไฟร์วอลล์

เมื่อต้องการเปิดใช้งานการเข้าถึงเซลล์ที่จำกัดแบบรีโมตให้ทำดังนี้:

1. ใน พื้นที่การนำทางให้คลิก การจัดการ HMC
2. คลิก **Remote Command Execution**
3. เลือก เปิดใช้งานการเรียกใช้งานคำสั่งรีโมต โดยใช้ ssh จากนั้นคลิก **OK**

ถึงตอนนี้ การเข้าถึงเซลล์ที่จำกัดแบบรีโมตถูกเปิดใช้งานแล้ว

การเปิดใช้งาน การเข้าถึงเว็บแบบรีโมต:

คุณสามารถเปิดใช้งานการเข้าถึงเว็บแบบรีโมตด้วย HMC ของคุณ

เมื่อต้องการเปิดใช้งานการเข้าถึงเว็บแบบรีโมตให้ทำดังนี้:

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

ถึงตอนนี้ การเข้าถึงเว็บแบบรีโมตถูกเปิดใช้งานแล้ว

การกำหนดคอนฟิก entry การเรดต์เป็นดีฟอลต์เกตเวย์:

ศึกษาเกี่ยวกับวิธีการตั้งค่าการเรดต์ entry ตามดีฟอลต์เกตเวย์ งานนี้สามารถใช้ได้กับการตั้งค่าที่ใช้เน็ตเวิร์กแบบเปิด

เมื่อต้องการกำหนดคอนฟิก entry การเรดต์เป็นดีฟอลต์เกตเวย์ให้ปฏิบัติตามดังนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก ค่าติดตั้งคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก เปลี่ยนค่าติดตั้งเครือข่าย หน้าต่าง Customize Network Settings จะเปิด
3. คลิกแท็บ **Routing**
4. ในส่วนข้อมูลดีฟอลต์เกตเวย์ ป้อนเกตเวย์แอดเดรสและอุปกรณ์เกตเวย์ของ entry การเรดต์ที่คุณต้องการกำหนดเป็นดีฟอลต์เกตเวย์
5. คลิก **OK**.

การตั้งค่าคอนฟิกโดเมนเนมเซอร์วิส:

ถ้าคุณวางแผนที่จะติดตั้งเน็ตเวิร์กแบบเปิดให้ตั้งค่าโดเมนเนมเซอร์วิส

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



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก ค่าติดตั้งคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก เปลี่ยนค่าติดตั้งเครือข่าย หน้าต่าง Change Network Settings จะเปิด
3. คลิกแท็บ **Name Services**
4. เลือก เปิดใช้งาน DNS เพื่อเปิดใช้งาน DNS
5. ระบุเซิร์ฟเวอร์ DNS และโดเมนซัพพลิคันทา แล้วคลิก **Add**

6. คลิก OK.

การตั้งค่าคอนฟิกโดเมนซ์ฟิกส์:

รายการโดเมนซ์ฟิกส์ใช้สำหรับ resolve IP แอดเดรส โดยเริ่มจาก entry แรกที่พบในรายการ

โดเมนซ์ฟิกส์คือสตริงที่ต่อท้ายด้วยชื่อโฮสต์ซึ่งช่วยในการแปลงค่า IP แอดเดรสของรายการ ตัวอย่างเช่น ชื่อโฮสต์ของ myname อาจแปลงไม่ได้ อย่างไรก็ตาม หากสตริง myloc.mycompany.com เป็นสมาชิกของตารางโดเมนซ์ฟิกส์ เครื่องจะพยายามแปลง myname.mloc.mycompany.com ด้วยเช่นกัน

เมื่อต้องการ กำหนดคอนฟิกของรายการโดเมนซ์ฟิกส์ให้ใช้ขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทาง ให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **เปลี่ยนค่าติดตั้งเครือข่าย** หน้าต่าง **Customize Network Settings** จะเปิด
3. คลิกแท็บ **Name Services**
4. ป้อนสตริงที่จะใช้เป็น entry ของโดเมนซ์ฟิกส์
5. คลิก **Add** เพื่อเพิ่ม entry นั้นลงในรายการ

การคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP:

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

เมื่อผู้ใช้งานชื่อเข้าใช้ HMC ระบบจะดำเนินการพิสูจน์ตัวตนของไฟล์รหัสผ่านภายในก่อน หากไม่พบไฟล์รหัสผ่านภายใน HMC สามารถติดต่อเซิร์ฟเวอร์ LDAP ระยะไกลสำหรับการพิสูจน์ตัวตนได้ คุณต้องคอนฟิก HMC ของคุณเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย LDAP

หมายเหตุ: ก่อนที่คุณจะคอนฟิก HMC เพื่อให้ใช้การพิสูจน์ตัวตน LDAP คุณต้องตรวจสอบให้แน่ใจว่ามีการเชื่อมต่อเน็ตเวิร์กการทำงานระหว่าง HMC และเซิร์ฟเวอร์ LDAP สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดคอนฟิกการเชื่อมต่อเน็ตเวิร์ก HMC โปรดดูที่ “การตั้งค่าชนิดเน็ตเวิร์ก HMC” ในหน้า 104

เมื่อต้องการกำหนดค่า HMC เพื่อให้ใช้การพิสูจน์ตัวตน LDAP ให้ดำเนินการตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทาง ให้คลิกไอคอน **ผู้ใช้และการรักษาความปลอดภัย** จากนั้นเลือก **การรักษาความปลอดภัยของระบบและคอนโซล**
2. ในบานหน้าต่างเนื้อหา เลือก **จัดการ LDAP** หน้าต่าง **นิยามเซิร์ฟเวอร์ LDAP** แสดงขึ้น
3. เลือก **เปิดใช้งาน LDAP**
4. กำหนดเซิร์ฟเวอร์ LDAP ที่ต้องการใช้เพื่อพิสูจน์ตัวตน
5. กำหนดแอตทริบิวต์ LDAP ที่ใช้ในการระบุผู้ใช้ที่กำลังได้รับ การพิสูจน์ตัวตน ค่าดีฟอลต์คือ uid แต่คุณสามารถใช้แอตทริบิวต์ของคุณเองได้

6. กำหนดแผนผังชื่อจำเพาะ รู้จักกันในชื่อของฐานการค้นหา สำหรับเซิร์ฟเวอร์ 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 ระบบจะดำเนินการพิสูจน์ตัวตนของไฟล์รหัสผ่านภายในก่อน 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 104

เมื่อต้องการกำหนดคอนฟิก HMC เพื่อให้ใช้เซิร์ฟเวอร์ KDC สำหรับการพิสูจน์ตัวตนระยะไกล ด้วย Kerberos ปฏิบัติดังต่อไปนี้:

1. เปิดใช้งานเซอร์วิส Network Time Protocol (NTP) บน HMC และตั้งค่าเซิร์ฟเวอร์ HMC และ KDC ให้ซิงโครไนซ์โดยใช้เซิร์ฟเวอร์ NTP เดียวกัน เมื่อต้องการเปิดใช้งานเซอร์วิส NTP บน HMC ให้ปฏิบัติดังต่อไปนี้:
 - a. ในพื้นที่การนำทางให้คลิกไอคอน HMC Management  จากนั้นเลือก ค่าติดตั้งคอนโซล
 - b. ในบานหน้าต่างเนื้อหา เลือก เปลี่ยนวันที่ และเวลา
 - c. เลือกแท็บ คอนฟิกูเรชัน NTP
 - d. เลือก เปิดใช้งานเซอร์วิส NTP บน HMC นี้
 - e. คลิก OK.
2. คอนฟิกแต่ละโปรไฟล์ผู้ใช้ของ HMC ระยะไกลเพื่อให้ใช้การพิสูจน์ตัวตนระยะไกลด้วย Kerberos แทนที่จะใช้การพิสูจน์ตัวตนภายใน
3. ทางเลือก: คุณสามารถอิมพอร์ตไฟล์คีย์เซอร์วิสลงใน HMC นี้ได้ ไฟล์คีย์เซอร์วิสจะมีบัญชีโฮสต์ที่ระบุ HMC ให้แก่เซิร์ฟเวอร์ไฟล์คีย์เซอร์วิสรู้จักกันในชื่อของคีย์แท็บ เมื่อต้องการอิมพอร์ตไฟล์คีย์เซอร์วิสลงใน HMC นี้ ให้ปฏิบัติดังต่อไปนี้:

- a. ในพื้นที่การนำทางให้คลิกไอคอน ผู้ใช้และการรักษาความปลอดภัย  จากนั้นเลือก การรักษาความปลอดภัยของระบบและคอนโซล
- b. ในบานหน้าต่างเนื้อหา เลือก จัดการ KDC
- c. เลือก การดำเนินการ > อิมพอร์ตเซอร์วิสคีย์ หน้าต่าง อิมพอร์ตคีย์เซอร์วิส จะปรากฏขึ้น

- d. พิมพ์ตำแหน่งของไฟล์คีย์เซิร์ฟเวอร์
- e. คลิก OK.

4. เพิ่มเซิร์ฟเวอร์ KDC ใหม่ลงใน HMC นี้ เมื่อต้องการเพิ่มเซิร์ฟเวอร์ KDC ใหม่ลงใน HMC นี้ให้ปฏิบัติตามดังต่อไปนี้:



- a. ในพื้นที่การนำทางให้คลิกไอคอน ผู้ใช้และการรักษาความปลอดภัย จากนั้นเลือก การรักษาความปลอดภัยของระบบและคอนโซล
- b. ในบานหน้าต่างเนื้อหา เลือกจัดการ KDC
- c. เลือก การดำเนินการ > เพิ่มเซิร์ฟเวอร์ KDC หน้าต่าง อิมพอร์ตคีย์เซิร์ฟเวอร์จะปรากฏขึ้น
- d. พิมพ์ชื่อกลุ่มระบบเครือข่ายและชื่อโฮสต์ หรือ IP แอดเดรสของเซิร์ฟเวอร์ KDC
- e. คลิก OK.

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน:

คอนฟิก HMC นี้เพื่อให้สามารถติดต่อผู้ให้บริการเกี่ยวกับความผิดพลาดได้โดยใช้การเชื่อมต่อทาง LAN โพรคัพหรือโมเด็ม หรือ VPN

การคอนฟิก HMC เพื่อให้สามารถเชื่อมต่อกับฝ่ายบริการและสนับสนุนได้โดยใช้วิธีการติดตั้ง Call-Home:

คอนฟิก HMC เพื่อให้เป็นเซิร์ฟเวอร์ Call-Home โดยใช้วิธีการ Call-Home

โปรซีเดรนี้จะอธิบายวิธีตั้งค่า HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้การเชื่อมต่อกับอินเทอร์เน็ตโดยตรง (ทาง LAN) และ โดยอ้อม (SSL)

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- ถ้า คุณกำหนดคอนฟิกการสนับสนุนอินเทอร์เน็ตผ่านทางพรีอ็อกซีเซิร์ฟเวอร์ คุณยังต้องมีสิ่งต่อไปนี้ด้วย:
 - IP แอดเดรสและพอร์ตของพรีอ็อกซีเซิร์ฟเวอร์
 - ข้อมูลการพิสูจน์ตัวตนสำหรับพรีอ็อกซี
- มีการใช้อะแดปเตอร์ที่กำหนดเป็น eth1 (ซึ่งกำหนดเป็นเน็ตเวิร์กแบบเปิด) สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC” ในหน้า 80
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

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



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ

2. ในบานหน้าต่างเนื้อหาคลิก **วิศวกรรมการตั้งค่า Call-Home** วิศวกรสถานะการเชื่อมต่อและเซิร์ฟเวอร์ Call-Home จะเปิดขึ้น ทำตามคำสั่งในวิศวกรเพื่อกำหนดคอนฟิก call-home

การคอนฟิกคอนโซลภายในเพื่อรายงานปัญหาไปยังส่วนให้บริการและสนับสนุน:

คอนฟิก HMC นี้เพื่อให้สามารถติดต่อผู้ให้บริการเกี่ยวกับความผิดพลาดได้โดยใช้การเชื่อมต่อทาง LAN โทรศัพท์หรือโมเด็มหรือ VPN

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้านี

การคอนฟิก HMC เพื่อติดต่อบริการและสนับสนุนโดยใช้อินเทอร์เน็ต ทาง LAN และ SSL:

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

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้สำหรับ ข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว ตรวจสอบสิ่งนี้ โดยการไปที่อินเทอร์เน็ตเฟส HMC และคลิก **ความสามารถในการให้บริการ>การจัดการ เซอร์วิส > จัดการข้อมูลลูกค้า**
- ถ้าคุณกำหนดคอนฟิกการสนับสนุนอินเทอร์เน็ตผ่านทางพรีอ็อกซีเซิร์ฟเวอร์ คุณจะต้อง มีสิ่งต่างๆ ต่อไปนี้เช่นกัน:
 - IP แอดเดรสและพอร์ตของพรีอ็อกซีเซิร์ฟเวอร์
 - ข้อมูลการพิสูจน์ตัวตนสำหรับพรีอ็อกซี
- คุณจำเป็นต้องคอนฟิกอย่างน้อยหนึ่งเน็ตเวิร์กอินเทอร์เน็ตเฟสที่เปิดอยู่ สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “เน็ตเวิร์กส่วนตัวและเน็ตเวิร์กแบบเปิดในสภาวะแวดล้อม HMC” ในหน้า 82
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN

ในการตั้งค่า HMC เป็นเซิร์ฟเวอร์ Call Home โดยใช้อินเทอร์เน็ตทาง LAN และ SSL ให้ทำดังนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **ความสามารถในการให้บริการ** จากนั้นเลือก **การจัดการกับการให้บริการ**
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity** หน้าต่างคอนโซลเซิร์ฟเวอร์ Call-Home จะปรากฏขึ้น
3. คลิก **Configure**.
4. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออก ให้เลือก **เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ Call-Home**
5. ยอมรับข้อตกลง
6. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออก ให้เลือกเพจ **Internet**
7. ทำเครื่องหมายในกล่อง **Allow an existing internet connections for service**
8. ถ้าคุณกำลังใช้พรีอ็อกซี SSL ให้เลือก **Use SSL proxy**
9. ถ้าคุณใช้พรีอ็อกซี SSL ให้ใส่แอดเดรสและพอร์ตของพรีอ็อกซีขอรับข้อมูลนี้ได้จากผู้บริหารเน็ตเวิร์ก

10. ถ้าคุณเลือก Use SSL proxy และพรีอ็อกซีต้องใช้การพิสูจน์ตัวตนด้วย user ID และรหัสผ่าน ให้เลือก **Authenticate with the SSL proxy** พิมพ์ userid และรหัสผ่าน ขอรหัสผ่านได้จากผู้บริหรเน็ตเวิร์ก
11. เลือก โปรโตคอลของอินเทอร์เน็ต ที่คุณต้องการใช้
12. บนเพจอินเทอร์เน็ตให้คลิก ทดสอบ
13. ในหน้าต่าง Test Internet ให้คลิก Start
14. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์
15. ในหน้าต่าง Test Internet ให้คลิก Cancel
16. ในหน้าต่าง คำติตตั้งการเชื่อมต่อขาออกให้คลิก ตกลง

การเชื่อมต่อระบบให้บริการและสนับสนุนโดยใช้โทรศัพท์และโมเด็ม:

อธิบายวิธีการตั้งค่า HMC เป็นเซิร์ฟเวอร์ call-home โดยใช้โมเด็มเป็นตัวเข้าถึงระบบสนับสนุนของ IBM

หมายเหตุ: ชนิดการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

ก่อนที่จะเริ่มงานนี้ให้ตรวจสอบให้แน่ใจว่า:

- คุณมีสายโทรศัพท์นาฬิกาที่จัดเตรียมไว้โดยเฉพาะ
- คุณมีข้อมูลที่จำเป็นสำหรับการตั้งค่าโมเด็ม สำหรับ ข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว คุณอาจตรวจสอบได้โดย การไปที่อินเทอร์เน็ตเฟส HMC และคลิก ความสามารถในการให้บริการ>การจัดการ เซอร์วิส >จัดการข้อมูลลูกค้า
- ตรวจสอบว่าคุณมีข้อมูลต่อไปนี้:
 - ประเภทของสายนาฬิกา กล่าวคือ เป็น tone หรือ pulse สายส่วนใหญ่เป็นประเภท tone แต่บางสายยังคงเป็นประเภท rotary หรือ pulse แบบเดิม
 - เมื่อยกหูโทรศัพท์แล้ว สายโทรศัพท์มีเสียงสัญญาณหรือไม่ สายโทรศัพท์ส่วนใหญ่มีเสียง แต่บางสายอาจไม่มีเสียง
 - ต้องใช้หมายเลขนำหน้าสำหรับการหมุนโทรศัพท์หรือไม่ หมายเลขนำหน้า สำหรับการหมุนโทรศัพท์คือหมายเลขหรือชุดหมายเลขที่ช่วยให้โทรออกได้

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



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity**
3. คลิก กำหนดค่า
4. ในหน้าต่างคำติตตั้งการเชื่อมต่อขาออกให้เลือก เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ call-home
5. ยอมรับข้อตกลง

6. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออก ให้คลิกแท็บ **โลคัล โมเด็ม**
7. บนหน้าโลคัลโมเด็ม ให้เลือกเช็kb็อกซ์อนุญาตให้ใช้ การหมุนโลคัลโมเด็มสำหรับเซิร์ฟเวอร์
8. บนหน้าโลคัลโมเด็ม ให้เลือกเช็kb็อกซ์โมเด็มคอนฟิगरูเรชั่น
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. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์
18. ในหน้าต่าง Test Telephone Number ให้คลิก **Cancel**
19. คุณสามารถกำหนดคอนฟิกหมายเลขโทรศัพท์ได้ไม่เกินห้าหมายเลข กำหนดคอนฟิก หมายเลขโทรศัพท์อย่างน้อยสองหมายเลข (หลักและรอง) ระบบจะลองหมุนหมายเลขตามลำดับที่กำหนดคอนฟิกไว้ เมื่อต้องการเพิ่ม หมายเลขเพิ่มเติมลงในรายการที่สามารถโทรได้ ให้ทำซ้ำขั้นตอนต่างๆ ในกระบวนการนี้
20. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออก ให้คลิก **ตกลง**

การเชื่อมต่อระบบให้บริการและสนับสนุนโดยใช้ VPN บน LAN:

ตั้งค่าเซิร์ฟเวอร์ call-home โดยใช้ VPN

หมายเหตุ: ขั้นตอนการเชื่อมต่อแบบ Internet virtual private network (VPN) และการหมุนหมายเลข พร้อมใช้งานเฉพาะบน HMC เวอร์ชัน 8.2.0 หรือก่อนหน้า

ก่อนที่จะเริ่มงานนี้ ให้ตรวจสอบให้แน่ใจว่า:

- ผู้บริหารเน็ตเวิร์กได้ตรวจสอบว่าอนุญาตให้ทำการเชื่อมต่อได้ สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การจัดเตรียมสำหรับการตั้งค่าของ HMC” ในหน้า 90
- มีการใช้อะแดปเตอร์ที่กำหนดเป็น eth1 (ซึ่งกำหนดเป็นเน็ตเวิร์กแบบเปิด) สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การเลือกค่าติดตั้งเน็ตเวิร์กบน HMC” ในหน้า 80
- ในทางกายภาพ สายเคเบิลอีเทอร์เน็ตเชื่อมต่อ HMC เข้ากับ LAN
- ข้อมูลติดต่อของลูกค้าได้ถูกตั้งค่าแล้ว ตรวจสอบสถานการณ์นี้โดยการคลิก **ความสามารถในการให้บริการ > การจัดการเซิร์ฟเวอร์ > จัดการข้อมูลลูกค้า บนอินเทอร์เน็ตเฟส HMC**

เมื่อต้องการกำหนดคอนฟิกเซิร์ฟเวอร์ call-home โดยใช้ VPN ให้ทำตามต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในส่วน Connectivity ให้คลิก **Manage Outbound Connectivity**
3. คลิก กำหนดค่า
4. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้เลือก เปิดใช้งาน ระบบโลคัลเป็นเซิร์ฟเวอร์ call-home
5. ยอมรับข้อตกลง
6. ในหน้าต่างค่าติดตั้งการเชื่อมต่อขาออกให้คลิกแท็บ **Internet VPN**
7. บนหน้า อินเทอร์เน็ต VPN คลิก อนุญาตให้ใช้ VPN และการเชื่อมต่ออินเทอร์เน็ตที่มีอยู่สำหรับเซิร์ฟเวอร์
8. บนหน้าอินเทอร์เน็ต VPN เลือกเช็kb็อกซ์ทดสอบ
9. ในหน้าต่าง Test Internet VPN ให้คลิก **Start**
10. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์
11. ในหน้าต่าง Test Internet VPN ให้คลิก **Cancel**
12. ในหน้าต่าง ค่าติดตั้งการเชื่อมต่อขาออกให้คลิก ตกลง

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 นี้รายงานข้อผิดพลาดให้ปฏิบัติดังต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในบานหน้าต่างเนื้อหา คลิกจัดการการเชื่อมต่อขาออก หน้าต่างคอนโซลเซิร์ฟเวอร์ Call-Home จะปรากฏขึ้น
3. คลิก ใช้คอนโซลเซิร์ฟเวอร์ call-home ที่พบ HMC จะแสดง IP แอดเดรสหรือชื่อโฮสต์ของ HMC ที่คอนฟิกสำหรับ Call-Home
4. คลิก OK.

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

การตรวจสอบว่าการเชื่อมต่อของคุณไปยังฝ่ายบริการและสนับสนุนนั้นทำงานอยู่:

ทดสอบการรายงานปัญหาเพื่อตรวจสอบให้แน่ใจว่า การเชื่อมต่อไปยังส่วนบริการ และสนับสนุนกำลังทำงานอยู่

เมื่อต้องการตรวจสอบว่าคอนฟิกูเรชัน call-home ทำงานอยู่ให้ทำดังนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในบานหน้าต่างเนื้อหา คลิก สร้างเหตุการณ์
3. เลือก ทดสอบการรายงานปัญหาโดยอัตโนมัติ และ พิมพ์ข้อคิดเห็น
4. คลิก **Request Service** รอ 2-3 นาที เพื่อให้คำร้องขอถูกส่ง
5. ในหน้าต่าง Service Management ให้เลือก **Manage Events**
6. เลือก **All open problems**
7. ตรวจสอบว่ามีกำหนดเหตุการณ์ PMH และหมายเลขให้กับหมายเลขปัญหา ที่คุณเปิด
8. เลือกเหตุการณ์ดังกล่าว และคลิก **ปิด**
9. บนหน้าต่าง ปิด ให้พิมพ์ชื่อของคุณและความคิดเห็นสั้นๆ

การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม:

คุณต้องให้สิทธิ์แก่ผู้ใช้ในการดูข้อมูลเกี่ยวกับระบบของคุณ

ก่อนที่จะให้สิทธิ์ผู้ใช้เพื่อดูข้อมูลระบบที่เก็บรวบรวมมา คุณต้องขอรับ IBM ID ก่อน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการขอรับ IBM ID โปรดดูที่ “เวิร์กช็อปเตรียมการติดตั้งและการคอนฟิกสำหรับ HMC” ในหน้า 91

เมื่อต้องการให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวมให้ปฏิบัติดังต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในบานหน้าต่างเนื้อหา เลือก ให้สิทธิ์ผู้ใช้
3. ป้อน IBM ID ของคุณ
4. คลิก **OK**.

ข้อมูลการบริการส่งข้อมูล:

คุณสามารถส่งข้อมูลไปยังผู้ให้บริการของคุณได้ในทันที หรือคุณสามารถจัดกำหนดการให้ส่งข้อมูลเป็นประจำได้

IBM จัดเตรียมฟังก์ชันสำหรับเว็บไซต์ที่ทำให้เป็นส่วนตัว ซึ่งใช้ข้อมูลที่เก็บรวบรวมโดย IBM Electronic Service Agent เพื่อใช้ฟังก์ชันเหล่านี้ คุณต้องลงทะเบียนบนเว็บไซต์ IBM Registration ก่อนที่ <http://www.ibm.com/account/profile> เมื่อต้องการอนุญาตให้ผู้ใช้ใช้ข้อมูล Electronic Service Agent เพื่อทำฟังก์ชันสำหรับเว็บไซต์ให้เป็นส่วนตัว โปรดดูที่ “การให้สิทธิ์ผู้ใช้ในการดูข้อมูลระบบที่เก็บรวบรวม” ในหน้า 119 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ข้อดีของการลงทะเบียน IBM ID กับระบบของคุณ โปรดดูที่ <http://www.ibm.com/support/electronic>

หมายเหตุ: คุณควรส่งผ่านข้อมูลผู้ให้บริการหลังจากที่ได้ติดตั้งและกำหนดคอนฟิก HMC เพื่อใช้งาน

หากต้องการส่งข้อมูลการบริการให้ทำดังนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในบานหน้าต่างเนื้อหา คลิก ข้อมูล เซอร์วิสการส่งข้อมูล
3. ดำเนินงานให้เสร็จสมบูรณ์ในหน้าต่างรายละเอียดเซอร์วิสการกระจายสัญญาณ แล้วคลิก OK.

กำหนดตารางเวลาข้อมูลเซอร์วิส:

กำหนดตารางเวลาเมื่อต้องการส่งข้อมูลเซอร์วิสเพื่อใช้ในการกำหนดปัญหา

หมายเหตุ: คุณควรส่งข้อมูลผู้ให้บริการเมื่อใดก็ตามที่ติดตั้ง Hardware Management Console (HMC) และกำหนดคอนฟิกเพื่อใช้งานแล้ว

เมื่อต้องการกำหนดตารางเวลาข้อมูลเซอร์วิสให้ทำตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก การจัดการกับการให้บริการ
2. ในบานหน้าต่างเนื้อหาให้คลิก กำหนดตารางเวลาข้อมูลเซอร์วิส
3. ในบานหน้าต่างเนื้อหาให้คลิกแท็บ กำหนดตารางเวลาและส่งข้อมูล เพื่อกำหนดตารางเวลาข้อมูลเซอร์วิส

หมายเหตุ: คุณยังสามารถคลิก แท็บต่อไปนี้เพื่อเลือกข้อมูลที่คุณต้องการส่ง และเพื่อกำหนดคอนฟิกการเชื่อมต่อ FTP:

- กำหนดตารางเวลาและส่งข้อมูล: ส่งข้อมูลไปยังผู้ให้บริการของคุณในทันทีหรือกำหนดตารางเวลาการส่ง
 - ส่งรายงานปัญหา: เลือกข้อมูลที่คุณต้องการ และปลายทางของข้อมูล
 - กำหนดคอนฟิกการเชื่อมต่อ FTP: จัดเตรียมข้อมูลคอนฟิกูเรชัน เพ่อนุญาตให้ใช้ FTP เพื่อปิดการไหลข้อมูลเซอร์วิส
4. เลือกชนิดของข้อมูลเซอร์วิสที่คุณต้องการเปิดใช้งานการส่งแบบประจำ หรือส่งโดยทันที
 - ข้อมูลการทดสอบการดำเนินการ (ฮาร์ทบีท) -- เปิดใช้งานเสมอ: ส่งไฟล์บันทึกการทำงานของเหตุการณ์ของปัญหา
 - ข้อมูลเซอร์วิสของฮาร์ดแวร์ (VPD): ส่ง Vital Product Data (VPD) สำหรับระบบที่ถูกจัดการทั้งหมดที่พ่วงต่อกับ HMC นี้
 - ข้อมูลเซอร์วิสของซอฟต์แวร์: ส่ง VPD สำหรับซอฟต์แวร์ทั้งหมดที่รันอยู่บนพาร์ติชัน
 - ข้อมูลการจัดการกับประสิทธิภาพการทำงาน: รวบรวมและส่งข้อมูลการจัดการกับประสิทธิภาพการทำงาน
 - อัปเดตข้อมูลแอ็คเซสคีย์: ตรวจสอบความถูกต้องและอัปเดตข้อมูลแอ็คเซสคีย์
 5. เลือกช่วงเวลา (ในหน่วยวัน) และเวลาเพื่อกำหนดตารางเวลาการส่ง แบบซ้ำๆ เมื่อต้องการส่งข้อมูลในทันทีให้คลิก ส่งเดี๋ยวนี้
 6. คลิกตกลง

ใช้วิธีใช้แบบออนไลน์สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดตารางเวลา ข้อมูลเซอร์วิส

การกำหนดคอนฟิก Events Manager for Call Home:

เรียนรู้วิธีการกำหนดคอนฟิกภารกิจ Events Manager for Call Home คุณสามารถมอนิเตอร์และอนุมัติข้อมูลใดๆที่กำลังส่งผ่านจาก HMC ไปยัง IBM ผ่านภารกิจนี้

โหมด Events Manager for Call Home (เปิดใช้งานหรือปิดใช้งาน) มีการตั้งค่าโดยใช้อินเตอร์เฟซบรรทัดคำสั่ง HMC การเปิดใช้งานภารกิจ Events Manager for Call Home จะบล็อก HMC ไม่ให้เรียกเหตุการณ์โฮมโดยอัตโนมัติเมื่อเกิดขึ้นเพื่อป้องกันการเรียกเหตุการณ์โฮมโดยไม่มี การอนุมัติ, HMCs ทั้งหมดที่รันอยู่ในสถานะแวดล้อมนี้ต้องมีการเปิดใช้งาน Events Manager for Call Home

เมื่อต้องการเปิดใช้งาน หรือปิดใช้งานภารกิจ Events Manager for Call Home ให้รัน คำสั่งต่อไปนี้:

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

หมายเหตุ: การเปิดใช้งานงาน Events Manager for Call Home จะพักเหตุการณ์ call home ไว้จนกว่าจะได้รับการอนุมัติสำหรับงาน call home หากคุณปิดใช้งานงาน Events Manager for Call Home จะไม่เปิดใช้งานคุณลักษณะ call home โดยอัตโนมัติ เชื้อต่อนี้ ป้องกันการเรียกโฮมโดยไม่ได้ตั้งใจของข้อมูลกลับไปยัง IBM เลือกจากอ็อปชันคำสั่งต่อไปนี้ เพื่อตั้งค่าคอนฟิกเรชันที่ต้องการ:

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

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

คุณสามารถลงทะเบียน HMC กับ Events Manager for Call Home หลังจากคุณลงทะเบียน HMC, events manager จะเคียวรี HMC ที่ลงทะเบียนสำหรับเหตุการณ์ใดๆ ซึ่งกำลังรอถูกเรียกโฮมไปยัง IBM Events Manager แสดงข้อมูลที่กำลังถูกส่งกลับไปยัง IBM และอนุมัติเหตุการณ์เหล่านี้ หลังจากอนุมัติแล้ว Event Manager จะแจ้ง HMC ที่ลงทะเบียนว่า สามารถดำเนินการเรียกโฮมต่อไปได้

ภารกิจ Events Manager for Call Home สามารถรันจาก HMC ใดๆ หรือจากหลาย HMCs เมื่อต้องการลงทะเบียนคอนโซลการจัดการที่มีภารกิจ Events Manager for Call Home ให้ทำขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน ความสามารถในการให้บริการ จากนั้นเลือก **Events Manager for Call Home**
2. จากบานหน้าต่าง **Events Manager for Call Home** คลิก **จัดการคอนโซล**
3. จากหน้าต่าง **จัดการคอนโซลที่ลงทะเบียน** คลิก **เพิ่มคอนโซล** เพื่อป้อนข้อมูลเพื่อลงทะเบียน คอนโซลการจัดการที่มีภารกิจ Events Manager for Call Home
4. คลิก **ตกลง** เพื่อ commit การเปลี่ยนแปลงในรายการ ของคอนโซลการจัดการที่ลงทะเบียน

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

การตั้งค่ารหัสผ่านสำหรับระบบที่ถูกจัดการ:

คุณต้องตั้งรหัสผ่านสำหรับเซิร์ฟเวอร์และ Advanced System Management (ASM) ของคุณ อ่านเพิ่มเติมเกี่ยวกับวิธีการใช้อินเตอร์เฟซ HMC เพื่อตั้งรหัสผ่านเหล่านี้

หากคุณได้รับข้อความ Authentication Pending HMC จะเตือนให้คุณตั้งรหัสผ่านสำหรับระบบที่ถูกจัดการ

หากคุณไม่ได้รับข้อความ Authentication Pending ให้ทำขั้นตอนต่อไปให้เสร็จสิ้น เพื่อตั้งรหัสผ่านสำหรับระบบที่ถูกจัดการ

การอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณ:

เมื่อต้องการอัปเดตรหัสผ่านเซิร์ฟเวอร์ของคุณให้ทำดังนี้:



1. ในพื้นที่การนำทางให้เลือกระบบที่ถูกจัดการ และคลิกไอคอน ผู้ใช้และการรักษาความปลอดภัย จากนั้นเลือก **ผู้ใช้และบทบาท**
2. คลิก **Change Password** หน้าต่าง อัปเดตรหัสผ่าน จะเปิด
3. พิมพ์ข้อมูลที่จำเป็น และคลิก **OK**

การอัปเดตรหัสผ่านทั่วไปสำหรับ Advanced System Management (ASM):

หมายเหตุ: ค่าดีฟอลต์ของรหัสผ่านสำหรับ ID ผู้ใช้ทั่วไปคือ general และค่าดีฟอลต์ของรหัสผ่านสำหรับ 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:

อ็พชั่นนี้ช่วยคุณตรวจสอบว่า คุณได้เชื่อมต่อกับเน็ตเวิร์ก อย่างถูกต้องหรือไม่

เมื่อต้องการทดสอบภาวะเชื่อมต่อเน็ตเวิร์ก, คุณต้องมีบทบาทใดบทบาทหนึ่ง ดังต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ตัวแทนบริการ

เมื่อต้องการทดสอบการเชื่อมต่อระหว่าง HMC และระบบที่ถูกจัดการ ให้ปฏิบัติตามนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **ค่าติดตั้งคอนโซล**
2. ในบานหน้าต่างเนื้อหา คลิก **ทดสอบการเชื่อมต่อเครือข่าย**
3. ในแท็บ **Ping** ให้พิมพ์ชื่อโฮสต์หรือ IP แอดเดรสของระบบใดๆ ซึ่งคุณต้องการเชื่อมต่อ เมื่อต้องการทดสอบเน็ตเวิร์กแบบเปิด ให้พิมพ์เกตเวย์ คลิก **Ping**

หากคุณยังไม่ได้สร้างโลจิคัลพาร์ติชันอื่นใด คุณจะไม่สามารถ ping แอดเดรสได้ คุณสามารถใช้ HMC เพื่อสร้าง โลจิคัลพาร์ติชันบนเซิร์ฟเวอร์ของคุณ – สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ *Logical partitioning*.

เมื่อต้องการทำความเข้าใจกับวิธีการใช้ HMC ในเน็ตเวิร์ก โปรดดูที่ “การเชื่อมต่อเน็ตเวิร์ก HMC” ในหน้า 80

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ การกำหนดค่า HMC เพื่อเชื่อมต่อกับ เครือข่าย โปรดดูที่ “การกำหนดคอนฟิก HMC โดยใช้เมนู HMC” ในหน้า 101

ขั้นตอน Postconfiguration

เมื่อคุณติดตั้งและตั้งค่าคอนฟิก HMC แล้ว ให้สำรองข้อมูล HMC ตามที่จำเป็น

การสำรองข้อมูล HMC ที่สำคัญ

คุณสามารถสำรองข้อมูลคอนโซลที่สำคัญลงในอุปกรณ์หน่วยความจำแฟลชแบบ USB ดีวีดี ผ่านทาง FTP หรือทางเน็ตเวิร์ก

เมื่อใช้ HMC, คุณสามารถสำรองข้อมูลที่สำคัญทั้งหมด, เช่น ข้อมูล ดังต่อไปนี้:

- ไฟล์ค่า Preference ผู้ใช้
- รายละเอียดผู้ใช้
- ไฟล์คอนฟิกูเรชัน-แพลตฟอร์ม HMC
- ล็อกไฟล์ HMC

- HMC อัปเดตผ่าน Install Corrective Service

ฟังก์ชันการสำรองข้อมูลจะบันทึกข้อมูล HMC ที่จัดเก็บอยู่บนฮาร์ดดิสก์ของ HMC ไปที่:

- สื่อบันทึกดีวีดี
- อุปกรณ์หน่วยความจำแฟลชแบบ USB
- ระบบโมดที่ประกอบเข้ากับระบบไฟล์ของ HMC (เช่น NFS)
- รีโมตไคลเอนต์ผ่านทาง FTP

สำรองข้อมูล HMC หลังจากที่คุณทำการเปลี่ยนแปลงใน HMC หรือในข้อมูลที่เกี่ยวข้องกับโลจิสติกส์พาร์ติชัน

หมายเหตุ: ก่อนที่จะบันทึกข้อมูลลงในสื่อบันทึกแบบถอดได้ ต้องจัดรูปแบบสื่อบันทึกนั้นก่อน เมื่อต้องการฟอร์แมตสื่อบันทึกให้คลิก การจัดการ HMC > การจัดการคอนโซล > ฟอร์แมต สื่อบันทึก และทำตามขั้นตอน

ถ้าต้องการสำรองข้อมูล HMC คุณต้องมีบทบาทใดบทบาทหนึ่ง ดังต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ผู้ควบคุมเครื่อง
- ตัวแทนบริการ

หากต้องการสำรองข้อมูลที่สำคัญของ HMC ให้ทำสิ่งต่อไปนี้:

1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management**  จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหาคลิกสำรองข้อมูล คอนโซลการจัดการ
3. เลือกอ็อปชันการเก็บถาวร คุณสามารถสำรองข้อมูลลงในสื่อบันทึกบนระบบภายในเครื่อง ระบบระยะไกลที่เชื่อมต่อ หรือส่งข้อมูลสำรองไปยังไคลเอนต์ระยะไกล
4. ปฏิบัติตามคำสั่งบนหน้าต่างเพื่อสำรองข้อมูล

การสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ทั้งหมดไว้บนระบบรีโมต

คุณสามารถใช้ HMC เพื่อสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ทั้งหมด ของ HMC ไว้บน ระบบรีโมต

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

เมื่อต้องการสำรองข้อมูลของฮาร์ดดิสก์ไดรฟ์ HMC ไว้บนระบบรีโมต คุณต้องเป็นสมาชิกของบทบาทอย่างใดอย่างหนึ่ง ต่อไปนี้:

- ผู้ดูแลระบบพิเศษ
- ผู้ควบคุมเครื่อง
- ตัวแทนบริการ

เมื่อต้องการสำรองข้อมูลฮาร์ดไดรฟ์ HMC ให้กับระบบรีโมต ให้ทำสิ่งต่อไปนี้:

1. บันทึกหมายเลขอินเตอร์เฟซ (eth0, eth1 เป็นต้น), MAC แอดเดรส และ IP แอดเดรสของแต่ละอะแดปเตอร์เครือข่ายบน HMC เมื่อต้องการดำเนินการดังกล่าว ให้คลิก การจัดการ HMC > การตั้งค่าคอนโซล > เปลี่ยนค่าติดตั้ง เครือข่าย > อะแดปเตอร์ LAN
2. ปิดและหยุดการจ่ายไฟ HMC
3. เปิดคอนโซล HMC โดยมีสื่อบันทึกการบูต HMC ในไดรฟ์ DVD หากต้องการเริ่มต้นอินเตอร์เฟซ HMC จากเน็ตเวิร์กบูตเซิร์ฟเวอร์ที่กำหนดคอนฟิกไว้ให้แน่ใจว่าเน็ตเวิร์กอินเตอร์เฟซคือหนึ่งในอุปกรณ์ต่อไปนี้ในลำดับการเริ่มทำงาน เมื่อต้องการดูรายการของอุปกรณ์สตาร์ทอัพ ให้กด F12 เมื่อเปิด HMC และเลือกเน็ตเวิร์กอินเตอร์เฟซที่คุณต้องการบูต
4. เลือกอีพซันสำรองข้อมูล และคลิก Next
5. เลือกเน็ตเวิร์กอินเตอร์เฟซเพื่อใช้สำหรับสื่อสารกับ รัมโบตเซิร์ฟเวอร์ หากคุณกำลังเริ่มต้น HMC โดยติดต่อกับเน็ตเวิร์กบูตเซิร์ฟเวอร์ และเซิร์ฟเวอร์นี้ยังเป็นรัมโบตเซิร์ฟเวอร์ที่คุณต้องการสำรองข้อมูล ให้เลือกค่ากำหนดดีฟอลต์ จากนั้นให้คลิก ถัดไป และไปยังขั้นตอนที่ 7 ถ้าคุณไม่ได้เลือกค่ากำหนดดีฟอลต์ไว้ให้ดำเนินการต่อด้วยขั้นตอนถัดไป

หมายเหตุ: หมายเลขอินเตอร์เฟซ (eth0, eth1) อาจไม่ตรงกับหมายเลขที่บันทึกในขั้นตอนที่ 1 สามารถใช้ MAC address ที่แสดงรายการไว้เพื่อระบุอินเตอร์เฟซที่ต้องการได้ สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การระบุอีเทอร์เน็ตพอร์ตที่จะถูกกำหนดเป็น eth0” ในหน้า 107

6. ถ้าคุณไม่ได้เลือกค่าติดตั้งดีฟอลต์ คุณต้องเลือก โพรโตคอลเครือข่ายเพื่อใช้กับอินเตอร์เฟซที่เลือกไว้ คุณสามารถเลือกที่จะรับ IP แอดเดรสจากเซิร์ฟเวอร์ DHCP ในเน็ตเวิร์กของคุณ หรือกำหนด IP แอดเดรส แบบคงที่ให้กับเน็ตเวิร์กอินเตอร์เฟซที่เลือก ทำการเลือก และคลิก Next
7. หากคุณไม่ได้เลือกค่าติดตั้งดีฟอลต์ ให้พิมพ์ IP แอดเดรสหรือชื่อโฮสต์ของรัมโบตเซิร์ฟเวอร์ของคุณ ไฟล์สำรองข้อมูลจะถูกสร้างขึ้นโดยใช้ยูลิทิตีบีบอัด gzip และคำสั่ง tar ระบุไฟล์ด้วยนามสกุล .tgz ในฟิลด์ File on remote host หากคุณสามารถเลือกค่ากำหนดดีฟอลต์เน็ตเวิร์กไว้ คุณต้องใช้ เซิร์ฟเวอร์ไคเร็กทอรีในการกำหนดคอนฟิกเน็ตเวิร์กบูตของคุณ ข้อมูลนี้จะถูกแสดงในฟิลด์ File on remote host หลังจากที่คุณ บ้อนข้อมูลที่ต้องการทั้งหมดเสร็จสิ้นแล้ว ให้คลิก Next
8. เลือกวิธีที่คุณต้องการใช้เพื่อถ่ายโอนข้อมูลจาก HMC ของคุณ ให้กับรัมโบตเซิร์ฟเวอร์ หากคุณเลือกการเข้ารหัสข้อมูล รัมโบตโฮสต์ของคุณจะต้องมีเซิร์ฟเวอร์ Secure Shell (SSH) ที่กำลังรันอยู่ หากคุณเลือก การถ่ายโอนข้อมูลโดยไม่มีการเข้ารหัส รัมโบตโฮสต์ของคุณต้องมี Network File Server (NFS) ที่กำลังรันอยู่ และไคเร็กทอรีที่คุณต้องการ สำรองข้อมูล ต้องถูกเอ็กซ์พอร์ตเพื่อทำการบันทึก ทำการเลือก และคลิก Next
9. ถ้าคุณเลือกถ่ายโอนข้อมูลโดยใช้การเข้ารหัส คุณต้องพิมพ์ ID ผู้ใช้และรหัสผ่านของรัมโบตเซิร์ฟเวอร์
10. ตรวจสอบข้อมูลที่คุณป้อนให้ถูกต้อง และคลิก Finish เมื่อการสำรองข้อมูลเสร็จสมบูรณ์ อินเตอร์เฟซ HMC จะปรากฏขึ้น

ถ้าคุณปรับเปลี่ยนลำดับของการเริ่มทำงานโดยกด F1 เมื่อคุณเปิด HMC คุณต้องบูต HMC และเปลี่ยนค่าติดตั้งอีกครั้ง เมื่อคุณเปลี่ยนลำดับการเริ่มทำงาน ให้แน่ใจว่าฮาร์ดดิสก์ของคุณจะถูกแสดงก่อนเน็ตเวิร์กอินเตอร์เฟซ ในลำดับการเริ่มทำงาน

การอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ

การอัปเดตและอัปเดตควรดำเนินการเป็นระยะๆ เพื่อให้ HMC สามารถเพิ่มคุณสมบัติการทำงานใหม่ๆ และปรับปรุงคุณลักษณะที่มีอยู่ ศึกษาเพิ่มเติมเกี่ยวกับความแตกต่างระหว่างการอัปเดต การอัปเดต และการโอนย้ายรหัสเครื่อง HMC ของคุณ รวมทั้งศึกษาวิธีการดำเนินการอัปเดต อัปเดต หรือโอนย้ายรหัสเครื่อง HMC

เมื่อคุณทำงานแต่ละงานเหล่านี้เสร็จสิ้น HMC จะรีบูต แต่พาร์ติชันไม่รีบูต

การอัปเดตรหัส HMC

ใช้การบำรุงรักษากับระดับ HMC ที่มีอยู่

คุณไม่จำเป็นต้องทำงาน Save upgrade data

การอัปเดตรหัส HMC

แทนที่ซอฟต์แวร์ HMC ด้วยรหัสใหม่หรือระดับโปรแกรมฟิร์มแวร์ของโปรแกรมเดียวกัน

คุณต้องบูตจากสื่อบันทึกที่ถูกต้อง

การโอนย้ายรหัส HMC

ย้ายข้อมูล HMC จาก HMC เวอร์ชันหนึ่งเป็นเวอร์ชันอื่น

การโอนย้ายระบบเป็นการอัปเดตชนิดหนึ่ง

การกำหนดเวอร์ชันและรหัสของรหัสเครื่อง HMC ของคุณ

เรียนรู้วิธีการดูเวอร์ชันและรหัสของรหัสเครื่อง HMC

ระดับของรหัสเครื่องบน HMC จะกำหนดคุณลักษณะที่มีอยู่ รวมถึงการบำรุงรักษาเซิร์ฟเวอร์เฟิร์มแวร์และการปรับปรุงสำหรับการอัปเดตเป็นรหัสใหม่

เมื่อต้องการดูเวอร์ชันและรหัสของรหัสเครื่อง HMC ให้ทำดังนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก อัปเดต Hardware Management Console
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รหัส ระดับการซ่อม บำรุง ระดับบิต และเวอร์ชันฐานของ HMC

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
- อินเทอร์เน็ตผ่าน VPN

เพื่อให้แน่ใจว่าคุณมีการเชื่อมต่ออินเทอร์เน็ต ให้ปฏิบัติตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **ความสามารถในการให้บริการ** จากนั้นเลือก การจัดการกับการให้

2. ในบานหน้าต่างเนื้อหาจัดการการเชื่อมต่อขาออก
3. เลือกแท็บสำหรับชนิดของการเชื่อมต่อขาออก ที่คุณเลือกใช้สำหรับ HMC ของคุณ (VPN อินเทอร์เน็ต หรือ SSL)

หมายเหตุ: ถ้าไม่มีการเชื่อมต่อกับส่วนบริการและสนับสนุน ให้ตั้งค่าการเชื่อมต่อบริการ ก่อนที่จะดำเนินการต่อสำหรับขั้นตอนนี้ สำหรับคำแนะนำเกี่ยวกับวิธีการตั้งค่าการเชื่อมต่อกับส่วนบริการและสนับสนุน โปรดดูที่ การตั้งค่าเซิร์ฟเวอร์ของคุณเพื่อเชื่อมต่อกับส่วนบริการและสนับสนุน IBM

4. คลิก Test
5. ตรวจสอบว่าการทดสอบเสร็จสมบูรณ์ ถ้าการทดสอบไม่เสร็จสมบูรณ์ ให้แก้ปัญหาการเชื่อมต่อและแก้ไข ปัญหา ก่อนที่จะดำเนินการต่อตามขั้นตอนนี้อีกทางหนึ่ง คุณสามารถ ขอรับอัปเดตบนดีวีดี
6. ดำเนินการต่อด้วย “ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก อัปเดต Hardware Management Console
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส์ ระดับการซ่อมบำรุง ระดับบิตและเวอร์ชันฐานของ HMC
4. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่”

ขั้นตอนที่ 3. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการดูระดับรหัสเครื่อง HMC ที่มีอยู่ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่ <http://www.ibm.com/eserver/support/fixes>
2. เลือกตระกูลที่เหมาะสมในรายการตระกูลผลิตภัณฑ์
3. เลือก **Hardware Management Console** ใน รายการชนิดผลิตภัณฑ์หรือโปรแกรมฟิกซ์
4. คลิก ทำต่อไป ไซด์ 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 สำหรับคำแนะนำโปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 122 จากนั้นให้ดำเนินการขั้นตอนถัดไป



2. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
3. ในบานหน้าต่างเนื้อหา คลิก อัปเดต Hardware Management Console วิศวกร Install Corrective Service จะเปิดขึ้น

4. ปฏิบัติตามคำแนะนำในเวิร์กช็อปเพื่อติดตั้งอัปเดต
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. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหาคลิก อัปเดต **Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิตต์ และเวอร์ชันฐานของ HMC
4. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
5. 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. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหาคลิก อัปเดต **Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิตต์ และเวอร์ชันฐานของ HMC
4. 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. ดำเนินการต่อยก “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 ให้เลือกกระดบ HMC ล่าสุด
3. เลื่อนลงไปยังพื้นที่ File name(s) / Package และระบุอัปเดตที่คุณ ต้องการสั่งซื้อ
4. ในคอลัมน์ Order ให้เลือก Go
5. คลิก Continue เพื่อลงชื่อเข้าใช้ด้วย IBM ID ของคุณ
6. ปฏิบัติตามพร้อมด้นหน้าจอเพื่อทำการสั่งซื้อ

การดาวน์โหลดอัปเดตรหัสเครื่อง HMC ลงในสื่อบันทึกแบบถอดออกได้

1. จากคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต ให้ไปที่ เว็บไซต์ Hardware Management Console ที่ <http://www-933.ibm.com/support/fixcentral/>
2. ภายใต้ Supported HMC products ให้เลือกกระดบ HMC ล่าสุด
3. เลื่อนลงไปยังพื้นที่ File name(s) / Package และระบุอัปเดตที่คุณ ต้องการดาวน์โหลด
4. คลิกอัปเดตที่คุณต้องการดาวน์โหลด
5. ยอมรับข้อตกลงไลเซนส์ และบันทึกอัปเดตลงในสื่อบันทึกแบบถอดออกได้

เมื่อเสร็จเรียบร้อย ให้ดำเนินการต่อยก “ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC”

ขั้นตอนที่ 4. ใช้อัปเดตรหัสเครื่อง HMC:

เมื่อต้องการใช้การอัปเดตรหัสเครื่อง HMC ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ก่อนที่คุณจะติดตั้งอัปเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูล HMC ของคุณ สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 122
2. ถ้าคุณได้รับหรือสร้างอัปเดตบนดิสก์ดรัม ให้ใส่แผ่นดิสก์ดังกล่าวในไดรฟ์ดิสก์ดรัม HMC ถ้าคุณได้รับหรือสร้างอัปเดตบนอุปกรณ์หน่วยความจำแบบ USB ให้เสียบอุปกรณ์หน่วยความจำนั้น
3. ก่อนที่คุณจะติดตั้งอัปเดตสำหรับรหัสเครื่อง HMC ให้สำรองข้อมูลคอนโซลที่สำคัญบน HMC ของคุณ สำหรับคำแนะนำ โปรดดูที่ “การสำรองข้อมูล HMC ที่สำคัญ” ในหน้า 122 จากนั้น ให้ดำเนินการขั้นตอนถัดไป

4. ในพื้นที่การนำทาง ให้คลิกไอคอน HMC Management  จากนั้นเลือก การจัดการกับคอนโซล

5. ในบานหน้าต่างเนื้อหาคลิก **อัปเดต Hardware Management Console** วิศวกร Install Corrective Service จะเปิดขึ้น
6. ปฏิบัติตามคำแนะนำในวิศวกรเพื่อติดตั้งอัปเดต
7. ปิดเครื่องรีสตาร์ท และกลับเข้าสู่ระบบ HMC เพื่อให้การอัปเดตมีผล
8. ดำเนินการต่อด้วย “ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์”

ขั้นตอนที่ 5. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์:

เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์แล้ว ให้ปฏิบัติตามขั้นตอนต่อไปนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **การจัดการกับคอนโซล**
2. ในบานหน้าต่างเนื้อหาคลิก **อัปเดต Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลปรากฏภายใต้หัวข้อ **ไดรเวอร์ HMC ปัจจุบัน** รวมถึง: เวอร์ชัน รีลีส ระดับการซ่อมบำรุง ระดับบิต และเวอร์ชันฐานของ HMC
4. ตรวจสอบว่าเวอร์ชันและรีลีสตรงกับ อัปเดตที่คุณติดตั้ง
5. หากระดับของโค้ดที่แสดงไม่ใช่ระดับที่คุณติดตั้ง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:
 - a. ลองอัปเดตรหัสเครื่องอีกครั้ง ถ้าคุณสร้างทีวีดีในขั้นตอนนี้ ให้ใช้สื่อบันทึกใหม่
 - b. ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การอัปเดตซอฟต์แวร์ HMC ของคุณ

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากรีลีสหนึ่งเป็นรีลีสถัดไป ในขณะที่ยังคงรักษาข้อมูลคอนฟิกูเรชัน HMC ของคุณ

เมื่อต้องการอัปเดตรหัสเครื่องบน HMC ให้ปฏิบัติตามขั้นตอนที่ 1–9

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. คลิก **ทำต่อไป** ไซต์ Hardware Management Console จะปรากฏขึ้น
3. นำทางไปยังเวอร์ชัน HMC ที่คุณต้องการอัปเดต
4. ค้นหาตำแหน่งส่วนดาวน์โหลดและสั่งซื้อ

หมายเหตุ: ถ้าคุณไม่มีการเข้าถึงอินเทอร์เน็ต โปรดติดต่อส่วนบริการและสนับสนุน IBM เพื่อสั่งซื้อการอัปเดตบนทีวีดี

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

ขั้นตอนที่ 2. ดูระดับรหัสเครื่อง HMC ที่มีอยู่:

เมื่อต้องการกำหนดระดับรหัสเครื่องที่มีอยู่บน HMC ให้ปฏิบัติตามขั้นตอนเหล่านี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล ในพื้นที่ การนำทางให้คลิก **อัปเดต**
2. ในบานหน้าต่างเนื้อหาคลิก **อัปเดต Hardware Management Console**
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส์ ระดับการซ่อมบำรุง ระดับบิตต์ และเวอร์ชันฐานของ HMC
4. ดำเนินการต่อด้วย “ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ”

ขั้นตอนที่ 3. สำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการ:

เมื่อต้องการสำรองข้อมูลโปรไฟล์ของระบบที่ถูกจัดการให้ทำดังนี้:

1. ในพื้นที่การนำทางให้เลือก 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 เพื่อให้สามารถเรียกคืนระดับก่อนหน้านั้นในกรณีที่เกิดปัญหา ในระหว่างการอัปเดตซอฟต์แวร์ ห้ามใช้ข้อมูลคอนโซลที่สำคัญนี้หลังจากที่อัปเดตเป็น ซอฟต์แวร์ HMC เวอร์ชันใหม่ได้สำเร็จ

หมายเหตุ: เมื่อต้องการ สำรองข้อมูลไปยังสื่อบันทึกแบบถอดออกได้ คุณจะต้องเตรียมสื่อบันทึกดังกล่าวไว้ให้พร้อม

เมื่อต้องการ สำรองข้อมูล HMC ให้ทำดังนี้:

1. ถ้าคุณวางแผนที่จะ สำรองข้อมูลไปยังสื่อบันทึก ให้ปฏิบัติตามขั้นตอนต่อไปนี้จะจัดรูปแบบ สื่อบันทึก:
 - a. ใส่สื่อบันทึกลงในไดรฟ์



- b. ในพื้นที่การนำทางให้คลิก **ความสามารถในการให้บริการ** จากนั้นเลือก การจัดการกับการให้บริการ
- c. ในบานหน้าต่างเนื้อหาคลิก **ฟอร์แมตสื่อบันทึก**
- d. เลือกชนิดของสื่อบันทึก
- e. เลือกชนิดการจัดรูปแบบ
- f. คลิก **OK**.



2. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก **การจัดการกับคอนโซล**
3. ในบานหน้าต่างเนื้อหาคลิก **สำรองข้อมูล คอนโซลการจัดการ** หน้าต่าง **สำรองข้อมูล คอนโซลการจัดการ**
4. เลือกอ็อปชันการเก็บถาวร คุณสามารถสำรองข้อมูลลงในสื่อบันทึกบนระบบภายในเครื่อง ระบบระยะไกลที่เชื่อมต่อกับระบบไฟล์ HMC (ตัวอย่างเช่น NFS) หรือส่งสำเนาสำรองไปยังไซต์ระยะไกลโดยใช้ File Transfer Protocol (FTP)
 - เมื่อต้องการสำรองข้อมูลลงในระบบภายในเครื่องให้เลือก **Back up to media on local system** และปฏิบัติตามคำแนะนำ
 - เมื่อต้องการสำรองข้อมูลไปยังระบบระยะไกลที่เชื่อมต่อให้เลือก **Back up to mounted remote system** และปฏิบัติตามคำแนะนำ
 - เมื่อต้องการสำรองข้อมูลไปยังไซต์ FTP ระยะไกลให้เลือก **Send back up critical data to remote site** และปฏิบัติตามคำแนะนำ
5. ดำเนินการต่อด้วย “ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกรेशन HMC ปัจจุบัน”

ขั้นตอนที่ 5. บันทึกข้อมูลการคอนฟิกรेशन HMC ปัจจุบัน:

ก่อนที่จะอัปเดตเป็นซอฟต์แวร์ HMC เวอร์ชันใหม่ ให้บันทึกข้อมูลคอนฟิกรेशन HMC เพื่อเป็นการป้องกัน

เมื่อต้องการ บันทึกข้อมูลคอนฟิกรेशन HMC ปัจจุบัน ให้ทำดังนี้:

1. เมื่อต้องการดูการดำเนินการที่กำหนดเวลาไว้สำหรับระบบที่ได้รับการจัดการ หรือ โลจิคัลพาร์ติชัน ให้เปิด **การจัดการ HMC > การจัดการคอนโซล** หากต้องการบันทึก การดำเนินการที่กำหนดเวลาไว้สำหรับ HMC เอง ให้เลือก **การจัดการ HMC > การจัดการคอนโซล** แล้วเลือก และข้ามไปที่ขั้นตอนที่ 3
2. เลือกระบบที่ถูกจัดการและพาร์ติชันใดๆ ที่ ต้องการบันทึกข้อมูลคอนฟิกรेशन 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”

ขั้นตอนที่ 6. บันทึกสถานะคำสั่งระยะไกล:

เมื่อต้องการบันทึกสถานะคำสั่งระยะไกลให้ทำดังนี้:

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

ขั้นตอนที่ 7. บันทึกข้อมูลอัปเกรด:

คุณสามารถบันทึกคอนฟิกูเรชัน HMC ปัจจุบันลงในพาร์ติชันของดิสก์ ที่กำหนดบน HMC หรือในสื่อบันทึกภายในเครื่องก็ได้ ให้บันทึกข้อมูลอัปเกรดในพื้นที่ก่อนที่จะอัปเกรดซอฟต์แวร์ HMC ของคุณให้เป็นรีลีสใหม่ แอ็คชันนี้อนุญาตให้คุณเรียกคืนคอนฟิกูเรชัน HMC ได้หลังจากการอัปเกรด

หมายเหตุ: อนุญาตให้มีข้อมูลสำรองได้เพียงระดับเดียวเท่านั้น แต่ละครั้งที่คุณบันทึกข้อมูลอัปเกรด ระดับก่อนหน้านี้จะถูกเขียนทับ

เมื่อต้องการ บันทึกข้อมูลอัปเกรดให้ทำดังนี้:



1. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก **บันทึกข้อมูลอัปเกรด** วิกิการ์ด **Save Upgrade Data** จะเปิดขึ้น
3. เลือกสื่อบันทึกที่คุณต้องการบันทึกข้อมูล อัปเกรด ถ้าคุณเลือกที่จะบันทึกสื่อบันทึกแบบถอดได้ ให้ใส่สื่อบันทึกในตอนนี้คลิก **Next**
4. คลิก **Finish**.
5. รอให้งานเสร็จสมบูรณ์ ถ้างาน **Save Upgrade Data** ล้มเหลว ให้ติดต่อระดับของการสนับสนุนถัดไปก่อนที่จะดำเนินการ

หมายเหตุ: ถ้างานบันทึกข้อมูลอัปเกรดล้มเหลว ห้ามดำเนินกระบวนการอัปเกรด

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

ขั้นตอนที่ 8. อัปเกรดซอฟต์แวร์ HMC:

เมื่อต้องการอัปเกรดซอฟต์แวร์ HMC ให้รีสตาร์ทระบบโดยใช้สื่อบันทึกแบบถอดออกได้ในไดรฟ์ DVD

1. ใส่สื่อบันทึกสำหรับการติดตั้งผลิตภัณฑ์ HMC ลงในไดรฟ์ดีวีดี



2. ในพื้นที่การนำทางให้คลิกไอคอน **HMC Management** จากนั้นเลือก การจัดการกับคอนโซล
3. ในพื้นที่การนำทาง เลือก **ปิดการทำงาน หรือรีสตาร์ท คอนโซลการจัดการ**
4. ตรวจสอบว่า **Restart the HMC** ถูกเลือกไว้
5. คลิก **OK**. HMC จะเริ่มทำงานอีกครั้ง และ ข้อมูลระบบจะเลื่อนอยู่บนหน้าต่าง
6. เลือก **Upgrade** และคลิก **Next**
7. เลือกจากตัวเลือกต่อไปนี้:

- ถ้าคุณบันทึกข้อมูลอัปเดตที่บันทึกไว้ในระหว่างงานก่อนหน้านี้ให้ทำขั้นตอนถัดไป
 - ถ้าคุณไม่ได้บันทึกข้อมูลอัปเดตก่อนหน้านี้ในขั้นตอนนี้ คุณจะต้อง บันทึกข้อมูลอัปเดตในตอนนี้ ก่อนที่คุณจะดำเนินการต่อ
8. เลือก Upgrade from media และคลิก Next
 9. ยืนยันค่าติดตั้ง และคลิก Finish
 10. ปฏิบัติตามพร้อมต์

หมายเหตุ:

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

ขั้นตอนที่ 9. ตรวจสอบว่าอัปเดตสำหรับรหัสเครื่อง HMC ได้รับการติดตั้งเสร็จสมบูรณ์:
เมื่อต้องการตรวจสอบว่าอัปเดตสำหรับ HMC ได้รับการติดตั้งเสร็จสมบูรณ์แล้ว ให้ทำดังนี้:



1. ในพื้นที่การนำทาง ให้คลิกไอคอน HMC Management จากนั้นเลือก การจัดการกับคอนโซล
2. ในบานหน้าต่างเนื้อหา คลิก อัปเดต Hardware Management Console
3. ในหน้าต่างใหม่ ดูและบันทึกข้อมูลที่ปรากฏภายใต้ หัวข้อ ไดรเวอร์ HMC ปัจจุบัน รวมถึง: เวอร์ชัน รีลีส์ ระดับการซ่อมบำรุง ระดับบิตต์ และเวอร์ชันฐาน ของ HMC
4. ตรวจสอบว่าเวอร์ชันและรีลีส์ตรงกับ อัปเดตที่คุณติดตั้ง
5. ถ้าระดับของโค้ดที่แสดงไม่ใช่ระดับ ที่คุณติดตั้ง ให้ลองทำการอัปเดตอีกครั้งโดยใช้ดีวีดีใหม่ ถ้ายังคงมีปัญหาอยู่ ให้ติดต่อระดับของการสนับสนุนถัดไป

การอัปเดต HMC จากตำแหน่งรีโมทโดยใช้อิมเมจการอัปเดตบนเครือข่าย

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากตำแหน่งรีโมท โดยใช้อิมเมจการอัปเดตเครือข่าย

ศึกษาวิธีการอัปเดตซอฟต์แวร์บน HMC จากตำแหน่งรีโมท โดยใช้อิมเมจการอัปเดตเครือข่าย ใช้ขั้นตอนต่อไปนี้ เพื่ออัปเดต 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 คุณต้องดาวน์โหลดอิมเมจไปยังเซิร์ฟเวอร์ ที่ยอมรับคำร้องขอ FTP
3. ตรวจสอบให้แน่ใจว่าคุณดาวน์โหลดไฟล์ต่อไปนี้:
 - img2a
 - img3a
 - base.img

- disk1.img
 - hmcnetworkfiles.sum
- บันทึกข้อมูลการอัปเดตบน HMC ดำเนินการบรรทัดคำสั่งต่อไปนี้เพื่อบันทึกข้อมูลการอัปเดต:
 - เพื่อบันทึกข้อมูลบนทั้ง DVD และ HDD ดำเนินการคำสั่งต่อไปนี้:


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

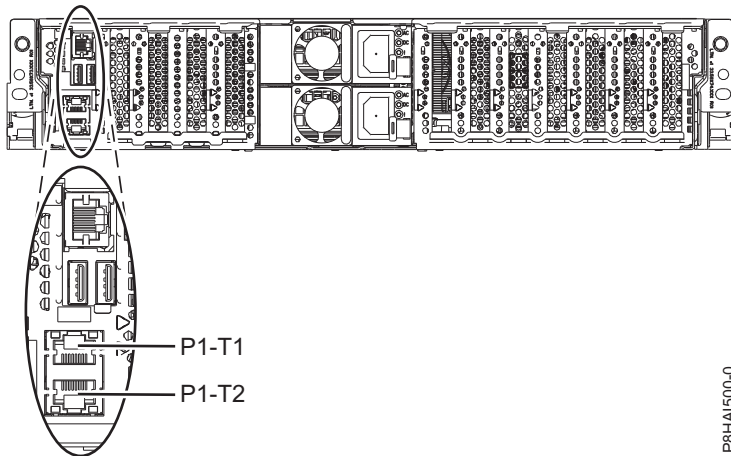

```
saveupgdata -r disk
```
 - คัดลอกไฟล์การอัปเดตไปยังพาร์ติชันดิสก์ที่สามารถบูตได้บน HMC รันคำสั่ง `getupgfiles` เพื่อคัดลอกไฟล์ ตัวอย่างเช่น: `getupgfiles -h <ftp server> -u <user id> -d <remote directory>` โดย
 - ftp server คือชื่อโฮสต์หรือ ip แอดเดรสของ เซิร์ฟเวอร์ FTP ที่คุณดาวน์โหลดอิมเมจเครือข่าย HMC ไว้
 - user id คือ id ผู้ใช้ที่ถูกต้องบนเซิร์ฟเวอร์ FTP หากคุณไม่ได้ระบุรหัสผ่านด้วยอาร์กิวเมนต์ `--passwd` คุณจะได้รับพร้อมท์สำหรับรหัสผ่าน
 - remote directory คือไดเรกทอรีบนเซิร์ฟเวอร์ FTP ของคุณที่บันทึกอิมเมจเครือข่าย HMC ไว้
 - รีบูต HMC เพื่ออัปเดตโค้ดที่คัดลอกไปยังพาร์ติชันดิสก์ที่บูตได้ รัน `chhmc -c alt diskboot -s enable --mode upgrade` เพื่อรีบูต HMC
 - รีบูต HMC และเริ่มต้นการอัปเดต รันคำสั่ง `hmcshutdown -r -t now` เพื่อเริ่มต้นการอัปเดต

ตำแหน่งพอร์ตของ HMC

คุณสามารถค้นหาคำแหน่งพอร์ตได้โดยใช้โค้ดตำแหน่ง ใช้ภาพประกอบ ตำแหน่งพอร์ตของ HMC เพื่อแม็ปโค้ดตำแหน่งกับตำแหน่งพอร์ตของ HMC บนเซิร์ฟเวอร์

โมเดล 8247-21L, 8247-22L, 8284-21A หรือตำแหน่งพอร์ต 8284-22A HMC

ใช้ไดอะแกรมและตารางนี้เพื่อแม็ปพอร์ต HMC บน 8247-21L, 8247-22L, 8284-21A หรือ 8284-22A



P8HA1500-0

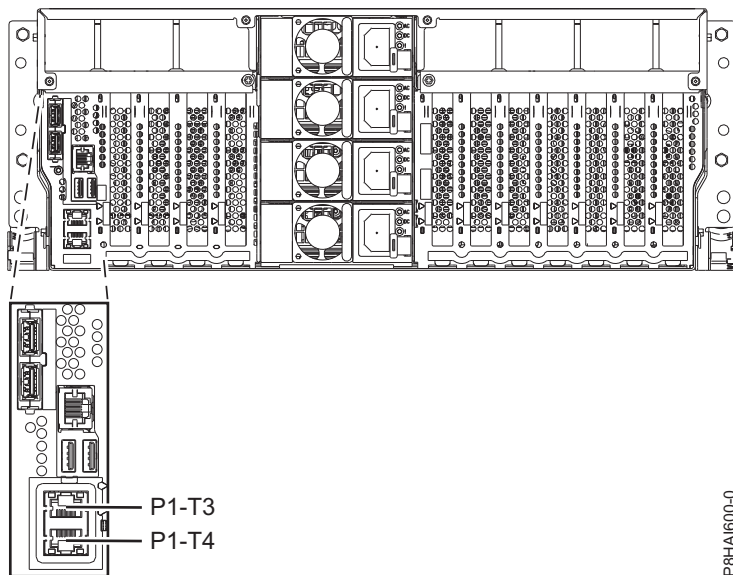
รูปที่ 85. 8247-21L, 8247-22L, 8284-21A หรือตำแหน่งพอร์ต 8284-22A HMC

ตารางที่ 57. 8247-21L, 8247-22L, 8284-21A หรือตำแหน่งพอร์ต 8284-22A HMC

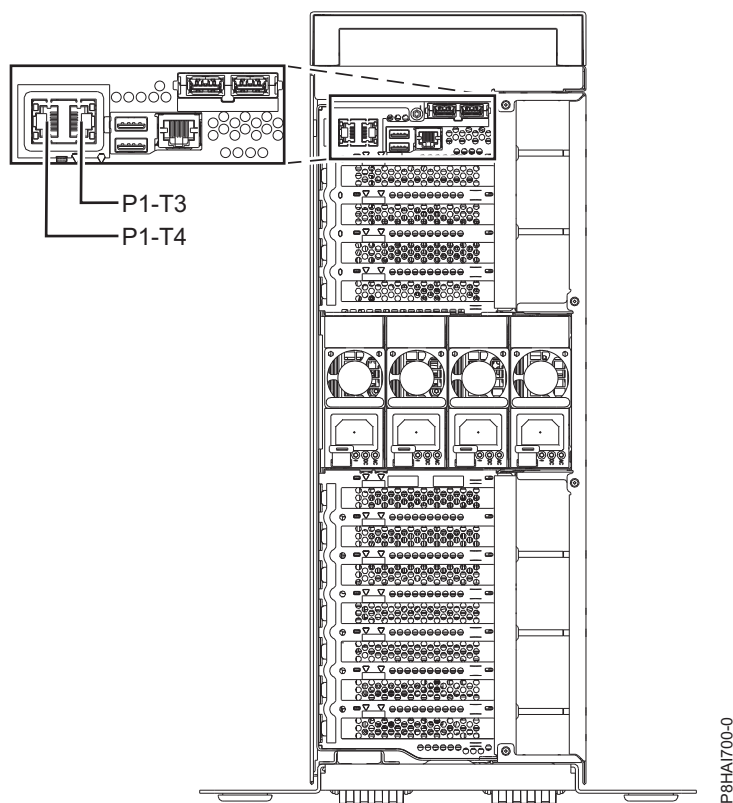
พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T1	ไม่มี
พอร์ต HMC 2	Un-P1-T2	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งของพอร์ต HMC เกี่ยวกับ 8247-21L, 8247-22L, 8284-21A หรือ 8284-22A โปรดดูตำแหน่งของชิ้นส่วนและ รหัสตำแหน่งสำหรับ 8247-21L, 8247-22L หรือ 8284-22A		

ตำแหน่งพอร์ตของโมเดล 8247-42L, 8286-41A, หรือ 8286-42A HMC

ใช้แผนภาพนี้และตารางเพื่อแมปพอร์ต HMC บน 8247-42L, 8286-41A หรือ 8286-42A



รูปที่ 86. มุมมอง ด้านหลัง - 8247-42L, 8286-41A หรือ 8286-42A ตำแหน่งพอร์ต HMC



รูปที่ 87. ตำแหน่งพอร์ต 8286-41A HMC แบบทาวเวอร์

ตารางที่ 58. ตำแหน่ง 8247-42L, 8286-41A หรือ 8286-42A พอร์ต HMC

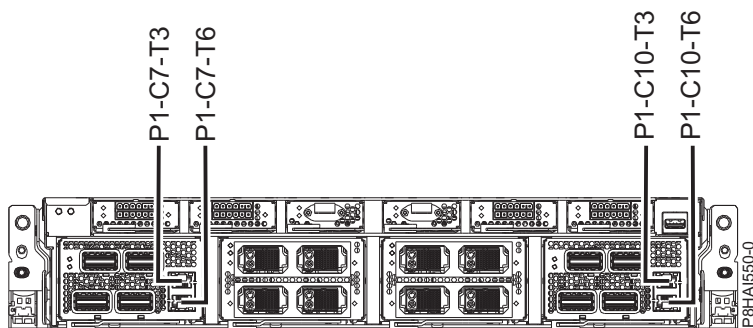
พอร์ต	โค้ดตำแหน่งฟิลิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-T3	ไม่มี

ตารางที่ 58. ตำแหน่ง 8247-42L, 8286-41A หรือ 8286-42A พอร์ต HMC (ต่อ)

พอร์ต	โค้ดตำแหน่งฟิสิกส์	LED ระบุ
พอร์ต HMC 2	Un-P1-T4	ไม่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ ตำแหน่งพอร์ต HMC บน 8247-42L, 8286-41A หรือ 8286-42A โปรดดู ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8247-42L, 8286-41A หรือ 8286-42A		

ตำแหน่งพอร์ตของโมเดล 9080-MHE, 9080-MME, 9119-MHE, and 9119-MME HMC

ใช้ไดอะแกรมและตารางนี้เพื่อแม็พพอร์ต HMC บน 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME



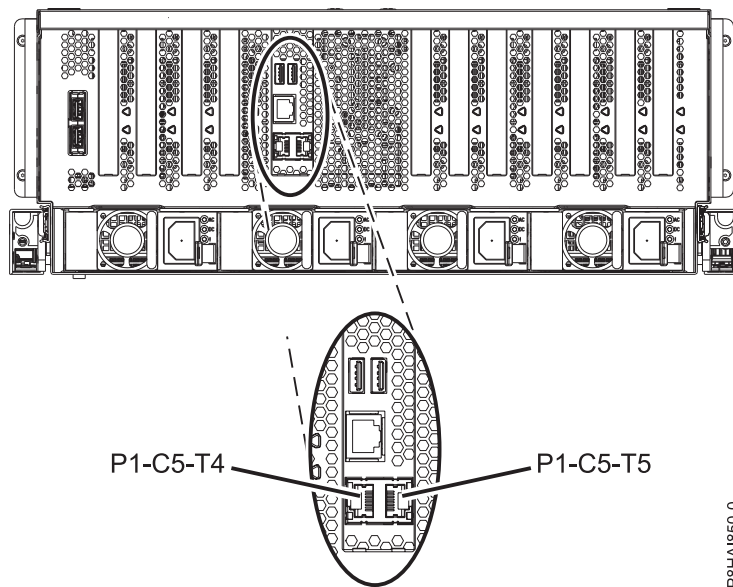
รูปที่ 88. ตำแหน่งพอร์ต 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME HMC

ตารางที่ 59. ตำแหน่งพอร์ต 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME HMC

พอร์ต	โค้ดตำแหน่งฟิสิกส์	LED ระบุ
การ์ดตัวประมวลผลเซิร์ฟเวอร์ 1 - พอร์ต HMC 1	Un-P1-C7-T3	ไม่มี
การ์ดตัวประมวลผลเซิร์ฟเวอร์ 1 - พอร์ต HMC 2	Un-P1-C7-T6	ไม่
การ์ดตัวประมวลผลเซิร์ฟเวอร์ 2 - พอร์ต HMC 1	Un-P1-C10-T3	ไม่
การ์ดตัวประมวลผลเซิร์ฟเวอร์ 2 - พอร์ต HMC 2	Un-P1-C10-T6	ไม่
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ต HMC บน 9080-MHE, 9080-MME, 9119-MHE และ 9119-MME โปรดดู ตำแหน่งพอร์ตและโค้ดตำแหน่งสำหรับตำแหน่ง 9080-MHE, 9080-MME, 9119-MHE หรือ 9119-MME		

ตำแหน่งพอร์ตของโมเดล 8408-44E และ 8408-E8E HMC

ใช้แผนภาพนี้และตารางเพื่อแม็พพอร์ต HMC บน 8408-44E และ 8408-E8E



รูปที่ 89. ตำแหน่งพอร์ต HMC 8408-44E and 8408-E8E

ตารางที่ 60. ตำแหน่งพอร์ต HMC 8408-44E and 8408-E8E

พอร์ต	โค้ดตำแหน่งฟิสิคัล	LED ระบุ
พอร์ต HMC 1	Un-P1-C5-T4	ไม่มี
พอร์ต HMC 2	Un-P1-C5-T5	ไม่มี
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งพอร์ต HMC บน 8408-44E และ 8408-E8E โปรดดู ตำแหน่งชิ้นส่วนและโค้ดตำแหน่งสำหรับ 8404-44E และตำแหน่ง 8408-E8E		

หมายเหตุ

ข้อมูลนี้พัฒนาขึ้นสำหรับผลิตภัณฑ์และบริการที่มีในประเทศสหรัฐอเมริกา

IBM อาจไม่นำเสนอผลิตภัณฑ์ การบริการ หรือคุณลักษณะที่กล่าวถึงใน เอกสารนี้ในประเทศอื่น โปรดปรึกษาตัวแทน IBM ในท้องถิ่น ของคุณสำหรับข้อมูลเกี่ยวกับผลิตภัณฑ์และการบริการที่มีอยู่ใน พื้นที่ของคุณขณะนี้ การอ้างอิงใดๆ ถึงผลิตภัณฑ์ โปรแกรม หรือการบริการของ IBM ไม่ได้มีวัตถุประสงค์ที่จะระบุหรือตีความว่าสามารถใช้ได้เฉพาะผลิตภัณฑ์ โปรแกรม หรือการบริการของ IBM เพียงอย่างเดียวเท่านั้น ผลิตภัณฑ์ โปรแกรม หรือบริการที่ทำงานได้เท่าเทียมกัน ซึ่งไม่ละเมิดทรัพย์สินทางปัญญาของ IBM อาจสามารถใช้แทนกันได้อย่างไรก็ตาม เป็นความรับผิดชอบของผู้ใช้ ในการประเมิน และตรวจสอบการทำงาน ของผลิตภัณฑ์ โปรแกรม หรือเซอร์วิส ที่ไม่ใช่ของ IBM

IBM อาจมีสิทธิบัตรหรือเอกสารซึ่งอยู่ระหว่างดำเนินการขอสิทธิบัตร ที่ครอบคลุมถึงหัวข้อที่ได้กล่าวไว้ในเอกสารนี้ การตกแต่งเอกสารนี้ไม่ได้ทำให้คุณได้รับใบอนุญาตสำหรับ สิทธิบัตรนี้ คุณสามารถสอบถามเกี่ยวกับไลเซนส์, โดยเขียนและส่งไปที่:

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

US

INTERNATIONAL BUSINESS MACHINES CORPORATION นำเสนอสิ่งพิมพ์นี้ "ตามสภาพ" โดยไม่มี การรับประกันประเภทใดๆ ไม่ว่าโดยชัดแจ้งหรือโดยนัย รวมถึงแต่ไม่จำกัดเฉพาะ การรับประกัน โดยนัยถึงการไม่ละเมิดสิทธิ การขายได้ หรือความเหมาะสมสำหรับวัตถุประสงค์เฉพาะ บางขอบเขตอำนาจไม่อนุญาตให้ปฏิเสธการรับประกันโดยชัดแจ้งหรือโดยนัย ในบางกรณี ดังนั้นข้อความนี้อาจไม่บังคับใช้ในกรณีของคุณ

ข้อมูลนี้อาจเกิดความผิดพลาดทางเทคนิค หรือการพิมพ์ ซึ่งจะมีการแก้ไขข้อมูลเหล่านั้นเป็นระยะๆ ซึ่งข้อมูลที่ถูกแก้ไขนี้จะอยู่ในเอกสารฉบับ ถัดไป IBM อาจปรับปรุงและ/หรือเปลี่ยนแปลงในผลิตภัณฑ์ และ/หรือโปรแกรมที่อธิบายในสิ่งพิมพ์นี้ได้ตลอดเวลา โดยไม่ต้องแจ้งให้ทราบ

การอ้างอิงใดๆ ในข้อมูลนี้โดยอ้างอิงเว็บไซต์ที่ไม่ใช่ของ IBM ระบุไว้เพื่อความสะดวกเท่านั้น และ ไม่ได้เป็นการสนับสนุน เว็บไซต์ดังกล่าวในลักษณะใดๆ เอกสารประกอบที่อยู่ในเว็บไซต์เหล่านั้น ไม่ได้เป็นส่วนหนึ่งของเอกสารประกอบสำหรับผลิตภัณฑ์ IBM นี้ และการใช้งานเว็บไซต์เหล่านั้น ถือเป็นการเสี่ยงของคุณเอง

IBM อาจใช้หรือแจกจ่ายข้อมูลใดๆ ที่คุณได้ให้ไว้ด้วยวิธีใดๆ ที่เชื่อว่ามีเหมาะสมโดยไม่มีข้อผูกมัดใดๆ กับคุณ

ข้อมูลประสิทธิภาพ และตัวอย่างลูกค้าที่ระบุมีการนำเสนอสำหรับวัตถุประสงค์การสาธิตเท่านั้น ผลลัพธ์ของประสิทธิภาพการทำงานจริงอาจขึ้นอยู่กับคอนฟิกูเรชันและเกณฑ์การทำงานที่ ระบุเฉพาะ

ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ได้จัดทำโดย IBM เป็นข้อมูลที่ได้รับมาจาก ผู้จำหน่ายของผลิตภัณฑ์เหล่านั้น จากการประกาศที่มีการเผยแพร่ หรือจากแหล่งข้อมูลที่มีอยู่ในสาธารณะอื่นๆ IBM ไม่ได้ทดสอบผลิตภัณฑ์ดังกล่าว และไม่สามารถยืนยัน ความถูกต้องของประสิทธิภาพ ความเข้ากันได้ หรือการเรียกร้องอื่นใดที่เกี่ยวข้องกับ ผลิตภัณฑ์ที่ไม่ใช่ของ IBM คำถาม เกี่ยวกับความสามารถในการทำงานของผลิตภัณฑ์ที่มีชื่อของ IBM ควรส่งไปที่ ชัฟฟลายเออร์ของผลิตภัณฑ์เหล่านั้น

ข้อความใดๆ ที่เกี่ยวข้องกับทิศทางในอนาคตและเจตจำนงค์ของ IBM อาจมีการเปลี่ยนแปลง หรือเพิกถอนได้โดยไม่ต้องแจ้งล่วงหน้า และนำเสนอเฉพาะเป้าหมาย และวัตถุประสงค์เท่านั้น

ราคาของ IBM ทั้งหมดที่แสดงเป็นราคาจำหน่ายปลีกที่แนะนำของ IBM เป็นราคาปัจจุบัน และอาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ ราคาของผู้แทนจำหน่ายอาจแตกต่างกันออกไป

โดยข้อมูลนี้มีวัตถุประสงค์เพื่อใช้ในการวางแผนเท่านั้น ข้อมูล เหล่านี้อาจมีการเปลี่ยนแปลงก่อนที่จะมีคำอธิบาย ของผลิตภัณฑ์ออกมา

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

ถ้าคุณดูเอกสารฉบับนี้โดยใช้สำเนาชั่วคราว รูปและสีของรูปประกอบอาจไม่แสดงให้เห็น

ห้ามทำซ้ำภาพวาดและข้อมูลเฉพาะที่อยู่ในเอกสารนี้ทั้งหมด หรือบางส่วนโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจาก IBM

IBM ได้จัดทำข้อมูลนี้เพื่อใช้กับเครื่องที่ระบุเฉพาะ IBM ไม่ได้แสดงว่าข้อมูลนี้เหมาะสมสำหรับวัตถุประสงค์อื่น

ระบบคอมพิวเตอร์ของ IBM มีกลไกที่ออกแบบมา เพื่อลดความเป็นไปได้ที่จะเกิดความเสียหาย หรือการสูญหายของข้อมูลที่ไม่สามารถตรวจพบ อย่างไรก็ตาม ความเสี่ยงเหล่านี้ยังไม่สามารถจำกัดให้หมดไปได้ ผู้ใช้ที่ประสบการณเกี่ยวกับ สัญญาณ ขาดหายที่ไม่ได้วางแผนไว้ล่วงหน้า ระบบขัดข้อง ระบบกำลังไฟฟ้าที่ไม่แน่นอนหรือขาดหาย หรือส่วนประกอบขัดข้อง ควรจะทำการตรวจสอบความถูกต้องของการดำเนินการ และข้อมูลที่ถูกบันทึกหรือส่งโดยระบบ ในช่วงเวลาหรือเวลาใกล้เคียงกับที่ สัญญาณขาดหายหรือขัดข้อง นอกจากนี้ ในการดำเนินงานที่มีความอ่อนไหว หรือสำคัญมาก ผู้ใช้ควรมีขั้นตอน เพื่อให้มั่นใจว่ามีการตรวจสอบข้อมูลอย่างเป็นอิสระก่อนที่จะเชื่อถือ ข้อมูลเหล่านั้น ผู้ใช้ควรทำการตรวจสอบ เว็บไซต์การสนับสนุนของ IBM เป็นระยะๆ สำหรับข้อมูลล่าสุด และโปรแกรมฟิร์มแวร์สำหรับ ระบบ และซอฟต์แวร์ที่เกี่ยวข้อง

ข้อความการให้สัตยาบัน

ผลิตภัณฑ์นี้ อาจไม่ได้รับการรับรองในประเทศของคุณสำหรับการเชื่อมต่อกับ สื่อใดๆ ก็ตามไปยังอินเทอร์เน็ตของเครือข่าย โทรคมนาคมแบบพบลิงก์ การรับรองเพิ่มเติมอาจเป็นข้อบังคับตามกฎหมายก่อนทำการเชื่อมต่อ ดังกล่าว โปรดติดต่อตัวแทน หรือผู้ค้าปลีกของ IBM ถ้ามีคำถามใดๆ

คุณลักษณะความสามารถเข้าถึงได้สำหรับเซิร์ฟเวอร์ IBM Power Systems

คุณลักษณะความสามารถเข้าถึงได้ช่วยให้ผู้ใช้ที่ทุพพลภาพ เช่น มีเคลื่อนไหวได้จำกัด หรือมีการมองเห็นที่จำกัด สามารถใช้เนื้อหาทางด้าน เทคโนโลยีสารสนเทศได้เป็นผลสำเร็จ

ภาพรวม

เซิร์ฟเวอร์ IBM Power Systems มีคุณลักษณะความสามารถเข้าถึงได้ที่สำคัญต่อไปนี้:

- การดำเนินการคีย์บอร์ดอย่างเดียว
- การดำเนินการที่ใช้โปรแกรมอ่านหน้าจอ

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

เอกสารคู่มือผลิตภัณฑ์ทางออนไลน์ของเซิร์ฟเวอร์ IBM Power Systems ใน IBM Knowledge Center เปิดใช้งาน สำหรับความสามารถเข้าถึงได้ คุณลักษณะความสามารถเข้าถึงได้ของ IBM Knowledge Center มีการอธิบายไว้ใน ส่วน ความสามารถเข้าถึงได้ของวิธีใช้ IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility)

การนำทางของคีย์บอร์ด

ผลิตภัณฑ์นี้ใช้คีย์การนำทางมาตรฐาน

ข้อมูลอินเตอร์เฟซ

ส่วนติดต่อผู้ใช้ของเซิร์ฟเวอร์ IBM Power Systems ไม่มีเนื้อหาที่กะพริบ 2 - 55 ครั้งต่อวินาที

ส่วนติดต่อผู้ใช้ของเว็บเซิร์ฟเวอร์ IBM Power Systems อาศัยสไตลชีตแบบต่อเรียงเพื่อจัดแสดง เนื้อหาอย่างสมบูรณ์ และเพื่อให้สามารถใช้งานได้ง่าย แอปพลิเคชันจัดเตรียมวิธีที่เทียบเท่าสำหรับ ผู้ใช้ที่มีการมองเห็นจำกัดเพื่อใช้ค่าติดตั้งหน้าจอของระบบ รวมถึงโหมดความเปรียบต่างสูง คุณสามารถควบคุมขนาดฟอนต์ โดยใช้ค่าติดตั้งอุปกรณ์ หรือเว็บเบราว์เซอร์

ส่วนติดต่อผู้ใช้ของเว็บเซิร์ฟเวอร์ IBM Power Systems มีแลนด์มาร์กการนำทาง WAI-ARIA ที่คุณสามารถใช้เพื่อนำทางไปยังพื้นที่นำทางในแอปพลิเคชันอย่างรวดเร็ว

ซอฟต์แวร์ของผู้จำหน่าย

เซิร์ฟเวอร์ IBM Power Systems มีซอฟต์แวร์ของผู้จำหน่ายบางรายการที่ไม่ได้ครอบคลุมภายใต้ข้อตกลงไลเซนส์ของ IBM IBM ไม่มีส่วนรับรองเกี่ยวกับคุณลักษณะความสามารถเข้าถึงได้ของผลิตภัณฑ์เหล่านี้ โปรดติดต่อผู้จำหน่ายสำหรับข้อมูลความสามารถเข้าถึงได้เกี่ยวกับผลิตภัณฑ์เหล่านี้

ข้อมูลความสามารถเข้าถึงได้ที่เกี่ยวข้อง

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

TTY เซอร์วิส

800-IBM-3383 (800-426-3383)

(ภายในอเมริกาเหนือ)

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

ข้อควรพิจารณานโยบายความเป็นส่วนตัว

ผลิตภัณฑ์ซอฟต์แวร์ของ IBM ซึ่งรวมถึงซอฟต์แวร์เป็นเซอร์วิสโซลูชัน (“ข้อเสนอซอฟต์แวร์”) อาจใช้คุกกี้หรือเทคโนโลยีอื่นเพื่อรวบรวมข้อมูลการใช้งานผลิตภัณฑ์เพื่อช่วยปรับปรุงประสิทธิภาพของผู้ใช้ชั้นปลาย และปรับแต่งการโต้ตอบให้เหมาะกับผู้ใช้ชั้นปลายแต่ละราย หรือสำหรับวัตถุประสงค์อื่นในหลายกรณี ไม่มีข้อมูลที่สามารถระบุตัวบุคคลได้ที่รวบรวมโดยข้อเสนอซอฟต์แวร์ Software Offering ของเรารายตัว สามารถใช้คุณเก็บรวบรวมข้อมูลที่ระบุเฉพาะบุคคลได้ ถ้าข้อเสนอซอฟต์แวร์นี้ใช้คุกกี้เพื่อรวบรวมข้อมูลที่สามารถระบุเฉพาะบุคคลข้อมูลเฉพาะเกี่ยวกับการใช้คุกกี้ของข้อเสนอนี้มีการระบุไว้ด้านล่าง

ขึ้นอยู่กับกำหนดคอนฟิกร์ที่ปรับใช้ Software Offering นี้ อาจใช้คุกกี้เซสชันที่รวบรวมชื่อผู้ใช้ของกำหนดคอนฟิกร์แต่ละรายและ IP แอดเดรสสำหรับการจัดการเซสชัน คุกกี้เหล่านี้สามารถปิดใช้งาน แต่การปิดใช้งานคุกกี้เหล่านี้ยังจะยกเลิกฟังก์ชันที่คุกกี้เปิดใช้งานด้วย

หากกำหนดคอนฟิกร์ที่ปรับใช้สำหรับ Software Offering มีให้คุณในฐานะลูกค้า ความสามารถในการรวบรวมข้อมูลการระบุตัวบุคคลจากผู้ใช้งานคุกกี้และเทคโนโลยีอื่น คุณควรค้นหาคำแนะนำด้านกฎหมายเกี่ยวกับกฎหมายใดๆ ที่มีผลบังคับใช้กับการรวบรวมข้อมูลดังกล่าว รวมถึงข้อกำหนดสำหรับการแจ้งให้ทราบและยอมรับ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เทคโนโลยีต่างๆ รวมถึงคุกกี้ โปรดดูที่นโยบายความเป็นส่วนตัวของ IBM ที่ <http://www.ibm.com/privacy> และถ้อยแถลงความเป็นส่วนตัวแบบออนไลน์ของ IBM ที่ <http://www.ibm.com/privacy/details> ส่วนที่ชื่อ “Cookies, Web Beacons and Other Technologies” และ “IBM Software Products and Software-as-a-Service Privacy Statement” ที่ <http://www.ibm.com/software/info/product-privacy>

เครื่องหมายการค้า

IBM ตราสัญลักษณ์ IBM และ ibm.com เป็นเครื่องหมายหรือเครื่องหมายการค้าจดทะเบียนของ International Business Machines Corp., ซึ่งจดทะเบียนในเขตอำนาจศาลหลายแห่งทั่วโลก ชื่อการบริการและผลิตภัณฑ์อื่นๆ อาจจะเป็นเครื่องหมายการค้าของ IBM หรือบริษัทอื่นๆ 2[h* APD20ABD002 16/04/2014]. รายชื่อของเครื่องหมายการค้า IBM ปัจจุบันสามารถดูได้บนเว็บไซต์ ข้อมูลเกี่ยวกับลิขสิทธิ์และเครื่องหมายการค้า at www.ibm.com/legal/copytrade.shtml.

Linux เป็นเครื่องหมายการค้าของ Linus Torvalds ในสหรัฐอเมริกา ประเทศอื่นๆ หรือทั้งคู่

Microsoft และ Windows คือเครื่องหมายการค้าของ Microsoft Corporation ในสหรัฐอเมริกา ประเทศอื่นๆ หรือทั้งสองกรณี

ประกาศเกี่ยวกับการปล่อยกำลังไฟฟ้า

เมื่อแนบมอนิเตอร์กับอุปกรณ์ คุณต้องใช้สายมอนิเตอร์ที่กำหนดให้ และอุปกรณ์ยังต้องการแรงดันไฟฟ้าที่เหมาะสม

คำประกาศเกี่ยวกับผลิตภัณฑ์คลาส A

คำชี้แจงเกี่ยวกับผลิตภัณฑ์คลาส A ต่อไปนี้ใช้กับเซิร์ฟเวอร์ IBM ที่มีตัวประมวลผล POWER8 และคุณลักษณะของตัวประมวลผล ยกเว้นว่าจะกำหนดให้ มีความเข้ากันได้ทางแม่เหล็กไฟฟ้า (EMC) คลาส B ในข้อมูลคุณลักษณะ

ข้อกำหนดของ Federal Communications Commission (FCC)

หมายเหตุ: เครื่องมือนี้ได้รับการทดสอบ และพบว่า เป็นไปตามข้อกำหนดของอุปกรณ์ดิจิทัลคลาส A ตามหมวด 15 ของกฎ FCC ข้อกำหนดเหล่านี้ถูกออกแบบมา เพื่อให้มีการป้องกันในระดับที่สมเหตุสมผลต่อการรบกวนที่เป็นอันตรายเมื่อเครื่องมือถูกใช้งานในสภาพการใช้งานเชิงพาณิชย์ อุปกรณ์นี้สามารถจะสร้าง ใช้งาน และสามารถแผ่คลื่นความถี่วิทยุ และหากไม่ได้ติดตั้งและใช้งานตามคู่มือการใช้งาน อาจเป็นเหตุให้เกิดการรบกวนที่สร้างความเสียหายต่อการสื่อสารทางวิทยุ การทำงานของอุปกรณ์นี้ในบริเวณที่พิกัดอาจก่อให้เกิดการรบกวนที่เป็นอันตราย ในกรณีนี้ ผู้ใช้งานจำเป็นต้องแก้ไขสัญญาณรบกวนโดยที่ควรรับผิดชอบค่าใช้จ่ายด้วยตนเอง

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

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

คำประกาศเกี่ยวกับความสอดคล้องของอุตสาหกรรมประเทศแคนาดา

CANICES-3 (A)/NMB-3(A)

คำประกาศความสอดคล้องของประชาคมยุโรป

ผลิตภัณฑ์นี้สอดคล้องกับข้อกำหนดในการป้องกันของข้อกำหนด EU Council Directive 2014/30/EU ตามร่างกฎหมายของรัฐบาลที่เกี่ยวกับความสามารถในความเข้ากันได้ทางแม่เหล็กไฟฟ้า IBM ไม่รับผิดชอบต่อความผิดพลาดเสียหายใดๆ ตามข้อกำหนดในการป้องกันซึ่งอันเกิดจากการดัดแปลงผลิตภัณฑ์โดยไม่ได้รับการแนะนำ รวมถึงการใช้การ์ดต่างๆ ที่ไม่ใช่ตัวเลือกของ IBM IBM

ข้อมูลติดต่อสำหรับประชาคมยุโรป:

IBM Deutschland GmbH

ระเบียบข้อบังคับทางเทคนิค Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

โทร: +49 800 225 5426

อีเมล: halloibm@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

คำประกาศของสมาคมอุตสาหกรรมเครื่องใช้ไฟฟ้าญี่ปุ่นและเทคโนโลยีสารสนเทศ

คำประกาศนี้อธิบายการปฏิบัติตามวัตต์ลินค่า Japan JIS C 61000-3-2

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

คำประกาศอธิบายของ Japan Electronics and Information Technology Industries Association (JEITA) สำหรับผลิตภัณฑ์ที่มีกำลังไฟฟ้าน้อยกว่าหรือเท่ากับ 20 A ต่อเฟส

高調波電流規格 JIS C 61000-3-2 適合品

แนวทาง JIS C ของญี่ปุ่นสำหรับผลิตภัณฑ์ที่มีกำลังไฟฟ้ามากกว่า 20 A เฟสเดียว

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- ・回路分類：6（単相、PFC 回路付）
- ・換算係数：0

แนวทาง JIS C ของญี่ปุ่นสำหรับผลิตภัณฑ์ที่มีกำลังไฟฟ้ามากกว่า 20 A ต่อเฟส, สามเฟส.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、PFC回路付)
- 換算係数 : 0

คำประกาศเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (EMI) - สาธารณรัฐประชาชนจีน

声 明

此为 A 级产品, 在生活环境中, 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) - ประเทศไทย

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

คำประกาศเกี่ยวกับความสอดคล้องของประเทศเยอรมนี

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

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

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

EN 55022 / EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

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

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

ข้อมูลทั่วไป:

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

คำชี้แจงเกี่ยวกับการรบกวนของคลื่นแม่เหล็กไฟฟ้า (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

ข้อกำหนดของ Federal Communications Commission (FCC)

อุปกรณ์นี้ได้รับการทดสอบ และพบว่าเป็นไปตามข้อกำหนดของอุปกรณ์ดิจิทัลคลาส B ตามหมวดที่ 15 ของ กฎ FCC ข้อกำหนดเหล่านี้ถูกออกแบบมาเพื่อให้การป้องกันในระดับที่สมเหตุสมผลต่อการรบกวนที่เป็นอันตราย เมื่ออุปกรณ์ถูกใช้งานในสภาพการใช้งานเชิงพาณิชย์

อุปกรณ์นี้สามารถที่จะก่อให้เกิด ใช้งาน และแผ่คลื่นความถี่วิทยุ และถ้าหากไม่ได้ติดตั้งและใช้งานตามคู่มือการใช้งาน อาจเป็นเหตุให้เกิดการรบกวนที่สร้างความเสียหายต่อการสื่อสารทางวิทยุ อย่างไรก็ตาม ไม่สามารถรับรองได้ว่าการรบกวนจะไม่เกิดขึ้นใน การติดตั้ง

หากอุปกรณ์นี้ ทำให้เกิดการรบกวนที่สร้างความเสียหายต่อการรับสัญญาณวิทยุ หรือโทรทัศน์ ซึ่งสามารถตรวจสอบโดยการ ปิดและเปิดอุปกรณ์ ผู้ใช้ จะได้รับการแนะนำให้พยายามแก้ไขการรบกวนโดยใช้หนึ่งในมาตรการต่อไปนี้:

- การปรับเปลี่ยน หรือย้ายเสาอากาศ

- เพิ่มระยะห่างระหว่างอุปกรณ์กับตัวรับสัญญาณ
- เชื่อมอุปกรณ์ไปยังปลั๊กบนวงจรที่ต่างจากวงจรที่ตัวรับเชื่อมต่ออยู่
- ปรีกษา IBM- ตัวแทนจำหน่ายที่ได้รับสิทธิจาก IBM หรือตัวแทนบริการ เพื่อขอความช่วยเหลือ

สายเคเบิลและตัวเชื่อมต่อที่ได้รับการหุ้มฉนวน และมีการเดินสายดินเอาไว้เรียบร้อยแล้ว จะต้องถูกนำมาใช้งาน เพื่อให้เป็นไปตามข้อกำหนดต่างๆ ในเรื่องการแผ่สัญญาณของ FCC สายเคเบิลและตัวเชื่อมต่อที่เหมาะสมสามารถหาได้จากตัวแทนจำหน่ายที่ได้รับสิทธิจาก IBM IBM- IBM ไม่มีส่วนรับผิดชอบต่อสัญญาณรบกวนเครื่องรับวิทยุหรือโทรทัศน์ที่เกิดขึ้นจากการเปลี่ยนแปลงหรือปรับแต่งอุปกรณ์นี้โดยไม่ได้รับอนุญาต การเปลี่ยนแปลงหรือปรับแต่งโดยไม่ได้รับอนุญาต อาจทำให้สิทธิในการใช้งานอุปกรณ์นี้ของผู้ใช้เป็นโมฆะ

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

คำประกาศเกี่ยวกับความสอดคล้องของอุตสาหกรรมแคนาดา

CANICES-3 (B)/NMB-3(B)

คำประกาศเกี่ยวกับความสอดคล้องของประชาคมยุโรป

ผลิตภัณฑ์นี้สอดคล้องกับข้อกำหนดในการป้องกันของข้อกำหนด EU Council Directive 2014/30/EU ตามร่างกฎหมายของรัฐบาลที่เกี่ยวกับความสามารถในความเข้ากันได้ทางแม่เหล็กไฟฟ้า IBM ไม่รับผิดชอบต่อความผิดพลาดเสียหายใดๆ ตามข้อกำหนดในการป้องกันซึ่งอันเกิดจากการดัดแปลงผลิตภัณฑ์โดยไม่ได้รับการแนะนำ รวมถึงการใช้การ์ดต่างๆ ที่ไม่ใช่ตัวเลือกของ IBM IBM

ข้อมูลติดต่อในประชาคมยุโรป:

IBM Deutschland GmbH

ระเบียบข้อบังคับทางเทคนิค Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

โทร: +49 800 225 5426

email: halloibm@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

คำประกาศของสมาคมอุตสาหกรรมเครื่องใช้ไฟฟ้าญี่ปุ่นและเทคโนโลยีสารสนเทศ

คำประกาศนี้อธิบายการปฏิบัติตามวัตต์ลินค่า Japan JIS C 61000-3-2

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

คำประกาศอธิบายของ Japan Electronics and Information Technology Industries Association (JEITA) สำหรับผลิตภัณฑ์ที่มี
กำลังไฟฟ้าน้อยกว่าหรือเท่ากับ 20 A ต่อเฟส

高調波電流規格 JIS C 61000-3-2 適合品

แนวทาง JIS C ของญี่ปุ่นสำหรับผลิตภัณฑ์ที่มีกำลังไฟฟ้ามากกว่า 20 A เฟสเดียว

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6 (単相、P F C回路付)
- 換算係数 : 0

แนวทาง JIS C ของญี่ปุ่นสำหรับผลิตภัณฑ์ที่มีกำลังไฟฟ้ามากกว่า 20 A ต่อเฟส, สามเฟส.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、P F C回路付)
- 換算係数 : 0

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

คำประกาศเกี่ยวกับความสอดคล้องของประเทศเยอรมนี

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

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

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.

New Orchard Road

Armonk, New York 10504

โทรศัพท์: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH

Technical Relations Europe, Abteilung M456

206 ระบบพลังงาน: การติดตั้งและตั้งค่า Hardware Management Console

IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

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

ข้อตกลงและเงื่อนไข

คำอนุญาตในการใช้เอกสารเหล่านี้เป็นไปตามข้อกำหนด และเงื่อนไขต่อไปนี้

ความสามารถในการใช้งาน: ข้อกำหนดและเงื่อนไขเหล่านี้ เป็นข้อกำหนดและเงื่อนไขเพิ่มเติมในเรื่องของเงื่อนไขการใช้งานสำหรับเว็บไซต์ผู้ผลิต 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 ไม่มีคำอนุญาต ไลเซนส์ หรือสิทธิ์อื่นใด ที่ได้ให้สิทธิ์ไว้ ทั้งโดยแจ้ง หรือโดยนัย กับเอกสารหรือข้อมูลใดๆ เนื้อหา ซอฟต์แวร์ หรือทรัพย์สินทางปัญญาที่มีอยู่ในที่นี้

ผู้ผลิต ขอสงวนสิทธิ์ในการเพิกถอนคำอนุญาตที่ให้ไว้ในที่นี้เมื่อใดก็ตามที่พิจารณาแล้วว่าการใช้เอกสารเหล่านี้ก่อนให้เกิดความเสียหาย ต่อผลประโยชน์ของบริษัท หรือเมื่อ IBM ได้พิจารณาแล้วว่าไม่มีการปฏิบัติตามข้อกำหนดข้างต้นไว้อย่างเหมาะสม

คุณไม่สามารถดาวน์โหลด ส่งออก หรือทำการส่งออกข้อมูลนี้เข้าได้ ยกเว้นได้ปฏิบัติตามกฎหมายและข้อบังคับที่กำหนดไว้ รวมถึงกฎหมายและข้อบังคับในการส่งออกทั้งหมดของสหรัฐอเมริกา

ผู้ผลิตไม่ขอรับประกันเกี่ยวกับเนื้อหาของเอกสารเหล่านี้ เอกสารเหล่านี้จัดเตรียมไว้ "ตามสภาพที่เป็น" โดยไม่มีการรับประกันใดๆ ไม่ว่าจะเป็นโดยเปิดเผยหรือโดยนัย รวมถึงแต่ไม่จำกัดเพียงการรับประกันโดยนัยของการขายสินค้า การไม่ละเมิด และความเหมาะสม สำหรับวัตถุประสงค์เฉพาะทาง



พิมพ์ในสหรัฐอเมริกา