Power Systems

Hardware Management Console 설치 및 구성

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에 v 페이지의 『안전 주의사항』, 93 페이지의 『 주의사항 』, *IBM* 시스템 안전 주의사항 매뉴얼(G229-9054) 및 *IBM* 환경 주의사항 및 사용자 안내서(Z125–5823)를 읽으십시오.

이 개정판은 새 개정판에서 별도로 명시하지 않는 한 IBM® Hardware Management Console 버전 9 릴리스 1 유지보수 레벨 930 및 모든 후속 릴리스와 수정에 적용됩니다.

© Copyright International Business Machines Corporation 2017, 2019.

목차

안전 주의사항

이 안내서 전체에 안전 주의사항이 인쇄되어 있습니다.

- **위험** 주의사항은 치명적일 수 있거나 인체에 극도로 위험한 상황에 대해 주의를 환기시킵니다.
- **경계** 주의사항은 일부 기존 상태로 인해 인체에 위험할 수 있는 상황에 대해 주의를 환기시킵니다.
- **주의** 주의사항은 프로그램, 장치, 시스템 또는 데이터의 손상 가능성에 대해 주의를 환기시킵니다.

세계 무역 안전 정보

일부 국가에서는 자국어로 제공할 제품 서적에 안전 정보를 포함시키도록 규정하고 있습니다. 귀하의 국가에 이 요구사항이 적용되는 경우에는 안전성 정보 문서를 제품과 함께 운송하는 관련 간행물 패키지(서적, DVD 또는 제품 일부)에 포함하여 제공합니다. 해당 문서의 안전성 정보는 미국 영어 원문을 참조하여 자국어로 제공됩니다. 미국 영문 간행물을 사용하여 본 제품을 설치하거나 작동하거나 서비스하기 전에 반드시 안전성 정보 문서를 숙지해야 합니다. 미국 영문 간행물의 안전성 정보를 정확하게 이해할 수 없는 경우에는 안전성 정보 문서를 참조해야 합니다.

안전성 정보 문서를 교체하거나 추가로 요청하고자 하는 경우에는 전화(IBM Hotline: 1-800-300-8751)로 문의하십시오.

독일 안전 정보

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

레이저 안전 정보

IBM 서버는 레이저 또는 LED를 활용하는 광학 기반의 I/O 카드 또는 피처를 사용할 수 있습니다.

레이저 준수

IBM 서버를 IT 장비 랙의 내부 또는 외부에 설치할 수 있습니다.

위험: 시스템에서 또는 시스템 주변에서 작업 중인 경우 다음의 예방 조치를 따르십시오.

전원, 전화 및 통신 케이블에서 나오는 전기 전압 및 전류는 위해합니다. 감전을 방지하려면 다음을 수행하십시오.

- IBM에서 전원 코드를 제공하는 경우 IBM에서 제공하는 전원 코드만을 사용하여 이 장치에 전원을 연결하십시오. IBM에서 제공하는 전원 코드를 다른 제품에 사용하지 마십시오.
- 전원 조립품을 열거나 수리하지 마십시오.
- 심한 뇌우가 발생할 때 케이블을 연결 또는 연결 해제하거나 이 제품의 설치, 유지보수 또는 재구성을 수행하지 마십시오.
- 이 제품에는 여러 개의 전원 코드가 설비되어 있을 수 있습니다. 모든 위해 전압을 제거하려면 전원 코드를 모두 연결 해제하십시오.
  - AC 전원의 경우 AC 전원에서 모든 전원 코드를 분리하십시오.
  - DC 배전 패널(PDP)을 사용하는 랙의 경우 고객의 DC 전원을 PDP에서 분리하십시오.
- 제품에 전원을 연결하는 경우 모든 전원 케이블이 올바르게 연결되어 있는지 확인하십시오.
  - AC 전원을 사용하는 랙의 경우 모든 전원 코드를 올바르게 연결 및 접지된 콘센트에 연결하십시오. 시스템 정격 플레이트를 참조하여 콘센트가 올바른 전압 및 위상 회전을 제공하는지 확인하십시오.
  - DC 배전 패널(PDP)을 사용하는 랙의 경우 고객의 DC 전원을 PDP에 연결하십시오. DC 전원 및 DC 전원 귀선을 연결할 때 올바른 극성을 사용했는지 확인하십시오.
- 이 제품에 연결할 장비를 올바로 배선된 콘센트에 연결하십시오.
- 가능하면 한 손으로만 신호 케이블을 연결하거나 연결 해제하십시오.

© Copyright IBM Corp. 2017, 2019

- 화재, 물 또는 구조적 손상의 흔적이 있으면 장비를 켜지 마십시오.
- 가능한 모든 위험 조건을 정정할 때까지 시스템의 전원 스위치를 켜려고 시도하지 마십시오.
- 전기 안전 위험이 존재한다고 가정하십시오. 서브시스템 설치 프로세서 중에 모든 연속성, 접지 및 전원 검사를 수행하여 시스템에서 안전 요구사항을 충족하는지 확인하십시오.
- 위험 조건이 존재하는 경우 검사를 중단하십시오.
- 설치 및 구성 프로시저에서 별도로 지시하지 않는 경우 장치 커버를 열기 전에 연결된 AC 전원 코드를 분리하고, 랙 배전 패널(PDP)에 있는 적용 가능한 회로 차단기를 끄고, 모든 통신 시스템, 네트워크 및 모뎀을 분리하십시오.

위험:

- 이 제품 또는 연결된 장치에서 커버를 설치 또는 이동하거나 열 때 다음 절차에서 설명한 바와 같이 케이블을 연결하거나 연결 해제하십시오.

  연결을 해제하려면 다음을 수행하십시오.

  1. 모든 전원을 끄십시오(달리 지시하지 않는 한).
  2. AC 전원의 경우 콘센트에서 전원 코드를 제거하십시오.
  3. DC 배전 패널(PDP)을 사용하는 랙의 경우 PDP에 있는 회로 차단기를 끄고 고객의 DC 전원에서 전원을 제거하십시오.
  4. 커넥터에서 신호 케이블을 제거하십시오.
  5. 장치에서 모든 케이블을 제거하십시오.

  연결하려면 다음을 수행하십시오.

  1. 모든 전원을 끄십시오(달리 지시하지 않는 한).
  2. 장치에 모든 케이블을 연결하십시오.
  3. 커넥터에 신호 케이블을 연결하십시오.
  4. AC 전원의 경우 전원 코드를 콘센트에 연결하십시오.
  5. DC 배전 패널(PDP)을 사용하는 랙의 경우 고객의 DC 전원에서 전원을 복원하고 PDP에 있는 회로 차단기를 켜십시오.
  6. 장치를 켜십시오.

  시스템 내부 및 주변에 날카로운 가장자리, 모서리 및 연결 부분이 존재할 수 있습니다. 장비를 다룰 때 베이거나, 긁히거나, 찔리지 않도록 주의하십시오. (D005)

(R001 파트 1/2):

위험: IT 랙 시스템에서 또는 시스템 주변에서 작업 중인 경우 다음의 예방 조치를 따르십시오.

- 무거운 장비 – 잘못 다룰 경우 신체 상해 또는 장비 손상이 발생할 수 있습니다.
- 랙 캐비닛에서 레벨 조정 패드를 항상 낮게 유지하십시오.
- 지진용 옵션이 설치되는 경우가 아니면 항상 안정장치 브래킷을 랙 캐비닛에 설치하십시오.
- 고르지 않은 면에 기계를 적재할 경우, 위해 상황을 방지하기 위해 항상 랙 캐비닛의 맨 아래에 가장 무거운 장치를 설치하십시오. 항상 랙 캐비닛의 맨 아래부터 시작하여 서버 및 선택적 장치를 설치하십시오.
- 랙 장착형 장치를 선반 또는 작업 공간으로 사용하지 마십시오. 랙 장착형 장치 위에 물건을 올려놓지 마십시오. 또한 랙 장착형 장치에 기대지 말고, 신체를 지지하는 데 이를 사용하지 마십시오(예: 사다리에서 작업하는 경우).

- 각 랙 캐비닛에는 두 개 이상의 전원 코드가 있을 수 있습니다.
  - AC 전원 랙의 경우 수리 중에 전원을 차단하도록 지시하면 랙 캐비닛에 있는 모든 전원 코드를 분리하십시오.

- DC 배전 패널(PDP)을 사용하는 랙의 경우 수리 중에 전원을 차단하도록 지시하면 시스템 장치와 연결된 전원을 제어하는 회로 차단기를 끄거나 고객의 DC 전원을 분리하십시오.

- 랙 캐비닛에 설치된 모든 장치를 동일한 랙 캐비닛에 설치된 전원 장치에 연결하십시오. 하나의 랙 캐비닛에 설치된 장치의 전원 코드 플러그를 다른 랙 캐비닛에 설치된 전원 코드로 연결하지 마십시오.
- 콘센트가 잘못 배선되면 시스템 또는 시스템에 연결된 장치의 금속 부분에 위험한 전압이 흐를 수 있습니다. 전기 충격을 방지하기 위해 콘센트가 올바로 배선 및 접지되었는지 확인하는 것은 고객의 책임입니다. (R001 파트 1/2)

(R001 파트 2/2):

경고:

- 내부 랙 주변 온도가 제조업체에서 권장하는 모든 랙 장착형 장치의 주변 온도를 초과하는 랙에 장치를 설치하지 마십시오.
- 공기 흐름이 방해를 받는 랙에 장치를 설치하지 마십시오. 장치에서 공기 흐름에 사용되는 장치의 측면, 앞면 또는 뒷면에서 공기 흐름이 방해를 받거나 감소되지 않는지 확인하십시오.
- 회로 과부하로 공급장치 배선 또는 과전류 계전기가 방해를 받지 않도록 공급장치 회로 설비에 연결할 때는 주의해야 합니다. 랙에 올바른 전원 연결을 제공하려면 랙의 설비에 있는 등급 레이블을 참조하여 공급장치 회로의 총 전원 요구사항을 판별하십시오.
- (슬라이딩 드로어의 경우) 랙 안정장치 브래킷이 랙에 연결되지 않았거나 랙이 볼트로 바닥면에 고정되지 않은 경우에는 드로어 또는 피처를 빼내거나 이를 설치하지 마십시오. 동시에 두 개 이상의 드로어를 당기지 마십시오. 동시에 두 개 이상의 드로어를 당기면 랙이 불안정해질 수 있습니다.

- (고정 드로어의 경우) 이 드로어는 고정 드로어이며 제조업체에서 달리 지정하지 않는 한, 서비스를 위해 이동해서는 안됩니다. 드로어를 랙에서 부분적으로 또는 완전히 이동하려고 하면 랙이 불안정해지거나 드로어가 랙에서 떨어질 위험이 있습니다. (R001 파트 2/2)

경고: 랙 캐비닛의 상부 위치에서 구성요소를 제거하면 재배치 중 랙 안정성이 향상됩니다. 실내 또는 건물 내에서 채워진 랙 캐비닛을 재배치하는 경우 항상 이러한 일반 지침을 준수하십시오.

- 랙 캐비닛의 맨 위부터 장치를 제거하여 랙 캐비닛의 무게를 줄이십시오. 가능하면 랙 캐비닛을 받았을 때의 구성으로 랙 캐비닛을 복원하십시오. 이 구성을 모르는 경우 다음의 예방 조치를 따라야 합니다.
  - 32U 위치(준수 ID RACK-001) 또는 22U(준수 ID RR001) 이상 위치에 있는 모든 장치를 제거하십시오.
  - 랙 캐비닛의 맨 아래에 가장 무거운 장치가 설치되어 있는지 확인하십시오.
  - 수신된 구성에서 명백히 허용하는 경우를 제외하고 32U(준수 ID RACK-001) 또는 22U(준수 ID RR001) 레벨 아래의 랙 캐비닛에 설치된 장치 사이에 비어 있는 U 레벨이 거의 존재하지 않도록 하십시오.
- 위치를 바꾸는 랙 캐비닛이 랙 캐비닛 스위트의 일부분인 경우 스위트에서 랙 캐비닛을 분리하십시오.
- 재배치 중인 랙 캐비닛에 분리형 아웃리거가 제공되는 경우 캐비닛을 재배치하기 전에 해당 아웃리거를 다시 설치해야 합니다.
- 잠재적인 위해 요소를 제거하려면 이동할 경로를 조사하십시오.
- 선택한 경로가 적재된 랙 캐비닛의 무게를 지지할 수 있는지 확인하십시오. 적재된 랙 캐비닛의 무게에 대해서는 랙 캐비닛과 함께 제공되는 문서를 참조하십시오.
- 모든 도어 입구가 최소한 760 x 230mm(30 x 80인치)인지 확인십시오.
- 모든 장치, 선반, 드로어, 도어 및 케이블이 고정되었는지 확인하십시오.
- 네 개의 레벨 조정 패드를 최고 위치로 올렸는지 확인하십시오.
- 이동 중 랙 캐비닛에 설치된 안정장치 브래킷이 없는지 확인하십시오.

- 10도 이상 기울어진 램프를 사용하지 마십시오.
- 랙 캐비닛이 새 위치에 놓여 있으면 다음 단계를 완료하십시오.
  - 네 개의 레벨 조정 패드를 낮추십시오.
  - 안정장치 브래킷을 랙 캐비닛에 설치하십시오. 또는 지진이 발생하는 환경에서는 랙을 볼트로 바닥면에 고정하십시오.
  - 랙 캐비닛에서 장치를 제거한 경우 랙 캐비닛을 맨 아래부터 맨 위까지 다시 채우십시오.
- 바꿀 위치가 먼 경우 랙 캐비닛을 받았을 때의 구성으로 랙 캐비닛을 복원하십시오. 원래의 포장 재료 또는 이와 같은 재료로 랙 캐비닛을 포장하십시오. 또한 레벨 조정 패드를 낮춰서 캐스터를 팔레트에서 벗겨 올리고 랙 캐비닛을 팔레트에 볼트로 고정하십시오.

(R002)

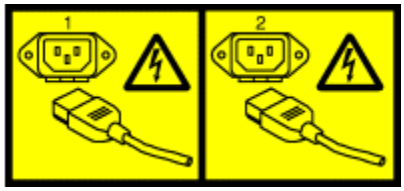
(L001)

위험: 이 레이블이 부착된 구성요소 안에는 위해 전압, 전류 또는 에너지 레벨이 존재합니다. 이 레이블이 있는 커버 또는 보호막을 열지 마십시오. (L001)

(L002)

위험: 랙 장착형 장치를 선반 또는 작업 공간으로 사용하지 마십시오. 랙 장착형 장치 위에 물건을 올려놓지 마십시오. 또한 랙 장착형 장치에 기대지 마십시오. 그리고 이를 사용하여 몸의 자세를 고정하지 마십시오(예: 사다리에서 작업 중인 경우). (L002)

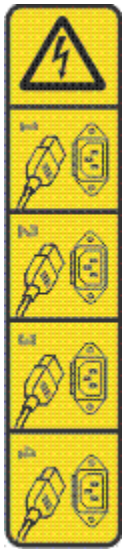
(L003)



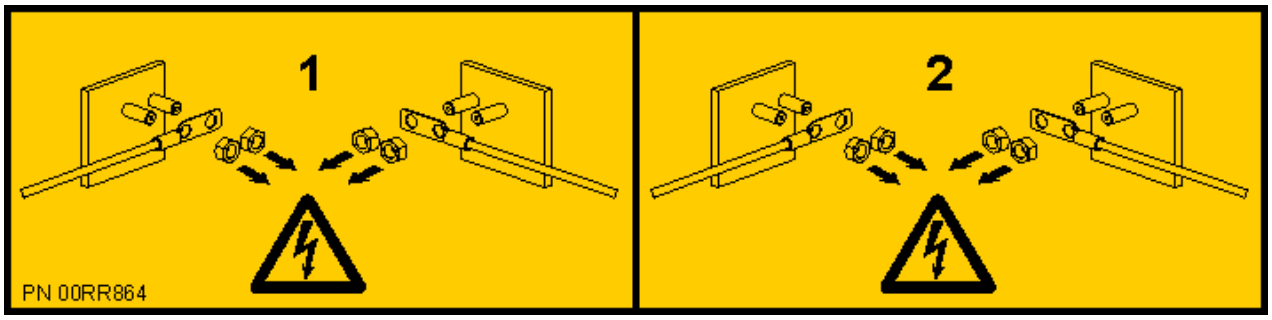
또는

또는

또는



또는



위험: 전원 코드가 여러 개입니다. 이 제품에는 복수의 AC 전원 코드 또는 복수의 DC 전원 케이블이 장착되어 있을 수 있습니다. 위해 전압을 모두 제거하려면 모든 전원 코드 및 전원 케이블을 분리하십시오. (L003)

(L007)

경고: 주변의 표면이 뜨겁습니다. (L007)

(L008)

경고: 근처에 위험한 움직이는 부품이 있습니다. (L008)

모든 레이저는 미국에서 1등급 레이저 제품에 대한 DHHS 21 CFR Subchapter J의 요구사항을 준수하는 것으로 인증되어 있습니다. 미국 외 지역에서는 1등급 레이저 제품으로 IEC 60825를 준수하는 것으로 인증되어 있습니다. 레이저 인증 번호 및 승인 정보에 대해서는 각 부품의 레이블을 참조하십시오.

경고: 이 제품에는 1등급 레이저 제품인 CD-ROM 드라이브, DVD-ROM 드라이브, DVD-RAM 드라이브 또는 레이저 모듈과 같은 장치가 하나 이상 있습니다. 다음 정보를 참고하십시오.

- 커버를 제거하지 마십시오. 레이저 제품의 커버를 제거하면 위험한 레이저 방사선에 노출될 수 있습니다. 이 장치 안에는 수리 가능한 부품이 없습니다.
- 여기에 지정된 것 외의 제어나 조정을 사용하거나 절차를 수행하면 위험한 방사선에 노출될 수 있습니다.

(C026)

경고: 데이터 처리 환경에는 1등급 전원 레벨을 초과하여 작동되는 레이저 모듈과 시스템 링크를 통해 전달되는 장비가 포함될 수 있습니다. 따라서 광케이블의 끝이나 열린 콘센트 안을 보지 마십시오. 분리된 광 섬유의 한 쪽 끝에 빛을 비춘 상태에서 다른 쪽 끝을 보고 광 섬유의 연속성을 확인해도 눈이 손상되지 않을 수 있지만 이 프로시저는 잠재적으로 위험합니다. 따라서 한 쪽 끝에 빛을 비춘 상태에서 다른 쪽 끝을 보고 광 섬유의 연속성을 확인하는 것은 권장하지 않습니다. 광 케이블의 연속성을 확인하려면 광학 광원 및 전력 미터를 사용하십시오. (C027)

경고: 이 제품에는 1M등급 레이저가 있습니다. 광학 기기를 직접 보지 마십시오. (C028)

경고: 일부 레이저 제품에는 삽입된 3A 또는 3B등급 레이저 다이오드가 있습니다. 다음 정보를 참고하십시오.

- 개봉하면 레이저가 방출됩니다.
- 광선을 응시하거나 광학 기기를 직접 보지 말고, 광선에 직접 노출되지 않도록 주의하십시오. (C030)

(C030)

경고: 배터리는 리튬을 함유하고 있습니다. 폭발 가능성을 방지하기 위해 배터리를 가열하거나 충전하지 마십시오.

다음은 금지사항입니다.

- 물 속에 던지거나 침수시키지 마십시오.
- 섭씨 100도(화씨 212도) 넘게 가열하지 마십시오.
- 수리하거나 해체하지 마십시오.

IBM 공인 부품으로만 교환하십시오. 해당 국가 규정에 따라 배터리를 재활용하거나 폐기하십시오. 미국의 경우 IBM은 이 배터리를 수거하는 프로세스를 제공합니다. 자세한 정보를 알려면 1-800-426-4333으로 문의하십시오. 문의하기 전에 배터리 장치의 IBM 부품 번호를 먼저 확인하십시오. (C003)

경고: IBM이 제공하는 공급업체 리프트 도구에 관하여:

- 리프트 도구는 권한이 있는 담당자만 조작할 수 있습니다.
- 리프트 도구는 장치(화물)를 랙 상단으로 들어올리거나, 설치하거나, 제거하는 작업을 지원하기 위해 사용됩니다. 이 도구는 주 램프로 화물을 옮기거나 팔레트 잭, 이동차, 지게차 및 이와 관련된 재배치 수단과 같은 지정된 도구의 대안으로는 사용되지 않습니다. 이를 실행할 수 없는 경우 특별히 훈련된 담당자 또는 서비스(예: 비계장치 또는 운반인)를 사용해야 합니다.
- 사용하기 전에 리프트 도구 운영자 매뉴얼의 컨텐츠를 읽고 완전히 숙지하십시오. 안전 규칙을 읽고, 이해하고, 준수하지 않거나 지시사항을 따르지 않을 경우 재산의 손상 및/또는 신체적 상해가 발생할 수 있습니다. 질문이 있는 경우 공급업체의 서비스 및 지원 센터에 문의하십시오. 로컬 서적 매뉴얼은 시스템에서 제공되는 보관함 부분에 보관해야 합니다. 최신 개정판 매뉴얼은 공급업체의 웹 사이트에 있습니다.
- 사용하기 전에 매번 안정장치 브레이크 기능 확인을 테스트하십시오. 안정장치 브레이크가 작동 중인 상태에서 리프트 도구를 과도하게 움직이거나 돌리지 마십시오.
- 안정장치(브레이크 페달 잭)가 완전히 맞물려 있지 않으면 플랫폼 로드 선반을 올리거나 내리거나 밀지 마십시오. 사용 중이거나 이동 중이 아니면 안정장치 브레이크가 맞물린 상태를 유지하십시오.
- 플랫폼이 올라온 상태에서는 미세한 위치 조정을 제외하고 리프트 도구를 움직이지 마십시오.
- 지정된 적재 용량을 초과하지 마십시오. 적재 용량 차트에서 확장 플랫폼의 가운데 및 가장자리에서의 최대 적재 용량에 관한 내용을 참조하십시오.
- 플랫폼의 중앙에 올바르게 놓여진 경우에만 적재량을 늘리십시오. 슬라이딩 플랫폼 선반의 가장자리에 200lb(91kg)를 초과하여 적재하지 마십시오. 또한 화물의 무게/질량 중심(CoG)을 고려하십시오.
- 플랫폼, 틸트 라이저, 각이 진 장치 설치 웨지 또는 기타 이러한 액세서리 옵션의 코너 적재는 피하십시오. 사용 이전에 제공된 하드웨어만을 사용하여 해당 플랫폼 -- 라이저 틸트, 웨지 등의 옵션을 주 리프트 선반이나 지게차의 4개(4x 또는 제공된 기타 모든 마운팅) 위치에 모두 고정하십시오. 화물 탑재 시 특별한 힘을 가하지 않고도 부드럽게 플랫폼에 올려지거나 내려지도록 설계되어 있으므로 밀거나 기울이지 않도록 주의하십시오. 라이저 틸트 [조정 가능한 앵글링 플랫폼] 옵션은 필요 시에 최종 미세 각도 조정 용도 외에는 항상 수평을 유지하십시오.
- 돌출된 화물 아래 서 있지 마십시오.
- 어느 한 쪽으로 기울어진 비평탄면에서 사용하지 마십시오(주 램프).
- 화물을 겹쳐서 쌓아두지 마십시오.
- 약물 또는 알콜의 영향이 있는 상태에서 조작하지 마십시오.
- 리프트 도구에 대해 사다리를 붙잡고 있지 마십시오(이 도구로 들어올리는 작업과 관련하여 규정된 절차에 따라 이에 대해 별도로 허용된 경우는 제외).
- 기울어질 위험이 있습니다. 플랫폼이 올려진 경우 화물을 밀거나 기대지 마십시오.
- 개인용 리프트 플랫폼 또는 스텝으로 사용하지 마십시오. 올라타지 마십시오.
- 리프트 부품 위에 서 있지 마십시오. 발을 올리지 마십시오.
- 기둥에 기어 오르지 마십시오.
- 손상되거나 오작동 중인 리프트 도구 머신을 조작하지 마십시오.
- 플랫폼 아래에는 눌리거나 끼이는 위험 지점이 있습니다. 사람이나 방해물이 없는 지점에 적은 양의 화물만 허용됩니다. 조작 중에 손이나 발이 닿지 않도록 하십시오.
- 찌르지 마십시오. 포장이 벗겨진 리프트 도구 머신을 팔레트 대차, 잭 또는 지게차로 들어올리거나 움직이지 마십시오.
- 기둥은 플랫폼보다 더 높이 펼쳐집니다. 천장 높이, 케이블 트레이, 스프링클러, 전등 및 기타 높은 위치에 있는 물품에 주의하십시오.
- 화물을 들어올린 상태에서 리프트 도구 머신 주변에 사람이 없는 상태로 방치하지 마십시오.
- 장비가 작동 중인 경우 손, 손가락 및 의복이 장비에 가까이 접근하지 않도록 주의하십시오.

- 윈치는 손으로만 돌리십시오. 윈치 핸들이 한 손으로 쉽게 돌려지지 않을 경우 과적 상태일 가능성이 높습니다. 윈치를 플랫폼 범위의 맨 위 또는 맨 아래를 지나도록 계속 돌리지 마십시오. 과도하게 풀어줄 경우 핸들이 분리되고 케이블이 손상될 수 있습니다. 내리거나 풀어주는 경우 항상 핸들을 잡고 계십시오. 윈치 핸들을 풀기 전에 항상 윈치에 하중이 걸려 있는지 확인하십시오.
- 윈치에서 사고가 발생하는 경우 중상을 입을 수 있습니다. 사람을 운송하지 마십시오. 장비를 올릴 때 딸깍하는 소리가 들렸는지 확인하십시오. 핸들을 풀어주기 전에 윈치가 제자리에 고정되어 있는지 확인하십시오. 이 윈치를 조작하기 전에 지시사항 페이지를 읽으십시오. 윈치가 저절로 풀어지도록 놔두지 마십시오. 자동으로 돌아가는 경우 윈치 드럼 주변의 케이블 랩핑이 고르지 못하게 되고, 케이블이 손상되고, 중상을 입을 수 있습니다.
- IBM 서비스 담당자가 사용할 수 있도록 이 도구를 적절하게 유지보수해야 합니다. IBM에서는 조작 전에 상태를 살펴보고 유지보수 이력을 점검합니다. 부적절한 경우 담당자에게는 도구를 사용하지 않을 권한이 있습니다. (C048)

NEBS(Network Equipment-Building System) GR-1089-CORE에 대한 전원 및 케이블링 정보

다음의 설명은 NEBS(Network Equipment-Building System) GR-1089-CORE를 준수하는 것으로 지정된 IBM 서버에 적용됩니다.

이 장비는 다음 위치에 설치할 수 있습니다.

- 네트워크 통신 설비
- NEC(National Electrical Code)가 적용되는 위치

이 장비의 옥내 포트는 옥내 또는 노출되지 않은 배선이나 케이블로 연결하는 경우에만 적합합니다. 이 장비의 옥내 포트는 옥외 설비(OSP) 또는 해당 배선으로 연결하는 인터페이스에 금속으로 연결할 수 없습니다. 이러한 인터페이스는 옥내 인터페이스(GR-1089-CORE에 설명된 유형 2 또는 유형 4 포트)로만 사용되며 노출된 OSP 케이블링에서 분리시켜야 합니다. 이러한 인터페이스를 OSP 배선에 연결하는 경우 1차 보호기를 추가하는 것으로써 충분히 보호되지 않습니다.

참고: 모든 이더넷 케이블의 양쪽 끝을 차폐하고 접지해야 합니다.

AC 전원 시스템에서는 외부 서지 보호 장치(SPD)를 사용할 필요가 없습니다.

DC 전원 시스템에서는 절연 DC 복귀(DC-I) 설계를 채택합니다. DC 배터리 복귀 터미널은 섀시 또는 프레임 접지에 연결되지 않습니다.

이 DC 전원 시스템은 GR-1089-CORE에서 설명하는 것과 같이 CBN(Common Bonding Network)에 설치하도록 설계되어 있습니다.

Hardware Management Console 설치 및 구성

Hardware Management Console(HMC) 하드웨어를 설치하고 관리 시스템에 연결하며 용도에 맞게 구성하는 방법에 대해 학습합니다. 이러한 태스크는 사용자 스스로 수행하거나 서비스 제공자에게 요청할 수 있습니다. 서비스 제공자에게 요청하는 경우 비용이 부과될 수 있습니다.

HMC 설치 및 구성의 새로운 사항

이 주제 콜렉션에 대한 이전 업데이트 이후 HMC 설치 및 구성 주제에서 새로 추가되거나 크게 변경된 정보에 대해 읽어보십시오.

2019년 2월

- 다음 주제가 추가되었습니다.
  - 82 페이지의 『HMC 보안 설정』
  - 84 페이지의 『향상된 비밀번호 정책』
  - 85 페이지의 『HMC를 보안 설정하는 동안 공통 문제점 해결』
  - 87 페이지의 『보안 프로파일: 일반 개인정보 보호법률(GDPR) 및 PCI-DSS(Payment Card Industry Data Security Standard) 』

2018년 8월

- 다음 주제가 업데이트되었습니다.
  - 24 페이지의 『7063-CR1 HMC 구성』
  - 89 페이지의 『HMC 포트 위치』

2017년 12월

- POWER9 프로세서가 포함되어 있는 IBM Power Systems 서버에 대한 정보가 추가되었습니다.

설치 및 구성 태스크

여러 가지 HMC 설치 및 구성 태스크와 연관된 태스크에 대해 학습합니다.

HMC를 설치 및 구성할 때 완료해야 하는 태스크를 상급 레벨에서 학습합니다. 다른 방식으로 HMC를 설치하고 구성할 수 있습니다. 완료하려는 태스크와 가장 일치하는 상황을 찾으십시오.

참고: POWER9™ 프로세서 기반 서버를 관리하는 경우 HMC가 9.1.0 버전 이상이어야 합니다. 추가 정보는 73 페이지의 『HMC 기계코드 버전 및 릴리스 판별』의 내용을 참조하십시오.

새 서버에 새 HMC 설치 및 구성

새 서버에 새 HMC를 설치 및 구성할 때 완료해야 하는 상위 레벨 태스크에 대해 자세히 학습합니다.

표 *1.* 새 서버에 새 *HMC*를 설치 및 구성할 때 완료해야 하는 태스크.

태스크	관련 정보
1. 정보를 수집하고 설치 전 구성 워크시트를 완료합니다.	48 페이지의 『HMC의 설치 전 구성 워크시트』 47 페이지의 『HMC 구성 준비』
2. 하드웨어의 포장을 해체합니다.	
3. HMC 하드웨어의 케이블을 연결합니다.	23 페이지의 『랙 장착형 7063-CR1 HMC』

© Copyright IBM Corp. 2017, 2019

표 *1.* 새 서버에 새 *HMC*를 설치 및 구성할 때 완료해야 하는 태스크. *(계속)*	
태스크	**관련 정보**
4. 전원 버튼을 눌러 HMC에 전원을 공급합니다.	
5. 로그인하여 HMC 웹 애플리케이션을 시작합니다.	
6. 설정 안내 마법사에 액세스하거나 HMC 메뉴를 사용하여 HMC를 구성합니다.	54 페이지의 『설정 안내 마법사를 통한 단축 경로를 사용하여 HMC 구성 』 54 페이지의 『메뉴를 사용하여 HMC 구성』
7. 서버를 HMC에 연결합니다.	

HMC 코드 업데이트 및 업그레이드

HMC 코드를 업데이트 및 업그레이드할 때 완료해야 하는 상위 레벨 태스크에 대해 학습합니다.

기존 HMC가 있고 HMC 코드를 업데이트 또는 업그레이드하려는 경우 다음과 같은 상위 레벨 태스크를 완료해야 합니다.

표 *2. HMC* 코드를 업데이트하거나 업그레이드할 때 완료해야 하는 태스크.	
태스크	**관련 정보**
1. 업그레이드를 획득합니다.	77 페이지의 『HMC 소프트웨어 업그레이드』
2. 기존 HMC 기계코드 레벨을 확인합니다.	
3. 관리 시스템의 프로파일 데이터를 백업합니다.	
4. HMC 데이터를 백업합니다.	
5. 현재의 HMC 구성 정보를 기록합니다.	
6. 원격 명령 상태를 기록합니다.	
7. 업그레이드 데이터를 저장합니다.	
8. HMC 소프트웨어를 업그레이드합니다.	
9. HMC 기계코드 업그레이드가 정상적으로 설치되었는지 확인합니다.	

기존 설치에 두 번째 HMC 추가

관리 시스템에 두 번째 HMC를 추가할 때 완료해야 하는 상위 레벨 태스크에 대해 자세히 학습합니다.

기존 HMC와 관리 시스템이 있고 두 번째 HMC를 이 구성에 추가하려는 경우 다음 단계를 완료하십시오.

표 *3.* 두 번째 *HMC*를 기존 설치에 추가할 때 완료해야 하는 태스크.	
태스크	**관련 정보**
1. HMC 하드웨어가 HMC 버전 7 코드를 지원하는지 확인합니다.	
2. 정보를 수집하고 설치 전 구성 워크시트를 완료합니다.	48 페이지의 『HMC의 설치 전 구성 워크시트』
3. 하드웨어의 포장을 해체합니다.	
4. HMC 하드웨어의 케이블을 연결합니다.	23 페이지의 『랙 장착형 7063-CR1 HMC』
5. 전원 버튼을 눌러 HMC에 전원을 공급합니다.	
6. HMC에 로그인합니다.	

표 3. 두 번째 *HMC*를 기존 설치에 추가할 때 완료해야 하는 태스크. *(계속)*	
태스크	**관련 정보**
7. HMC 코드 레벨이 일치해야 합니다. 코드가 서로 일치하도록 한 HMC의 코드를 변경합니다.	73 페이지의 『HMC 기계코드 버전 및 릴리스 판별』 77 페이지의 『HMC 소프트웨어 업그레이드』
8. 설정 안내 마법사에 액세스하거나 HMC 메뉴를 사용하여 HMC를 구성합니다.	54 페이지의 『메뉴를 사용하여 HMC 구성』
9. 콜-홈 설정 마법사를 사용하여 이 HMC를 서비스용으로 구성합니다.	66 페이지의 『콜-홈 설정 마법사를 사용하여 서비스 및 지원 센터에 연결할 수 있도록 HMC 구성』
10. 서버를 HMC에 연결합니다.	

HMC 설정

HMC 소프트웨어를 구성하기 전에 HMC 하드웨어를 설정해야 합니다. 데스크 설치 HMC 또는 랙 마운트 HMC의 설정에 대해 자세히 학습합니다.

랙에 7042-CR9 HMC 설치

7042-CR9 Hardware Management Console(HMC)을 랙에 설치하는 방법에 대해 학습합니다.

시작하기 전에

부품 명세를 확인하십시오. 다음 일러스트레이션은 랙 캐비닛에 서버를 설치할 때 필요한 품목을 보여줍니다. 누락되거나 손상된 품목이 있을 경우 구매처에 문의하십시오.

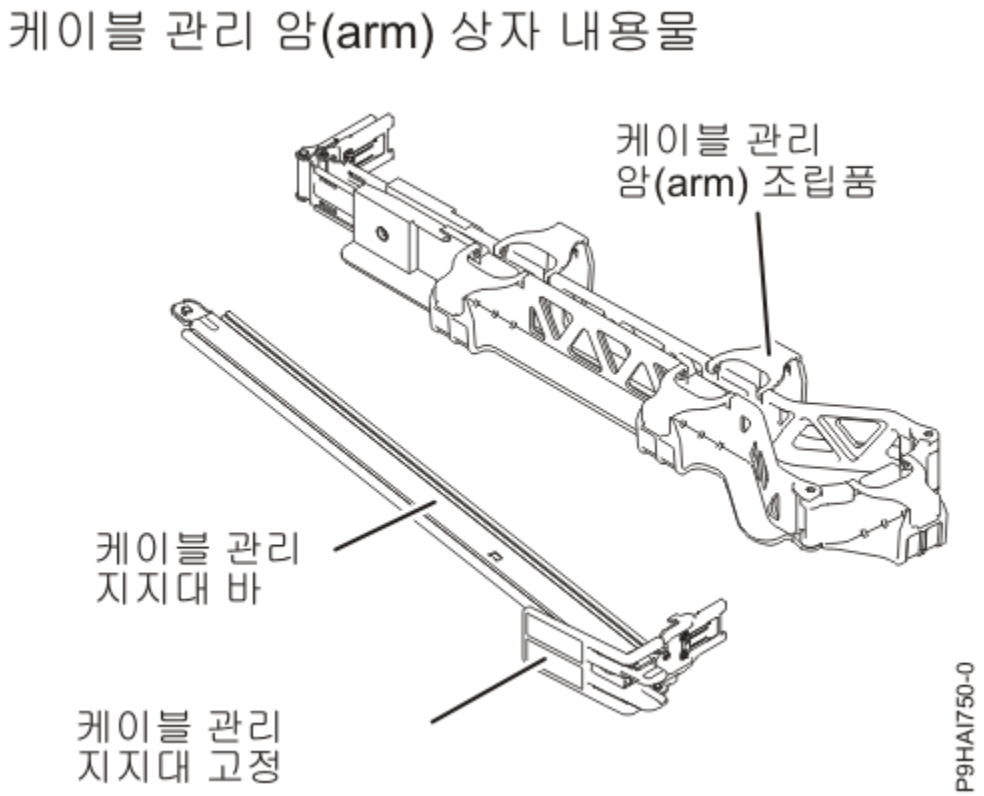


그림 *1.* 케이블 관리 암*(arm)* 상자 내용물

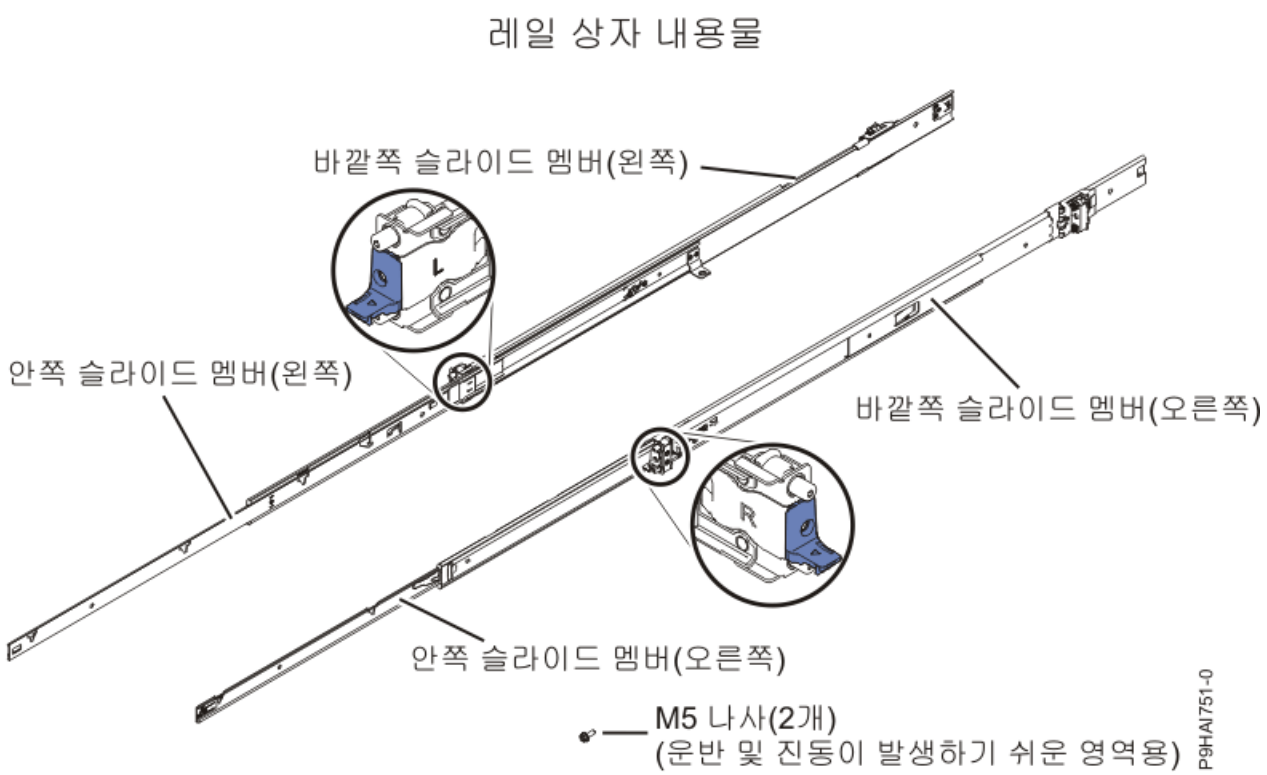


그림 *2.* 레일 상자 내용물

참고: 이 설치에는 슬라이드 레일 상자와 케이블 관리 암 상자가 모두 필요합니다.

이 태스크 정보
7042-CR9 HMC를 랙에 설치하려면 다음 단계를 완료하십시오.

프로시저

1. 랙에서 설치 중인 서버에 따라 사용 가능한 공간을 선택하여 서버를 설치하십시오.

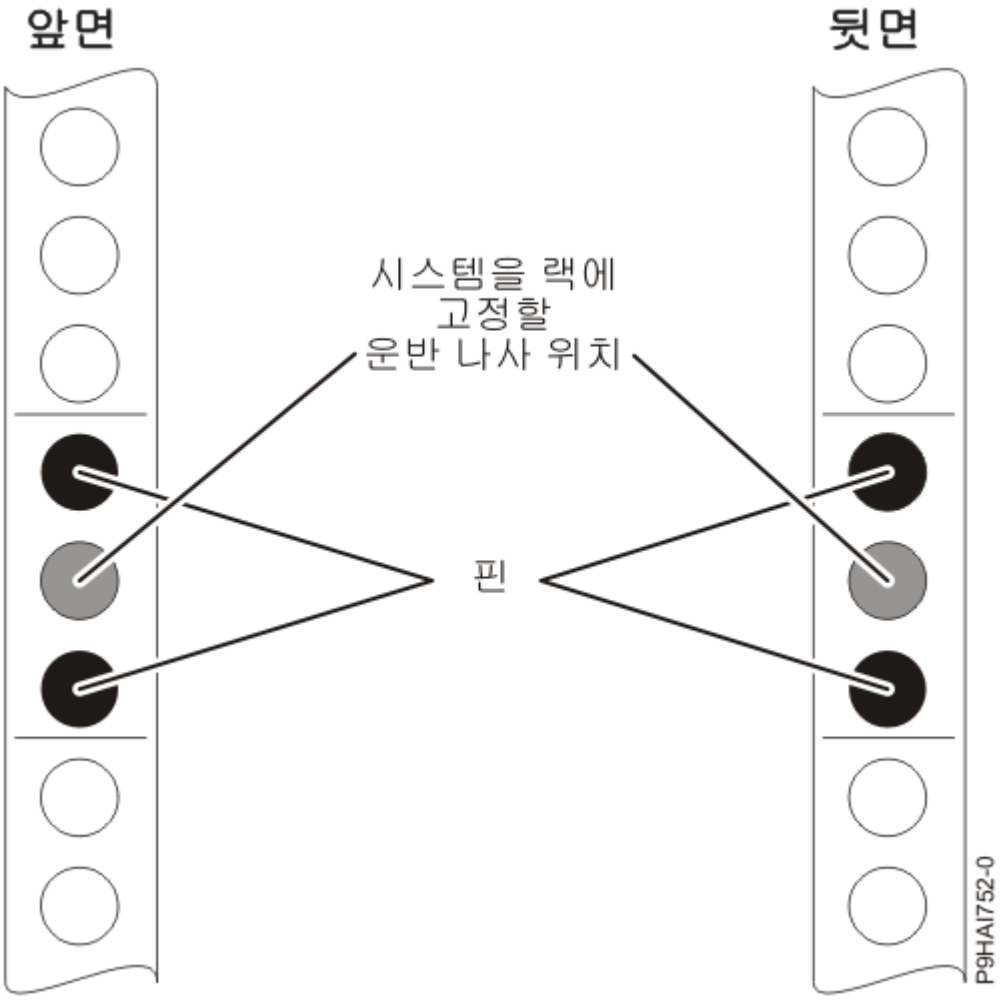


그림 *3.* 랙 공간 식별

참고: 1 단위(1 U)의 공간이 필요하며 1 단위 공간의 맨 아래 단위(U)에 슬라이드 레일이 설치됩니다.

2. 찰깍 소리가 날 때까지 바깥쪽 슬라이드 멤버를 뒤 쪽으로 늘리십시오. 뒷면의 랙 장착 브래킷이 잠금 해제된 위치로 회전됩니다.

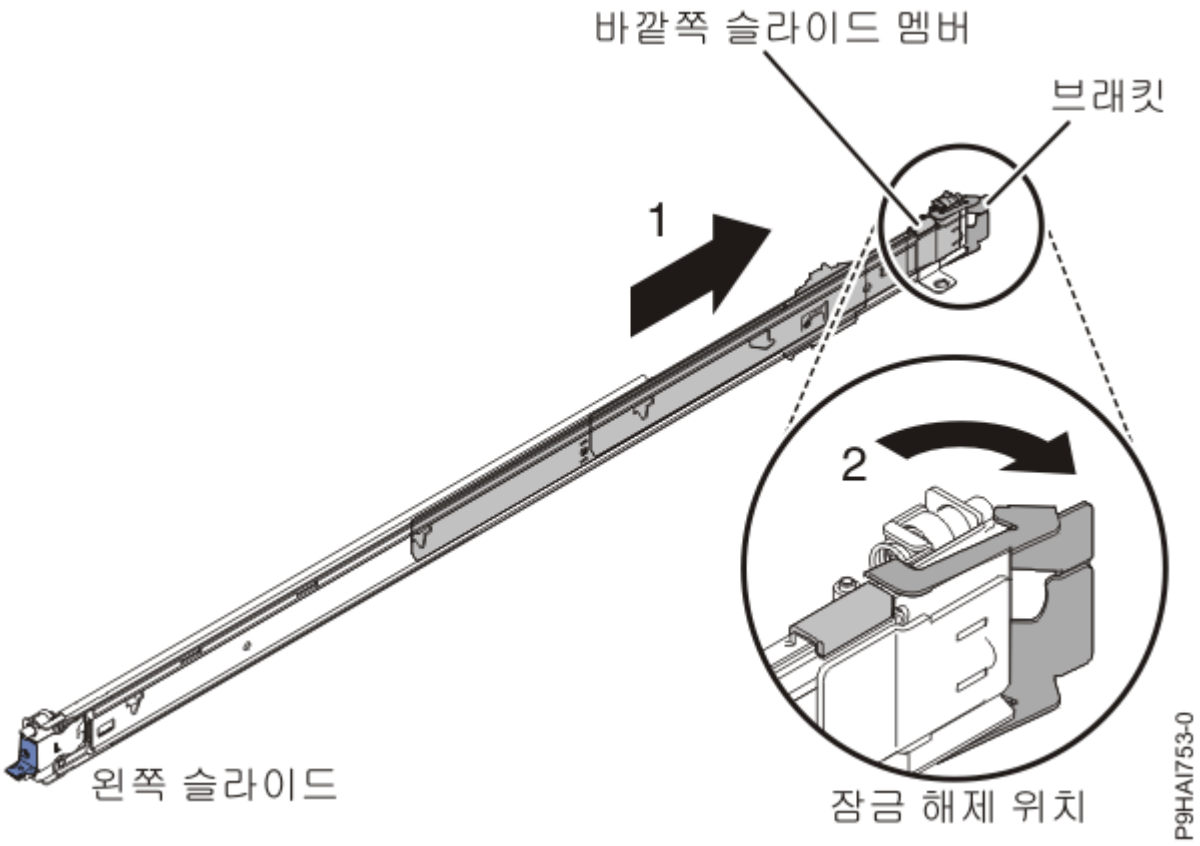


그림 *4.* 슬라이드 레일 및 바깥쪽 슬라이드 멤버

참고: 각 슬라이드 레일 끝에 **R(오른쪽)** 또는 **L(왼쪽)**으로 표시되어 있습니다.

3. 바깥쪽 슬라이드 멤버의 뒷면 끝을 랙의 뒷면에 있는 구멍에 맞추십시오. 핀이 구멍에 들어가도록 핀의 위치를 맞추고 슬라이드를 안으로 미십시오. 두 개의 슬라이드 핀이 EIA 플랜지의 맨 위 및 맨 아래 구멍을 통해 돌출됩니다. 뒷면의 랙 장착 브래킷 잠금이 제자리에 들어갈 때까지 슬라이드를 랙의 뒷면 쪽으로 미십시오.

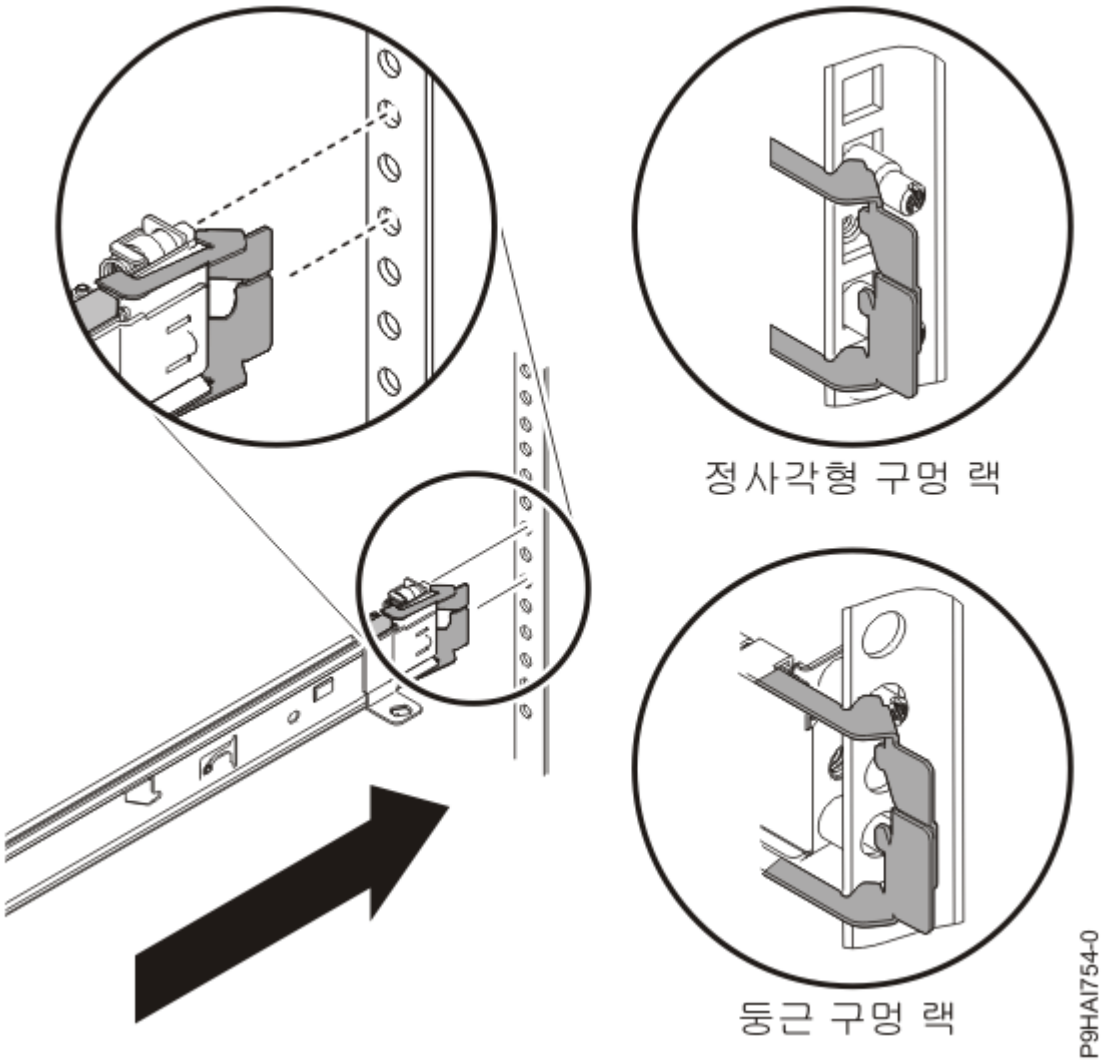


그림 *5.* 랙 후면의 구멍에 핀을 맞춥니다.

4. 앞면 걸쇠를 열기 위치로 돌리고 바깥쪽 슬라이드 멤버의 앞면 끝을 랙의 앞면에 있는 구멍에 맞추십시오. 핀을 EIA 플랜지의 구멍에 맞추고 구멍을 통해 핀이 돌출되도록 슬라이드를 앞으로 당기십시오. 앞면 걸쇠를 닫힘 위치로 회전하여 슬라이드의 앞면을 잠그십시오. 기타 바깥쪽 슬라이드 멤버에 대해서도 2 - 4단계를 반복하십시오.

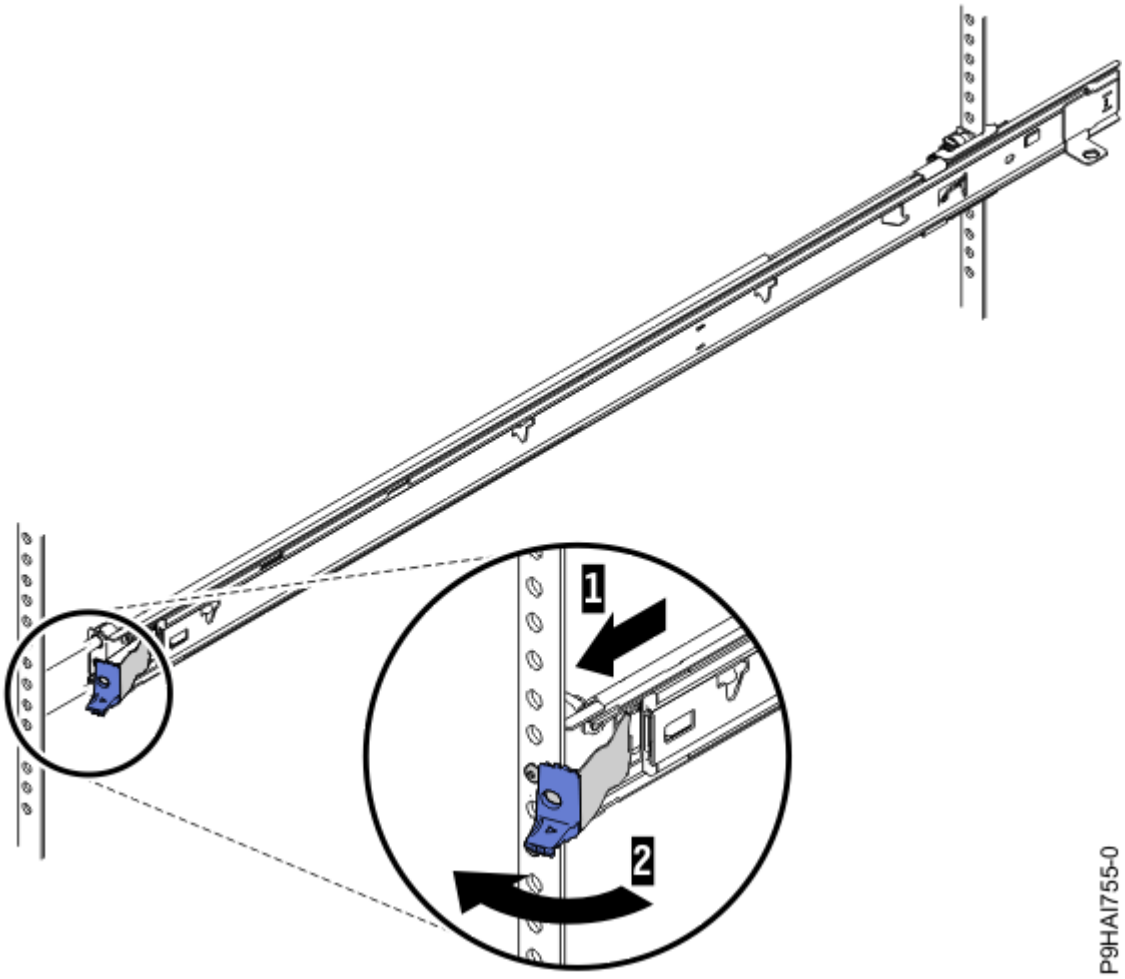


그림 *6.* 앞면 슬라이드 레일 걸쇠

5. 해제 걸쇠**(1)**를 누르십시오. 랙 캐비닛을 이동하거나 랙 캐비닛을 진동 빈발 지역에 설치하는 경우, 서버의 앞면에서 고정 M5 나사**(2)**를 단단히 조이십시오.

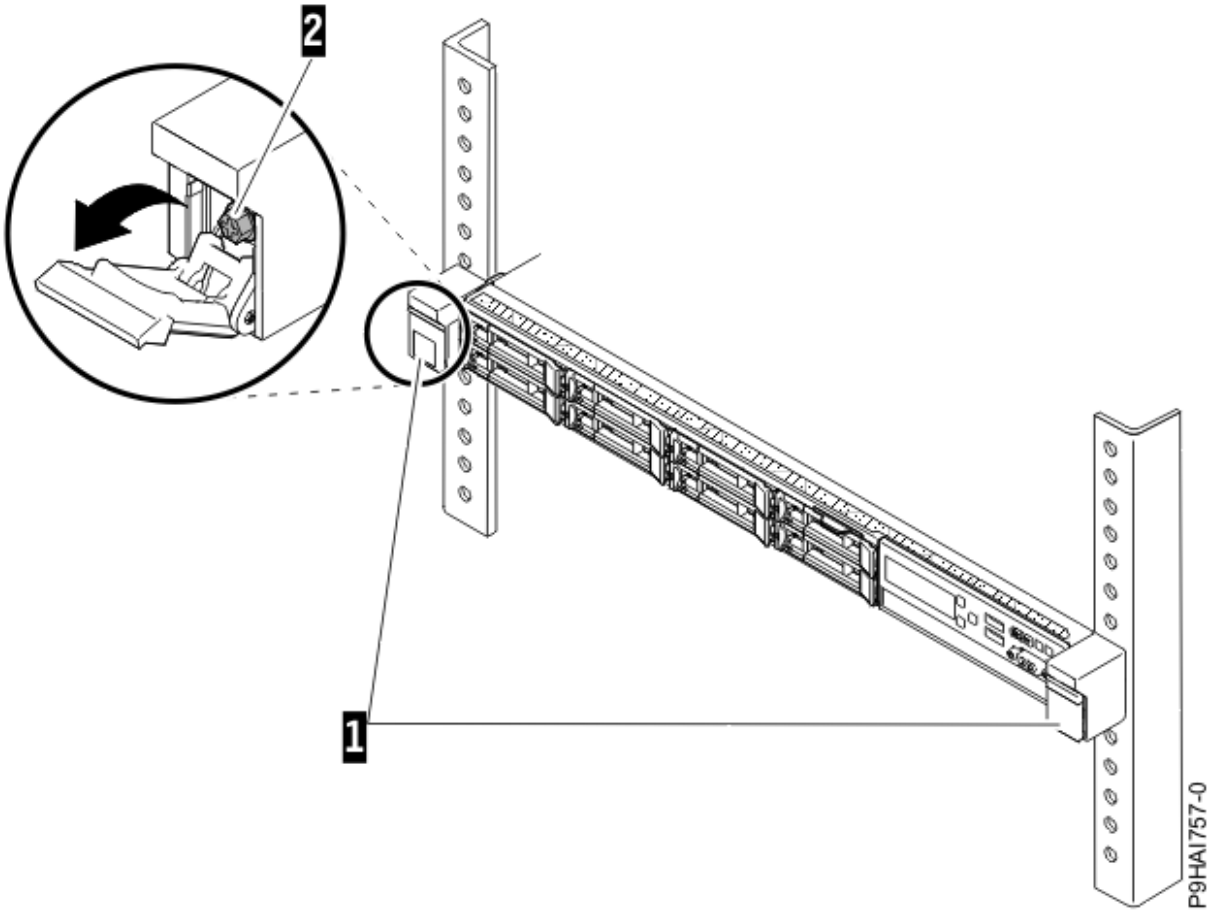


그림 7. 랙 앞면 레일 및 핀

6. 슬라이드 레일이 두 번 찰깍하며 제 위치에 걸릴 때까지 슬라이드 레일**(1)**을 앞으로 당기십시오. 조심스럽게 서버를 들어 올려, 서버의 뒷면 네일 헤드**(2)**가 슬라이드 레일의 슬롯과 정렬되도록 슬라이드 레일 위에 기울여 놓으십시오. 뒷면 네일 헤드가 두 개의 뒷면 슬롯에 끼워질 때까지 서버를 아래로 민 다음 다른 네일 헤드가 슬라이드 레일의 다른 슬롯에 끼워질 때까지 서버의 앞면**(3)**을 천천히 내리십시오. 시스템이 슬라이드 레일에 고정되도록 앞면 걸쇠가 앞면 네일 헤드를 덮는지 확인하십시오.

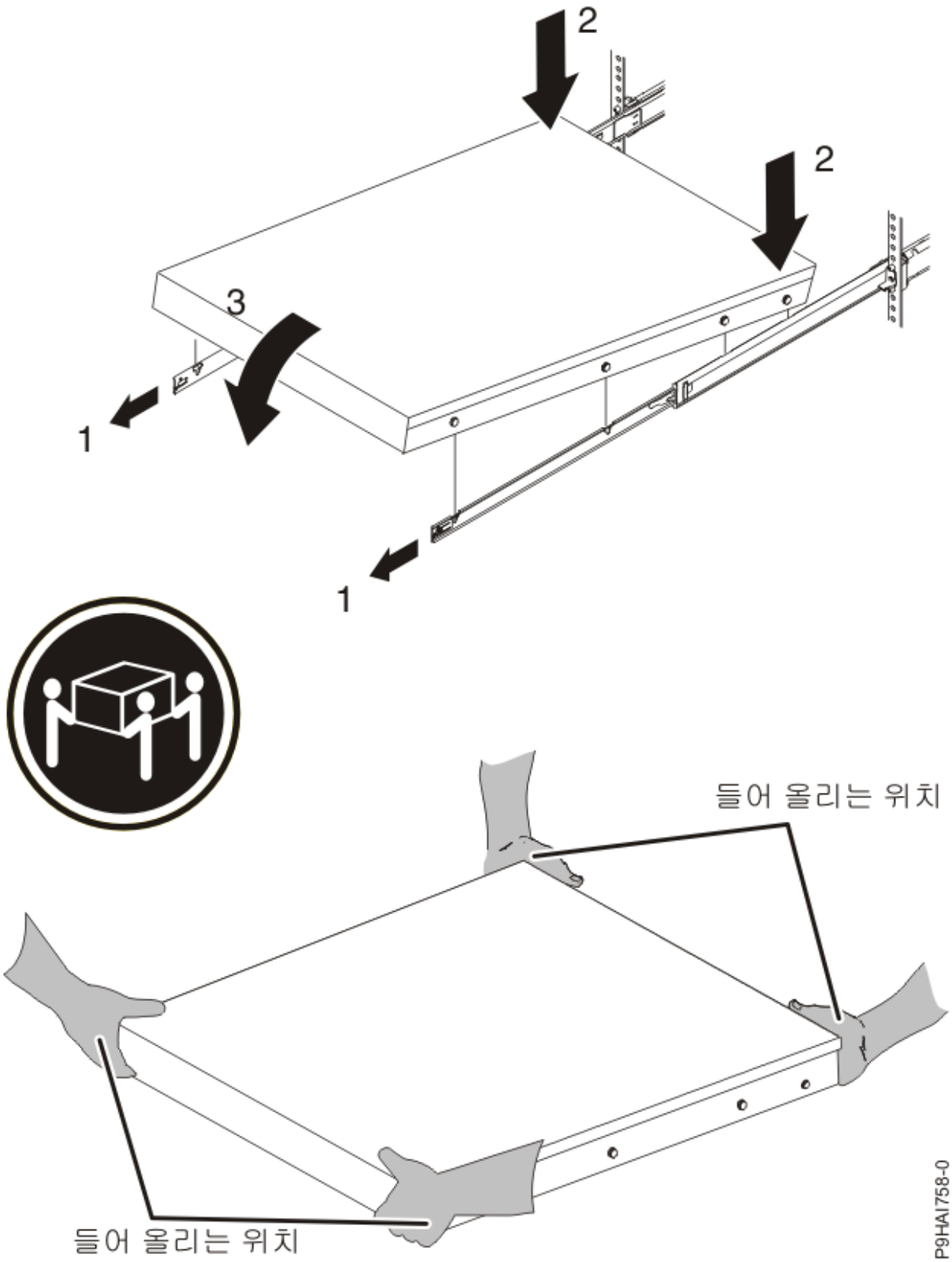


그림 *8.* 확장된 슬라이드 레일, 레일의 슬롯과 정렬된 서버 네일 헤드 및 들어 올리는 위치

참고: 들어 올릴 때 안전 규칙을 따르십시오. 1 U 서버를 설치하는 경우, 서버를 들어 올릴 때 두 사람이 있어야 합니다. 10 페이지의 그림 8에서 설명한 위치에 손을 두어야 합니다.

7. 슬라이드 레일의 잠금 레버**(1)**를 들어 올려 서버**(2)**가 찰깍 소리를 내며 제 위치에 끼워질 때까지 랙으로 미십시오.

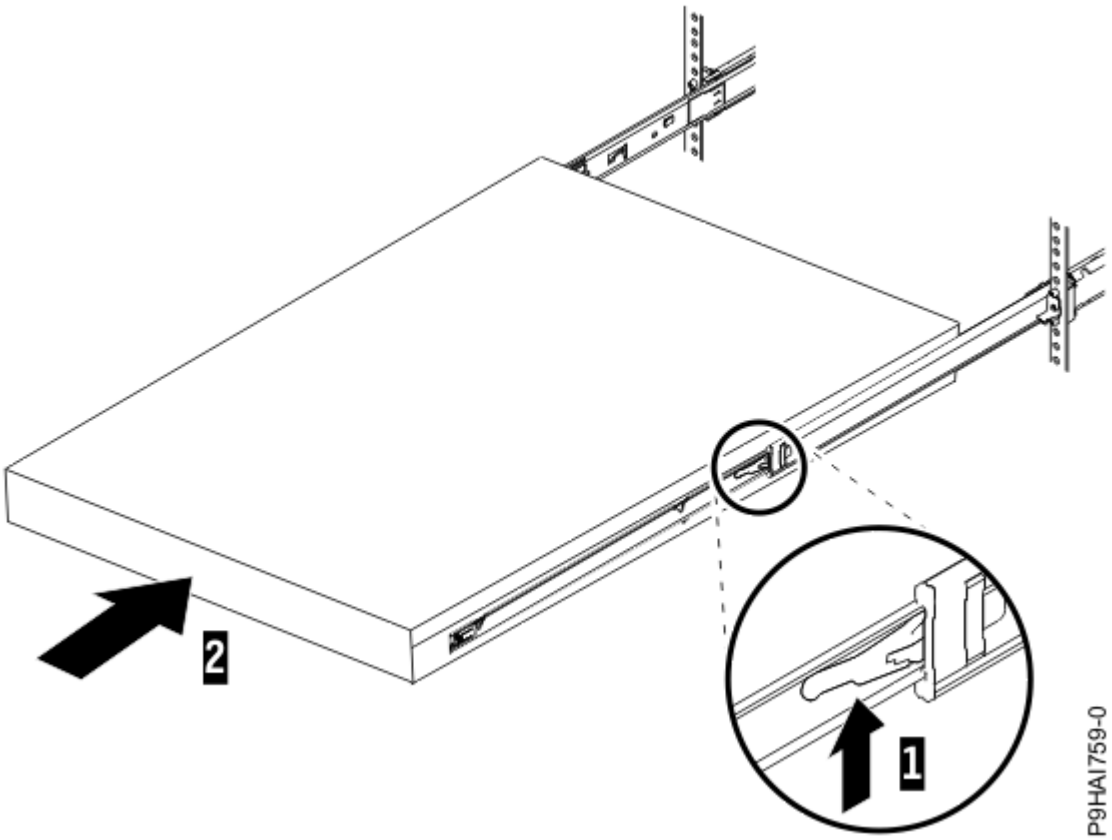


그림 *9*. 해제 걸쇠 및 서버

8. 서버의 어느 쪽에나 케이블 관리 암(arm)을 설치할 수 있습니다. 12 페이지의 그림 10에서는 서버의 왼쪽에 설치된 모습을 표시합니다. 이는 전원 공급 장치에 대한 액세스를 제공하기 위해 전원 공급 장치의 반대쪽에 경첩이 연결되도록 케이블 관리 암(arm)을 설치할 때 가장 적합합니다. 오른쪽에 케이블 관리 암(arm)을 설치하려면 지시사항을 따라 반대편에 하드웨어를 설치하십시오. 슬라이드 레일의 뒷면에 있는 가로 슬롯에 핀**(1)**을 아래로 놓으십시오. 그런 다음 막대의 다른 쪽 끝을 랙**(2)**을 향해 돌리십시오.

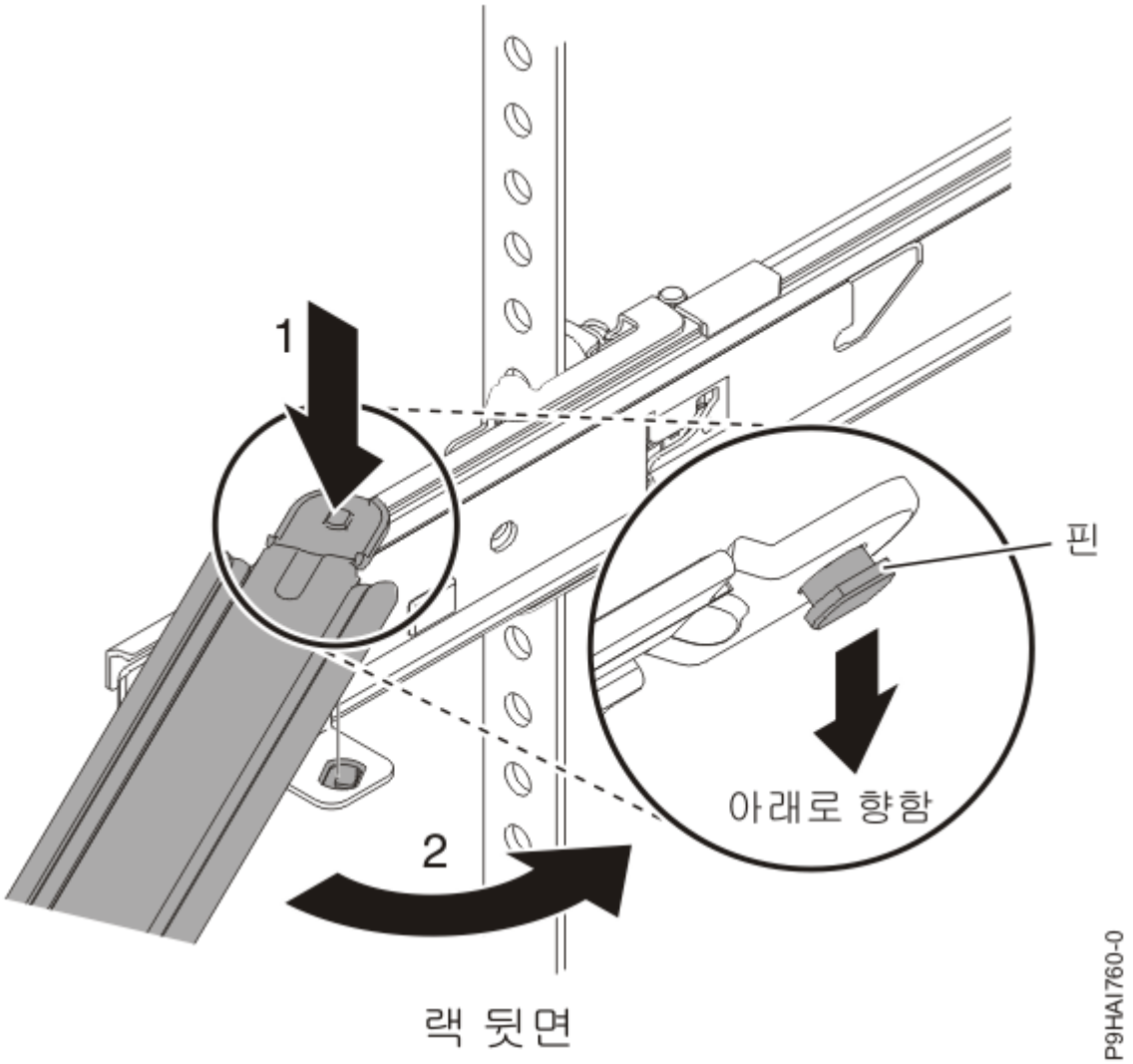


그림 *10.* 지지대 암*(arm)* 연결

참고: 케이블 관리 지지대 막대가 제대로 작동하려면 슬라이드의 맨 위에 있어야 합니다.

9. 지지대 암(arm)의 연결되지 않은 쪽 끝에 대문자 **O**가 있는 케이블 관리 고정 브래킷을 설치하십시오. 지지대 암(arm)이 안전하게 설치되어 있는지 확인하십시오.

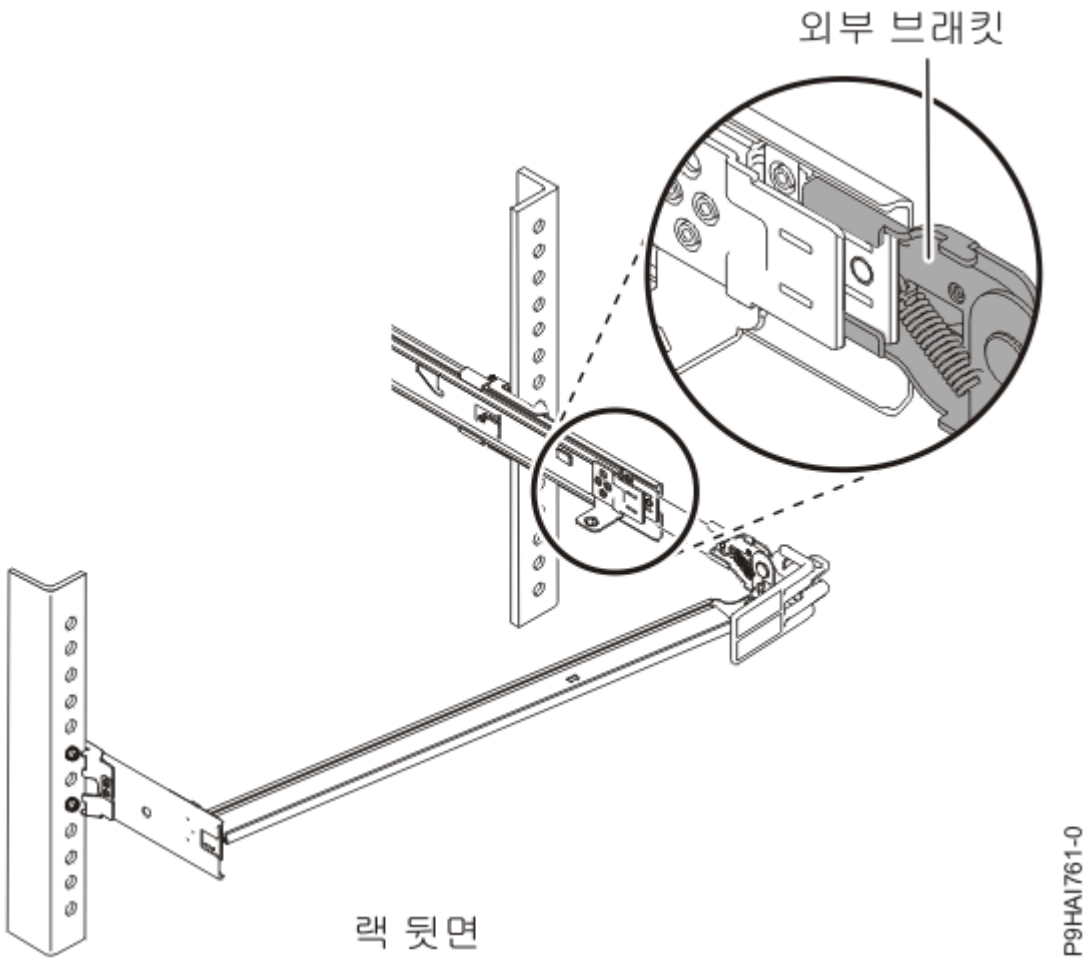


그림 *11.* 슬라이드 레일에 고정 브래킷 연결

참고: 외부 핀을 식별할 수 있도록 케이블 관리 암(arm) 핀에는 대문자 **O**가 인쇄되어 있습니다.

10. 케이블 관리 암(arm)을 지지대 암(arm)에 놓으십시오. 케이블 관리 암(arm) 탭을 슬라이드 레일의 내부 및 외부 슬롯으로 모두 이동하십시오. 제자리에 고정될 때까지 탭을 밀어 넣으십시오.

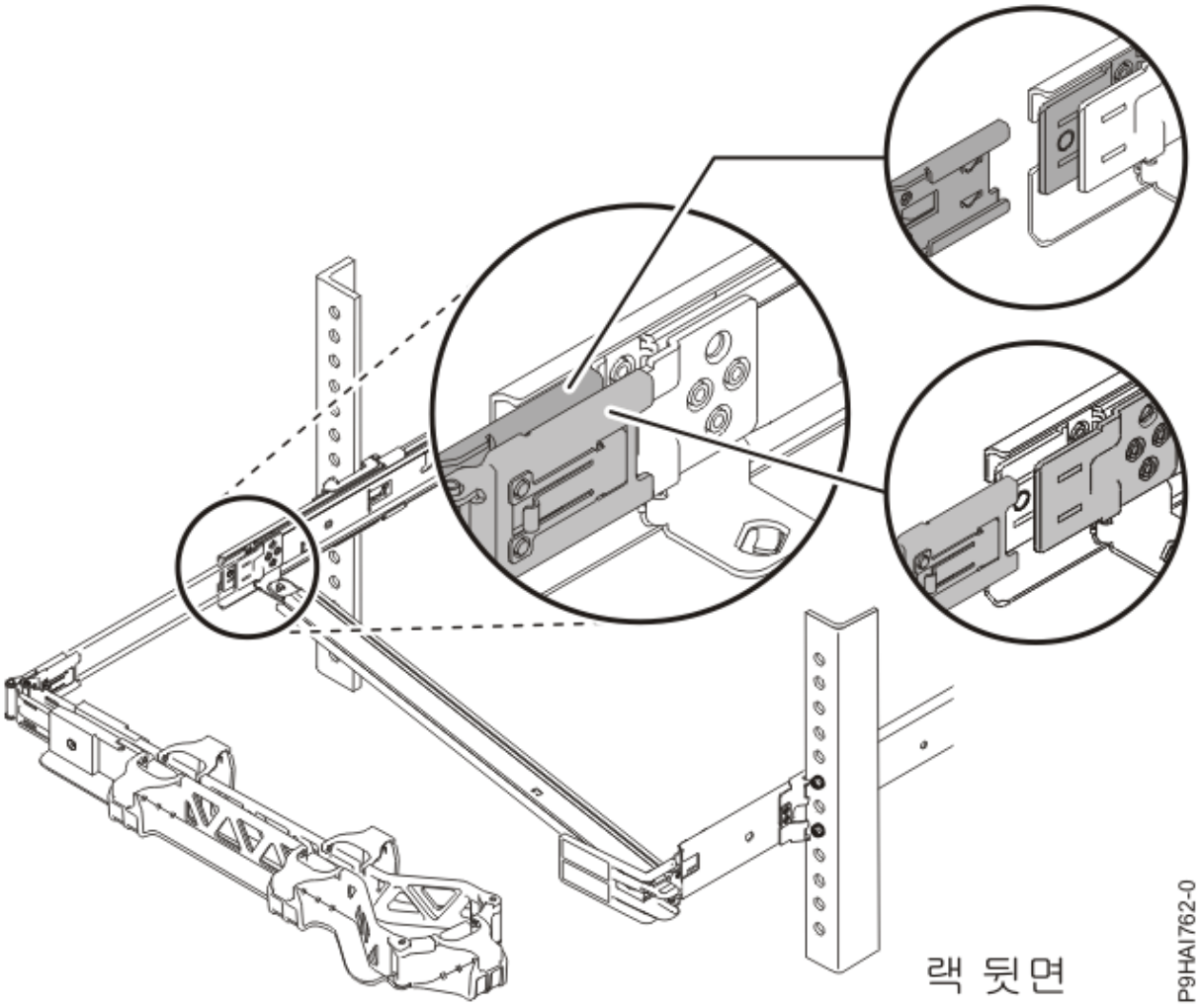


그림 *12.* 케이블 관리 암*(arm)* 연결

11. 케이블 관리 암(arm)을 회전하여 케이블 관리 지지대 암(arm)을 쉽게 열고 닫을 수 있도록 케이블 관리 지지대의 위 및 아래 탭을 밀어서 고정 브래킷을 열 수 있습니다.

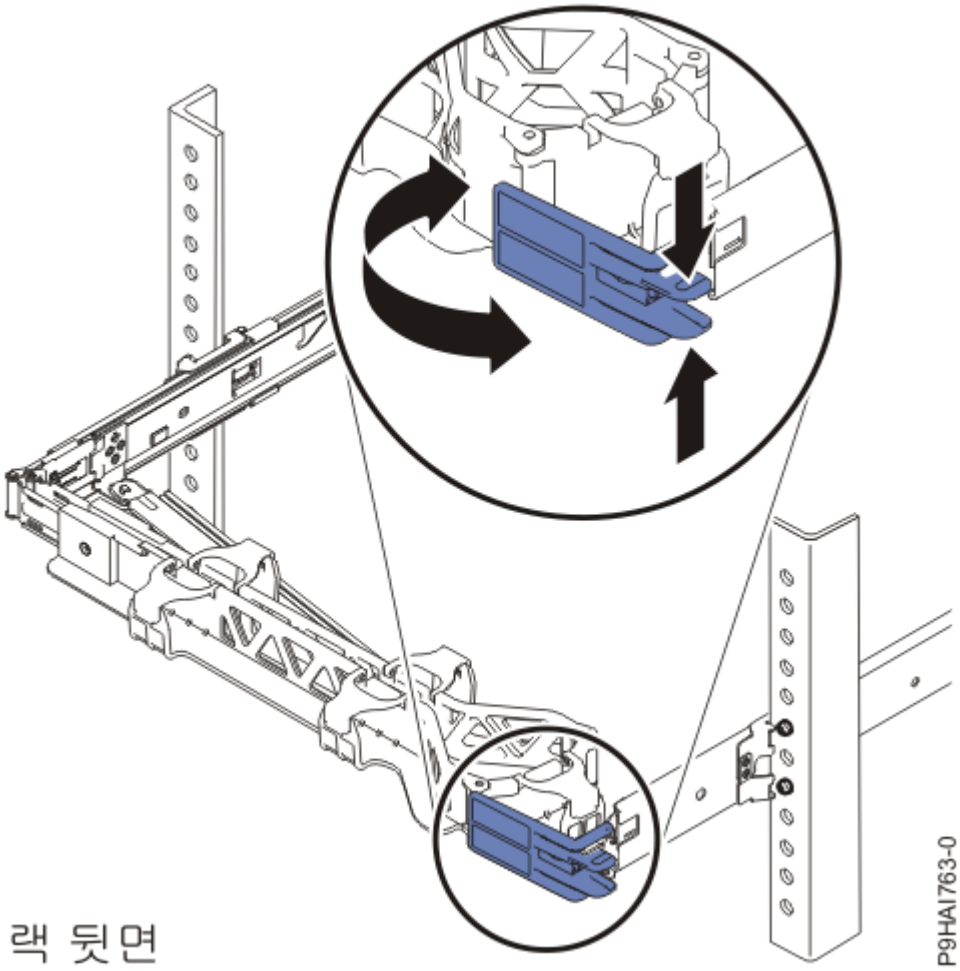


그림 *13.* 케이블 관리 지지대 고정 브래킷

12. 전원 코드와 기타 케이블(키보드, 모니터 및 마우스 케이블 등)을 서버의 뒷면에 연결하십시오. 케이블 관리 암(arm)에 케이블과 전원 코드를 돌려 케이블 타이 또는 벨크로 테이프로 고정하십시오.

    참고: 케이블 스트랩의 위치가 다른 시스템과 약간 다를 수 있습니다. 시스템의 뒷면에 제공된 케이블 스트랩을 사용하여 케이블을 고정하고 늘어지지 않도록 하십시오.

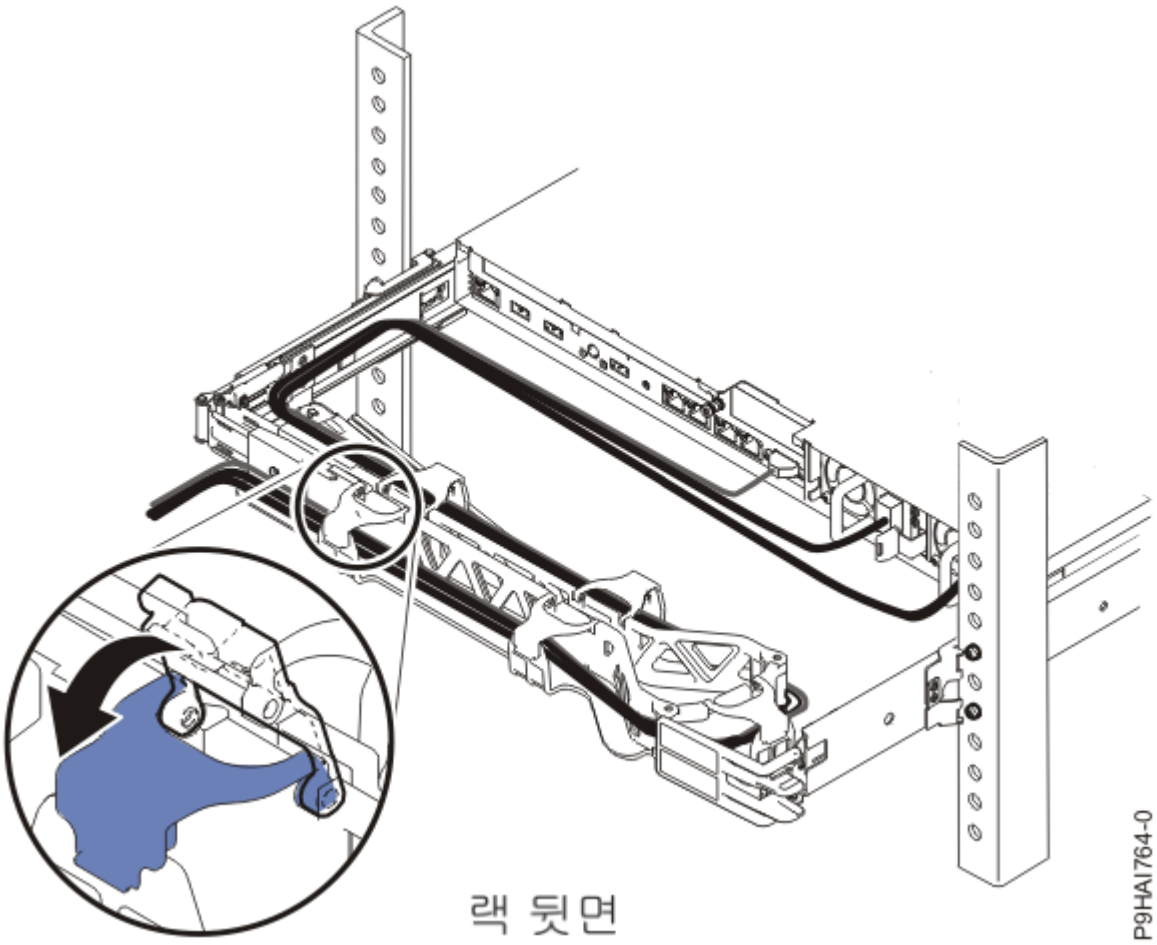


그림 *14.* 전원 코드 연결 및 케이블 배선

13. 케이블 관리 암(arm)이 적절히 이동할 수 있도록 케이블은 케이블 스트랩과 번들로 제공되어야 합니다.

    참고: 케이블이 하단 시스템에 걸리지 않도록 U 공간 아래 늘어지지 않도록 하십시오. 케이블 관리 암(arm)이 움직일 때 케이블이 팽팽히 당겨지는 것을 방지하도록 모든 케이블에 여유를 두십시오.

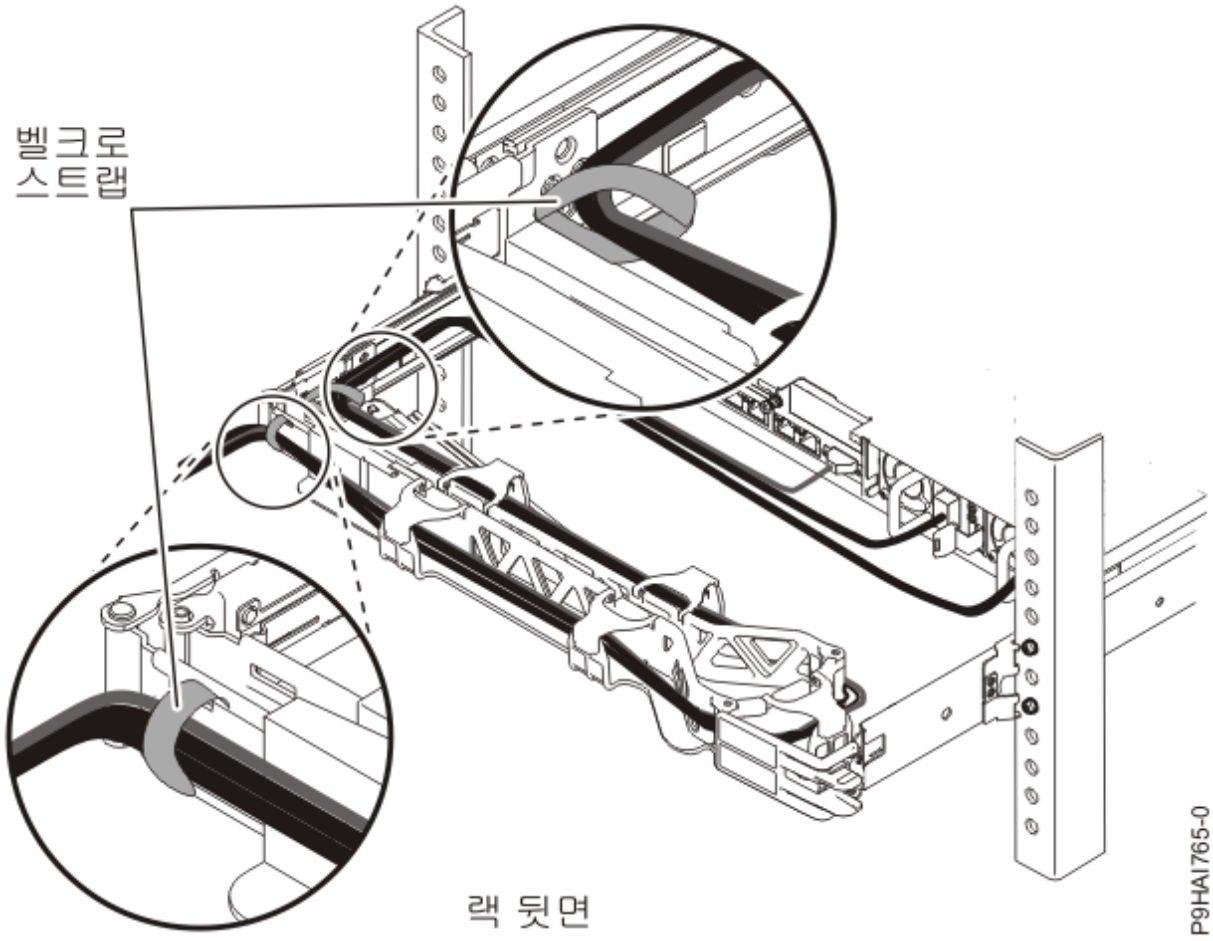


그림 *15.* 벨크로 테이프

14. 시스템이 설치된 랙을 운송하거나 진동 빈발 지역의 경우, 슬라이더의 뒷면에 M5 나사를 삽입하십시오. 필요한 경우, 케이블 타이를 사용하여 케이블 관리 암(arm)의 움직이는 끝을 랙에 고정하십시오.

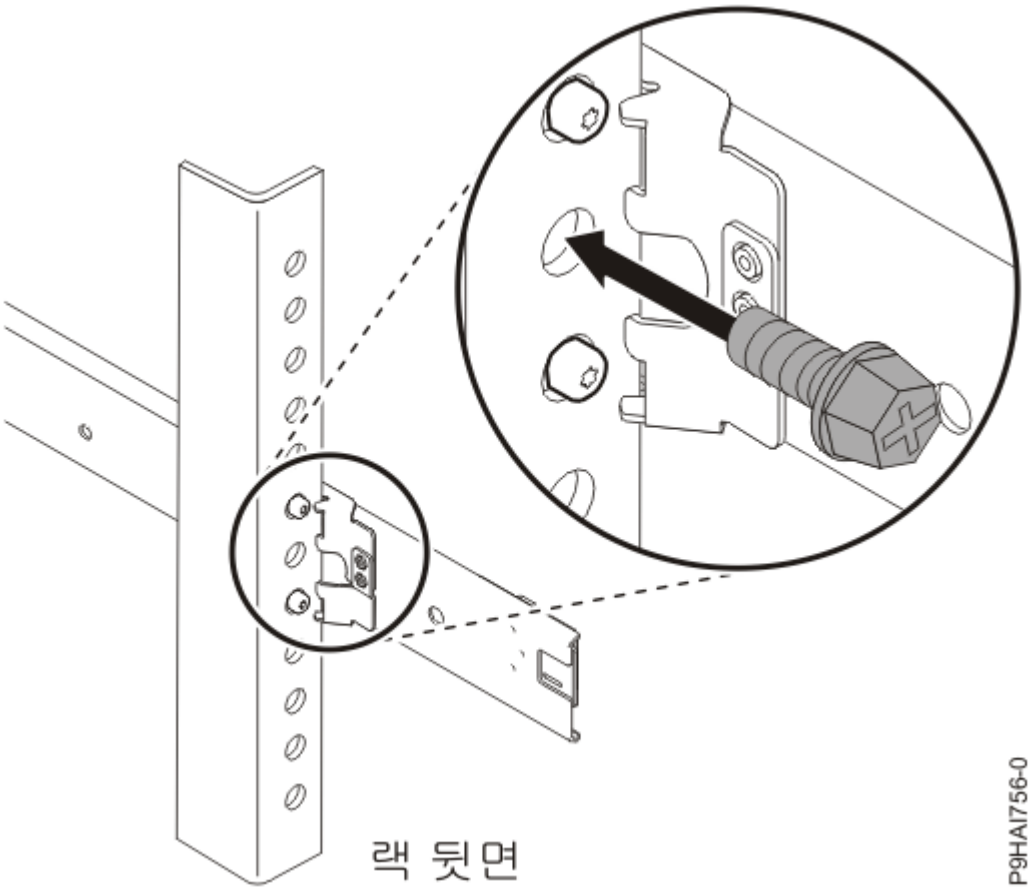


그림 *16.* 운송을 위한 서버 고정

랙에 7063-CR1 설치

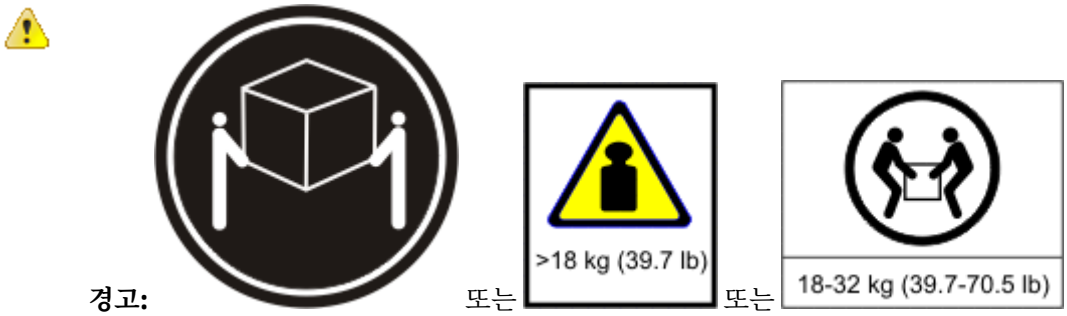
7063-CR1 HMC(Hardware Management Console)를 랙에 설치하는 방법에 대해 학습합니다.

온라인 설치 문서를 볼 수 있거나 같은 정보를 PDF 버전으로 출력할 수 있습니다. PDF 버전을 보거나 출력하려면 Hardware Management Console 설치 및 구성을 참조하십시오.

랙 장착형 7063-CR1 시스템 설치를 위한 전제조건

이 정보를 사용하여 시스템 설치를 위해 필요한 전제조건에 대해 이해할 수 있습니다.

이 태스크 정보



경고: 또는 또는

이 부품 또는 장치의 무게는 18 - 32kg(39.7 - 70.5lb)입니다. 이 부품 또는 장치를 안전하게 들려면 두 사람이 필요합니다. (C009)

서버 설치를 시작하기 전에 다음 문서를 읽어야 할 수 있습니다.

- 이 문서의 최신 버전은 온라인으로 유지보수됩니다. 랙에 7063-CR1 설치(http://www.ibm.com/support/knowledgecenter/POWER8/p9hai/p9hai_install7063_kickoff.htm)를 참조하십시오.

- 서버 설치를 계획하려면 사이트 및 하드웨어 계획의 내용을 참조하십시오.

프로시저

설치를 시작하기 전에 다음과 같은 항목이 있는지 확인하십시오.

- 2 크기의 십자형 드라이버
- 일자 드라이버
- 박스 커터
- 정전기 방지(ESD) 밴드
- 한 개의 EIA(Electronic Industries Association) 단위(1U) 공간이 있는 랙

참고: 설치된 랙이 없는 경우, 랙을 설치하십시오. 지시사항은 랙 및 랙 기능(http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm)을 참조하십시오.

시스템에 대한 자원 명세 완료
이 정보를 사용하여 시스템에 대한 자원 명세를 완료할 수 있습니다.

프로시저

1. 주문한 상자를 모두 받았는지 확인하십시오.
2. 필요에 따라 서버 구성요소의 포장을 푸십시오.
3. 각 서버 구성요소를 설치하기 전에 부품 명세를 완료하고 주문한 모든 부품이 배달되었는지 확인하십시오.

   참고:

   주문 정보는 제품에 포함되어 있습니다. 마케팅 담당자 또는 IBM 비즈니스 파트너로부터 주문 정보를 얻을 수도 있습니다.

   올바르지 않거나 누락되거나 손상된 부품이 있는 경우 다음 중 하나에 문의하십시오.

   - IBM 리셀러
   - IBM Rochester Manufacturing Automated Information Line(1-800-300-8751)(미국 전용)
   - Directory of worldwide contacts 웹사이트(http://www.ibm.com/planetwide). 사용자의 위치를 선택하여 서비스 및 지원 담당자 정보를 확인하십시오.

랙에서 7063-CR1 시스템의 위치 판별 및 표시
시스템 장치를 랙에 설치할 위치를 결정해야 할 수 있습니다.

프로시저

1. 랙 안전 주의사항(http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm)을 읽으십시오.
2. 랙에서 시스템 장치를 배치할 위치를 결정하십시오. 랙에 시스템 장치를 설치하려고 계획할 때 다음과 같은 정보를 고려하십시오.
   - 랙의 하단에 더 크고 무거운 장치를 구성하십시오.
   - 랙의 하단부터 시스템 장치를 설치하도록 계획하십시오.
   - 계획에서 EIA(Electronic Industries Alliance) 위치를 기록하십시오.
3. 필요한 경우 20 페이지의 그림 17에 표시된 대로 장치를 배치하려는 랙 격납장치 내부에 접근할 수 있도록 필러 패널을 제거하십시오.

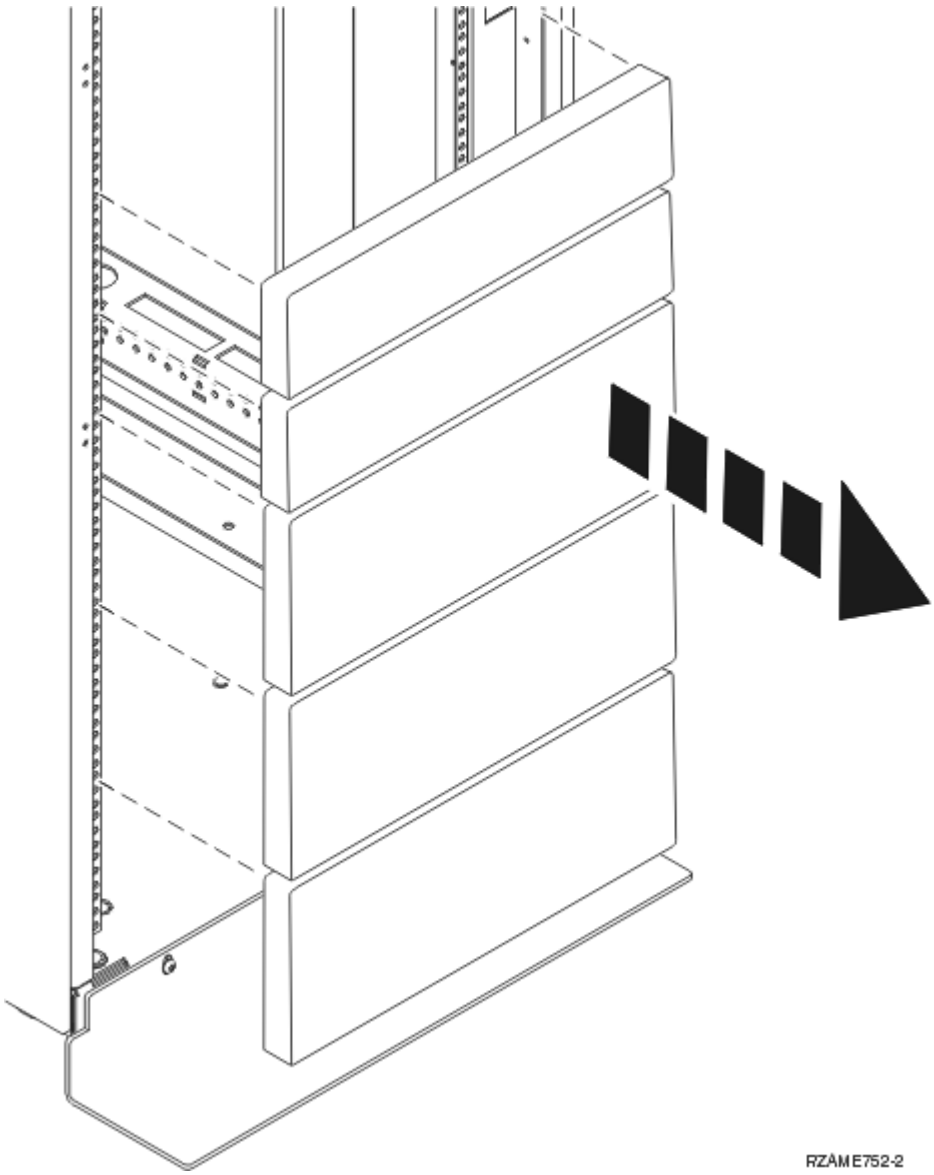


그림 *17.* 필러 패널 제거

4. 시스템을 랙에 배치할 위치를 결정하십시오. EIA 위치를 기록하십시오.
5. 랙 앞면을 마주보고 오른쪽부터 작업을 시작하여 테이프, 마커 또는 연필을 사용하여 각 EIA 단위의 하단 구멍을 표시하십시오.
6. 랙 왼쪽의 해당 구멍에서 20 페이지의 『5』 단계를 반복하십시오.
7. 랙의 뒷면으로 이동하십시오.
8. 오른쪽에서 랙의 앞면에 표시된 하단 EIA 단위에 해당하는 EIA 단위를 찾으십시오.
9. 하단 EIA 단위를 표시하십시오.
10. 랙 왼쪽의 해당 구멍에 표시하십시오.

시스템 섀시 및 랙에 고정 레일 연결

섀시 및 랙에 레일을 설치해야 합니다. 이 프로시저를 사용하여 이 태스크를 수행하십시오.

이 태스크 정보

주의: 레일 고장을 방지하고 사용자 및 장치에 대한 잠재적인 위험도 방지하려면 랙에 맞는 올바른 레일 및 부품을 가지고 있어야 합니다. 랙에 정사각형 지지 플랜지 구멍 또는 나사 지지 플랜지 구멍이 있는 경우 레일 및 부품이 랙에서 사용되는 지지 플랜지 구멍에 맞아야 합니다. 와셔 또는 스페이서를 사용하여

맞지 않는 하드웨어를 설치하지 마십시오. 랙에 맞는 올바른 레일 및 부품이 없는 경우 IBM 리셀러에게 문의하십시오.

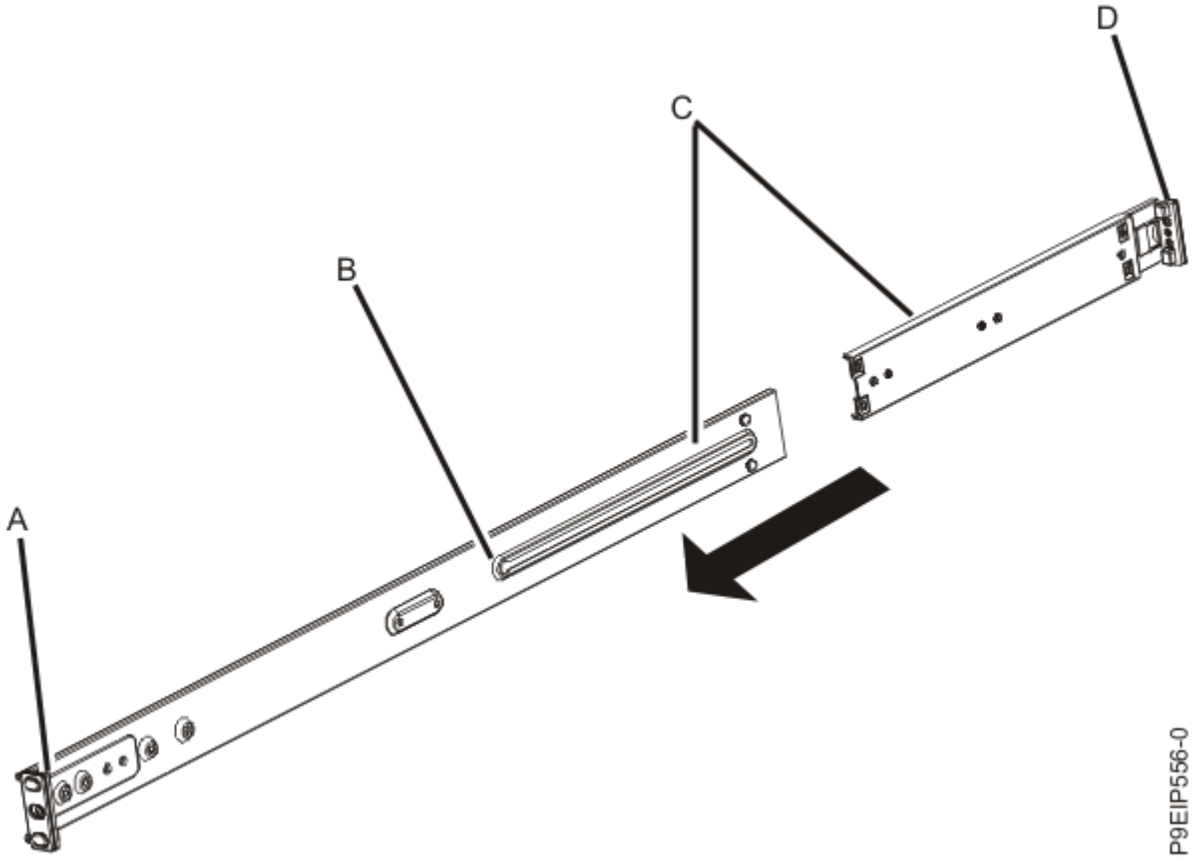
참고: 시스템에는 1 EIA 랙 단위(1U)의 공간이 필요합니다.

레일을 설치하기 위해 필요한 부품을 가지고 있는지 확인하십시오. 다음과 같은 부품이 레일 킷에 포함되어 있습니다.

- 슬라이드 레일 나사(각 슬라이드 레일의 두 부품을 연결하는 데 사용됨)
- 슬라이드 레일 랙 나사(레일을 랙에 고정하는 데 사용됨)
- 레일
- 10 - 32 x 0.635cm(0.25in.) 나사(레일을 시스템 섀시에 연결하는 데 사용됨)

프로시저

1. 레일 조각을 패키지에서 제거한 후 작업대에 놓으십시오.
2. 레일 랙 사각 핀 (**A**) 및 (**D**)를 레일 랙 둥근 핀으로 바꾸십시오.
3. 각 랙 슬라이드 레일의 두 부품을 연결하십시오. 랙 슬라이드 레일의 두 부품을 연결하려면 다음과 같은 태스크를 수행하십시오.
   a. 왼쪽 랙 슬라이드 레일의 두 조각을 식별하십시오. 짧은 조각과 긴 조각(**C**)을 맞추십시오. 랙 레일 핀이 동일한 방향(**A** 및 **D**)을 가리키는지 확인하십시오.



   b. 랙 슬라이드 레일의 짧은 조각에는 금속 핀이 있습니다. 이 핀을 랙 슬라이드 레일의 긴 조각에 있는 구멍(**B**)에 삽입하십시오. 랙 레일의 짧은 조각을 랙 레일의 긴 조각에 밀어 넣으십시오.
   c. 랙 슬라이드 레일의 두 조각에 있는 구멍을 맞추십시오. 십자형 드라이버를 사용하여 랙 슬라이드 레일에 있는 구멍을 통해 두 나사산 레일 나사를 느슨하게 조여 두 부품을 연결하십시오.

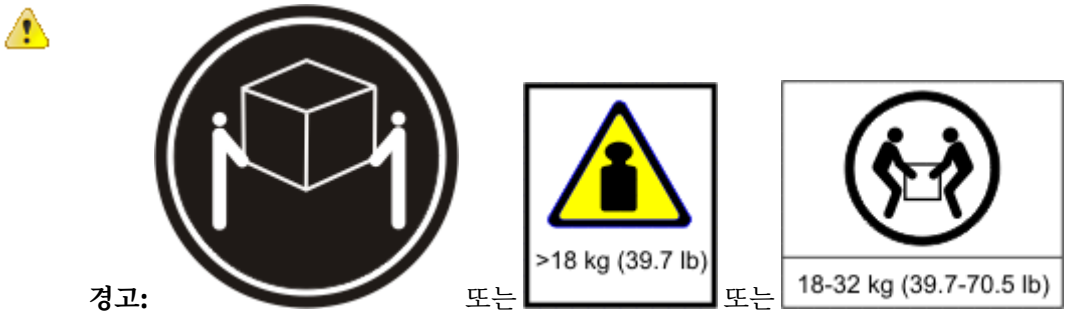
      참고: 랙 슬라이드 레일 나사를 단단히 조이지 마십시오.
   d. 오른쪽 슬라이드 레일에 대해 이 단계를 반복하십시오.
4. 랙 슬라이드 레일을 랙에 설치하십시오.

a. 랙의 앞면으로 이동하십시오.
b. 왼쪽 랙 슬라이드 레일을 선택한 후 이전에 표시한 EIA 단위를 찾으십시오. 각 슬라이드 레일에는 랙 뒷면을 지정하는 **Back**도 표시되어 있습니다. 랙 슬라이드 레일의 앞쪽 끝을 잡고 있어야 합니다.
c. 레일을 랙 앞쪽에서 랙 뒤쪽까지 확장한 후 랙 슬라이드 레일 핀을 이전에 표시한 랙 플랜지에 있는 구멍에 맞추십시오.
d. 뒷면 랙 레일 걸쇠가 딸깍 소리를 내며 고정될 때까지 랙 레일 핀을 뒷면 랙 플랜지에 밀어 넣으십시오.
e. 랙 레일의 앞면을 랙 레일 플랜지의 앞면 쪽으로 잡아당기십시오. 슬라이드 레일 핀을 레일 플랜지에 있는 구멍에 맞추고 레일 걸쇠가 딸각 소리를 내며 고정될 때까지 잡아당기십시오.
f. 드라이버를 사용하여 2단계에서 설치한 레일 나사를 조이십시오.

   참고: 액세스할 2U 공간이 필요하고 레일 나사를 조여야 할 수 있습니다.
g. 오른쪽 레일에 대해서는 4a - 4f단계를 반복하십시오.

랙에 시스템 설치 및 전원 케이블 연결 및 라우팅
레일에 시스템을 설치한 후 전원 케이블을 연결하고 라우팅하십시오.

이 태스크 정보



경고: 또는 또는

이 부품 또는 장치의 무게는 18 - 32kg(39.7 - 70.5lb)입니다. 이 부품 또는 장치를 안전하게 들려면 두 사람이 필요합니다. (C009)

프로시저

1. 시스템 섀시 상단에서 플라스틱 보호 필름을 제거하십시오.
2. 랙의 앞면으로 이동하십시오.
3. 두 명이 시스템 양쪽에서 시스템을 들고 섀시의 양쪽 측면에 있는 시스템 섀시 레일을 랙 슬라이드 레일에 맞추십시오.
4. 랙 뒷면 쪽으로 시스템을 조심스럽게 미십시오.
5. 시스템 섀시의 양쪽 측면에 있는 핸들을 통과하여 와셔로 나사를 조여 랙에 시스템을 고정하십시오.

   참고: 나사로 와셔를 사용해야 합니다. 레일 킷에 포함된 두 개의 더 긴 나사((1.5cm(0.59in.)) 각각에 와셔를 밀어 넣으십시오. 시스템 앞면의 오른쪽 및 왼쪽에 와셔로 나사를 고정하십시오.
6. 전원 코드를 전원 공급 장치에 꽂으십시오.

   참고: 지금 전원 코드의 반대쪽 끝을 전원에 연결하지 마십시오.

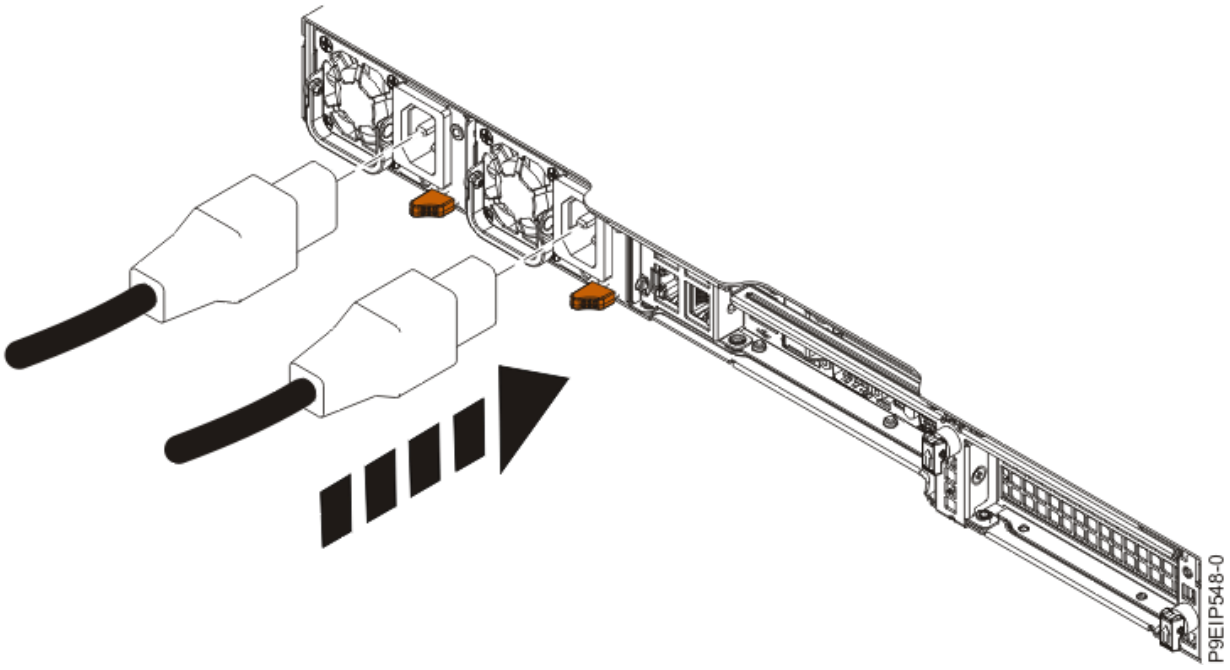


그림 *18.* 전원 공급 장치에 전원 코드 꽂기

7. 23 페이지의 『랙 장착형 7063-CR1 HMC』에서 계속하십시오.

랙 장착형 7063-CR1 HMC

랙 장착형 HMC(Hardware Management Console)를 물리적으로 설치하는 방법에 대해 학습합니다.

프로시저

1. HMC가 랙에 설치되어 있고 전원 코드가 전원 공급 장치에 연결되어 있는지 확인하십시오. 추가 정보는 22 페이지의 『랙에 시스템 설치 및 전원 케이블 연결 및 라우팅』의 내용을 참조하십시오. HMC를 랙에 설치한 후 다음 단계를 계속 진행하십시오.
2. 키보드, 모니터 및 마우스를 연결하십시오.

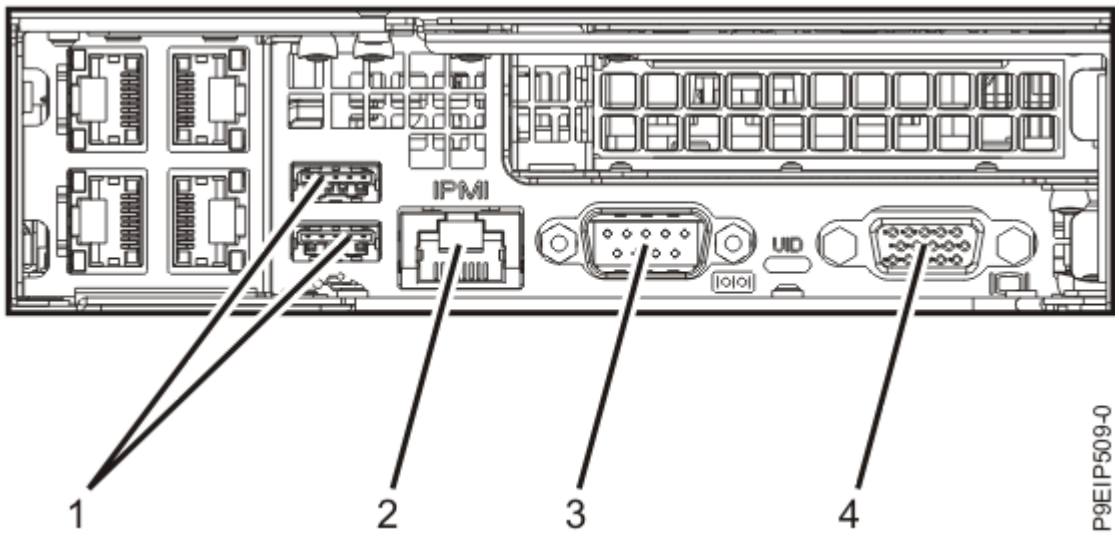


그림 *19.* 뒷면 포트

표 *4.* 입력 및 출력 포트	
ID	**설명**
1	키보드 및 마우스를 위해 사용되는 USB 2.0
2	이더넷 IPMI(Intelligent Platform Management Interface)
3	직렬 IPMI
4	모니터를 위해 사용되는 VGA(Video Graphics Array). 1024 x 768, 60Hz VGA 설정만 지원됩니다. 최대 3m까지의 케이블만 지원됩니다.

참고: 시스템에는 사용 가능한 두 개의 앞면 포트가 있습니다. 앞면 직렬 포트는 작동하지 않습니다.

3. 관리 시스템 연결에 사용될 이더넷 케이블에 연결하십시오.

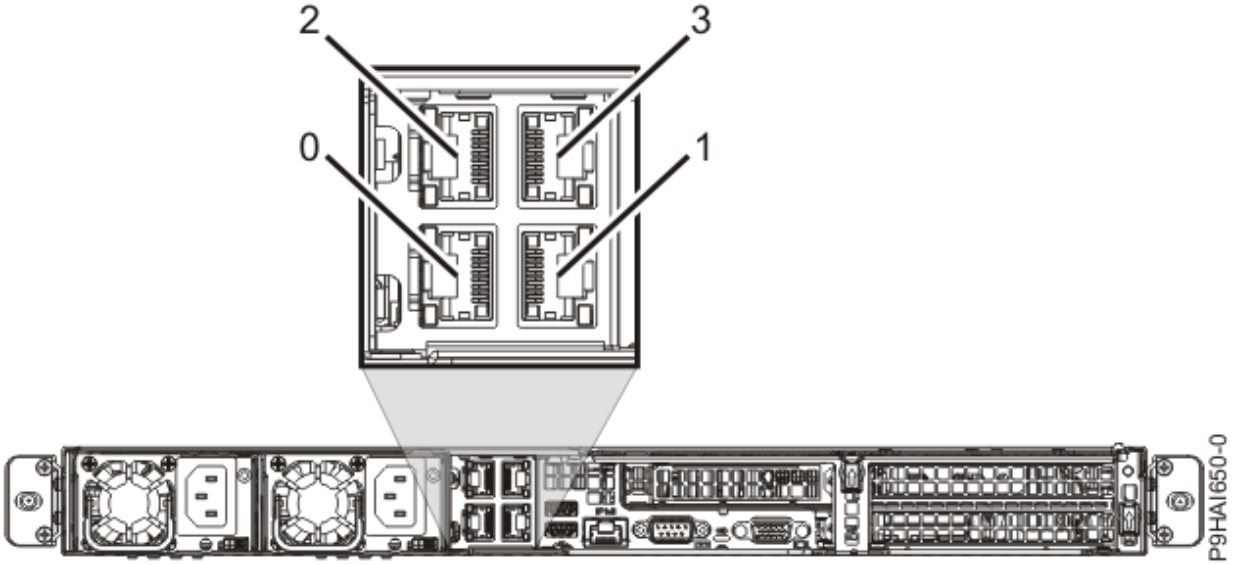


그림 *20.* 이더넷 포트

참고: HMC 네트워크 연결에 대해 더 자세히 학습하려면, 39 페이지의 『HMC 네트워크 연결』을 참조하십시오.

4. 관리 시스템이 이미 설치되어 있는 경우 설치가 진행될 때 HMC 및 관리 시스템 이더넷 포트의 녹색 상태 표시등을 관찰하여 이더넷 케이블 연결이 활성인지 확인할 수 있습니다.
5. 이더넷 IPMI(Intelligent Platform Management Interface) 포트를 네트워크에 연결하십시오.

   참고: HMC의 BMC(Baseboard Management Controller)에 액세스하려면 이 연결이 필요합니다. 서비스 태스크와 HMC 펌웨어 유지보수를 위해 BMC에 대한 액세스가 필요합니다. 추가 정보는 39 페이지의 『HMC 네트워크 연결 유형』의 내용을 참조하십시오.

6. 시스템 전원 코드 및 연결된 다른 모든 장치의 전원 코드를 교류(AC) 전원에 꽂으십시오.
7. 표시기로 전원 공급 장치 LED를 사용하여 전원 상태를 확인하십시오. 자세한 정보는 7063-CR1 시스템의 LED를 참조하십시오.

결과

다음으로 HMC 소프트웨어를 설치하고 구성해야 합니다. 24 페이지의 『7063-CR1 HMC 구성』에서 계속하십시오.

7063-CR1 HMC 구성

HMC(Hardware Management Console)를 설치하고 구성하는 방법에 대해 학습합니다.

HMC와 함께 제공된 HMC 버전을 확인하십시오. Fix Central 웹 사이트에서 사용 가능한 최신 HMC 버전을 다운로드할 수 있습니다. 이동식 매체(예: DVD 또는 USB)를 사용하여 HMC 패키지에서 부트 가능 ISO 파일(ISO 이미지)을 작성하십시오.

참고: 다음 표에서는 HMC 및 BMC 인터페이스에 대한 사전 정의된(기본값) 로그인 정보에 대해 설명합니다.

표 *5.*

콘솔 또는 인터페이스	기본 ID	기본 비밀번호	설명
BMC	ADMIN	ADMIN	ADMIN 사용자 ID 및 비밀번호는 처음 BMC에 로그인할 때 사용됩니다.
HMC	hscroot	abc123	hscroot 사용자 ID 및 비밀번호는 처음 HMC에 로그인할 때 사용됩니다. 대소문자를 구분하며 수퍼 관리자 역할의 구성원만 사용할 수 있습니다.
HMC	root	passw0rd	루트 사용자 ID 및 비밀번호는 서비스 제공자가 유지보수 프로시저를 수행하는 데 사용합니다. HMC에 로그인할 때 사용할 수 없습니다.

참고: 다음과 같은 설치가 예로 제공됩니다.

USB 플래시 드라이브를 사용하여 HMC 설치

USB 플래시 드라이브를 사용하여 HMC를 설치하려면 Linux 시스템에 대해 다음의 단계를 완료하십시오.

참고: 예를 들어, 다른 운영 체제에서 다음을 참조하십시오.

- Windows: USB 플래시 설치 매체(Windows)
- Mac: USB 플래시 설치 매체(macOS)

1. Fix Central 웹 사이트에서 원하는 HMC 버전을 다운로드하십시오.
2. **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** 명령을 실행하십시오(여기서 **sdx**는 USB 드라이브의 이름임).

   참고: 플러그를 연결할 때 Linux 명령 `lsblk`를 실행하여 USB 드라이브의 장치 이름을 판별할 수 있습니다.
3. USB 드라이브를 삽입하고 시스템의 전원을 켜십시오.

   참고: USB 드라이브는 4GB 이상이어야 합니다. 시스템 뒷면에 있는 특정 USB 드라이브는 너무 넓어 USB 포트에 맞지 않습니다. 계속하기 전에 USB 드라이브가 맞는지 테스트하십시오.
4. Petitboot 메뉴가 표시되면 **USB** 아래에 있는 **Hardware Management Console 설치** 옵션을 선택하십시오.

콘솔 뷰어에서 원격 매체를 사용하여 HMC 설치

콘솔 뷰어에서 원격 매체를 사용하여 HMC를 설치하려면 다음의 단계를 완료하십시오.

1. BMC 웹 인터페이스에 로그인하십시오(`http://<bmc-ip>`).
2. **원격 제어**를 선택하십시오.
3. **콘솔 경로 재지정**을 선택하십시오.
4. **콘솔 시작**을 클릭하십시오.
5. Java™ iKVM 뷰어에서 **가상 매체** > **가상 스토리지**를 선택하십시오.

6. **논리 드라이브 유형** 아래에서 **ISO 파일**을 선택하십시오.
7. **이미지 열기**를 클릭하고 시스템에서 ISO 파일을 찾으십시오.
8. **플러그인**을 눌러 ISO 파일을 마운트하십시오.
9. 시스템의 전원을 켜십시오.
10. Petitboot 메뉴가 표시되면 **CD/DVD** 아래에 있는 **Hardware Management Console 설치** 옵션을 선택하십시오.

외부 USB가 장착된 DVD 드라이브를 사용하여 HMC 설치

외부 USB가 장착된 DVD 드라이브를 사용하여 HMC를 설치하려면 다음 단계를 완료하십시오.

1. Fix Central 웹 사이트에서 원하는 HMC 복구 버전을 다운로드하십시오.
2. 이미지로 DVD-R 매체에 HMC 복구 DVD 이미지를 작성하십시오. 또는 DVD로 된 복구 매체를 주문할 수 있습니다.
3. 전원을 차단하십시오.
4. 외부 USB DVD 드라이브를 HMC에 연결하고 HMC 복구 DVD를 삽입하십시오.

   참고: USB DVD 드라이브를 외부 전원에 연결하거나 USB Y 케이블로 추가 USB 포트에 연결하여 충분한 전력을 DVD 드라이브에 공급해야 할 수 있습니다.
5. HMC의 전원을 켜십시오.

   참고: 설치 중에 디스플레이 모니터에 신호가 표시되지 않을 수 있습니다. 디스플레이 모니터에 상태가 표시되는 프로세스에는 2분 또는 3분이 소요될 수 있습니다.
6. Petitboot 부트로더가 시작되면 자동 부트를 중지하도록 이동하십시오.

   참고: 10초의 제한시간이 적용됩니다. 10초 내에 조치를 취하지 않으면 시스템의 하드 디스크 드라이브에서 부팅을 시도합니다.
7. Petitboot 메뉴에 **CD/DVD** 장치가 나타날 때까지 기다리십시오.

   참고: 이 프로세스에는 최대 1분이 소요될 수 있습니다.
8. **CD/DVD** 아래에 있는 **Hardware Management Console 설치** 옵션을 선택하십시오.

SMB 파일 서버에 의해 호스팅되는 원격 매체를 사용하여 HMC 설치

SMB(Server Message Block) 파일 서버에 의해 호스팅되는 원격 매체를 사용하여 HMC를 설치하려면 다음 단계를 완료하십시오.

1. 복구 ISO 파일을 SMB 호환 파일 서버의 공유 호스트로 복사하십시오.

   참고: SMBv3(Server Message Block version 3)는 지원되지 않습니다.
2. BMC 웹 인터페이스에 로그인하십시오(`http://<bmc-ip>`).
3. **가상 매체**를 선택하십시오.
4. **CD-ROM 이미지**를 선택하십시오.
5. 다음과 같은 정보를 완료하십시오.

   공유 호스트

   SMB 호스트의 IP입니다. 호스트 이름을 사용하는 경우 BMC의 DNS(Domain Name System)가 올바르게 구성되었는지 확인하십시오.

   이미지의 경로

   시스템에 대한 SMB 경로입니다. 예를 들면, `/<share name>/<rest of path>/<name of iso>.iso`입니다.

   사용자(선택사항)

   SMB 호스트에 로그인하는 데 사용되는 사용자 이름입니다.

비밀번호(선택사항)

사용자의 비밀번호입니다.

6. **저장**을 클릭하십시오.
7. **마운트**를 클릭하십시오.
8. 이제 장치 1에 **마운트된 iso 파일이 없습니다.**라는 메시지가 표시됩니다.

   참고: 이 메시지가 표시되지 않으면 정보를 다시 확인한 후 6 - 8단계를 반복하십시오.
9. 시스템의 전원을 켜십시오.
10. Petitboot 메뉴가 표시되면 **CD/DVD** 아래에 있는 **Hardware Management Console 설치** 옵션을 선택하십시오.

선택사항: 포함된 USB 메모리 키를 사용하여 HMC 펌웨어 레벨을 업데이트합니다.

참고: 구성에 USB 메모리 키의 HMC 펌웨어 업데이트가 포함된 경우, 다음 단계를 완료하여 HMC 펌웨어 레벨을 업데이트하십시오.

포함된 USB 메모리 키를 사용하여 HMC 펌웨어 레벨을 업데이트하려면 다음 단계를 완료하십시오.

1. USB 메모리 키 드라이브를 시스템 뒷면의 USB 포트에 삽입하십시오.
2. 시스템의 전원을 켜고 HMC에 로그온하십시오.
3. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
4. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
5. HMC 수정 서비스 설치 마법사에서 화면의 지시사항을 따르십시오.

다음으로 HMC 소프트웨어를 구성해야 합니다. 지침은 39 페이지의 『HMC 구성』을 참조하십시오.

관련 개념

BMC 연결 구성

관리 콘솔에 대한 BMC의 네트워크 설정을 구성하거나 볼 수 있습니다.

HMC 가상 어플라이언스 설치

HMC(Hardware Management Console) 가상 어플라이언스 설치 방법에 대해 학습합니다.

HMC 가상 어플라이언스는 기존 x86 또는 POWER® 가상화 인프라에 설치할 수 있습니다. HMC 가상 어플라이언스에서는 다음과 같은 x86 가상화 하이퍼바이저를 지원합니다.

- 커널 기반 가상 머신(KVM: Kernel-based virtual machine)
- Xen
- VMware

HMC 가상 어플라이언스에서는 다음과 같은 POWER 가상화 하이퍼바이저를 지원합니다.

- PowerVM®

HMC 가상 어플라이언스 실행에 필요한 최소 요구사항:

- 8GB 메모리(16GB 권장됨)
- 네 개의 가상 프로세서
- 두 개의 네트워크 인터페이스(최대 네 개가 허용됨)
- 한 개의 디스크 드라이브(500GB의 사용 가능한 디스크 공간이 포함됨)

참고:

PowerVM 가상화 하이퍼바이저에는 160GB의 디스크 공간이 필요합니다(권장되는 디스크 공간은 500GB임).

최소 PowerVM프로세서 요구사항은 1.0 처리 단위와 네 개의 공유 가상 프로세서(제한된 공유 모드)입니다.16GB 메모리가 권장됩니다.

참고:

1. HMC 가상 어플라이언스를 호스팅하는 시스템의 프로세서는 Intel VT-x 또는 AMD-V 하드웨어 가상화 가능 프로세서여야 합니다.
2. 사용자에게 제공되는 HMC 가상 어플라이언스 DVD는 부트 가능하지 않습니다. 먼저 매체를 마운트한 다음 매체에서 `.tgz` 파일을 복사해야 합니다. DVD를 마운트하는 방법은 사용 중인 운영 체제에 따라 다를 수 있습니다.
3. 다음 예에서 사용되는 명령 구문은 사용 중인 운영 체제에 따라 다를 수 있습니다.

관련 정보

HMC V8 네트워크 설치 이미지 및 설치 지시사항

x86에 HMC 가상 어플라이언스 설치

x86 환경에 HMC(Hardware Management Console) 가상 어플라이언스를 설치하는 방법에 대해 학습합니다.

KVM 하이퍼바이저를 사용하여 *HMC* 가상 어플라이언스 설치

커널 기반 가상 머신(KVM) 하이퍼바이저를 사용하여 HMC(Hardware Management Console) 가상 어플라이언스를 설치하는 방법에 대해 학습합니다.

KVM에 HMC 가상 어플라이언스를 설치하려면 다음 단계를 완료하십시오.

참고: 다음에서는 명령행 인터페이스를 사용하며 루트 사용자 권한이 필요합니다. 명령 구문은 운영 체제에 따라 다를 수 있습니다.

1. 가상화 패키지가 Red Hat Enterprise Linux(RHEL) 버전 7.0 이상에 설치되어 있는지 확인하십시오.
2. `<KVM vHMC installation filename>.tar.gz` 파일을 호스트 시스템에 다운로드하십시오.
3. `mkdir -p /var/lib/libvirt/images/vHMC` 명령을 실행하십시오.
4. `cd /var/lib/libvirt/images/vHMC` 명령을 실행하십시오.
5. 가상 디스크 이미지를 추출하려면 다음 명령을 실행하십시오. `tar -zxvf <KVM vHMC installation filename>.tgz`

   참고: 이 명령에서 HMC 가상 어플라이언스 .tar 파일의 전체 경로를 지정하십시오.
6. **domain.xml** 파일은 `<KVM vHMC installation filename>.tar.gz` 파일에서 제공됩니다. 다음 단계를 완료하십시오.
   a. **domain.xml** 파일을 편집하고 디스크에 대한 경로가 올바른지 확인하십시오. 이 파일은 **DISK_PATH** 문자열을 포함합니다.
   b. 디스크 장치에 대한 버스 값에 `virtio`가 사용되는지 확인하십시오.
   c. 사용자의 VM에 다른 이름을 사용할 수 있습니다. **domain.xml** 파일 내의 기본 이름은 **vHMC**입니다.
   d. 매체 액세스 제어(MAC) 주소가 **domain.xml** 파일에서 설정되는지 확인하십시오. 이 파일은 **MAC_ADDRESS** 문자열을 포함합니다.

      참고: MAC 주소가 자동으로 생성되도록 하려면 이 행을 제거하십시오.
   e. 브릿지가 이더넷 장치와 일치하는지 확인하십시오. 기본 **domain.xml** 파일은 하나의 이더넷을 지정합니다.
   f. 활성화 엔진을 사용 중인 경우 **AEDISK**를 활성화 엔진 가상 디스크 이미지의 이름으로 바꾸십시오. 그렇지 않으면 디스크 요소를 제거하십시오.
7. VM을 정의하려면 다음 명령을 실행하십시오. `virsh define <domain>.xml`.
8. 가상 HMC가 정의된 VM의 목록에 추가되었는지 확인하려면 `virsh list --all` 명령을 실행하십시오.
9. VM을 시작하려면 `virsh start vHMC` 명령을 실행하십시오.
10. 사용자 콘솔의 가상 네트워크 컴퓨팅(VNC)을 디스플레이 번호를 판별하려면 `virsh vncdisplay vHMC` 명령을 실행하십시오.
11. VNC 뷰어를 사용하여 콘솔에 연결하려면 `vncviewer HOSTNAME:ID` 명령을 실행하십시오. 여기서, `ID`는 디스플레이 번호이며 예를 들어, `0`입니다.).

참고: 원격 액세스가 필요한 경우, 방화벽을 삭제하거나 포트 5900에 대한 액세스를 허용하도록 구성해야 합니다.

Xen 하이퍼바이저를 사용하여 *HMC* 가상 어플라이언스 설치

Xen 하이퍼바이저를 사용하여 HMC(Hardware Management Console) 가상 어플라이언스를 설치하는 방법에 대해 학습합니다.

HMC 가상 어플라이언스는 Xen 버전 4.2 이상을 지원합니다.

Xen 하이퍼바이저를 사용하여 HMC 가상 어플라이언스를 설치하려면 다음 단계를 완료하십시오.

참고: 다음 단계에서는 명령행 인터페이스를 사용하며 루트 사용자 권한이 필요합니다. 명령 구문은 운영 체제에 따라 다를 수 있습니다.

1. 가상화 패키지가 Red Hat Enterprise Linux(RHEL) 버전 6.4 이상에 설치되어 있는지 확인하십시오.
2. `<XEN vHMC installation filename>.tar.gz` 파일을 호스트 시스템에 다운로드하십시오.
3. `mkdir -p /var/lib/libvirt/images/vHMC` 명령을 실행하십시오.
4. `cd /var/lib/libvirt/images/vHMC` 명령을 실행하십시오.
5. 가상 디스크 이미지를 추출하려면 다음 명령을 실행하십시오. `tar -zxvf <XEN vHMC installation filename>.tgz`

   참고: 이 명령에서 HMC 가상 어플라이언스 .tar 파일의 전체 경로를 지정하십시오.
6. **vhmc.cfg** 파일이 `<XEN vHMC installation filename>.tar.gz` 파일에서 제공됩니다. 텍스트 편집기에서 **vhmc.cfg** 파일을 열고 다음 값을 편집하십시오.
   a. 가상 HMC의 이름 변경(선택적): **vhmc.cfg** 파일을 편집하고 디스크의 경로가 올바른지 확인하십시오. 이 파일은 **DISK_PATH** 문자열을 포함합니다.
   b. **DISK_PATH**를 `disk1.img`의 경로로 바꾸십시오.

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

   c. **ethernet adapter**를 바꾸고 MAC 주소를 추가하십시오(선택적).

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

   선택적 MAC 주소:

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

   참고: 가상 HMC가 다시 부팅되면 Xen 하이퍼바이저가 자동으로 MAC 주소를 재생성합니다. 선택적 MAC 주소를 추가하면 이 문제가 해결됩니다.
   d. **FLOPPYPATH**를 바꾸십시오(활성화 엔진을 사용하는 경우에 해당됩니다).

   ```
   device_model_args = [ "-fda", "FLOPPYPATH" ]
   ```
7. VM을 작성하고 시작하려면 `xl create vHMC.cfg` 명령을 실행하십시오.
8. VM이 정의된 가상 머신의 목록에 추가되었는지 확인하려면 `xl list` 명령을 실행하십시오.
9. VM 로컬 콘솔에 액세스하려면 `vncviewer localhost 0` 명령을 실행하십시오.

*VMware ESXi*를 사용하여 *HMC* 가상 어플라이언스 설치

VMware ESXi를 사용하여 HMC(Hardware Management Console) 가상 어플라이언스를 설치하는 방법에 대해 학습합니다.

vSphere 클라이언트에서 그래픽 사용자 인터페이스를 사용하여 VMware ESXi에 HMC 가상 어플라이언스를 설치하여 OVF(Open Virtualization Format) 템플리트를 배치할 수 있습니다.

참고: VMware ESXi 버전 6.0 이상에 HMC 가상 어플라이언스를 설치할 수 있습니다.

vSphere 클라이언트를 사용하여 VMware ESXi에 HMC 가상 어플라이언스를 설치하려면 다음 단계를 완료하십시오.

참고: 명령 구문은 운영 체제에 따라 다를 수 있습니다.

1. Tar 아카이브 파일(<VMware vHMC installation file name>.tgz)을 확보하십시오.
2. tar 명령을 사용하여 Tar 아카이브 파일에서 OVA 파일을 추출하십시오.
3. vSphere 클라이언트를 시작하고 ESXi 호스트에 로그인하십시오.
4. **파일** 메뉴에서 **OVF 템플리트 배치**를 선택하십시오.
5. **찾아보기**를 클릭하고 OVA 파일을 선택하십시오.
6. **다음**을 클릭하십시오.
7. 배치가 완료된 후에 **닫기**를 클릭하고 HMC 가상 어플라이언스 아이콘을 선택하여 HMC 가상 어플라이언스의 전원을 켜십시오.

POWER에 HMC 가상 어플라이언스 설치
가상화된 POWER 환경에 HMC(Hardware Management Console) 가상 어플라이언스를 설치하는 방법에 대해 학습합니다.

***PowerVM*에서의 *HMC* 가상 어플라이언스 설치(논리 파티션)**
PowerVM 환경에 HMC(Hardware Management Console) 가상 어플라이언스를 설치하는 방법에 대해 학습합니다.

HMC 가상 어플라이언스는 펌웨어 레벨 FW910 이상에서 POWER9 서버를 지원합니다. 자세한 정보는 POWER8® 및 POWER9 Linux on Power® 시스템에 대해 지원되는 Linux 분배(https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm)를 참조하십시오.

참고:

1. HMC 가상 어플라이언스를 호스팅하는 서버를 관리할 수 없습니다.
2. 이 HMC 가상 어플라이언스를 호스팅하는 서버를 관리 중인 다른 HMC 가상 어플라이언스를 호스팅하는 서버를 관리할 수 없습니다.

   예를 들어, HMC 가상 어플라이언스 A가 서버 A에서 실행 중이고 HMC 가상 어플라이언스 B가 서버 B에서 실행 중입니다. 동시에 HMC 가상 어플라이언스 A는 서버 B를 관리할 수 없으며 HMC 가상 어플라이언스 B는 서버 A를 관리할 수 없습니다. HMC 가상 어플라이언스 중 하나는 다른 서버를 관리할 수 있지만 HMC 가상 어플라이언스 모두 동시에 서로를 관리할 수 없습니다.

.

자동화된 HMC 설치 이미지(선택사항)

HMC 설치 마법사에 대해 프롬프트하지 않고 HMC 가상 어플라이언스를 자동으로 설치하는 자동화된 설치 이미지를 작성할 수 있습니다.

참고: PowerVM에서의 HMC 가상 어플라이언스는 파티션에 지정되는 어댑터에 대한 지원을 그래픽으로 제공하지 않습니다. 지원되는 웹 브라우저를 사용하여 사용자 인터페이스 지원을 위한 HMC에 연결할 수 있습니다.

자동화된 HMC 설치 이미지를 작성하려면 다음 단계를 완료하십시오.

1. mkdir -p oldiso 및 mkdir -p newiso 명령을 실행하여 두 개의 디렉토리를 작성하십시오.
2. sudo mount -o loop <image_path> oldiso 명령을 실행하여 HMC 설치 이미지를 **oldiso** 디렉토리에 마운트하십시오.
3. cp -r oldiso/* newiso 명령을 실행하여 **oldiso** 디렉토리의 컨텐츠를 **newiso** 디렉토리에 복사하십시오.
4. sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg 명령을 실행하여 자동화된 설치를 위한 Grub 파일을 편집하십시오.
5. sudo chown 0444 newiso/boot/grub/grub.cfg 명령을 실행하여 Grub 파일을 읽기 전용으로 설정하십시오.
6. mkisofs -o <new_iso_name> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso 명령을 실행하

여 새 HMC 설치 ISO를 작성하십시오. 여기서, **ISO 레이블**은 HMC-<hmc version release number>여야 합니다(예: HMC-8.0.870.0).

참고: 활성화 엔진 및 구성 파일의 설정 방법에 대한 자세한 정보는 33 페이지의 『HMC 가상 어플라이언스에 대한 활성화 엔진 사용』의 내용을 참조하십시오.

논리적 볼륨 설정

논리적 볼륨을 설정하려면 다음 단계를 완료하십시오.

1. 관리 시스템을 선택하십시오.
2. 메뉴 POD에서 **시스템 조치** > **Power VM** > **가상 스토리지**를 선택하십시오.
3. **시스템 VIOS 관리** > **조치** > **가상 스토리지 관리**를 선택하십시오.
4. **가상 디스크** 탭을 선택하십시오.
5. **가상 디스크 작성**을 클릭하고 다음 정보를 입력하십시오.
   - **가상 디스크 이름**: 가상 디스크의 이름입니다.
   - **스토리지 풀 이름**: 스토리지 풀의 이름입니다.
   - **가상 디스크 크기**: 가상 디스크의 크기입니다.
   - **지정된 파티션**: 논리 파티션의 이름입니다.

   참고: 최소 160GB의 디스크 공간이 필요합니다(권장되는 디스크 공간은 500GB임).

설치 매체 설정 - 매체 라이브러리 작성

매체 라이브러리를 작성하려면 다음 단계를 완료하십시오.

1. 관리 시스템을 선택하십시오.
2. 메뉴 POD에서 **시스템 조치** > **Power VM** > **가상 스토리지**를 선택하십시오.
3. **시스템 VIOS 관리** > **조치** > **가상 스토리지 관리**를 선택하십시오.
4. **광학 장치** 탭을 선택하십시오.
5. **라이브러리 작성**을 클릭하고 다음 정보를 입력하십시오.
   - **스토리지 풀**: 스토리지 풀의 이름입니다.
   - **매체 라이브러리 크기**: 매체 라이브러리의 크기입니다.
6. **확인**을 클릭하십시오.

설치 매체 설정 - 매체를 VIOS에 업로드

매체를 VIOS(Virtual I/O Server)에 업로드하려면 다음 단계를 완료하십시오.

1. VIOS에 로그인하십시오.
2. VIOS 루트 모드에서 `oem_setup_env` 명령을 실행하십시오.
3. NFS 연결을 허용하려면 `nfso -o nfs_use_reserved_ports=1` 명령을 실행하십시오.
4. NFS를 로컬 VIOS 폴더에 마운트하려면 `mount <server_ip>:/Mountpoint <local_folder>` 명령을 실행하십시오.
5. HMC 설치 ISO 및 활성화 엔진 구성 이미지(선택사항)를 포함하는 NFS 마운트를 확인하려면 `ls` 명령을 실행하십시오.

설치 매체 설정 - 매체를 매체 라이브러리에 링크

매체를 매체 라이브러리에 링크하려면 다음 단계를 완료하십시오.

1. **시스템 VIOS 관리** > **조치** > **가상 스토리지 관리**로 돌아가서 **선택적 장치** 탭을 선택하십시오.
2. **가상 광학 매체** 섹션의 **조치** 메뉴에서 **매체 추가**를 선택하십시오.
3. **가상 매체 추가** 창에서 **VIOS 파일 시스템에서 기존 파일 추가**를 선택하고 다음 정보를 입력하십시오.

- **매체 이름**: 매체의 이름입니다(예: HMCInstall 또는 AEDrive).
- **광학 매체 파일 이름**: 설치 ISO 파일의 파일 이름입니다(예: 01234567-ppc64ie.iso).

4. **확인**을 클릭하십시오.
5. 활성화 엔진 구성 이미지를 작성한 경우 활성와 엔진 구성 이미지를 추가하도록 3 - 4단계를 반복하십시오. 그렇지 않으면 6단계를 진행하십시오.
6. 매체 이름이 사용 가능한 **가상 광학 매체** 목록에 표시되는지 검증하여 광학 매체가 매체 라이브러리에 업로드되는지 확인하십시오.

논리 파티션 설정

논리 파티션을 설정하려면 다음 단계를 완료하십시오.

1. 관리 시스템을 선택하십시오.
2. 메뉴 POD에서 **시스템 조치** > **파티션** > **파티션**을 선택하십시오.
3. **파티션 작성**을 클릭하고 다음 정보를 입력하십시오.
   - **파티션 이름**: 파티션의 이름입니다.
   - **파티션 ID**: 파티션의 이름입니다.
   - **파티션 유형**: 운영 체제(**AIX/Linux** 또는 **IBM i**)를 선택합니다.
4. **확인**을 클릭하십시오.
5. 프로세서의 수와 파티션 메모리의 크기를 할당하십시오.

   참고: 최소 네 개의 가상 프로세서와 8GB의 메모리가 필요합니다.
6. 메뉴 POD에서 **파티션 조치** > **가상 I/O** > **가상 네트워크**를 선택하십시오.
7. **가상 네트워크 연결**을 클릭하고 **새 가상 이더넷 어댑터 표시 및 연결** 선택란을 선택하십시오. 테이블에서 논리적 파티션에 연결할 가상 네트워크 어댑터를 선택하십시오.

   참고: 최대 네 개의 가상 네트워크 어댑터가 사용 가능합니다.
8. 메뉴 POD에서 **파티션 조치** > **가상 I/O** > **가상 스토리지**를 선택하십시오.
9. **가상 광학 장치** 탭에서 **가상 광학 장치 추가**를 클릭하십시오.
10. **장치 이름**(예: HMCInstall 또는 AEDrive)을 입력하고 테이블에서 원하는 Virtual I/O Server를 선택하십시오.

    참고: AEDrive 설치는 선택사항입니다.
11. **확인**을 클릭하십시오.
12. 10단계에서 추가한 가상 광학 장치가 이제 테이블에 나열되어 있는지 확인하십시오.
13. **조치** 메뉴에서 **로드**를 클릭하십시오.
14. 논리 파티션에 지정할 매체 파일을 선택하고 **확인**을 클릭하십시오.
15. 13단계에서 로드한 가상 광학 장치가 이제 테이블에 나열되어 있는지 확인하십시오.

HMC 가상 어플라이언스 시작

참고: HMC ISO 이미지 파일을 사용하여 파티션에 HMC 가상 어플라이언스를 설치하는 경우 웹 사용자 인터페이스에 대한 로컬 그래픽 콘솔 액세스 권한이 없습니다.

PowerVM에서 HMC 가상 어플라이언스를 시작하려면 다음 단계를 완료하십시오.

1. 관리 파티션을 선택하십시오.
2. **조치** > **콘솔** > **터미널 창 열기**를 선택하여 논리 파티션에 대한 활성 연결을 여십시오.
3. **조치** > **활성화**를 선택하여 논리 파티션을 활성화하십시오.
4. **활성화(정상)** 및 **현재 구성**을 선택하십시오.
5. **완료**를 클릭하십시오.
6. 터미널 창으로 전환하십시오.

7. **부트** 메뉴에서 **1 = SMS 메뉴**를 선택하십시오.
8. **기본** 메뉴에서 **5 = 부트 옵션 선택**을 선택하십시오.
9. **다중 부트** 메뉴에서 **1 = 설치/부트 장치 선택**을 선택하십시오.
10. **장치 유형 선택** 메뉴에서 **5 = 모든 장치 나열**을 선택하십시오.
11. 장치 위치 기반인 `HMCInstall` 장치를 선택하십시오.
12. **2. 정상 모드 부트**를 선택하십시오.
13. 확인하려면 **1. 예**를 선택하십시오.
14. **HMC 설치** 마법사에서 화면의 지시사항을 따르십시오.

    참고: 자동화된 HMC 설치 이미지를 사용한 경우 이 단계를 건너뛰십시오.
15. 설치가 완료되고 시스템이 시작된 후 **언어 선택** 대화 상자에서 언어를 선택해야 합니다.
16. 라이센스 계약에 동의하십시오.

    참고: 명령을 실행하기 전에 명령 제어기가 명령을 허용할 준비가 되었는지 확인하십시오. 예를 들어, **`lshmc -V`** 명령 실행이 성공할 때까지 실행합니다.
17. `hscroot`로 로그인하고 **chhmc** 명령을 사용하여 네트워크를 구성하십시오.

    다음 예제는 HMC에서 네트워크를 구성하고 SSH(Secure Shell) 및 원격 웹 액세스를 사용으로 설정하는 데 사용할 수 있는 **chhmc** 명령의 순서를 표시합니다.

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

    - **ethX**는 구성할 네트워크 인터페이스 이름입니다.
    - **hmc ip address**는 HMC의 IP 주소입니다.
    - **hmc network mask**는 HMC의 네트워크 마스크입니다.
    - **hmc hostname**은 HMC의 호스트 이름입니다.
    - **hmc domain**은 HMC의 도메인 이름입니다.
    - **gateway ip**는 네트워크의 게이트웨이 IP 주소입니다.
    - **name server**는 네트워크의 이름 서버 주소입니다.
    - **domain search**는 HMC에서 검색할 도메인의 이름입니다.
    - 모든 IP 주소에서 액세스할 수 있도록 하려면 **ip address** 대신 **-a 0.0.0.0 -nm 0**을 사용하십시오.

    참고: 다중 가상 이더넷 어댑터를 사용하는 경우 각 인터페이스의 HMC 가상 어플라이언스에서 **`cat /etc/sysconfig/network-scripts/ifcfg-ethX`** 명령을 실행하십시오. MAC(Media Access Control) 주소를 HMC에서 파티션의 가상 네트워크에 대한 어댑터 보기에 표시되는 항목과 비교하십시오. 가상 이더넷 어댑터에 대한 자세한 정보는 **가상 이더넷 어댑터 설정값 보기**를 클릭하십시오. 이 단계를 통해 사용할 올바른 인터페이스를 결정할 수 있습니다.
18. 시스템을 다시 시작하십시오.

HMC 가상 어플라이언스에 대한 활성화 엔진 사용

HMC(Hardware Management Console) 가상 어플라이언스에 대한 활성화 엔진을 사용하는 방법에 대해 학습합니다.

활성화 엔진은 가상 머신 내의 다양한 구성요소가 시스템 시작 동안 구성될 수 있도록 허용하는 프레임워크입니다. 활성화 엔진을 사용하려면 HMC 가상 어플라이언스가 처음 시작에서 관리 준비 상태가 되도록 XML 구성 프로파일을 설정해야 합니다. XML 구성 프로파일 구성에 대한 자세한 정보는 34 페이지의 『활성화 엔진에 대한 구성 프로파일 설정』을 참조하십시오. 다음 옵션을 구성하는 데 구성 파일을 사용할 수 있습니다.

- 기본 키보드(US) 설정

- 기본 로케일(US)
- 키보드 설정 사용 안함
- 디스플레이 설정 사용 안함
- 라이센스 계약 및 기계코드 계약
- 설치 마법사 사용 안함
- 콜홈 마법사 사용 안함
- 최대 4개의 네트워크 인터페이스 카드 구성
- 각 인터페이스에 대한 방화벽 설정 구성
- IPv4 DHCP 서버로 네트워크 인터페이스를 구성하십시오.
- 개인용이며 개방형인 인터페이스를 구성하십시오.
- 기본 게이트웨이 인터페이스 장치를 구성하십시오.

참고: vHMC-Conf.xml 구성 파일에 정의된 이더넷 어댑터의 수는 **domain.xml**, **vHMC.cfg** 또는 **VMWare** 구성 파일에 정의된 네트워크 어댑터와 관련되어야 합니다.

활성화 엔진에는 XML 구성이 있는 가상 디스크가 필요합니다. 텍스트 편집기로 **user_data** 파일을 편집할 수 있고 다음 예제에 표시되는 XML 구성 안내서를 사용할 수 있습니다.

Linux 환경에서 활성화 엔진 구성으로 가상 ISO 디스크 이미지를 작성하려면 다음 단계를 완료하십시오.

1. 디렉토리를 작성하십시오.

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

2. 편집된 **user_data** 파일을 디렉토리에 복사하십시오.

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

3. 활성화 엔진 구성으로 가상 디스크 이미지를 작성하십시오.

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

활성화 엔진에 대한 구성 프로파일 설정
XML 태그를 사용하여 활성화 엔진 구성 파일을 설정하는 방법에 대해 학습합니다.

구성 파일

XML 태그를 학습하려면 다음 구성 파일 예제를 사용하십시오.

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

```
         <RPD>Enabled</RPD>
         <FCS>Enabled</FCS>
         <I5250>Enabled</I5250>
         <PING>Enabled</PING>
         <L2TP>Disabled</L2TP>
         <SLP>Enabled</SLP>
         <RSCT>Enabled</RSCT>
         <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
         <SSH>Enabled</SSH>
         <NTP>Disabled</NTP>
         <SNMPTraps>Disabled</SNMPTraps>
         <SNMPAgents>Disabled</SNMPAgents>
      </Firewall>
   </Ethernet>
   <NTPServers>
      <ntpparam ntpserver="" ntpversion=""/>
   </NTPServers>
</vHMC-Configuration>
```

구성 파일에 대한 XML 태그

XML 태그는 다양한 속성에 대한 특정 값을 설정하기 위해 활성화 엔진 구성 파일에서 사용됩니다. 활성화 엔진 구성 파일에서 이러한 값을 수동으로 설정할 수 있습니다. 각 태그에 대한 설명 및 허용되는 값을 보려면 다음 표를 참조하십시오.

표 *6. XML* 태그.

태그	설명	허용 가능한 값	참고
ConfigurationVersion	사용할 구성 버전을 정의하는 필수 요소	**2.0**	
LicenseAgreement	HMC 가상 어플라이언스 라이센스 계약을 표시하는 필수 요소		
AcceptLicense	HMC 가상 어플라이언스 라이센스 계약을 동의하는 필수 요소	• **예**: 라이센스 계약을 동의합니다. • **아니오**: HMC 라이센스 계약을 동의하도록 사용자에게 프롬프트합니다.	올바르지 않은 값이 입력되면 활성화 엔진은 기본 설정값인 **아니오**를 사용합니다.
Locale	로케일 설정을 정의하는 필수 요소입니다.	**en_US.UTF-8**	올바르지 않은 값이 입력되면 활성화 엔진은 기본 설정값인 **US**를 사용합니다.
SetupWizard	**HMC 설정** 마법사를 사용하거나 사용하지 않는 필수 요소	• **예**: **HMC 설정** 마법사를 표시합니다. • **아니오**: **HMC 설정** 마법사 표시를 사용하지 않습니다.	올바르지 않은 값이 입력되면 활성화 엔진은 기본 설정값인 **예**를 사용합니다.
SetupCallHomeWizard	**HMC 콜홈** 마법사를 사용하거나 사용하지 않는 필수 요소	• **예**: **HMC 콜홈** 마법사를 표시합니다. • **아니오**: **HMC 콜홈** 마법사 표시를 사용하지 않습니다.	올바르지 않은 값이 입력되면 활성화 엔진은 기본 설정값인 **예**를 사용합니다.
SetupKeyboard	키보드 구성을 정의하는 필수 요소입니다.	• **예**: 키보드 구성을 위해 사용자에게 프롬프트를 표시합니다. • **아니오**: 기본 키보드 구성을 허용합니다(US).	올바르지 않은 값이 입력되면 활성화 엔진은 기본 설정값인 **예**를 사용합니다.
SetupDisplay	디스플레이 구성을 사용하거나 사용하지 않는 필수 요소입니다.	• **예**: 디스플레이 구성을 위해 사용자에게 프롬프트를 표시합니다. • **아니오**: 기본 디스플레이 구성을 허용합니다.	올바르지 않은 값이 입력되면 활성화 엔진은 기본 설정값인 **예**를 사용합니다.

표 *6. XML* 태그. *(계속)*

태그	설명	허용 가능한 값	참고
Ethernet	이더넷 어댑터 구성의 값을 보유하는 필수 요소입니다. 최대 네 개의 이더넷 어댑터를 구성할 수 있습니다.	**Enable**: • **예**: 이 어댑터를 구성합니다. • **아니오**: 이 어댑터를 구성하지 않습니다. **DefaultGatewayDevice**: • **예**: 이 어댑터를 기본 네트워크 어댑터로 구성합니다. • **아니오**: 이 어댑터를 기본 네트워크 어댑터로 구성하지 않습니다. **PrivateInterface**: • **예**: 이 어댑터를 개인용 인터페이스로 구성합니다. **예**는 인터페이스를 IPv4 DHCP 서버로 구성하는 데 필요합니다. • **아니오**: 이 어댑터를 개인용 인터페이스로 구성하지 않습니다. **아니오**는 인터페이스를 IPv4 정적 유형으로 구성하는 데 필요합니다.	이더넷 어댑터 섹션에 올바르지 않은 값이 입력되거나 다중 **기본 게이트웨이 장치**가 정의되는 경우 활성화 엔진에서 기본 구성을 실행합니다. 이 구성에서 선택적 요소를 생략할 수 있습니다. 최소 하나의 IPV4 또는 IPV6 구성이 필요합니다. IP 구성을 지정하지 않으면 활성화 엔진이 기본 구성을 사용합니다.
HostName	네트워크 호스트 이름을 정의하는 선택적 요소입니다.	모든 호스트 이름 문자열입니다.	요소가 지정되지 않으면 활성화 엔진이 기본 로컬 호스트 **HostName** 값을 사용합니다.
Domain	네트워크 도메인을 정의하는 선택적 요소입니다.	유효한 도메인 값입니다(예: **example.us.com**).	요소가 지정되지 않으면 활성화 엔진이 비어 있는 기본 **Domain** 값을 사용합니다.
DNSServers	네트워크 DNS 서버를 정의하는 선택적 요소입니다.	하나의 DNS 서버 값 또는 쉼표로 구분된 최대 세 개의 유효한 IPv4 또는 IPv6 주소를 사용할 수 있습니다. • 예제 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • 예제 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • 예제 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844, ::ffff:903:201	요소가 지정되지 않으면 활성화 엔진이 비어 있는 기본 **DNSServers** 값을 사용합니다.

표 *6. XML* 태그. *(계속)*

태그	설명	허용 가능한 값	참고
IP4Config	IPv4 구성 설정을 정의하는 선택적 요소입니다.	**IPType**: IPv4 구성 유형을 정의하는 필수 요소입니다. • **Static**: 정적 구성을 사용하여 이 어댑터를 구성합니다. • **DHCP**: DHCP 구성을 사용하여 이 어댑터를 구성합니다. • **DHCPServer**: IPv4 DHCP 서버가 되도록 이 어댑터를 구성합니다(**PrivateInterface**는 **예**여야 함). **IPAddress**: **Static** 또는 **DHCPServer** 구성이 선택된 경우에만 필수인 선택적 요소입니다. • **Static 구성**: 유효한 모든 IPv4 주소 값입니다. • **DHCPServer 구성**: IP 범위 내에 있는 DHCP 서버 IP입니다. **Netmask**: **Static** 구성이 선택된 경우에만 필수인 선택적 요소입니다. • 유효한 모든 IPv4 넷마스크 값입니다. **Gateway**: **Static** 구성이 선택된 경우에만 필수인 선택적 요소입니다. • 유효한 모든 IPv4 넷마스크 값입니다.	
IP6Config	IPv6 구성 설정을 정의하는 선택적 요소입니다.	**IPType**: IPv6 구성 유형을 정의하는 필수 요소입니다. • **Static**: 정적 구성을 사용하여 이 어댑터를 구성합니다. • **DHCP**: DHCP 구성을 사용하여 이 어댑터를 구성합니다. **IPAddress**: 길거나 짧은 IPv6 형식 및 길거나 짧은 IPv6 접두부를 사용할 수 있습니다. • 예제 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888 • 예제 2: IPv6: 2001:4860:4860::8888 • 예제 3: IPv6: 2001:4860:4860::8888/128 접두부가 지정되지 않으면 활성화 엔진은 기본 설정값인 /64 접두부를 사용합니다. **Gateway**: • 유효한 모든 IPv6 주소 값입니다.	

표 6. *XML* 태그. *(계속)*			
태그	**설명**	**허용 가능한 값**	**참고**
Firewall	방화벽 설정을 정의하는 선택적 요소입니다.	**PEGASUS**: • **사용**: PEGASUS 포트를 열 수 있습니다. • **사용 안함**: PEGASUS 포트를 사용하지 않습니다. **RPD**: • **사용**: RMC 포트를 열 수 있습니다. • **사용 안함**: RMC 포트를 사용하지 않습니다. **FCS**: • **사용**: FCS 포트를 열 수 있습니다. • **사용 안함**: FCS 포트를 사용하지 않습니다. **I5250**: • **사용**: 5250 포트를 열 수 있습니다. • **사용 안함**: 5250 포트를 사용하지 않습니다. **PING**: • **사용**: Ping 포트를 열 수 있습니다. • **사용 안함**: Ping 포트를 사용하지 않습니다. **L2TP**: • **사용**: L2TP 포트를 열 수 있습니다. • **사용 안함**: L2TP 포트를 사용하지 않습니다. **SLP**: • **사용**: SLP 포트를 열 수 있습니다. • **사용 안함**: SLP 포트를 사용하지 않습니다. **RSCT**: • **사용**: RSCT 포트를 열 수 있습니다. • **사용 안함**: RSCT 포트를 사용하지 않습니다. **SECUREREMOTEACCESS**: • **사용**: 보안 원격 액세스 포트를 열 수 있습니다. • **사용 안함**: 보안 원격 액세스 포트를 사용하지 않습니다. **SSH**: • **사용**: SSH 포트를 열 수 있습니다. • **사용 안함**: SSH 포트를 사용하지 않습니다.	

표 6. *XML* 태그. *(계속)*			
태그	**설명**	**허용 가능한 값**	**참고**
Firewall	방화벽 설정을 정의하는 선택적 요소입니다.	**NTP**: • **사용**: NTP 포트를 열 수 있습니다. • **사용 안함**: NTP 포트를 사용하지 않습니다. **SMNPTraps**: • **사용**: SMNP 트랩 포트를 열 수 있습니다. • **사용 안함**: SMNP 트랩 포트를 사용하지 않습니다. **SMNPAgents**: • **사용**: SMNP 에이전트 포트를 열 수 있습니다. • **사용 안함**: SMNP 에이전트 포트를 사용하지 않습니다.	

NTPServers	**NTPServers** 태그는 HMC 가상 어플라이언스에 최대 다섯 개의 NTP 서버를 구성하려는 경우에 필요합니다.	**NTPServers**: `<ntpparam ntpserver="server" ntpversion="version"/>`을 허용합니다.
		ntpparam:
		• **ntpserver**: 유효한 IPv4 또는 IPv6 값 및 유효한 호스트 이름을 허용합니다.
		• **ntpversion**: 1 - 4의 숫자 값을 허용합니다.
		예제:
		`<NTPServers>`
		`<ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>`
		`<ntpparam ntpserver="192.168.34.1" ntpversion="4"/>`
		`<ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>`
		`</NTPServers>`	

HMC 구성

네트워크 연결을 설정하고 HMC를 구성하고 구성 후 단계를 완료하고 HMC를 업그레이드 및 업데이트하는 방법에 대해 학습합니다.

HMC의 네트워크 설정값 선택

HMC(Hardware Management Console)에서 사용할 수 있는 네트워크 설정값에 대해 학습합니다.

HMC 네트워크 연결

네트워크에서 HMC(Hardware Management Console)의 사용 방법에 대해 학습합니다.

여러 가지 유형의 네트워크 연결을 사용하여 HMC를 관리 시스템에 연결할 수 있습니다. 네트워크에 연결하도록 HMC를 구성하는 방법에 대한 자세한 정보는 54 페이지의 『HMC 구성』의 내용을 참조하십시오. 네트워크에서의 HMC 사용에 대한 자세한 정보는 다음 정보를 참조하십시오.

HMC 네트워크 연결 유형

사용자 네트워크를 사용하여 HMC 원격 관리 및 서비스 기능을 사용하는 방법에 대해 학습합니다.

HMC는 다음과 같은 유형의 로컬 통신을 지원합니다.

HMC 대 관리 시스템
대다수의 하드웨어 관리 기능을 수행하는 데 사용되며, 여기서 HMC는 관리 시스템의 서비스 프로세서를 통해 제어 함수 요청을 발행합니다. HMC와 서비스 프로세서 사이의 연결을 서비스 네트워크라고 하기도 합니다. 이 연결은 관리 시스템 관리에 필요합니다.

HMC 대 논리 파티션
논리 파티션에서 실행되는 운영 체제의 플랫폼 관련 정보(하드웨어 오류 이벤트, 하드웨어 명세)를 수집하고, 이러한 운영 체제에서 특정 플랫폼 활동(동적 LPAR, 동시 수리)을 조정하는 데 사용됩니다. 서비스 및 오류 통지 기능을 사용하려는 경우 이 연결을 작성해야 합니다.

HMC 대 BMC

참고: BMC(Baseboard Management Controller) 연결은 HMC 모델 7063-CR1에만 적용할 수 있습니다.

서비스 및 유지보수 태스크를 수행하는 데 사용됩니다. BMC 연결은 시스템에서 HMC 펌웨어를 로드하고 유지보수하는 데 사용됩니다. 이 연결은 HMC에서 BMC에 액세스하는 데 필요합니다.

HMC 대 원격 사용자
원격 사용자에게 HMC 기능에 대한 액세스를 제공합니다. 원격 사용자는 다음과 같은 방식으로 HMC에 액세스할 수 있습니다.

- 원격 클라이언트(HMC 버전 6 이상을 사용하는 경우) 또는 웹 브라우저(HMC 버전 7 이상을 사용하는 경우)를 사용하여 모든 HMC GUI 기능에 원격으로 액세스
- 웹 브라우저를 사용하여 모든 HMC GUI 기능에 원격으로 액세스
- SSH(Secure Socket Shell)를 사용하여 HMC 명령행 기능에 원격으로 액세스
- 가상 단말기 서버를 사용하여 가상 논리 파티션 콘솔에 원격으로 액세스

HMC 대 서비스 및 지원 센터
하드웨어 오류 보고서, 명세 데이터 및 마이크로코드 업데이트 등의 데이터를 서비스 제공자와 상호 전송하는 데 사용됩니다. 이 통신 경로를 사용하여 자동 서비스 호출을 사용할 수 있습니다.

HMC는 모델에 따라 최대 네 개까지 개별 이더넷 인터페이스를 지원할 수 있습니다. HMC의 독립형 버전은 하나의 내장 이더넷 어댑터와 최대 두 개의 플러그 인 어댑터를 사용하여 세 개의 HMC 인터페이스만 지원합니다. 이들 각 인터페이스는 다음과 같은 방식으로 사용됩니다.

- HMC 대 관리 시스템 통신에 대해 하나의 네트워크 인터페이스를 독점적으로 사용할 수 있는데, 이는 관리 시스템의 서비스 프로세서 및 HMC만 해당 네트워크에 있음을 의미합니다. HMC 대 관리 시스템 통신에 대해 하나 이상의 네트워크 인터페이스를 독점적으로 사용할 수 있는데, 이는 관리 시스템의 서비스 프로세서 및 HMC만 해당 네트워크에 있음을 의미합니다. SSL(Secure Sockets Layer) 프로토콜 및 비밀번호 보호를 위해 서비스 프로세서에 대한 네트워크 인터페이스를 암호화하는 경우에도 별도의 전용 네트워크를 두면 이러한 인터페이스에 상위 레벨의 보안을 제공할 수 있습니다.
- HMC 대 논리 파티션 통신의 경우 HMC 및 관리 시스템의 논리 파티션간 네트워크 연결에는 주로 개방형 네트워크 인터페이스가 사용됩니다. 이러한 개방형 네트워크 인터페이스는 HMC를 원격으로 관리하는 데에도 사용할 수 있습니다.
- 선택적으로, 세 번째 인터페이스를 사용하여 논리 파티션에 연결하고 HMC를 원격으로 관리할 수 있습니다. 또한 이 인터페이스는 논리 파티션의 다른 그룹에 대한 별도의 HMC 연결로 사용할 수도 있습니다. 예를 들어, 일반 비즈니스 트랜잭션이 실행되는 LAN과 분리된 관리 LAN을 가질 수 있습니다. 원격 관리자는 이 방식으로 HMC 및 다른 관리 장치에 액세스할 수 있습니다. 논리 파티션은 다른 네트워크 보안 도메인(예: 방화벽 뒤)에 있을 수도 있고, 이러한 두 도메인에 대해 서로 다른 HMC 네트워크 연결을 가질 수도 있습니다.

HMC용 웹 브라우저 요구사항

Hardware Management Console(HMC) 버전 9.1.0은 Google Chrome 버전 57, Microsoft Internet Explorer(IE) 버전 11.0, Mozilla Firefox 버전 45 및 52 Extended Support Release(ESR) 및 Safari 버전 10.1로 지원됩니다.

브라우저가 인터넷 프록시를 사용하도록 구성된 경우에는 로컬 IP 주소가 예외 목록에 포함되어야 합니다. 예외 목록에 대한 자세한 정보는 네트워크 관리자에게 문의하십시오. HMC에 도달하기 위해 여전히 프록시가 필요한 경우, 인터넷 옵션 창의 고급 탭 아래에 있는 프록시 연결을 통해 HTTP 1.1을 사용할 수 있도록 설정하십시오.

원격으로 HMC에 연결된 경우에 ASMI가 작동하려면 세션 쿠키를 사용해야 합니다. asm 프록시 코드는 세션 정보를 저장하고 사용합니다. 다음 단계에 따라 세션 쿠키를 사용하십시오.

Internet Explorer에서 세션 쿠키 사용

1. 도구를 선택하고 인터넷 옵션을 클릭하십시오.
2. 개인정보를 선택하고 고급을 클릭하십시오.
3. 세션 쿠키 항상 허용이 선택되어 있는지 확인하십시오. 선택되어 있지 않으면 자동 쿠키 처리 무시를 선택하고 세션 쿠키 항상 허용을 선택하십시오.
4. 자사 쿠키 및 타사 쿠키 아래 프롬프트를 선택하십시오.
5. 확인을 클릭하십시오.

Firefox에서 세션 쿠키 사용

1. 도구를 선택하고 옵션을 클릭하십시오.
2. 쿠키를 클릭하십시오.
3. 사이트에 쿠키 설정 허용을 선택하십시오.
4. 예외를 선택하고 HMC를 추가하십시오.
5. 확인을 클릭하십시오.

HMC 환경의 개인용 및 개방형 네트워크
HMC(Hardware Management Console)는 개인용 및 개방형 네트워크를 사용하도록 구성할 수 있습니다. 개인용 네트워크를 이용하면 선택한 범위의 경로지정 불가능 IP 주소를 사용할 수 있습니다. 공용 또는 "개방형" 네트워크는 HMC와 논리 파티션 및 정규 네트워크의 기타 시스템 사이의 네트워크 연결을 기술합니다.

사설망

HMC 사설망에서는 HMC와 HMC가 연결된 각 관리 시스템이 유일한 장치입니다. HMC는 각 관리 시스템의 FSP(Flexible Service Processor)에 연결됩니다.

대다수 시스템에서 FSP는 **HMC1** 및 **HMC2**로 레이블된 두 개의 이더넷 포트를 제공합니다. 최대 두 개의 HMC에 연결할 수 있습니다.

일부 시스템에는 이중 FSP 옵션이 있습니다. 이 상황에서는 두 번째 FSP가 예비 백업으로 작용합니다. FSP가 두 개인 시스템의 기본적인 설정 요구사항은 두 번째 FSP가 없는 시스템과 근본적으로 동일합니다. HMC를 각 FSP에 연결해야 하므로 FSP가 하나 이상이거나 관리 시스템이 다중일 경우 추가의 네트워크 하드웨어(예: LAN 스위치 또는 허브)가 필요합니다.

참고: 관리 시스템의 각 FSP 포트는 단 하나의 HMC에 연결해야 합니다.

공용 네트워크

개방형 네트워크는 방화벽이나 라우터에 연결하여 인터넷에 연결할 수 있습니다. 인터넷에 연결하면 HMC는 보고해야 할 하드웨어 오류가 있을 경우 홈을 호출할 수 있습니다.

HMC가 자체적으로 각 네트워크 인터페이스에서 자신의 방화벽을 제공합니다. 기본 방화벽은 HMC 설정 안내 마법사를 실행할 때 자동으로 구성되지만 초기 HMC 설치 및 구성 이후에 방화벽 설정을 사용자 정의할 수 있습니다.

HMC
HMC(Hardware Management Console)를 DHCP(동적 호스트 구성 프로토콜) 서버로 사용할 수 있습니다.

첫 번째 네트워크 인터페이스를 사설망으로 구성하려는 경우 다양한 DHCP 서버 IP 주소에서 선택하여 이의 클라이언트에 지정할 수 있습니다. 선택 가능한 주소 범위에는 라우트 불가능 표준 IP 주소 범위의 세그먼트가 포함되어 있습니다.

이러한 표준 범위 외에 특별한 IP 주소 범위가 IP 주소용으로 예약되어 있습니다. 이러한 특수 범위는 HMC 연결 개방형 네트워크가 라우트 불가능 주소 범위 중 하나를 사용할 경우 충돌을 방지하기 위해 사용할 수 있습니다. 선택된 범위에 따라, 사설망의 HMC 네트워크 인터페이스에는 자동으로 해당 범위의 첫 번째 IP 주소가 지정되며 서비스 프로세서에는 나머지 범위의 주소가 지정됩니다.

HMC의 DHCP 서버는 자동 할당을 사용하는데, 이는 각각의 고유한 서비스 프로세서 이더넷 인터페이스가 시작될 때마다 동일한 IP 주소가 재지정됨을 의미합니다. 각 이더넷 인터페이스는 내장 MAC(Media Access Control) 주소에 따라 고유한 ID를 갖는데, 이로써 DHCP 서버는 동일한 IP 매개변수를 재지정할 수 있습니다. **eth0** 및 **eth1** HMC 포트를 DHCP 주소로 사용하도록 구성할 수 있습니다.**eth0** 및 **eth1** HMC 포트를 DHCP 주소로 사용하도록 구성할 수 있습니다.

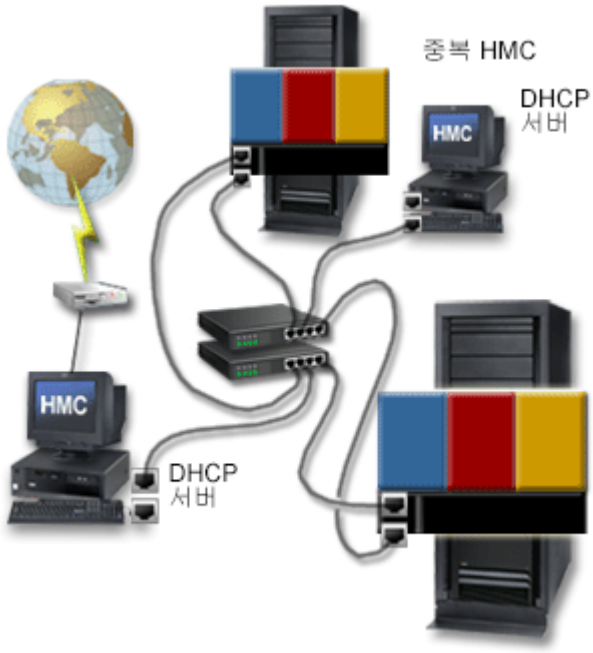
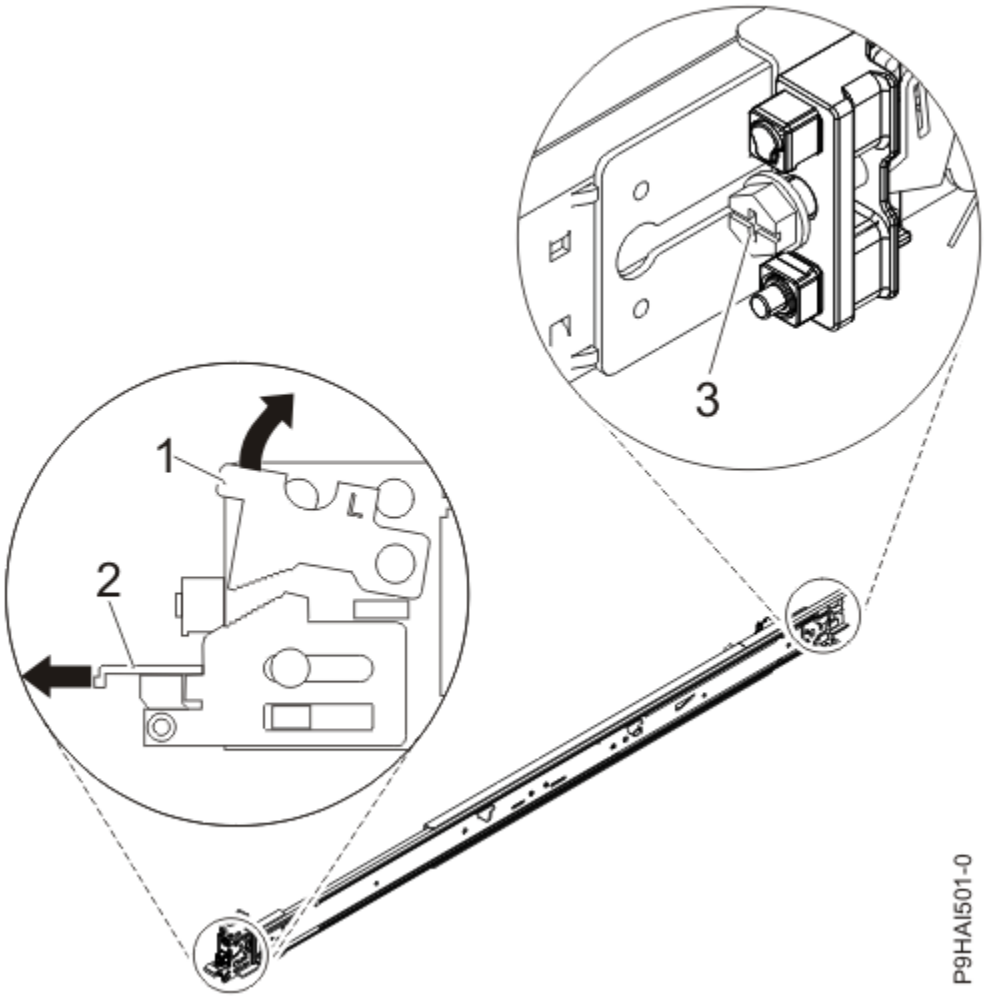


그림 *21.* 한 *HMC*가 *DHCP* 서버인 사설망

참고: IPv6를 사용하는 경우, 감지 프로세스를 수동으로 수행해야 합니다. IPv6의 경우 자동 감지를 사용할 수 없습니다.

HMC를 DHCP 서버로 구성하는 방법에 대한 자세한 정보는 61 페이지의 『HMC를 DHCP 서버로 구성』의 내용을 참조하십시오.

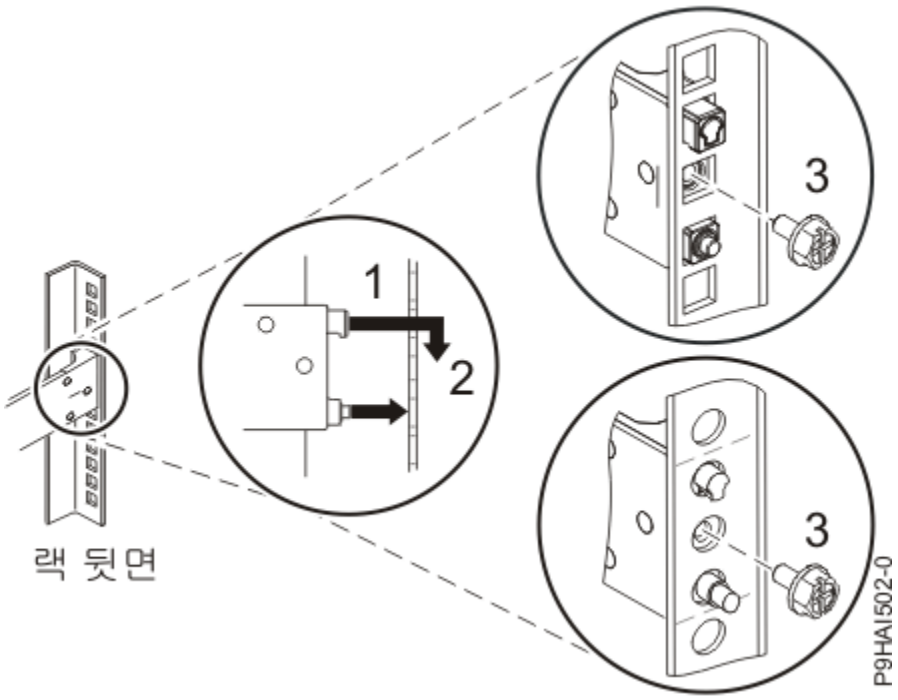


이 그림은 두 개의 관리 시스템이 있는 예비 HMC 환경을 보여줍니다. 첫 번째 HMC는 각 FSP의 첫 번째 포트에 연결되어 있고 예비 HMC는 각 HMC의 두 번째 포트에 연결되어 있습니다. 다른 범위의 IP 주소를 사용하여 각 HMC가 DHCP 서버로 구성되어 있습니다. 연결은 별도의 사설망을 통해 이루어집니다. 따라서 FSP 포트를 둘 이상의 HMC에 연결하지 않는 것이 중요합니다.

HMC에 연결된 각 관리 시스템의 FSP 포트에는 고유한 IP 주소가 필요합니다. 각 FSP가 고유의 IP 주소를 갖도록 하려면 HMC의 내장 DHCP 서버 기능을 사용하십시오. FSP가 활성 네트워크 링크를 감지하면 DHCP 서버를 찾기 위한 브로드캐스트 요청을 발행합니다. 올바로 구성된 경우 HMC는 선택한 주소 범위 중 하나를 할당하여 해당 요청에 응답합니다.

여러 개의 FSP가 있는 경우 HMC가 사설망에 FSP로 연결할 수 있도록 자체의 LAN 스위치 또는 허브가 있어야 합니다. 이 개인용 세그먼트는 더 큰 관리 스위치의 개인용 가상 *LAN*(VLAN)에서 여러 개의 포트로 존재할 수 있습니다. 여러 개의 개인용 VLAN이 있는 경우 이들이 격리되어 있는지와 크로스오버 트래픽이 없는지 확인해야 합니다.

HMC가 둘 이상인 경우 동일한 개방형 네트워크에서 각 HMC를 논리 파티션에 연결하고 HMC 상호간에도 연결해야 합니다.



이 그림은 두 개의 HMC가 사설망의 단일 관리 서버에 연결되고 공용 네트워크의 세 논리 파티션에 연결된 모습입니다. HMC의 네트워크 인터페이스가 세 개가 되도록 이더넷 어댑터를 추가할 수 있습니다. 이 세 번째 네트워크를 관리 네트워크로 사용하거나 CSM(Cluster Systems Manager) 관리 서버에 연결할 수 있습니다.

콜-홈 서버에 사용할 연결 방식 결정
콜-홈 서버 사용 시 갖게 되는 연결 옵션에 대해 자세히 학습합니다.

LAN 기반 인터넷 연결 또는 모뎀을 통한 전화 접속 연결을 사용하여 하드웨어 서비스 관련 정보를 IBM에 송신하도록 HMC(Hardware Management Console)를 구성할 수 있습니다.

LAN 기반 인터넷 연결 구성 시 두 개의 통신 선택사항을 갖게 됩니다. 첫 번째 선택사항은 표준 SSL(Secure Sockets Layer)을 사용하는 것입니다. 프록시 서버를 통해 인터넷에 연결할 때 SSL 통신을 사용할 수 있습니다. SSL 연결 시 기업 보안 지침에 대한 순응도가 더욱 좋습니다.

참고: 개방형 네트워크 인터페이스 연결이 IPv6(Internet Protocol Version 6)만을 사용하는 경우, 인터넷 VPN을 사용하여 지원에 연결할 수 없습니다. 사용되는 프로토콜에 대한 자세한 정보는 46 페이지의 『인터넷 프로토콜 선택』의 내용을 참조하십시오.

다음과 같은 인터넷 연결 사용에 따른 이점이 있습니다.

- 전송 속도 개선
- 고객 비용 감축(예: 전용 아날로그 전화 회선 비용)
- 신뢰성 증대

선택하는 연결 방법에 관계 없이 다음과 같은 보안 특성이 적용됩니다.

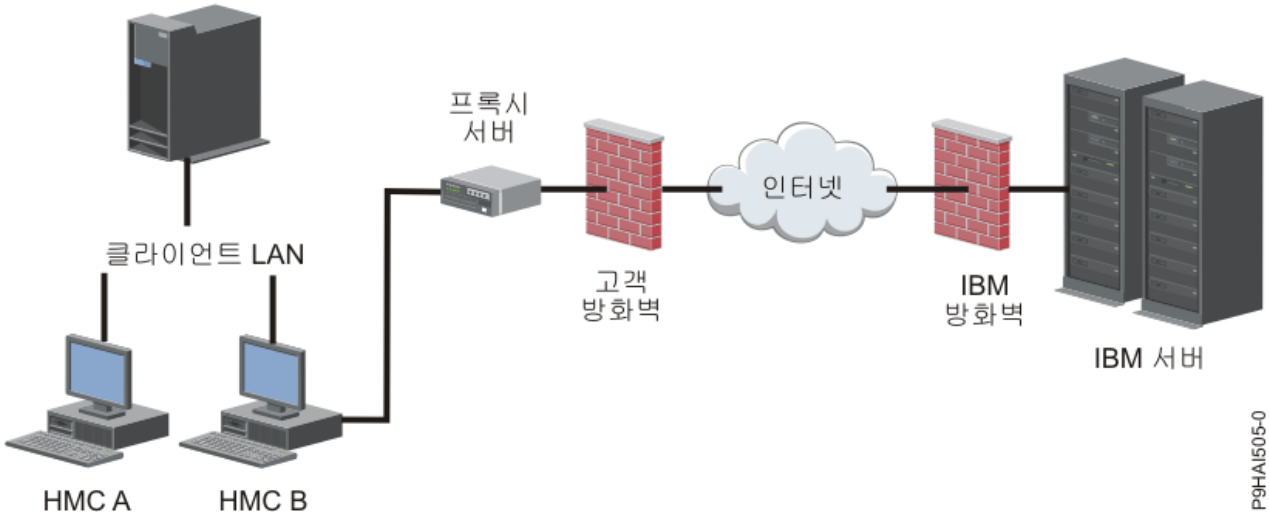
- 원격 지원 기능 요청은 항상 HMC에서 IBM으로 시작됩니다. 인바운드 연결은 절대 IBM Service Support System에서 시작되지 않습니다.
- HMC와 IBM Service Support System 사이에서 전송되는 모든 데이터는 고급 암호화 기술을 사용하여 암호화됩니다. 선택하는 연결 방법에 따라 SSL 또는 IPSec ESP(Encapsulating Security Payload)를 사용하여 암호화됩니다.
- 암호화된 연결을 초기화할 때 HMC는 대상 목적지를 IBM Service Support System의 목적지로 인증합니다.

IBM Service Support System으로 송신되는 데이터는 전적으로 하드웨어 문제점 및 구성에 관한 정보로 이루어집니다. 애플리케이션 또는 고객 데이터는 IBM에 전송되지 않습니다.

프록시 서버에서 간접 인터넷 연결 사용

설치 시 HMC를 사설망에 두어야 하는 경우, 요청을 인터넷에 전달할 수 있는 SSL 프록시를 사용하여 간접적으로 인터넷에 연결할 수 있습니다. SSL 프록시 사용에 따른 다른 잠재 이점 중 하나는 프록시가 로깅 및 감사 기능을 지원할 수 있다는 점입니다.

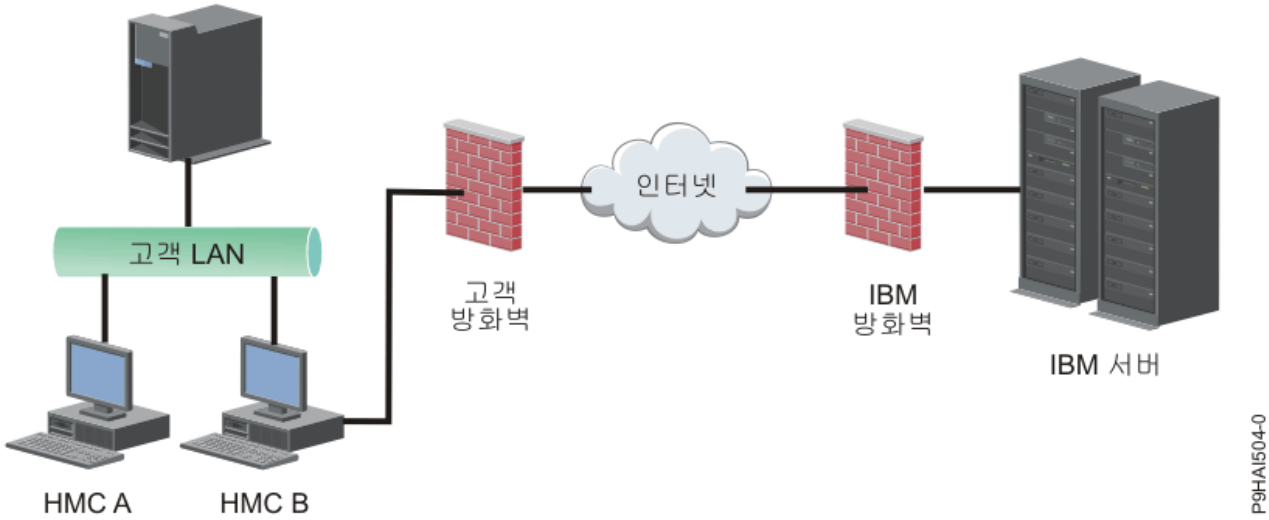
SSL 소켓을 전달하려면 프록시 서버가 기본 프록시 헤더 기능(RFC 2616에 기술됨)과 CONNECT 메소드를 지원해야 합니다. 선택적으로, 프록시 서버를 통해 소켓 전달을 시도하기 전에 HMC가 인증하도록 기본 프록시 인증(RFC 2617)을 구성할 수 있습니다.



HMC가 정상적으로 통신하기 위해서는 클라이언트의 프록시 서버가 443 포트와의 연결을 허용해야 합니다. HMC가 연결할 수 있는 대상을 특정 IP 주소로 제한하도록 프록시 서버를 구성할 수 있습니다. 46 페이지의 『인터넷 SSL 주소 리스트』의 IP 주소 목록을 참조하십시오.

직접 인터넷 SSL 연결 사용

HMC를 인터넷에 연결할 수 있고 설정된 TCP 패킷이 46 페이지의 『인터넷 SSL 주소 리스트』에 설명된 목적지로 아웃바운드 플로우하도록 외부 방화벽을 설정할 수 있는 경우, 직접 인터넷 연결을 사용할 수 있습니다.



인터넷 *SSL*을 사용하여 원격 지원에 연결

모든 통신은 HMC(Hardware Management Console)에서 시작하는 TCP 소켓을 통해 처리되며 높은 수준의 SSL을 사용하여 전송되는 데이터를 암호화합니다. 이러한 연결이 가능한 외부 방화벽을 구성할 수 있도록 목적지 TCP/IP 주소가 공개됩니다(46 페이지의 『인터넷 SSL 주소 리스트』 참조).

참고: 모든 통신에 표준 HTTPS 포트 443이 사용됩니다.

HMC는 인터넷에 직접 연결하거나 고객이 제공하는 프록시 서버를 통해 간접적으로 연결할 수 있습니다. 사용자 설치에 가장 적합한 방식은 사용자 엔터프라이즈의 보안 및 네트워킹 요구사항에 의해 결정됩니다. HMC(직접 또는 SSL 프록시를 통해)는 인터넷 SSL 연결을 사용하도록 구성된 경우 다음과 같은 주소를 사용합니다.

인터넷 프로토콜 선택
HMC(Hardware Management Console)가 서비스 제공자에 연결할 때 사용되는 IP 주소 버전을 결정합니다.

대부분의 사용자는 IPv4(Internet Protocol Version 4)를 사용하여 서비스 제공자에 연결합니다. IPv4 주소는 인터넷 액세스 시 점으로 구분된 4바이트 IPv4 주소를 나타내는 형식(예: 9.60.12.123)으로 표시됩니다. 또한 IPv6(Internet Protocol Version 6)를 사용하여 서비스 제공자에 연결할 수도 있습니다. IPv6는 종종 고유한 주소 공간을 보장하기 위해 네트워크 관리자가 사용합니다. 설치 시 사용된 인터넷 프로토콜을 확실히 모를 경우 네트워크 관리자에게 문의하십시오. 각 버전 사용에 관한 자세한 정보는 62 페이지의 『IPv4 주소 설정』 및 62 페이지의 『IPv6 주소 설정』을 참조하십시오.

인터넷 *SSL* 주소 리스트
HMC(Hardware Management Console)가 인터넷 SSL 연결을 사용 중일 때 사용하는 주소에 대해 학습합니다.

HMC는 인터넷 SSL 연결을 사용하도록 구성된 경우 다음과 같은 IPv4 주소를 사용하여 IBM Service and Support에 접속합니다.

다음 IPv4 주소는 모든 지역에 사용됩니다.

- 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

다음 IPv4 주소는 아메리카 지역에 사용됩니다.

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

다음 IPv4 주소는 아메리카 이외의 지역에 사용됩니다.

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

참고: HMC가 이러한 서버에 연결할 수 있도록 방화벽을 구성하는 경우, 지리적 영역에 특정되는 IP 주소만 있으면 됩니다.

HMC는 인터넷 SSL 연결을 사용하도록 구성된 경우 다음과 같은 IPv6 주소를 사용하여 IBM Service and Support에 접속합니다.

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

다중 콜-홈 서버 사용
콜-홈 서버를 둘 이상 사용하는 경우 알아야 하는 사항을 학습합니다.

단일 지점의 실패를 방지하려면 다중 콜-홈 서버를 사용하도록 HMC(Hardware Management Console)를 구성해야 합니다. 첫 번째 사용 가능한 콜-홈 서버가 각 서비스 에이전트를 처리합니다. 이 콜-홈 서버에서 연결 또는 전송이 실패하는 경우 한 요청이 성공하거나 모두 시도될 때까지 사용 가능한 다른 콜-홈 서버를 사용하여 서비스 요청이 재시도됩니다.

문제점 분석에 의해 주어진 관리 시스템의 1차 분석 콘솔로 식별되는 연결된 HMC가 문제점을 보고합니다. 또한 이 1차 콘솔이 문제점 보고서를 2차 HMC로 복제합니다. 2차 HMC는 1차 HMC가 네트워크에서 인식할 수 있어야 합니다. 다음과 같은 경우 2차 HMC는 1차 HMC에 의해 추가 콜-홈 서버로 인식됩니다.

- 1차 HMC가 "감지된" 콜-홈 서버를 사용하도록 구성되어 있고 콜-홈 서버가 1차 HMC와 동일한 서브네트에 있거나 동일한 시스템을 관리합니다.
- 콜-홈 서버가 아웃바운드 연결에 사용할 수 있는 콜-홈 서버 콘솔 리스트에 수동으로 추가되었습니다.

HMC 구성 준비

구성 단계를 시작하기 전에 알아야 하는 필수 구성 설정값에 대해 학습합니다.

HMC를 구성하려면 관련 개념을 이해해야 하고 의사결정을 하며 정보도 준비해야 합니다.

HMC를 다음 위치에 연결할 때 필요한 정보에 대해 학습합니다.

- 관리 시스템의 서비스 프로세서
- 관리 시스템의 논리 파티션
- 원격 워크스테이션
- IBM 서비스 - “콜-홈” 기능 구현

참고: 추가의 연결 및 보안 정보를 사용할 수 있습니다. 자세한 정보는 **IBM POWER6 프로세서 기반 시스템 이상 및 IBM Storage Systems DS8000의 HMC Connectivity Security에 대한 ESA** 백서를 참조하십시오(IBM Electronic Service Agent(http://www-01.ibm.com/support/esa/security.htm)에서 사용 가능).

HMC 구성을 준비하려면 다음 단계를 완료하십시오.

1. 설치하려는 HMC 코드 버전의 최신 레벨을 획득하여 설치하십시오.
2. 관리하는 서버와 관련하여 HMC의 실제 위치를 판별하십시오. HMC가 관리 시스템으로부터 25피트 이상 떨어져 있는 경우 서비스 담당자가 HMC에 액세스할 수 있도록 관리 시스템에서 HMC로 웹 브라우저 액세스를 제공해야 합니다.
3. HMC가 관리하는 서버를 식별합니다.
4. 서버 관리에 개인용 네트워크를 사용할지 개방형 네트워크를 사용할지 여부를 결정하십시오. 개인용 네트워크를 사용하기로 한 경우 CSM(Cluster Systems Management) 구성을 사용하는 경우가 아니면 DHCP를 사용하십시오. CSM은 IPv6를 지원하지 않습니다. CSM에 액세스하려면 두 개의 네트워크가 있어야 합니다. CSM에 대한 자세한 정보는 해당 기능과 함께 제공된 문서를 참조하십시오. 개인용 및 개방형 네트워크에 대한 자세한 정보는 61 페이지의 『개인용 또는 개방형 네트워크 선택』을 참조하십시오.
5. 개방형 네트워크를 사용하여 FSP를 관리하는 경우 ASMI(Advanced System Management Interface) 메뉴를 사용하여 수동으로 FSP의 주소를 설정해야 합니다. 개인용의 경로 지정 불가능 네트워크가 권장됩니다.
6. 두 개의 HMC가 있는 경우 1차 및 2차 HMC를 지정하십시오. 1차 HMC는 물리적으로 시스템과 더 가까워야 하고 홈을 호출하도록 구성된 HMC여야 합니다.
7. HMC를 원격 워크스테이션, 논리 파티션 및 네트워크 장치에 연결할 때 필요한 네트워크 설정을 판별하십시오.
8. HMC가 홈을 호출하는 방법을 정의하십시오. 콜홈 옵션에는 아웃바운드 전용 SSL(Secure Socket Layer) 인터넷 연결, 모뎀 또는 VPN(가상 사설망) 연결이 포함되어 있습니다.
9. 작성하는 HMC 사용자, 이의 비밀번호 및 역할을 결정하십시오. **hscroot** 및 **hscpe** 사용자에게 비밀번호를 지정해야 합니다.
10. 콜홈 구성 시 필요한 다음과 같은 회사 연락처 정보를 기록하십시오.
    - 회사 이름
    - 관리자 연락처
    - 이메일 주소
    - 전화번호

- 팩스 번호
- 실제 HMC 위치의 상세 주소

11. 콜-홈을 통해 IBM Service에 정보가 전송될 때 이메일을 사용하여 운영자 또는 시스템 관리자에게 통지하려는 경우, 사용할 SMTP(Simple Mail Transfer Protocol) 서버와 이메일 주소를 식별하십시오.
12. 다음과 같은 비밀번호를 정의해야 합니다.
    - HMC를 FSP에 인증할 때 사용되는 액세스 비밀번호
    - **관리** 사용자에게 사용되는 ASMI 비밀번호
    - **일반** 사용자에게 사용되는 ASMI 비밀번호

    처음으로 HMC에서 새 서버로 연결할 때 비밀번호를 작성하십시오. HMC가 예비 HMC이거나 두 번째 HMC인 경우 HMC 사용자 비밀번호를 획득하여 관리 서버의 FSP에 처음 연결할 때 이를 입력하십시오.

이러한 준비 단계를 완료하면 48 페이지의 『HMC의 설치 전 구성 워크시트』를 완성하십시오.

HMC의 설치 전 구성 워크시트
이 워크시트를 사용하여 설치에 필요한 설치 정보를 준비할 수 있습니다.

네트워크 설정값

LAN 인터페이스: 이 HMC가 관리 시스템, 논리 파티션, 서비스 및 지원 센터, 원격 사용자에게 연결할 때 사용되는 가용 어댑터(예: eth0, eth1)를 선택하십시오. 추가 정보는 39 페이지의 『HMC 네트워크 연결』의 내용을 참조하십시오.HMC를 통한 연결은 개인용 또는 개방형 네트워크에서 가능합니다.

이더넷 어댑터 속도 및 양방향 전송
원하는 이더넷 어댑터 속도와 양방향 전송 모드를 입력하십시오. 사용자 하드웨어에서 최적의 결과를 생성할 속도와 양방향 전송 모드를 모를 경우 자동 감지 옵션이 최적 옵션을 결정합니다. 기본 = 매체 속도 자동 감지가 이더넷 어댑터의 양방향 전송 모드에서 속도를 지정합니다. 고정된 매체 속도를 지정해야 하는 경우가 아니면 자동 감지를 선택하십시오. FSP(스위치/HMC)에 연결된 모든 장치는 기본 FSP 설정이며 변경할 수 없으므로 자동(속도)/자동(양방향) 모드로 설정되어야 합니다.

표 *7.* 이더넷 어댑터 속도 및 양방향 전송.

특성	**eth0**	**eth1**	**eth2**	**eth3**
속도 및 양방향 전송 모드 선택				
매체 속도(자동 감지, 10/100/1000 전이중/반이중)				

개인용 및 개방형 네트워크에 대한 자세한 정보는 41 페이지의 『HMC 환경의 개인용 및 개방형 네트워크』를 참조하십시오.

표 *8.* 개인용 또는 개방형 네트워크.

특성	**eth0**	**eth1**	**eth2**	**eth3**
각 어댑터에 **개인용** 또는 **개방형** 네트워크를 지정하십시오.				

DHCP(동적 호스트 구성 프로토콜)를 이용하면 동적 클라이언트를 자동으로 구성할 수 있습니다. 이 HMC를 DHCP 서버로 지정할 수 있습니다. 이것이 사설망의 첫 번째 또는 유일한 HMC인 경우 HMC를 DHCP 서버로 사용할 수 있습니다. HMC를 DHCP 서버로 사용하면 HMC가 네트워크의 관리 시스템을 자동으로 구성 및 감지합니다.

사설망으로 지정된 이더넷 어댑터의 경우 다음 표를 완성하십시오.

표 *9. DHCP* 서버.		
특성	**eth0**	**eth1**
이 HMC를 DHCP 서버로 지정하시겠습니까? (예/아니오)		
"예"일 경우 사용하려는 IP 주소 범위를 기록하십시오.		

7063-CR1 HMC를 사용 중인 경우 HMC의 BMC(Baseboard Management Controller)에 액세스하려면 이더넷 **IPMI** 포트를 네트워크에 연결해야 합니다. 추가 정보는 61 페이지의 『BMC 연결 구성』의 내용을 참조하십시오. BMC 연결을 위해 다음 표를 완성하십시오.

표 *10. BMC* 연결.	
특성	**IPMI**
DHCP 모드를 통해 이 연결을 구성하시겠습니까? (예/아니오)	
"아니오"일 경우 아래에 지정된 정적 주소를 나열하십시오.	
IP 주소:	
서브넷 마스크 :	
게이트웨이:	

개방형 네트워크로 지정된 이더넷 어댑터의 경우 다음 표를 완성하십시오. 다른 인터넷 프로토콜 버전에 대한 자세한 정보는 56 페이지의 『HMC 네트워크 유형 구성』을 참조하십시오.

IPv6 사용

IPv6를 사용하는 경우 네트워크 관리자와 상담하여 IP 주소 획득 방식을 결정하십시오. 그런 후 다음 표를 완성하십시오.

표 *11. IPv6*(정적).				
특성	**eth0**	**eth1**	**eth2**	**eth3**
정적으로 지정되는 IP 주소를 사용하고 계십니까? "예"일 경우 여기에 주소를 기록하십시오.				

표 *12. IPv6*(*DHCP* 서버).				
특성	**eth0**	**eth1**	**eth2**	**eth3**
DHCP 서버로부터 IP 주소를 가져오십니까? (예/아니오)				

표 *13. IPv6*(*IPv6* 라우터).				
특성	**eth0**	**eth1**	**eth2**	**eth3**
IPv6 라우터로부터 IP 주소를 가져오십니까?				

IPv6 주소 설정에 대한 자세한 정보는 62 페이지의 『IPv6 주소 설정』을 참조하십시오. IPv6 주소만 사용하는 데 대한 자세한 정보는 62 페이지의 『IPv6 주소만 사용』을 참조하십시오.

IPv4 사용

IPv4를 사용하는 개방형 네트워크로 지정된 이더넷 어댑터의 경우 다음 표를 완성하십시오.

표 *14. IPv4.*				
특성	**eth0**	**eth1**	**eth2**	**eth3**
IP 주소를 자동으로 획득하시겠습니까? (예/아니오)				
"아니오"일 경우 아래에 지정된 주소를 나열하십시오.				
TCP/IP 인터페이스 주소:				
TCP/IP 인터페이스 네트워크 마스크:				
방화벽 설정값:				
HMC 방화벽 설정을 구성하시겠습니까? (예/아니오)				
"예"일 경우 방화벽을 통해 허용되어야 하는 IP 주소와 애플리케이션을 나열하십시오.				

TCP/IP 정보

SE(Support Element) 및 HMC(Hardware Management Console)의 경우 각 노드에 고유한 TCP/IP 주소가 필요합니다. 지정된 네트워크 마스크는 기본적으로 로컬 개인용 LAN의 고유 주소를 생성하는 데 사용됩니다. 관리 대상 TCP/IP 주소를 갖는 대형 네트워크에 노드를 연결하는 경우 사용될 TCP/IP 주소를 지정할 수 있습니다. 기본은 시스템에 의해 생성되는 것입니다.

방화벽 설정값

HMC 방화벽 설정값은 HMC의 특정 네트워크 애플리케이션에 대한 액세스를 허용 또는 거부하는 보안 장벽을 작성합니다. 각 실제 네트워크 인터페이스에 대해 개별적으로 이러한 제어 설정을 지정하여 각 네트워크에서 액세스할 수 있는 HMC 네트워크 애플리케이션을 제어할 수 있습니다.

하나 이상의 어댑터를 개방형 네트워크 어댑터로 구성한 경우 HMC가 LAN에 액세스할 수 있도록 다음과 같은 추가 정보를 제공해야 합니다.

표 *15.* 개방형 네트워크 어댑터.	
로컬 호스트 정보	
HMC 호스트 이름	
도메인 이름	
HMC의 설명:	
게이트웨이 정보	
게이트웨이 주소: (nnn.nnn.nnn.nnn)	
게이트웨이 장치:	
DNS 사용	

표 *15.* 개방형 네트워크 어댑터. *(계속)*	
로컬 호스트 정보	
DNS를 사용하시겠습니까?(예/아니오)	
“예”일 경우 아래에 DNS 서버 검색 순서를 지정하십시오.	
1.	
2.	
도메인 접미부 검색 순서:	
1.	
2.	

로컬 호스트 정보
사용자의 HMC(Hardware Management Console)를 네트워크에 식별시키려면 HMC의 호스트 이름과 도메인 이름을 입력하십시오. 네트워크에서 짧은 호스트 이름만 사용하는 경우가 아니면 완전한 호스트 이름을 입력하십시오. 도메인 이름의 예: name.yourcompany.com

게이트웨이 정보
기본 게이트웨이를 정의하려면 IP 패킷의 경로 지정에 사용되는 TCP/IP 주소를 작성하십시오. 게이트웨이 주소는 소스와 동일한 서브넷에 대상 스테이션이 없는 경우 데이터 전송 시 각 컴퓨터나 네트워크 장치에 알려줍니다.

DNS 사용
DNS(Domain Name System)는 IP 기반 컴퓨터를 찾기 위한 표준 명명 규칙을 제공하는 데 사용됩니다. DNS 서버를 정의하면 IP 주소가 아닌 호스트 이름을 사용하여 서버 및 HMC(Hardware Management Console)를 식별할 수 있습니다.

DNS 서버 탐색 순서
호스트 이름과 IP 주소를 맵핑하기 위해 탐색할 DNS 서버의 IP 주소를 입력하십시오. 이 탐색 순서는 DNS가 사용되는 경우에만 사용할 수 있습니다.

도메인 접미부 탐색 순서
사용 중인 도메인 접미부를 입력하십시오. HMC는 DNS 탐색 시 규정되지 않은 이름을 추가하기 위해 도메인 접미부를 사용합니다. 접미부는 나열된 순서대로 탐색됩니다. 이 탐색 순서는 DNS가 사용되는 경우에만 사용할 수 있습니다.

이메일 통지

시스템에서 하드웨어 문제점이 발생하는 경우 이메일로 통지를 받으려면 이메일 주소를 나열하십시오.

표 *16.* 이메일 통지.	
특성	**입력 필드**
이메일 주소:	
SMTP 서버:	
포트:	
통지 대상 오류:	
콜-홈 문제점 이벤트에 한함	
모든 문제점 이벤트	

SMTP 서버
시스템 이벤트를 통지받을 서버의 SMTP(Simple Mail Transfer Protocol) 주소를 입력하십시오. SMTP 서버 이름의 예는 다음과 같습니다. `relay.us.ibm.com`

SMTP는 이메일 전송 시 사용되는 프로토콜입니다. SMTP를 사용하는 경우 클라이언트는 SMTP 프로토콜을 사용하여 메시지를 송신하고 SMTP 서버와 통신합니다.

서버의 SMTP 주소를 모르거나 확실하지 않은 경우 네트워크 관리자에게 문의하십시오.

포트
시스템 이벤트를 통지받을 서버의 포트 번호를 입력하거나 기본 포트를 사용하십시오.

통지받을 이메일 주소
시스템 이벤트 발생 시 통지받을 구성된 이메일 주소를 입력하십시오.

- 콜-홈 기능을 작성하는 이벤트가 발생하는 경우에만 통지를 수신하려면 **콜-홈 문제점 이벤트에 한함**을 선택하십시오.
- 종류에 관계 없이 이벤트 발생 시 통지를 수신하려면 **모든 문제점 이벤트**를 선택하십시오.

서비스 연락처 정보

표 *17.* 서비스 연락처 정보.

특성	**입력 필드**
회사 이름	
관리자 이름	
이메일 주소	
전화번호	
대체 전화번호	
팩스 번호	
대체 전화번호	
상세 주소	
상세 주소 2	
구/군/시	
시/도	
우편번호	
국가 또는 지역	
HMC 위치(위의 관리자 주소와 동일한 경우 “상동”으로 지정):	
상세 주소	
상세 주소 2	
구/군/시	
시/도	
우편번호	
국가 또는 지역	

서비스 권한 부여 및 연결

서비스 제공자에 접속하기 위한 연결 유형을 선택하십시오. 보안 특성 및 구성 요구사항을 포함하는 이러한 방법에 대한 설명은 68 페이지의 『기존 콜-홈 서버를 선택하여 HMC의 서비스 및 지원 센터에 연결』을 참조하십시오.

표 *18.* 서비스 권한 부여 및 연결.	
특성	**입력 필드**
인터넷을 통한 SSL(Secure Sockets Layer)	_____
인터넷을 통한 VPN(가상 사설망)	_____

인터넷을 통한 SSL(Secure Sockets Layer):

HMC를 통한 기존 인터넷 연결이 있는 경우 이를 사용하여 서비스 제공자를 호출할 수 있습니다. 기존 인터넷 연결을 통해 암호화된 SSL(Secure Sockets Layer)을 사용하여 서비스 제공자에 직접 연결할 수 있습니다. SSL 프록시를 사용한 간접 연결을 사용하여 암호화된 SSL의 사용을 구성하려는 경우 **SSL 프록시 사용**을 선택하십시오.

표 *19. SSL.*	
특성	**입력 필드**
SSL 프록시 사용 여부? (예/아니오)	
"예"일 경우 아래 정보를 나열하십시오.	
주소:	
포트:	
SSL 프록시를 사용한 인증?	
"예"일 경우 아래 정보를 나열하십시오.	
사용자:	
비밀번호:	

사용되는 인터넷 연결 프로토콜

다른 인터넷 프로토콜에 대한 자세한 정보는 56 페이지의 『HMC 네트워크 유형 구성』을 참조하십시오.

___ IPv4

___ IPv6

___ IPv4 및 IPv6

VPN(가상 사설망)

HMC를 통한 기존 인터넷 연결이 있는 경우 이를 사용하여 서비스 제공자를 호출할 수 있습니다. 기존 인터넷 연결을 통해 VPN(가상 사설망)으로 서비스 제공자에 직접 연결할 수 있습니다.

참고: 인터넷을 통해 VPN(가상 사설망)을 선택하는 경우 다른 옵션을 선택할 수 없습니다.

콜-홈 서버

콜-홈 서버로 서비스 및 지원 센터에 연결하기 위해 구성하려는 HMC를 결정합니다. 다중 콜-홈 서버 사용에 대한 자세한 정보는 46 페이지의 『다중 콜-홈 서버 사용』을 참조하십시오.

___ 이 HMC

___ 다른 HMC

다른 HMC에 체크한 경우 콜-홈 서버로 구성된 다른 HMC를 여기에 나열하십시오.

표 *20.* 콜-홈 서버로 구성된 다른 *HMC.*
콜-홈 서버로 구성된 HMC 호스트 이름 또는 IP 주소 리스트

추가 지원에 따른 이점

내 시스템 및 프리미엄 검색

표 *21.* 내 시스템 및 프리미엄 검색.	
특성	**입력 필드**
IBM ID 나열	_____
추가 IBM ID 나열	_____

전자 서비스 웹 사이트의 내 시스템 및 프리미엄 검색 섹션에 있는 귀중한 사용자 정의 지원 정보에 액세스하려면 고객은 이 시스템에 자신의 IBM ID를 등록해야 합니다. 아직 ID가 없는 경우 www.ibm.com/account/profile에서 IBM ID를 등록할 수 있습니다.

참고: IBM은 IBM Electronic Service Agent 애플리케이션에서 수집한 정보를 사용하여 개별화된 웹 기능을 제공합니다. 이러한 기능을 사용하려면 먼저 IBM 등록 웹 사이트(http://www.ibm.com/account/profile)에 등록해야 합니다.

사용자에게 Electronic Service Agent 정보를 사용하여 웹 기능을 개별화할 수 있는 권한을 부여하려면 IBM 등록 웹 사이트에 등록한 IBM ID를 입력하십시오. 시스템에 IBM ID를 등록한 고객에게 제공되는 귀중한 지원 정보를 확인하려면 http://www.ibm.com/support/electronic으로 가십시오.

HMC 구성

네트워크 연결, 보안, 서비스 애플리케이션 및 일부 사용자 기본설정을 구성하는 방법에 대해 학습합니다.

HMC 구성에 적용할 사용자 정의 레벨에 따라, 사용자의 요구에 맞게 HMC를 설정할 수 있는 몇 가지 옵션이 부여됩니다. 설치 안내 마법사는 HMC 설정을 용이하게 하도록 고안된 HMC의 툴입니다. 권장되는 HMC 환경을 빠르게 작성할 수 있는 마법사 내의 단축 경로를 선택하거나 마법사가 안내하는 설정값을 모두 탐색하도록 선택할 수 있습니다. HMC 메뉴를 사용하여 HMC 구성을 통해 마법사의 도움 없이 구성 단계를 수행할 수도 있습니다.

시작하기 전에 단계를 성공적으로 완료하는 데 필요한 필수 구성 정보를 수집하십시오. 47 페이지의 『HMC 구성 준비』의 필수 정보 목록을 참조하십시오. 준비를 완료하면 48 페이지의 『HMC의 설치 전 구성 워크시트』를 완성하고 이 섹션으로 돌아옵니다.

설정 안내 마법사를 통한 단축 경로를 사용하여 HMC 구성

대부분의 경우 기본 설정값을 사용하여 효율적으로 작동하도록 HMC를 설정할 수 있습니다. 이 단축 경로 체크리스트를 사용하여 HMC를 서비스용으로 준비할 수 있습니다. 이러한 단계를 완료하면 HMC는 (직접 연결되는) 사설망에서 DHCP(Dynamic Host Configuration Protocol) 서버로 구성됩니다.

메뉴를 사용하여 HMC 구성

이 절에서는 HMC 구성 프로세스를 볼 수 있는 전체 HMC 구성 태스크의 목록을 제공합니다. 설치 안내 마법사를 사용하지 않을 경우 이 옵션을 선택하십시오.

구성 설정값을 적용하려면 HMC를 재시작해야 하므로 이 체크리스트를 인쇄하여 HMC 구성 시 참고하십시오.

이 정보에는 이 문서에 포함되지 않는 태스크에 대한 참조가 포함되어 있습니다. HMC 또는 웹의 IBM Power Systems Hardware Information에 액세스할 수 있습니다. HMC에서 IBM Knowledge Center는 작업 표시줄의 오른쪽 상단 구석에서 액세스할 수 있습니다. 웹에서 IBM Knowledge Center는 https://www.ibm.com/support/knowledgecenter에서 액세스할 수 있습니다.

이 정보에는 이 PDF에 포함되지않은 태스크에 대한 참조가 포함되어 있습니다. HMC 시작 페이지의 **추가 자원** 섹션에서 추가 지원 자원에 액세스할 수 있습니다.

선행 조건

HMC 메뉴를 사용하여 HMC 구성을 시작하기 전에 47 페이지의 『HMC 구성 준비』에 설명된 구성 준비 활동을 완료하십시오.

표 *22.* 수동 *HMC* 구성 태스크 및 관련 정보	
태스크	**관련 정보**
1. HMC를 시작합니다.	55 페이지의 『HMC 시작』
2. 날짜 및 시간을 설정합니다.	
3. 사전 정의된 비밀번호를 변경합니다.	
4. 추가 사용자를 작성하고 이 단계를 완료하면 이 체크리스트로 돌아옵니다.	
5. 네트워크 연결을 구성합니다.	56 페이지의 『HMC 네트워크 유형 구성』
6. HMC 모델 7063-CR1의 경우 BMC(Baseboard Management Controller) IP 주소를 구성해야 합니다.	61 페이지의 『BMC 연결 구성』
7. 개방형 네트워크와 고정 IP 주소를 사용하는 경우 식별 정보를 설정합니다.	
8. 개방형 네트워크와 고정 IP 주소를 사용하는 경우 경로 지정 항목을 기본 게이트웨이로 구성합니다.	64 페이지의 『경로 지정 항목을 기본 게이트웨이로 구성』
9. 개방형 네트워크와 고정 IP 주소를 사용하는 경우 도메인 이름 서비스를 구성합니다.	64 페이지의 『도메인 이름 서비스 구성』
10. 고정 IP 주소를 사용하고 있고 DNS가 사용되는 경우 도메인 접미부를 구성합니다.	65 페이지의 『도메인 접미부 구성』
11. IBM 서비스 및 지원에 연결하여 이 단계를 완료하면 이 체크리스트로 돌아오도록 서버를 구성합니다.	66 페이지의 『서비스 및 지원 센터에 오류를 보고하도록 로컬 콘솔 구성』
12. 콜홈용 이벤트 관리자를 구성합니다.	69 페이지의 『콜홈용 이벤트 관리자 구성』
13. 관리 시스템을 전원에 연결합니다.	
14. 관리 시스템의 비밀번호 및 각 ASMI 비밀번호(일반 및 관리)를 설정합니다.	70 페이지의 『관리 시스템의 비밀번호 설정』
15. ASMI에 액세스하여 관리 시스템의 날짜 및 시간을 설정합니다.	
16. 관리 시스템을 시작하고 이 단계를 완료하면 이 체크리스트로 돌아옵니다.	
17. 관리 시스템에 하나의 논리 파티션이 있는지 확인합니다.	
18. 선택사항: 다른 관리 시스템을 추가하고 이 단계를 완료하면 이 체크리스트로 돌아옵니다.	
19. 선택사항: HMC에 새 서버를 설치하는 경우 논리 파티션을 구성하고 운영 체제를 설치합니다.	
20. 이번에 새 서버를 설치하지 않을 경우 선택적 구성 이후 태스크를 수행하여 구성을 추가로 사용자 정의하십시오.	72 페이지의 『구성 이후 단계』

HMC 시작

HMC에 로그인하여 인터페이스에 표시할 언어를 선택할 수 있습니다. 처음으로 HMC에 로그인할 때에는 기본 사용자 ID `hscroot` 및 비밀번호 `abc123`을 사용하십시오.

이 태스크 정보

HMC를 시작하려면 다음 프로시저를 수행하십시오.

프로시저

1. 전원 버튼을 눌러 HMC를 켜십시오.
2. 영어가 기본설정 언어인 경우 4 단계에서 계속하십시오.

   기본설정 언어가 영어 이외의 언어인 경우 로케일을 변경하도록 프롬프트되면 숫자 **2**를 입력하십시오.

   참고: 이 프롬프트는 조치가 없는 경우 30초 후에 제한시간 초과됩니다.
3. **로케일 선택** 창의 목록에서 표시할 로케일을 선택한 후 **확인**을 클릭하십시오. 로케일은 HMC 인터페이스가 사용하는 언어를 식별합니다.
4. **Hardware Management Console 웹 애플리케이션 로그온 및 시작**을 클릭하십시오.
5. 다음의 기본 사용자 ID와 비밀번호를 사용하여 HMC에 로그인하십시오.

   ID: `hscroot`
   비밀번호: `abc123`

   HMC Enhanced
   향상된 PowerVM 기능이 있는 새 고급 GUI를 표시합니다.

   HMC Classic
   향상된 PowerVM 기능이 없는 표준 GUI를 표시합니다.

   참고: HMC가 DHCP 서버 역할을 수행하는 경우, HMC가 처음으로 서비스 프로세서에 연결할 때 기본 비밀번호를 사용합니다.
6. Enter를 누르십시오.

날짜 및 시간 변경

배터리 작동 시계가 HMC(Hardware Management Console)의 날짜 및 시간을 유지합니다. 배터리를 교체하거나 시스템을 다른 시간대로 이동한 경우 콘솔 날짜 및 시간을 재설정해야 합니다. HMC의 날짜 및 시간 변경 방법에 대해 학습합니다.

이 태스크 정보

날짜 및 시간 정보를 변경하는 경우 HMC가 관리하는 시스템과 논리 파티션에는 변경이 적용되지 않습니다.

HMC의 날짜 및 시간을 변경하려면 다음 단계를 완료하십시오.

프로시저

1. 다음 역할 중 하나의 멤버인지 확인하십시오.
   - 수퍼 관리자
   - 서비스 담당자
   - 운영자
   - 뷰어
2. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
3. 컨텐츠 분할창에서 **날짜 및 시간 변경**을 클릭하십시오.
4. **시계** 필드에서 **UTC**를 선택한 경우 시간 설정은 자동으로 선택한 시간대의 일광 절약 시간제로 조정됩니다. 날짜, 시간 및 시간대를 입력하고 **확인**을 클릭하십시오.

결과

HMC 네트워크 유형 구성

관리 시스템, 논리 파티션, 원격 사용자, 서비스 및 지원 센터와 통신할 수 있도록 HMC를 구성합니다.

개방형 네트워크를 사용하여 관리 시스템에 연결하도록 *HMC* 설정값 구성
개방형 네트워크를 사용하여 관리 시스템에 연결 및 관리할 수 있도록 HMC를 구성합니다.

시작하기 전에

개방형 네트워크를 사용하여 관리 시스템에 연결할 수 있도록 HMC 네트워크 설정값을 구성하려면 다음을 수행하십시오.

표 *23.* 개방형 네트워크를 사용하여 관리 시스템에 연결하도록 *HMC* 설정값 구성	
태스크	**관련 정보**
1. 관리 시스템에 사용할 인터페이스를 결정합니다. **eth0**가 권장됩니다.	48 페이지의 『HMC의 설치 전 구성 워크시트』
2. HMC의 이더넷 포트를 식별합니다.	59 페이지의 『eth0으로 정의된 이더넷 포트 식별』
3. 다음 태스크를 수행하여 이더넷 어댑터를 구성합니다.	
a. 매체 속도를 설정합니다.	60 페이지의 『매체 속도 설정』
b. 개방형 네트워크 유형을 선택합니다.	61 페이지의 『개인용 또는 개방형 네트워크 선택』
c. 정적 주소를 설정합니다.	62 페이지의 『IPv6 주소 설정』
d. 방화벽을 설정합니다.	63 페이지의 『HMC 방화벽 설정값 변경』
e. 기본 게이트웨이를 구성합니다.	64 페이지의 『경로 지정 항목을 기본 게이트웨이로 구성』
f. DNS를 구성합니다.	64 페이지의 『도메인 이름 서비스 구성』
4. 있을 경우 추가 어댑터를 구성합니다.	
5. 관리 서버와 HMC 사이의 연결을 테스트합니다.	71 페이지의 『HMC와 관리 시스템 사이의 연결 테스트』

사설망을 사용하여 관리 시스템에 연결하도록 *HMC* 설정값 구성
사설망을 사용하여 관리 시스템에 연결 및 관리할 수 있도록 HMC를 구성합니다.

시작하기 전에

사설망을 사용하여 관리 시스템에 연결할 수 있도록 HMC 네트워크 설정값을 구성하려면 다음을 수행하십시오.

표 *24.* 사설망을 사용하여 관리 시스템에 연결하도록 *HMC* 설정값 구성	
태스크	**관련 정보**
1. 관리 시스템에 사용할 인터페이스를 결정합니다.	48 페이지의 『HMC의 설치 전 구성 워크시트』
2. HMC의 이더넷 포트를 식별합니다.	59 페이지의 『eth0으로 정의된 이더넷 포트 식별』
3. HMC를 DHCP 서버로 구성합니다.	61 페이지의 『HMC를 DHCP 서버로 구성』
4. 관리 서버와 HMC 사이의 연결을 테스트합니다.	71 페이지의 『HMC와 관리 시스템 사이의 연결 테스트』

개방형 네트워크를 사용하여 논리 파티션에 연결하도록 *HMC* 설정값 구성

시작하기 전에

개방형 네트워크를 사용하여 논리 파티션에 연결할 수 있도록 HMC 네트워크 설정값을 구성하려면 다음을 수행하십시오.

표 *25.* 개방형 네트워크를 사용하여 논리 파티션에 연결하도록 *HMC* 설정값 구성	
태스크	**관련 정보**
1. 관리 시스템에 사용할 인터페이스를 결정합니다.	48 페이지의 『HMC의 설치 전 구성 워크시트』
2. HMC의 이더넷 포트를 식별합니다.	59 페이지의 『eth0으로 정의된 이더넷 포트 식별』
3. 다음 태스크를 수행하여 이더넷 어댑터를 구성합니다.	
a. 매체 속도를 설정합니다.	60 페이지의 『매체 속도 설정』
b. 개방형 네트워크 유형을 선택합니다.	61 페이지의 『개인용 또는 개방형 네트워크 선택』
c. 정적 주소를 설정합니다.	62 페이지의 『IPv6 주소 설정』
d. 방화벽을 설정합니다.	63 페이지의 『HMC 방화벽 설정값 변경』
e. 기본 게이트웨이를 구성합니다.	64 페이지의 『경로 지정 항목을 기본 게이트웨이로 구성』
f. DNS를 구성합니다.	64 페이지의 『도메인 이름 서비스 구성』
4. 있을 경우 추가 어댑터를 구성합니다.	
5. 관리 서버와 HMC 사이의 연결을 테스트합니다.	71 페이지의 『HMC와 관리 시스템 사이의 연결 테스트』

개방형 네트워크를 사용하여 원격 사용자에 연결하도록 *HMC* 설정값 구성

시작하기 전에

개방형 네트워크를 사용하여 원격 사용자에 연결할 수 있도록 HMC 네트워크 설정값을 구성하려면 다음을 수행하십시오.

표 *26.* 개방형 네트워크를 사용하여 원격 사용자에 연결하도록 *HMC* 설정값 구성	
태스크	**관련 정보**
1. 관리 시스템에 사용할 인터페이스를 결정합니다.	48 페이지의 『HMC의 설치 전 구성 워크시트』
2. HMC의 이더넷 포트를 식별합니다.	59 페이지의 『eth0으로 정의된 이더넷 포트 식별』
3. 다음 태스크를 수행하여 이더넷 어댑터를 구성합니다.	
a. 매체 속도를 설정합니다.	60 페이지의 『매체 속도 설정』
b. 개방형 네트워크 유형을 선택합니다.	61 페이지의 『개인용 또는 개방형 네트워크 선택』
c. 정적 주소를 설정합니다.	62 페이지의 『IPv6 주소 설정』
d. 방화벽을 설정합니다.	63 페이지의 『HMC 방화벽 설정값 변경』
e. 기본 게이트웨이를 구성합니다.	64 페이지의 『경로 지정 항목을 기본 게이트웨이로 구성』
f. DNS를 구성합니다.	64 페이지의 『도메인 이름 서비스 구성』
g. 접미부를 구성합니다.	65 페이지의 『도메인 접미부 구성』
4. 있을 경우 추가 어댑터를 구성합니다.	

시작하기 전에

문제점이 보고되도록 HMC 콜-홈 서버 설정값을 구성하려면 다음을 수행하십시오.

표 *27. HMC* 콜-홈 서버 설정값 구성	
태스크	**관련 정보**
1. 모든 필수 고객 정보가 있는지 확인	48 페이지의 『HMC의 설치 전 구성 워크시트』
2. 오류를 보고하도록 이 HMC를 구성하거나 오류를 보고할 기존 콜-홈 서버 선택	66 페이지의 『서비스 및 지원 센터에 오류를 보고하도록 로컬 콘솔 구성』 68 페이지의 『기존 콜-홈 서버를 선택하여 HMC의 서비스 및 지원 센터에 연결』
3. 콜-홈 구성이 작동 중인지 확인	68 페이지의 『서비스 및 지원 센터에 대한 연결이 작동하는지 확인』
4. 사용자에게 수집된 시스템 데이터를 볼 수 있는 권한 부여	69 페이지의 『사용자에게 수집된 시스템 데이터를 볼 수 있는 권한 부여』
5. 시스템 데이터의 전송 스케줄	69 페이지의 『서비스 정보 전송』

*eth0*으로 정의된 이더넷 포트 식별
HMC에 eth0로 정의된 이더넷 포트를 사용하여 관리 서버에 이더넷 연결을 해야 합니다.

HMC의 PCI 슬롯에 추가 이더넷 어댑터를 설치하지 않았고 HMC를 관리 시스템의 DHCP 서버로 사용하려는 경우 1차 내장 이더넷 포트를 eth0 또는 eth1로 정의해야 합니다.

추가 이더넷 어댑터를 PCI 슬롯에 설치한 경우 eth0로 정의되는 포트는 설치한 이더넷 어댑터의 유형과 위치에 따라 달라집니다.

참고: 다음 일반 규칙이 모든 구성에 적용되지 않을 수 있습니다.

다음 표에는 이더넷 배치 규칙이 HMC 유형별로 설명되어 있습니다.

표 *28.* 이더넷 배치의 *HMC* 유형 및 연관된 규칙	
HMC 유형	**이더넷 배치 규칙**
두 개의 내장 이더넷 포트가 있는 랙 마운트 HMC	HMC는 단 하나의 추가 이더넷 어댑터를 지원합니다. • 추가 이더넷 어댑터를 설치하는 경우 해당 포트는가 eth0로 정의됩니다. 이 경우 1차 내장 이더넷 포트가 eth1으로 정의되고 2차 내장 이더넷 포트가 eth2로 정의됩니다. • 이더넷 어댑터가 이중 포트 이더넷 어댑터인 경우 Act/link A로 레이블된 포트가 eth0이 됩니다. Act/link B로 레이블된 포트는 eth1이 됩니다. 이 경우 1차 내장 이더넷 포트가 eth2으로 정의되고 2차 내장 이더넷 포트가 eth3로 정의됩니다. • 어댑터가 설치되지 않은 경우 1차 내장 이더넷 포트가 eth0으로 정의됩니다.

표 *28.* 이더넷 배치의 *HMC* 유형 및 연관된 규칙 *(계속)*	
HMC 유형	**이더넷 배치 규칙**
단일의 내장 이더넷 포트가 있는 독립형 모델	설치한 이더넷 어댑터의 유형에 따라 정의가 달라집니다. • 이더넷 어댑터를 하나만 설치한 경우 이 어댑터가 `eth0`으로 정의됩니다. • 이더넷 어댑터가 이중 포트 이더넷 어댑터인 경우 `Act/link A`로 레이블된 포트가 `eth0`이 됩니다. `Act/link B`로 레이블된 포트는 `eth1`이 됩니다. 이 경우 1차 내장 이더넷 포트는 `eth2`로 정의됩니다. • 어댑터가 설치되지 않은 경우 내장 이더넷 포트가 `eth0`으로 정의됩니다. • 이더넷 어댑터가 여러 개 설치된 경우 60 페이지의 『이더넷 어댑터의 인터페이스 이름 판별』을 참조하십시오.

이더넷 어댑터의 인터페이스 이름 판별
HMC를 DHCP 서버로 구성한 경우 이 서버는 HMC가 `eth0` 및 `eth1`로 식별하는 네트워크 인터페이스 카드(NIC) 커넥터에서만 작동할 수 있습니다. 또한 이더넷 케이블을 꽂아야 하는 NIC 커넥터도 판별해야 합니다. HMC가 `eth0` 및 `eth1`로 식별하는 NIC 커넥터를 판별하는 데 대해서도 자세히 학습합니다.

이 태스크 정보
HMC가 이더넷 어댑터에 지정하는 이름을 결정하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **네트워크 설정값 변경** 창에서 **LAN 어댑터** 탭을 클릭하십시오. 다음 예제 항목은 이 이더넷 포트가 `eth0`: `Ethernet eth0 52:54:00:fa:b6:8e(<IP address of HMC>)`로 식별됨을 표시합니다.
4. 결과를 기록하십시오. LAN 어댑터 설정값을 보거나 변경해야 하는 경우 **세부사항**을 클릭하십시오.
5. **확인**을 클릭하십시오.

매체 속도 설정
이더넷 어댑터의 양방향 모드와 속도를 포함하는 매체 속도를 지정하는 방법에 대해 학습합니다.

시작하기 전에
HMC 어댑터 설정의 기본값은 **Autodetection**입니다. 이 어댑터가 LAN 스위치에 연결된 경우, 스위치 포트 설정을 일치시켜야 합니다. 매체 속도와 양방향을 설정하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **LAN 어댑터** 탭을 클릭하십시오.
4. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
5. 근거리 통신망(LAN) 정보 섹션에서 **Autodetection** 또는 해당하는 매체 속도와 양방향 조합을 선택하십시오.

6. **확인**을 클릭하십시오.

개인용 또는 개방형 네트워크 선택
개인용 서비스 네트워크는 HMC(Hardware Management Console)와 관리 시스템으로 구성됩니다. 개인용 서비스 네트워크는 자신이 관리하는 콘솔과 시스템으로 제한되며 회사 네트워크와 분리되어 있습니다. 개방형 네트워크는 개인용 서비스 네트워크와 회사 네트워크로 구성됩니다. 개방형 네트워크에는 콘솔 및 관리 시스템 외에 네트워크 엔드포인트가 포함되며 여러 서브네트와 네트워크 장치에 걸쳐 있을 수 있습니다.

이 태스크 정보

개인용 및 공용 네트워크를 선택하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **LAN 어댑터** 탭을 클릭하십시오.
4. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
5. **LAN 어댑터** 탭을 클릭하십시오.
6. 근거리 통신망(LAN) 정보 페이지에서 **개인용** 또는 **개방형**을 선택하십시오.
7. **확인**을 클릭하십시오.

*HMC*를 *DHCP* 서버로 구성
DHCP(동적 호스트 구성 프로토콜)를 이용하면 동적 클라이언트를 자동으로 구성할 수 있습니다.

HMC(Hardware Management Console)를 DHCP 서버로 구성하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오. 네트워크 설정값 사용자 정의 창이 열립니다.
3. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
4. **개인용**을 선택한 후 네트워크 유형을 선택하십시오.
5. DHCP 서버 섹션에서 HMC를 DHCP 서버로 사용하려면 **DHCP 서버 사용**을 선택하십시오.

   참고: 사설망에서만 HMC를 DHCP 서버로 구성할 수 있습니다. 개방형 네트워크를 사용하는 경우 **DHCP 사용** 옵션을 선택하는 옵션이 사용 불가능합니다.
6. DHCP 서버의 주소 범위를 입력하십시오.
7. **확인**을 클릭하십시오.

사설망에서 HMC를 DHCP 서버로 구성한 경우, HMC DHCP 사설망이 올바로 구성되어 있는지 확인해야 합니다. HMC를 사설망에 연결하는 데 대한 정보는 61 페이지의 『개인용 또는 개방형 네트워크 선택』을 참조하십시오.

추가 정보는 41 페이지의 『HMC』의 내용을 참조하십시오.

BMC 연결 구성
관리 콘솔에 대한 BMC의 네트워크 설정을 구성하거나 볼 수 있습니다.

참고: 이 태스크는 7063-CR1에만 적용됩니다. HMC의 BMC(Baseboard Management Controller)에 액세스하려면 이 연결이 필요합니다.

BMC 연결을 구성하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **BMC/IPMI 설정값 변경**을 클릭하십시오.

3. 연결 모드(**DHCP** 또는 **Static**)을 선택하십시오.

   Static 모드를 선택한 경우 다음 주소를 완료하십시오.

   - **IP 주소**
   - **서브넷 마스크**
   - **게이트웨이**
4. **확인**을 클릭하십시오.

Petitboot 부트로더 인터페이스를 사용하여 BMC 네트워크 연결을 구성할 수도 있습니다. 자세한 정보는 펌웨어 IP 주소 구성을 참조하십시오.

IPv4 주소 설정
HMC에서 IPv4 주소를 설정하는 방법에 대해 학습합니다.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **LAN 어댑터** 탭을 클릭하십시오.
4. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
5. **기본 설정값** 탭을 클릭하십시오.
6. IPv4 주소를 선택하십시오.
7. IP 주소를 지정하도록 선택한 경우 TCP/IP 인터페이스 주소와 TCP/IP 인터페이스 네트워크 마스크를 입력하십시오.
8. **확인**을 클릭하십시오.

IPv6 주소 설정
HMC에서 IPv6 주소를 설정하는 방법에 대해 학습합니다.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **LAN 어댑터** 탭을 클릭하십시오.
4. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
5. **IPv6 설정값** 탭을 클릭하십시오.
6. **Autoconfig** 옵션을 선택하거나 정적 IP 주소를 추가하십시오.
7. IP 주소를 추가한 경우 IPv6 주소와 접두부 길이를 입력하고 **확인**을 클릭하십시오.
8. **확인**을 클릭하십시오.

IPv6 주소만 사용
IPv6 주소만 사용하도록 HMC를 구성하는 방법에 대해 학습합니다.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **LAN 어댑터** 탭을 클릭하십시오.

4. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
5. **IPv4 주소 없음**을 선택하십시오.
6. **IPv6 설정값** 탭을 클릭하십시오.
7. **DHCPv6를 사용하여 IP 설정값 구성**을 선택하거나 정적 IP 주소를 추가한 후 **확인**을 클릭하십시오.

다음에 수행할 작업
확인을 클릭한 후 변경사항이 적용하려면 HMC를 다시 시작해야 합니다.

***HMC* 방화벽 설정값 변경**
개방형 네트워크에서 방화벽은 외부에서 회사 네트워크로의 액세스를 제어하는 데 사용됩니다. HMC의 각 이더넷 어댑터에도 방화벽이 있습니다. HMC를 원격으로 제어하거나 다른 사용자에게 원격 액세스 권한을 부여하려면 개방형 네트워크에 연결된 HMC에서 이더넷 어댑터의 방화벽 설정값을 수정하십시오.

이 태스크 정보

방화벽을 구성하려면 다음 단계를 수행하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오.
3. **LAN 어댑터** 탭을 클릭하십시오.
4. 작업하려는 LAN 어댑터를 선택하고 **상세 정보**을 클릭하십시오.
5. **방화벽** 탭을 클릭하십시오.
6. 다음 방법 중 하나를 사용하면 방화벽을 통해 특정 애플리케이션을 사용하여 IP 주소를 허용하거나 IP 주소를 하나 이상 지정할 수 있습니다.
   - 방화벽을 통해 특정 애플리케이션을 사용하여 IP 주소를 허용하십시오.
     a. 맨 위 상자에서 애플리케이션을 강조표시하십시오.
     b. **수신 허용**을 클릭하십시오. 애플리케이션이 선택되었음을 나타내기 위해 맨 아래 상자에 애플리케이션이 표시됩니다.
   - 방화벽을 통해 허용할 IP 주소를 지정합니다.
     a. 맨 위 상자에서 애플리케이션을 강조표시하십시오.
     b. **IP 주소별 수신 허용**을 클릭하십시오.
     c. 허용되는 호스트 창에서 IP 주소와 네트워크 마스크를 입력하십시오.
     d. **추가**를 클릭하고 **확인**을 클릭하십시오.
7. **확인**을 클릭하십시오.

제한된 원격 쉘 액세스 사용
방화벽 구성 시 제한된 원격 쉘 액세스를 사용가능하게 할 수 있습니다.

이 태스크 정보
제한된 원격 쉘 액세스를 사용하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리**를 클릭하십시오.
2. **원격 명령 실행**을 클릭하십시오.
3. **SSH 기능을 사용하여 원격 명령 실행 가능**을 선택한 후 **확인**을 클릭하십시오.

다음에 수행할 작업
이제 제한된 원격 쉘 액세스를 사용할 수 있습니다.

원격 웹 액세스 사용
HMC(Hardware Management Console)에 대한 원격 웹 액세스를 사용할 수 있습니다.

이 태스크 정보
원격 웹 액세스를 사용하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리**를 클릭하십시오.
2. **원격 조작**을 클릭하십시오.
3. **사용**을 선택한 후 **확인**을 클릭하십시오.

다음에 수행할 작업
이제 원격 웹 액세스를 사용할 수 있습니다.

경로 지정 항목을 기본 게이트웨이로 구성
경로 지정 항목을 기본 게이트웨이로 구성하는 방법에 대해 학습합니다. 이 태스크는 개방형 네트워크를 사용 중일 때 사용 가능합니다.

시작하기 전에
경로 지정 항목을 기본 게이트웨이로 구성하려면 다음 단계를 수행하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오. 네트워크 설정값 사용자 정의 창이 열립니다.
3. **경로 지정** 탭을 클릭하십시오.
4. 기본 게이트웨어 정보 섹션에서 디롤트 게이트웨이로 설정하려는 경로 지정 항목의 게이트웨이 주소와 게이트웨이 장치를 입력하십시오.
5. **확인**을 클릭하십시오.

도메인 이름 서비스 구성
개방형 네트워크를 설정하려는 경우 도메인 이름 서비스를 구성하십시오.

이 태스크 정보

개방형 네트워크를 설정하려는 경우 도메인 이름 서비스를 구성하십시오. DNS(Domain Name System)는 호스트 이름과 이의 연관된 IP(Internet Protocol) 주소를 관리하기 위한 분산 데이터베이스 시스템입니다. 도메인 이름 서비스 구성에는 DNS 사용 및 도메인 접미부 탐색 순서 지정이 포함됩니다.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오. 네트워크 설정값 변경 창이 열립니다.
3. **이름 서비스** 탭을 클릭하십시오.
4. **DNS 사용**을 선택하여 DNS를 사용할 수 있게 하십시오.
5. DNS 서버와 도메인 접미부 탐색 순서를 지정하고 **추가**를 클릭하십시오.
6. **확인**을 클릭하십시오.

도메인 접미부 구성
도메인 접미부 리스트는 리스트의 첫 번째 항목부터 IP 주소를 분석할 때 사용됩니다.

이 태스크 정보

도메인 접미부는 IP 주소 분석에 사용되는 호스트 이름에 추가되는 스트링입니다. 예를 들어, 호스트 이름 myname은 분석할 수 없습니다. 그러나 myloc.mycompany.com 스트링이 도메인 접미부 테이블의 요소이면 myname.mloc.mycompany.com이 분석됩니다.

도메인 접미부 항목을 구성하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정값 변경**을 클릭하십시오. 네트워크 설정값 사용자 정의 창이 열립니다.
3. **이름 서비스** 탭을 클릭하십시오.
4. 도메인 접미부 항목으로 사용할 스트링을 입력하십시오.
5. **추가**를 클릭하여 이를 리스트에 추가하십시오.

LDAP 원격 인증을 사용하도록 *HMC* 구성
LDAP(Lightweight Directory Access Protocol) 원격 인증을 사용하도록 Hardware Management Console(HMC)을 구성할 수 있습니다.

시작하기 전에

사용자가 HMC에 로그인하면 먼저 로컬 비밀번호 파일에 대해 인증이 수행됩니다. 로컬 비밀번호 파일을 찾지 못하는 경우 HMC는 인증을 위해 원격 LDAP 서버에 연결합니다. LDAP 원격 인증을 사용하도록 HMC를 구성해야 합니다.

참고: LDAP 인증을 사용하도록 HMC를 구성하기 전에, HMC와 LDAP 서버 사이에 작동 중인 네트워크 연결이 존재하는지 확인해야 합니다. HMC 네트워크 연결 구성에 대한 자세한 정보는 56 페이지의 『HMC 네트워크 유형 구성』을 참조하십시오.

이 태스크 정보
HMC가 LDAP 인증을 사용하도록 구성하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **사용자 및 보안** 아이콘()을 클릭한 다음 **시스템 및 콘솔 보안**을 선택하십시오.
2. 컨텐츠 분할창에서 **LDAP 관리**를 선택하십시오. LDAP 서버 정의 창이 열립니다.
3. **LDAP 사용**을 선택하십시오.
4. 인증에 사용할 LDAP 서버를 정의하십시오.
5. 인증 중인 사용자를 식별하는 데 사용되는 LDAP 속성을 정의하십시오. 기본값은 **uid**지만 사용자 자신의 속성을 사용할 수 있습니다.
6. LDAP 서버의 식별 이름 트리(검색 기반이라고도 함)를 정의하십시오.
7. **확인**을 클릭하십시오.
8. LDAP 인증을 사용하려는 사용자의 경우 로컬 인증 대신 LDAP 원격 인증을 사용하도록 자신의 프로파일을 구성해야 합니다.

Kerberos 원격 인증에 키 분배 센터 서버를 사용하도록 *HMC* 구성
Kerberos 원격 인증에 키 분배 센터(KDC) 서버를 사용하도록 HMC를 구성할 수 있습니다.

시작하기 전에

사용자가 HMC에 로그인하면 먼저 로컬 비밀번호 파일에 대해 인증이 확인됩니다. 로컬 비밀번호 파일을 찾지 못하는 경우 HMC는 인증을 위해 원격 Kerberos 서버에 연결합니다. Kerberos 원격 인증을 사용하도록 HMC를 구성해야 합니다.

참고: Kerberos 원격 인증에 KDC 서버를 사용하도록 HMC를 구성하기 전에, HMC와 KDC 서버 사이에 작동 중인 네트워크 연결이 존재하는지 확인해야 합니다. HMC 네트워크 연결 구성에 대한 자세한 정보는 56 페이지의 『HMC 네트워크 유형 구성』을 참조하십시오.

이 태스크 정보

Kerberos 원격 인증에 KDC 서버를 사용하도록 HMC를 구성하려면 다음 단계를 완료하십시오.

프로시저

1. HMC에서 NTP(Network Time Protocol) 서비스를 사용 가능하게 하고 동일한 NTP 서버와 시간을 동기화하도록 HMC 및 KDC 서버를 설정하십시오. HMC에서 NTP 서비스를 사용할 수 있게 하려면 다음 단계를 완료하십시오.
   a) 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
   b) 컨텐츠 분할창에서 **날짜 및 시간 변경**을 선택하십시오.
   c) **NTP 구성** 탭을 선택하십시오.
   d) **이 HMC에서 NTP 서비스 사용**을 선택하십시오.
   e) **확인**을 클릭하십시오.
2. 로컬 인증 대신 Kerberos 원격 인증을 사용하도록 각 원격 HMC 사용자의 프로파일을 구성하십시오.
3. 선택적으로, 서비스 키 파일을 이 HMC로 가져올 수 있습니다. 서비스 키 파일에는 HMC를 KDC 서버에 식별해주는 호스트 프린시펄이 포함되어 있습니다. 서비스 키 파일은 키탭*(keytab)*이라고도 합니다. 서비스 키 파일을 이 HMC로 가져오려면 다음 단계를 완료하십시오.
   a) 탐색 영역에서 **사용자 및 보안** 아이콘()을 클릭한 다음 **시스템 및 콘솔 보안**을 선택하십시오.
   b) 컨텐츠 분할창에서 **KDC 관리**를 선택하십시오.
   c) **조치 > 서비스 키 가져오기**를 선택하십시오. 서비스 키 가져오기 창이 열립니다.
   d) 서비스 키 파일의 위치를 입력하십시오.
   e) **확인**을 클릭하십시오.
4. 새 KDC 서버를 이 HMC에 추가하십시오. 새 KDC 서버를 이 HMC에 추가하려면 다음 단계를 완료하십시오.
   a) 탐색 영역에서 **사용자 및 보안** 아이콘()을 클릭한 다음 **시스템 및 콘솔 보안**을 선택하십시오.
   b) 컨텐츠 분할창에서 **KDC 관리**를 선택하십시오.
   c) **조치 > KDC 서버 추가**를 선택하십시오. 서비스 키 가져오기 창이 열립니다.
   d) KDC 서버의 호스트 이름 또는 IP 주소와 영역을 입력하십시오.
   e) **확인**을 클릭하십시오.

서비스 및 지원 센터에 오류를 보고하도록 로컬 콘솔 구성

LAN 연결성을 사용하여 콜홈 오류를 보고할 수 있도록 HMC를 구성합니다.

콜-홈 설정 마법사를 사용하여 서비스 및 지원 센터에 연결할 수 있도록 *HMC* 구성
콜-홈 마법사를 사용하여 HMC를 콜-홈 서버로 구성합니다.

시작하기 전에
이 프로시저에서는 인터넷과의 직접(LAN 기반) 및 간접(SSL) 연결을 사용하여 HMC를 콜-홈 서버로 구성하는 방법에 대해 설명합니다.

이 태스크를 시작하기 전에 다음을 확인하십시오.

- 네트워크 관리자가 연결이 허용되는 것을 확인했습니다. 추가 정보는 47 페이지의 『HMC 구성 준비』의 내용을 참조하십시오.
- 프록시 서버를 통해 인터넷 지원을 구성하는 경우 다음 정보도 있어야 합니다.
  - 프록시 서버의 포트 및 IP 주소
  - 프록시 인증 정보
- **eth1**로 지정된 어댑터(개방형 네트워크로 지정된 어댑터)가 사용됩니다. 추가 정보는 39 페이지의 『HMC의 네트워크 설정값 선택』의 내용을 참조하십시오.
- 실제로 이더넷 케이블이 HMC를 LAN에 연결합니다.

콜-홈 마법사를 사용하여 HMC를 콜-홈 서버로 구성하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **콜홈 설정 마법사**를 클릭하십시오. 연결 및 콜-홈 서버 마법사가 열립니다. 마법사의 지시를 따라 콜-홈을 구성하십시오.

서비스 및 지원 센터에 오류를 보고하도록 로컬 콘솔 구성
LAN 연결성을 사용하여 콜홈 오류를 보고할 수 있도록 HMC를 구성합니다.

LAN 기반 인터넷 및 *SSL*을 사용하여 서비스 및 지원 센터에 접속하도록 *HMC* 구성
인터넷과의 직접(LAN 기반) 및 간접(SSL) 연결을 사용하여 HMC를 콜-홈 서버로 구성하는 방법에 대해 설명합니다.

시작하기 전에

이 태스크를 시작하기 전에 다음을 확인하십시오.

- 네트워크 관리자가 연결이 허용되는 것을 확인했습니다. 추가 정보는 47 페이지의 『HMC 구성 준비』의 내용을 참조하십시오.
- 고객 문의처 정보가 구성되어 있습니다. HMC 인터페이스로 이동한 후 **서비스 가능성 > 서비스 관리 > 고객 정보 관리**를 클릭하여 연락처 정보를 확인하십시오.
- 프록시 서버를 통해 인터넷 지원을 구성하는 경우 다음 정보도 있어야 합니다.
  - 프록시 서버의 포트 및 IP 주소
  - 프록시 인증 정보
- 개방형 네트워크 인터페이스가 하나 이상 구성되어 있어야 합니다. 추가 정보는 41 페이지의 『HMC 환경의 개인용 및 개방형 네트워크』의 내용을 참조하십시오.
- 실제로 이더넷 케이블이 HMC를 LAN에 연결합니다.

이 태스크 정보
LAN 기반 인터넷 및 SSL을 사용하여 HMC를 콜홈 서버로 구성하려면 다음 단계를 수행하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 연결 섹션에서 **아웃바운드 연결 관리**를 클릭하십시오. 콜-홈 서버 콘솔 창이 열립니다.

3. **구성**을 클릭하십시오.
4. 아웃바운드 연결 설정값 창에서 **로컬 시스템을 콜-홈 서버로 사용**을 클릭하십시오.
5. 계약에 동의하십시오.
6. 아웃바운드 연결 설정값 창에서 **인터넷** 페이지를 선택하십시오.
7. **기존 인터넷 연결을 서비스에 사용** 상자에 체크하십시오.
8. SSL 프록시를 사용하는 경우 **SSL 프록시 사용** 상자에 체크하십시오.
9. SSL 프록시를 사용하는 경우 프록시의 주소와 포트를 작성하십시오. 이 정보는 네트워크 관리자에게 확인하십시오.
10. **SSL 프록시 사용**에 체크했고 프록시가 사용자 ID 및 비밀번호 인증을 필요로 하는 경우 **SSL 프록시 인증** 상자에 체크하십시오. 사용자 ID 및 비밀번호를 입력하십시오. 네트워크 관리자로부터 사용자 ID와 비밀번호를 확인하십시오.
11. 사용하려는 **인터넷 프로토콜**을 선택하십시오.
12. **인터넷** 페이지에서 **테스트**를 클릭하십시오.
13. 인터넷 테스트 창에서 **시작**을 클릭하십시오.
14. 테스트가 정상적으로 완료되었는지 확인하십시오.
15. 인터넷 테스트 창에서 **취소**를 클릭하십시오.
16. 아웃바운드 연결 설정값 창에서 **확인**을 클릭하십시오.

기존 콜-홈 서버를 선택하여 *HMC*의 서비스 및 지원 센터에 연결
오류를 보고하기 위해 HMC(Hardware Management Console)로 인식되거나 검색되는 기존 HMC(Hardware Management Console) 콜-홈 서버를 선택하십시오.

시작하기 전에

발견된 HMC는 콜-홈 서버로 사용할 수 있는 HMC로, 이 HMC와 동일한 서브네트에 있거나 동일한 관리 시스템을 관리합니다.

HMC가 오류를 보고할 때 홈을 호출하기 위한 감지된 HMC를 선택하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **아웃바운드 연결성 관리**를 클릭하십시오. 콜-홈 서버 콘솔 창이 열립니다.
3. **발견된 콜홈 서버 콘솔 사용**을 클릭하십시오. HMC는 콜-홈용으로 구성된 HMC의 IP 주소 또는 호스트 이름을 표시합니다.
4. **확인**을 클릭하십시오.

결과
다른 서브네트에 있는 기존의 HMC 콜-홈 서버를 직접 추가할 수도 있습니다. 콜홈용으로 구성된 HMC의 IP 주소 또는 호스트 이름을 선택하고 **추가**를 클릭한 후 **확인**을 클릭하십시오.

서비스 및 지원 센터에 대한 연결이 작동하는지 확인
서비스 및 지원 센터에 대한 연결이 작동하는지 확인하기 위해 문제점 보고를 테스트합니다.

이 태스크 정보
콜-홈 구성이 작동 중인지 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 분할창 영역에서 **이벤트 작성**을 클릭하십시오.

3. **자동 문제점 보고 테스트**를 선택하고 설명을 입력하십시오.
4. **서비스 요청**을 클릭하십시오. 요청이 전송되는 몇 분간 대기하십시오.
5. 서비스 관리 창에서 **이벤트 관리**를 선택하십시오.
6. **공개된 모든 문제점**을 선택하십시오.
7. 열어본 문제점 번호에 지정된 PMH 이벤트와 번호를 확인하십시오.
8. 이벤트를 선택하고 **닫기**를 클릭하십시오.
9. **닫기** 창에서 이름과 간략한 설명을 입력하십시오.

사용자에게 수집된 시스템 데이터를 볼 수 있는 권한 부여
시스템에 대한 데이터를 볼 수 있는 권한을 사용자에게 부여해야 합니다.

시작하기 전에
수집된 시스템 데이터를 볼 수 있는 권한을 사용자에게 부여하기 전에 IBM ID를 획득해야 합니다. IBM ID 획득에 대한 자세한 정보는 48 페이지의 『HMC의 설치 전 구성 워크시트』를 참조하십시오.

이 태스크 정보
수집된 시스템 데이터를 볼 수 있는 권한을 사용자에게 부여하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **사용자 권한 부여**를 선택하십시오.
3. IBM ID를 입력하십시오.
4. **확인**을 클릭하십시오.

서비스 정보 전송
정보를 즉시 서비스 제공자에게 전송하거나 정기적으로 정보가 전송되도록 스케줄할 수 있습니다.

시작하기 전에
IBM은 IBM Electronic Service Agent에서 수집한 정보를 사용하여 개별화된 웹 기능을 제공합니다. 이러한 기능을 사용하려면 먼저 IBM 등록 웹 사이트(http://www.ibm.com/account/profile)에 등록해야 합니다. Electronic Service Agent 정보를 사용하여 웹 기능을 개별화할 수 있는 권한을 사용자에게 부여하려면 69 페이지의 『사용자에게 수집된 시스템 데이터를 볼 수 있는 권한 부여』를 참조하십시오. IBM ID를 시스템에 등록하는 데 따르는 이점에 대한 자세한 정보는 http://www.ibm.com/support/electronic을 참조하십시오.

참고: 사용을 위해 HMC를 설치 및 구성하는 즉시 서비스 제공자에게 정보를 전송해야 합니다.

이 태스크 정보
서비스 정보를 전송하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **서비스 정보 전송**을 클릭하십시오.
3. **서비스 정보 전송** 창의 태스크를 완료하고 **확인**을 클릭하십시오.

콜홈용 이벤트 관리자 구성
콜홈 작업에 대해 이벤트 관리자를 구성하는 방법에 대해 학습합니다. 이 작업을 통해 HMC에서 IBM으로 전송되는 모든 데이터를 모니터하고 승인할 수 있습니다.

콜홈 모드에 대한 이벤트 관리자(사용 또는 사용 안함)는 HMC 명령행 인터페이스를 사용하여 설정됩니다. 콜홈 작업에 대해 이벤트 관리자를 사용하면 이벤트가 발생할 때 HMC가 자동으로 이벤트를 콜홈하는 것을 방지할 수

있습니다. 승인 없이 이벤트가 콜홈되는 것을 방지하려면 이 환경에서 실행 중인 모든 HMC가 사용 가능한 콜홈용 이벤트 관리자를 갖고 있어야 합니다.

콜홈 작업에 대해 이벤트 관리자를 사용 또는 사용 안함으로 설정하려면 다음 명령을 실행하십시오.

chhmc -c emch

-s {enable | disable}

[--callhome {enable | disable}]

[--help]

참고: 콜홈 작업에 대해 이벤트 관리자를 사용하면 이벤트가 콜홈 작업에 대해 승인될 때까지 콜홈 이벤트를 보류합니다. 콜홈 작업에 대해 이벤트 관리자를 사용 안함으로 설정한 경우, 콜홈 기능을 자동으로 사용으로 설정하지 않습니다. 이 설정으로 인해 데이터를 IBM으로 의도치 않게 콜홈하는 것이 방지됩니다. 다음 명령 옵션 중 하나를 선택하여 필수 구성을 설정하십시오.

- 콜홈 작업에 대해 이벤트 관리자를 사용으로 설정하려는 경우: **chhmc -c emch -s enable**
- 콜홈 작업에 대해 이벤트 관리자를 사용 안함으로 설정하고 자동 콜홈을 다시 사용으로 설정하려는 경우: **chhmc -c emch -s disable --callhome enable**
- 콜홈 작업에 대해 이벤트 관리자를 사용 안함으로 설정하고 자동 콜홈을 다시 사용으로 설정하지 않으려는 경우: **chhmc -c emch -s disable --callhome disable**

HMC가 이 환경에 배치되는 기타 HMC와 통신할 수 있는지 확인하십시오. 콜홈용 이벤트 관리자는 HMC가 등록될 때 테스트 연결 기능을 갖습니다.

콜홈용 이벤트 관리자에 HMC를 등록할 수 있습니다. HMC를 등록한 후에 이벤트 관리자가 등록된 HMC에서 IBM으로 콜홈되도록 대기 중인 모든 이벤트를 조회합니다. 이벤트 관리자는 IBM으로 다시 전송된 데이터를 표시하고 해당 이벤트를 승인합니다. 승인 후에 이벤트 관리자가 등록된 HMC에 콜홈 조작을 사용하여 승인될 수 있음을 알립니다.

콜홈 작업에 대한 이벤트 관리자는 임의의 HMC 또는 다중 HMC에서 실행될 수 있습니다. 관리 콘솔을 콜홈 작업에 대한 이벤트 관리자에 등록하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 다음 **콜홈용 이벤트 관리자**를 선택하십시오.
2. **콜홈용 이벤트 관리자** 분할창에서 **관리 콘솔**을 클릭하십시오.
3. **등록된 콘솔 관리** 창에서 **콘솔 추가**를 클릭하여 관리 콘솔을 콜홈용 이벤트 관리자 작업에 등록하기 위한 정보를 입력하십시오.
4. **확인**을 클릭하여 등록된 관리 콘솔의 목록에 대한 변경을 커미트하십시오.

참고: 콜홈용 이벤트 관리자는 이벤트 관리자 모드를 사용 안함으로 설정한 상태에서 사용할 수 있습니다. HMC 및 보기 이벤트를 이벤트 관리자에 등록할 수는 있으나 이벤트 관리자가 해당 이벤트가 콜홈되는 시기를 제어하지 않습니다.

관리 시스템의 비밀번호 설정

서버와 ASM(Advanced System Management)의 비밀번호를 설정해야 합니다. HMC 인터페이스를 사용하여 비밀번호를 설정하는 방법에 대해 추가로 읽으십시오.

시작하기 전에

`Authentication Pending` 메시지를 수신하는 경우, HMC는 관리 시스템의 비밀번호를 설정하도록 프롬프트합니다.

이 태스크 정보

Authentication Pending> 메시지를 수신하지 못하는 경우 다음 단계를 완료하여 관리 시스템의 비밀번호를 설정하십시오.

서버 비밀번호 업데이트

시작하기 전에
서버 비밀번호를 업데이트하려면 다음을 완료하십시오.

프로시저

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘()을 클릭한 다음 **사용자 및 역할**을 선택하십시오.
2. **비밀번호 변경**을 클릭하십시오. 비밀번호 업데이트 창이 열립니다.
3. 필수 정보를 입력하고 **확인**을 클릭하십시오.

ASM(Advanced System Management) 일반 비밀번호 업데이트

시작하기 전에

참고: 일반 사용자 ID의 기본 비밀번호는 `general`이고 관리자 ID의 기본 비밀번호는 `admin`입니다.

ASM 일반 비밀번호를 업데이트하려면 다음을 완료하십시오.

프로시저

1. HMC의 탐색 영역에서 관리 시스템을 선택하십시오.
2. 태스크 영역에서 **조작**을 클릭하십시오.
3. **ASM(Advanced System Management)**을 클릭하십시오. ASM 인터페이스 시작 창이 열립니다.
4. 서비스 프로세서 IP 주소를 선택하고 **확인**을 클릭하십시오. ASM 인터페이스가 열립니다.
5. ASMI 시작 분할창에서 사용자 ID와 비밀번호를 지정하고 **로그인**을 클릭하십시오.
6. 탐색 영역에서 **로그인 프로파일**을 펼치십시오.
7. **비밀번호 변경**을 선택하십시오.
8. 필수 정보를 지정하고 **계속**을 클릭하십시오.

ASM(Advanced System Management) 관리자 비밀번호 재설정

시작하기 전에
관리자 비밀번호를 재설정하려면 권한이 있는 서비스 제공자에게 문의하십시오.

***HMC*와 관리 시스템 사이의 연결 테스트**
네트워크에 올바르게 연결되었는지 확인하는 방법에 대해 학습합니다.

이 태스크 정보

네트워크 연결을 테스트하려면 다음 역할 중 하나의 멤버여야 합니다.

- 수퍼 관리자
- 서비스 담당자

HMC와 관리 시스템 사이의 연결을 테스트하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 연결 테스트**를 클릭하십시오.

3. Ping 탭에서 연결하려는 시스템의 호스트 이름 또는 IP 주소를 입력하십시오. 개방형 네트워크를 테스트하려면 게이트웨이를 입력하십시오. **Ping**을 클릭하십시오.

결과

논리 파티션을 작성하지 않은 경우 주소를 Ping할 수 없습니다. HMC를 사용하여 서버에 논리 파티션을 작성할 수 있습니다. 자세한 정보는 논리 파티셔닝을 참조하십시오.

네트워크에서 HMC가 사용되는 방식을 이해하려면 39 페이지의 『HMC 네트워크 연결』을 참조하십시오.

네트워크에 연결하도록 HMC를 구성하는 방법에 대한 자세한 정보는 54 페이지의 『메뉴를 사용하여 HMC 구성』의 내용을 참조하십시오.

구성 이후 단계

HMC를 설치 및 구성한 후 필요한 대로 HMC 데이터를 백업하십시오.

관리 콘솔 데이터 백업

이 태스크는 HMC 조작을 지원하는 데 중요한 HMC 하드 디스크에 저장되는 데이터를 백업(또는 아카이브)합니다.

시작하기 전에

원격 시스템에는 NFS(Network File System) 또는 SSH(Secure Shell)가 구성되어 있어야 하며 HMC에서 이 네트워크에 액세스할 수 있어야 합니다. 이 태스크를 완료하려면 HMC를 시스템 종료한 후 다시 부팅해야 합니다. 이러한 태스크의 수행에는 반드시 HMC를 사용하십시오.

이 태스크 정보

HMC 하드 디스크 드라이브를 원격 시스템에 백업하려면 다음 역할 중 하나의 멤버여야 합니다.

- 수퍼 관리자
- 운영자
- 서비스 담당자

논리 파티션과 연관된 정보 또는 HMC를 변경한 후에는 HMC 데이터를 백업하십시오.

HMC 하드 드라이브에 저장된 HMC 데이터는 로컬 시스템의 DVD-RAM에 저장되거나 HMC 파일 시스템에 마운트되어 있는 원격 시스템(예: NFS)에 저장되거나 FTP(File Transfer Protocol)를 사용하여 원격 사이트로 전송될 수 있습니다.

참고: HMC 모델 7063-CR1의 경우 외부 USB DVD 드라이브를 연결할 수 있습니다.

HMC를 사용하여 다음과 같은 중요한 데이터를 모두 백업할 수 있습니다.

- 사용자 기본설정 파일
- 사용자 정보
- HMC 플랫폼 구성 파일
- HMC 로그 파일
- 수정 서비스 설치를 통한 HMC 업데이트

HMC 하드 드라이브를 원격 시스템으로 백업하려면 단음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **관리 콘솔 데이터 백업**을 클릭하십시오.
3. **관리 콘솔 데이터 백업** 창에서 수행할 아카이브 옵션을 선택하십시오.
4. **다음**을 클릭한 후 선택한 옵션에 따라 적절한 지시사항을 따르십시오.

5. 백업 프로세스를 계속하려면 **확인**을 클릭하십시오.

HMC 기계코드 업데이트, 업그레이드 및 마이그레이션

새로운 기능을 추가하고 기존 기능을 개선하도록 HMC에 대한 업데이트 및 업그레이드가 정기적으로 발표됩니다. HMC 기계코드의 업데이트와 업그레이드 및 마이그레이션이 서로 어떻게 다른지 알아봅니다. 또한 HMC 기계코드의 업데이트, 업그레이드 또는 마이그레이션 수행 방법에 대해서도 학습합니다.

이러한 태스크를 모두 완료하면 HMC는 재부트되지만 파티션은 그렇지 않습니다.

HMC 코드 업데이트
기존 HMC 레벨에 유지보수를 적용합니다.

업그레이드 데이터 저장 태스크를 수행할 필요가 없습니다.

HMC 코드 업그레이드
HMC 소프트웨어를 동일한 프로그램의 새 릴리스 또는 수정사항 레벨로 대체합니다.

복구 매체를 통한 부팅이 필요합니다.

HMC 코드 마이그레이션
한 HMC 버전에서 다른 버전으로 HMC 데이터를 이동합니다.

마이그레이션은 업그레이드의 한 종류입니다.

참고: HMC 모델 7063-CR1의 경우 외부 USB DVD 드라이브를 연결할 수 있습니다.

HMC 기계코드 버전 및 릴리스 판별

HMC 기계코드 버전 및 릴리스를 확인하는 방법에 대해 학습합니다.

이 태스크 정보

HMC의 기계코드 레벨에 따라 새 릴리스로 업그레이드하기 위한 개선 및 동시 서버 펌웨어 유지보수 등 사용 가능한 기능이 결정됩니다.

HMC 기계코드 버전 및 릴리스를 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 **현재 HMC 드라이버 정보** 표제 아래에 표시되는 정보를 보고 기록하십시오.

인터넷 연결로 HMC용 기계코드 업데이트 획득 및 적용

HMC에 인터넷 연결이 되는 경우 HMC용 기계코드 업데이트를 획득하는 방법에 대해 학습합니다.

이 태스크 정보

HMC용 기계코드 업데이트를 획득하려면 모든 단계를 완료하십시오.

1 단계. 인터넷 연결이 되는지 확인

이 태스크 정보

서비스 및 지원 시스템 또는 웹 사이트에서 사용자의 HMC 또는 서버로 업데이트를 다운로드하려면 다음 연결 중 하나가 있어야 합니다.

- SSL 프록시를 사용하거나 사용하지 않은 SSL 연결성
- 인터넷 VPN

인터넷 연결이 되는지 확인하려면 다음을 수행하십시오.

프로시저

1. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **아웃바운드 연결성 관리**를 클릭하십시오.
3. HMC에 대해 선택한 아웃바운드 연결 유형(인터넷 VPN 또는 SSL 연결)의 탭을 선택하십시오.

   참고: 서비스 및 지원 센터에 대한 연결이 존재하지 않을 경우 이 프로시저를 진행하기 전에 서비스 연결을 설정하십시오. 서비스 및 지원 센터에 대한 연결 설정 방법에 대해서는 IBM 서비스 및 지원 센터에 연결하기 위한 서버 설정을 참조하십시오.
4. **테스트**를 클릭하십시오.
5. 테스트가 정상적으로 완료되었는지 확인하십시오.

   테스트가 성공적이지 않은 경우 이 프로시저를 진행하기 전에 연결 문제를 진단하고 문제점을 정정하십시오. 대안으로 DVD의 업데이트를 가져올 수 있습니다.

   참고: HMC 모델 7063-CR1의 경우 외부 USB DVD 드라이브를 연결할 수 있습니다.
6. 74 페이지의 『2 단계. 기존 HMC 기계코드 레벨 확인』에서 계속하십시오.

2 단계. 기존 *HMC* 기계코드 레벨 확인

이 태스크 정보

기존 HMC 기계코드 레벨을 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 현재 HMC 드라이버 정보 표제 아래에 표시되는 정보를 보고 기록하십시오.
4. 74 페이지의 『3 단계. 사용할 수 있는 HMC 기계코드 레벨 확인』에서 계속하십시오.

3 단계. 사용할 수 있는 *HMC* 기계코드 레벨 확인

이 태스크 정보

사용 가능한 HMC 기계코드 레벨을 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 인터넷 연결이 되는 컴퓨터나 서버에서 http://www.ibm.com/eserver/support/fixes로 이동하십시오.
2. 제품군 리스트에서 적절한 제품군을 선택하십시오.
3. 제품 또는 수정사항 유형 리스트에서 **Hardware Management Console**을 선택하십시오.
4. **계속**을 클릭하십시오.

   Hardware Management Console 사이트가 표시됩니다.
5. 사용 중인 HMC 버전 레벨로 화면이동하여 사용할 수 있는 HMC 레벨을 확인하십시오.

   참고: 원할 경우 서비스 및 지원 센터에 문의할 수 있습니다.
6. 74 페이지의 『4 단계. HMC 기계코드 업데이트 적용』에서 계속하십시오.

4 단계. *HMC* 기계코드 업데이트 적용

이 태스크 정보

HMC 기계코드 업데이트를 적용하려면 다음 단계를 완료하십시오.

프로시저

1. HMC 기계코드에 대한 업데이트를 설치하기 전에 HMC의 중요 콘솔 정보를 백업하십시오.
   지침은 72 페이지의 『관리 콘솔 데이터 백업』을 참조하십시오. 그런 후 다음 단계를 계속 진행하십시오.
2. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
3. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오. 수정 서비스 설치 마법사가 열립니다.
4. 마법사의 지시를 따라 업데이트를 설치하십시오.
5. 시스템 종료를 수행한 후 HMC를 재시작하여 업데이트를 적용하십시오.
6. **Hardware Management Console 웹 애플리케이션 로그온 및 시작**을 클릭하십시오.
7. HMC 인터페이스에 로그인하십시오.

***5* 단계. *HMC* 기계코드 업데이트가 정상적으로 설치되었는지 확인**

이 태스크 정보

HMC 기계코드 업데이트가 정상적으로 설치되었는지 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 현재 HMC 드라이버 정보 표제 아래에 표시되는 정보를 보고 기록하십시오.
4. 설치한 업데이트와 버전 및 릴리스가 일치하는지 확인하십시오.
5. 표시된 코드 레벨이 설치한 레벨이 아닌 경우 다음 단계를 수행하십시오.
   a. HMC의 네트워크 연결을 선택하십시오.
   b. 다른 저장소를 사용하여 펌웨어 업데이트를 재시도하십시오.
   c. 문제점이 지속되면 다음 레벨의 지원에 문의하십시오.

DVD 또는 FTP 서버를 사용하여 HMC용 기계코드 업데이트 획득 및 적용

DVD 또는 FTP 서버를 사용하여 HMC(Hardware Management Console)용 기계코드 업데이트를 획득하는 방법에 대해 학습합니다.

이 태스크 정보

HMC 기계코드 업데이트를 획득하려면 모든 단계를 완료하십시오.

참고: HMC 모델 7063-CR1의 경우 외부 USB DVD 드라이브를 연결할 수 있습니다.

***1* 단계. 기존 *HMC* 기계코드 레벨 확인**

시작하기 전에

기존 HMC 기계코드 레벨을 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.

3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 현재 HMC 드라이버 정보 표제 아래에 표시되는 정보를 보고 기록하십시오.
4. 76 페이지의 『2 단계. 사용할 수 있는 HMC 기계코드 레벨 확인』에서 계속하십시오.

2 단계. 사용할 수 있는 *HMC* 기계코드 레벨 확인

시작하기 전에

사용 가능한 HMC 기계코드 레벨을 확인하려면 다음 단계를 완료하십시오.

이 태스크 정보

프로시저

1. 인터넷 연결이 있는 컴퓨터 또는 서버에서 Fix Central 웹 사이트로 이동하십시오.
2. 사용 중인 HMC 버전 레벨로 화면이동하여 사용할 수 있는 HMC 레벨을 확인하십시오.

   참고: 원할 경우 IBM 서비스 및 지원 센터에 문의할 수 있습니다.
3. 76 페이지의 『3 단계. HMC 기계코드 업데이트 획득』에서 계속하십시오.

3 단계. *HMC* 기계코드 업데이트 획득

시작하기 전에

HMC 기계코드 업데이트를 획득하려면 다음 단계를 완료하십시오.

이 태스크 정보

HMC 기계코드 업데이트는 Fix Central 웹 사이트를 통해 주문하거나 서비스 및 지원 센터에 문의하거나 FTP 서버로 다운로드할 수 있습니다.

Fix Central 웹 사이트를 통한 HMC 기계코드 업데이트 주문

1. 인터넷 연결이 있는 컴퓨터 또는 서버에서 Fix Central 웹 사이트로 이동하십시오.
2. 지원되는 HMC 제품 중에서 최신 HMC 레벨을 선택하십시오.
3. 파일 이름/패키지 영역으로 화면이동한 후 주문하려는 업데이트를 찾으십시오.
4. 주문 열에서 **이동**을 선택하십시오.
5. IBM ID를 사용하여 로그인하려면 **계속**을 클릭하십시오.
6. 화면의 프롬프트를 따라 주문을 제출하십시오.

이동 매체로 HMC 기계코드 업데이트 다운로드

1. 인터넷 연결이 있는 컴퓨터 또는 서버에서 Fix Central 웹 사이트로 이동하십시오.
2. 지원되는 HMC 제품 중에서 최신 HMC 레벨을 선택하십시오.
3. 파일 이름/패키지 영역으로 화면이동한 후 다운로드하려는 업데이트를 찾으십시오.
4. 다운로드하려는 업데이트를 클릭하십시오.
5. 라이센스 계약에 동의하고 업데이트를 이동 매체에 저장하십시오.

다음에 수행할 작업

완료되면 76 페이지의 『4 단계. HMC 기계코드 업데이트 적용』에서 계속하십시오.

4 단계. *HMC* 기계코드 업데이트 적용

시작하기 전에

HMC 기계코드 업데이트를 적용하려면 다음 단계를 완료하십시오.

프로시저

1. HMC 기계코드에 대한 업데이트를 설치하기 전에 HMC 데이터를 백업하십시오. 추가 정보는 72 페이지의 『관리 콘솔 데이터 백업』의 내용을 참조하십시오.
2. 업데이트를 DVD-RAM에 획득하거나 작성한 경우 HMC의 DVD 드라이브에 삽입하십시오. 업데이트를 USB 메모리 장치에 획득하거나 작성한 경우 메모리 장치를 삽입하십시오.
3. HMC 기계코드에 대한 업데이트를 설치하기 전에 HMC의 중요 콘솔 정보를 백업하십시오.
   지침은 72 페이지의 『관리 콘솔 데이터 백업』을 참조하십시오. 그런 후 다음 단계를 계속 진행하십시오.
4. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
5. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오. 수정 서비스 설치 마법사가 열립니다.
6. 마법사의 지시를 따라 업데이트를 설치하십시오.
7. 시스템 종료를 수행한 후 재시작하고 다시 HMC에 로그인하여 업데이트를 적용하십시오.
8. 77 페이지의 『5 단계. HMC 기계코드 업데이트가 정상적으로 설치되었는지 확인』에서 계속하십시오.

5 단계. *HMC* 기계코드 업데이트가 정상적으로 설치되었는지 확인

시작하기 전에

HMC 기계코드 업데이트가 설치되었는지 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 현재 HMC 드라이버 정보 표제 아래에 표시되는 정보를 보고 기록하십시오.
4. 설치한 업데이트와 버전 및 릴리스가 일치하는지 확인하십시오.
5. 표시된 코드 레벨이 설치한 레벨이 아닌 경우 다음 단계를 수행하십시오.
   a. 기계코드 업데이트를 재시도하십시오. 이 프로시저를 위해 DVD를 작성한 경우 새 매체를 사용하십시오.
   b. 문제점이 지속되면 다음 레벨의 지원에 문의하십시오.

HMC 소프트웨어 업그레이드

HMC 구성 데이터를 유지하면서 HMC 관련 소프트웨어를 한 릴리스에서 다음 릴리스로 업그레이드하는 방법에 대해 학습합니다.

이 태스크 정보

HMC의 기계코드를 업그레이드하려면 모든 단계를 완료하십시오.

참고: HMC 모델 7063-CR1의 경우 외부 USB DVD 드라이브를 연결할 수 있습니다.

1 단계. 업그레이드 획득

이 태스크 정보

Fix Central 웹 사이트를 통해 HMC 기계코드 업그레이드를 주문할 수 있습니다.

Fix Central 웹 사이트를 통해 업그레이드를 획득하려면 다음 단계를 완료하십시오.

프로시저

1. 인터넷 연결이 되는 컴퓨터 또는 서버에서 Hardware Management Console 웹 사이트(http://www-933.ibm.com/support/fixcentral/)로 이동하십시오.

2. **계속**을 클릭하십시오.

   Hardware Management Console 사이트가 표시됩니다.
3. 업그레이드하려는 목표 HMC 버전을 탐색하십시오.
4. 다운로드 및 주문 섹션을 찾으십시오.

   참고: 인터넷에 액세스할 수 없는 경우, IBM 서비스 및 지원 센터에 문의하여 DVD 형태로 업그레이드를 주문하십시오.
5. 화면의 프롬프트를 따라 주문을 제출하십시오.
6. 업그레이드한 후 78 페이지의 『2 단계. 기존 HMC 기계코드 레벨 확인』에서 계속하십시오.

2 단계. 기존 *HMC* 기계코드 레벨 확인

이 태스크 정보
HMC의 기존 기계코드 레벨을 판별하려면 다음 단계를 따르십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.탐색 영역에서 **업데이트**를 클릭하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 현재 HMC 드라이버 정보 표제 아래에 표시되는 정보를 보고 기록하십시오.
4. 78 페이지의 『3 단계. 관리 시스템의 프로파일 데이터 백업』에서 계속하십시오.

3 단계. 관리 시스템의 프로파일 데이터 백업

이 태스크 정보

관리 시스템의 프로파일 데이터를 백업하려면 다음 단계를 완료하십시오.

프로시저

1. 프로파일 데이터를 저장할 시스템을 선택하십시오.
2. **조치 > 모든 조치 보기 > 레거시 > 파티션 데이터 관리 > 백업**을 클릭하십시오.
3. 백업 파일 이름을 입력하고 이 정보를 기록하십시오.
4. **확인**을 클릭하십시오.
5. 각 시스템에 대해 해당 단계를 반복하십시오.
6. 78 페이지의 『4 단계. HMC 데이터 백업』에서 계속하십시오.

4 단계. *HMC* 데이터 백업

이 태스크 정보
소프트웨어 업그레이드 중 문제점 발생 시 이전 레벨을 복원할 수 있도록 HMC 소프트웨어의 새 버전을 설치하기 전에 HMC 데이터를 백업하십시오. 정상적으로 HMC 소프트웨어의 새 버전으로 업그레이드한 이후에는 이러한 중요 콘솔 데이터를 사용하지 마십시오.

참고: 이동 매체로 백업하려면 해당 매체를 사용할 수 있어야 합니다.

HMC 데이터를 백업하려면 다음 단계를 완료하십시오.

프로시저

1. 매체로 백업하려는 경우 다음 단계를 수행하여 매체를 포맷하십시오.

   a. 매체를 드라이브에 삽입하십시오.

b. 탐색 영역에서 **서비스 가능성** 아이콘()을 클릭한 다음 **서비스 관리**를 선택하십시오.
c. 컨텐츠 분할창에서 **매체 포맷**을 클릭하십시오.
d. 매체 유형을 선택하십시오.
e. 포맷 유형을 선택하십시오.
f. **확인**을 클릭하십시오.

2. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
3. 컨텐츠 분할창에서 **관리 콘솔 데이터 백업**을 클릭하십시오.
   백업 관리 콘솔 데이터 창이 열립니다.
4. 아카이브 옵션을 선택하십시오.
   로컬 시스템 또는 HMC 파일 시스템에 마운트된 원격 시스템(예: NFS)의 매체로 백업하거나 파일 전송 프로토콜(FTP)을 사용하여 원격 사이트로 백업을 송신할 수 있습니다.
   - 로컬 시스템으로 백업하려면 **로컬 시스템의 매체로 백업**을 선택하고 지시사항을 따르십시오.
   - 마운트된 원격 시스템으로 백업하려면 **마운트된 원격 시스템으로 백업**을 선택하고 지시사항을 따르십시오.
   - 원격 FTP 사이트로 백업하려면 **중요 데이터를 원격 사이트로 백업 송신**을 선택하고 지시사항을 따르십시오.
5. 79 페이지의 『5 단계. 현재의 HMC 구성 정보 기록』에서 계속하십시오.

5 단계. 현재의 *HMC* 구성 정보 기록

이 태스크 정보
HMC 소프트웨어의 새 버전으로 업그레이드하기 전에 예방 조치로 HMC 구성 정보를 기록하십시오.

현재의 HMC 구성을 기록하려면 다음 단계를 완료하십시오.

프로시저

1. HMC 구성 정보를 기록하려는 관리 시스템 또는 파티션을 선택하십시오.
2. 메뉴 POD에서 **조치 > 스케줄 조작**을 선택하십시오.
   선택한 대상에 스케줄된 모든 조작이 표시됩니다.
3. **정렬 > 오브젝트별**을 선택하십시오.
4. 각 오브젝트를 선택하고 다음 상세 정보를 기록하십시오.
   - 오브젝트 이름
   - 스케줄 날짜
   - 조작 시간(24시간제 형식으로 표시)
   - 반복적(해당하는 경우 다음 단계를 완료하십시오):
     a. **보기 > 상세 정보 스케줄**을 선택하십시오.
     b. 간격 정보를 기록하십시오.
     c. 스케줄된 조작 창을 닫으십시오.
     d. 스케줄된 각 조작에 대해 반복하십시오.
5. **스케줄된 조작 사용자 정의** 창을 닫으십시오.
6. 80 페이지의 『6 단계. 원격 명령 상태 기록』에서 계속하십시오.

6 단계. 원격 명령 상태 기록

이 태스크 정보

원격 명령 상태를 기록하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **사용자 및 보안** 아이콘()을 클릭한 다음 **시스템 및 콘솔 보안**을 선택하십시오.
2. 컨텐츠 분할창에서 **원격 명령 실행 사용 가능**을 클릭하십시오.
3. **SSH 기능을 사용하여 원격 명령 실행 가능** 선택란이 체크되어 있는지 여부를 기록하십시오.
4. **취소**를 클릭하십시오.
5. 80 페이지의 『7 단계. 업그레이드 데이터 저장』에서 계속하십시오.

7 단계. 업그레이드 데이터 저장

이 태스크 정보

현재의 HMC 구성을 HMC의 지정된 디스크 파티션 또는 로컬 매체에 저장할 수 있습니다. 업그레이드 데이터는 HMC 소프트웨어를 새 릴리스로 업그레이드하기 직전에 저장하십시오. 업그레이드 후 HMC 구성 설정값을 복원할 수 있습니다.

참고: 백업 데이터는 한 개 레벨만 허용됩니다. 즉, 업그레이드 데이터를 저장할 때마다 이전 레벨이 겹쳐쓰입니다.

업그레이드 데이터를 저장하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **업그레이드 데이터 저장**을 클릭하십시오. **업그레이드 데이터 저장** 마법사가 열립니다.
3. 업그레이드 데이터를 저장하려는 매체를 선택하십시오. 이동 매체에 저장하려는 경우 지금 매체를 삽입하십시오. **다음**을 클릭하십시오.
4. **완료**를 클릭하십시오.
5. 태스크가 완료될 때까지 대기하십시오.

   업그레이드 데이터 저장 태스크에 실패하는 경우 계속하기 전에 다음 레벨의 지원에 문의하십시오.

   참고: 업그레이드 데이터 저장 태스크에 실패하는 경우 업그레이드 프로세스를 계속하지 마십시오.
6. **확인**을 클릭하십시오.
7. 80 페이지의 『8 단계. HMC 소프트웨어 업그레이드』에서 계속하십시오.

8 단계. *HMC* 소프트웨어 업그레이드

이 태스크 정보

HMC 소프트웨어를 업그레이드하려면 DVD 드라이브의 이동 매체를 사용하여 시스템을 재시작하십시오.

프로시저

1. HMC 제품 설치 매체를 DVD 드라이브에 삽입하십시오.
2. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
3. 컨텐츠 분할창에서 **시스템 종료 또는 관리 콘솔 재시작**을 선택하십시오.
4. **HMC 재시작**이 선택되었는지 확인하십시오.

5. **확인**을 클릭하십시오.
   HMC가 재시작되고 시스템 정보가 창에서 화면이동됩니다.
6. **업그레이드**를 선택하고 **다음**을 클릭하십시오.
7. 다음 옵션 중에서 선택하십시오.
   - 이전 태스크 중에 업그레이드 데이터를 저장한 경우 다음 단계를 계속 진행하십시오.
   - 이 프로시저에서 이전에 업그레이드 데이터를 저장하지 않은 경우 계속하기 전에 지금 업그레이드 데이터를 저장해야 합니다.
8. **매체를 통한 업그레이드**를 선택하고 **다음**을 클릭하십시오.
9. 설정값을 확인하고 **완료**를 클릭하십시오.
10. 프롬프트를 따르십시오.

    참고:
    - 화면이 공백이 되는 경우 정보를 보려면 스페이스 바를 누르십시오.
    - 첫 번째 DVD를 설치하는 데 약 20분이 소요됩니다.
11. 로그인 프롬프트에서 사용자 ID와 비밀번호를 사용하여 로그인하십시오.
    HMC 코드 설치가 완료되었습니다.
12. 81 페이지의 『9 단계. HMC 기계코드 업그레이드가 정상적으로 설치되었는지 확인』에서 계속하십시오.

9 단계. *HMC* 기계코드 업그레이드가 정상적으로 설치되었는지 확인

이 태스크 정보
HMC 업그레이드가 설치되었는지 확인하려면 다음 단계를 완료하십시오.

프로시저

1. 탐색 영역에서 **HMC 관리** 아이콘()을 클릭한 다음 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오.
3. 새 창에서 HMC 버전, 릴리스, 유지보수 레벨, 빌드 레벨 및 기준 버전 등 현재 HMC 드라이버 정보 표제 아래에 표시되는 정보를 보고 기록하십시오.
4. 설치한 업데이트와 버전 및 릴리스가 일치하는지 확인하십시오.
5. 표시된 코드 레벨이 설치한 레벨이 아닌 경우 새 DVD를 사용하여 업그레이드 태스크를 재시도하십시오. 문제점이 지속되면 다음 레벨의 지원에 문의하십시오.

네트워크 업그레이드 이미지를 사용하여 HMC를 원격 위치에서 업그레이드

네트워크 업그레이드 이미지를 사용하여 HMC에 있는 소프트웨어를 원격 위치에서 업그레이드하는 방법에 대해 학습합니다.

이 태스크 정보
네트워크 업그레이드 이미지를 사용하여 HMC에 있는 소프트웨어를 원격 위치에서 업그레이드하는 방법에 대해 학습합니다.

프로시저

1. 인터넷이 연결되어 있는 컴퓨터에서 Hardware Management Console 지원 및 다운로드 웹 사이트(http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html)로 이동하십시오.
2. 적절한 HMC V9 네트워크 이미지를 다운로드하여 FTP 서버에 저장하십시오.
   이러한 파일을 직접 HMC로 다운로드할 수는 없습니다. FTP 요청을 수락하는 서버에 이미지 파일을 다운로드해야 합니다.
3. 다음 파일을 다운받으십시오.
   - img2a

- img3a
- base.img
- disk1.img
- hmcnetworkfiles.sum

4. 업그레이드 데이터를 HMC에 저장하십시오. 다음 명령행을 실행하여 업그레이드 데이터를 저장하십시오.
   - DVD와 HDD 둘 다에 데이터를 저장하려면 다음 명령을 실행하십시오.

     mount /media/cdrom

     saveupgdata -r diskdvd
   - 데이터를 HDD에 저장하려면 다음 명령을 실행하십시오.

     saveupgdata -r disk
5. 업그레이드 파일을 HMC의 부트 가능한 디스크 파티션에 복사하십시오. **getupgfiles** 명령을 실행하여 파일을 복사하십시오.

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

   여기서,
   - **ftp server**는 HMC 네트워크 이미지를 다운로드한 FTP 서버의 호스트 이름 또는 IP 주소입니다.
   - **user id**는 FTP 서버의 유효 사용자 ID입니다. `--passwd` 인수로 비밀번호를 지정하지 않는 경우에는 비밀번호를 입력하도록 프롬프트됩니다.
   - **remote directory**는 FTP 서버에 있는 HMC 네트워크 이미지가 저장된 디렉토리입니다.
6. 부트 가능 디스크 파티션에 복사된 코드를 업그레이드하려면 HMC를 다시 시작하십시오. HMC를 다시 시작하려면 **chhmc -c altdiskboot -s enable --mode upgrade**를 실행하십시오.
7. HMC를 다시 시작하고 업그레이드를 시작하십시오. 업그레이드를 시작하려면 **hmcshutdown -r -t now** 명령을 실행하십시오.

HMC 보안 설정

기업 보안 표준을 기반으로 하는 HMC(Hardware Management Console)의 보안을 향상시키는 방법을 학습합니다.

HMC의 기본 구성은 대부분의 엔터프라이즈 사용자에게 충분한 보안을 제공합니다. HMC(Hardware Management Console) 버전 8.4.0 이상을 사용하면 기업 보안 표준을 기반으로 하는 HMC의 보안을 더욱 향상시킬 수 있습니다. HMC의 보안을 향상시키려면 HMC를 최소 보안 레벨 1로 설정해야 합니다. 사용자 환경 및 기업 보안 요구사항에 따라 레벨 2 및 레벨 3의 보안을 선택할 수도 있습니다.

참고: 보안 레벨을 변경하기 전에 기업 보안 준수 팀에게 문의하십시오.

보안 레벨 1

HMC를 보안 설정하려면(보안 레벨 1) 다음 단계를 완료하십시오.

1. 기본 `hscroot` 사용자의 사전 정의된 비밀번호를 변경하십시오. 비밀번호 정책에 대한 자세한 정보는 84 페이지의 『향상된 비밀번호 정책』의 내용을 참조하십시오.
2. HMC가 물리적으로 보안 설정된 환경에 속하지 않는 경우 다음 명령을 실행하여 `grub` 비밀번호를 설정하십시오. `chhmc -c grubpasswd -s enable --passwd <new grub password>`
3. HMC에서 IMM(Integrated Management Module)을 구성한 경우 강력한 IMM 비밀번호를 설정하십시오.
4. 모든 서버에서 *admin* 사용자 및 일반 사용자에 대해 강력한 비밀번호를 설정하십시오.
5. 최근에 릴리스된 보안 수정사항으로 HMC를 업데이트하십시오. 보안 수정사항에 대한 자세한 정보는 IBM Fix Central을 참조하십시오.

보안 레벨 2

여러 사용자가 있는 경우 다음 단계를 완료하여 HMC의 보안을 향상시키십시오.

1. HMC에서 각 사용자의 계정을 작성하고 사용자에게 필요한 역할 및 자원을 지정하십시오. HMC에서 다양한 역할에 대한 자세한 정보는 HMC 태스크, 사용자 역할, ID, 연관된 명령을 참조하십시오.

   참고: HMC에서 작성되는 사용자에게 필요한 자원 및 역할만 지정해야 합니다. 필요한 경우 사용자 정의 역할도 작성할 수도 있습니다.
2. 서로 다른 Hardware Management Console 간의 사용자 데이터 복제를 사용으로 설정하십시오. 사용자 데이터 복제는 마스터-슬레이브 모드 또는 피어-피어 모드에서 수행할 수 있습니다. 사용자 데이터 복제에 대한 자세한 정보는 데이터 복제 관리를 참조하십시오.
3. 인증 기관에서 서명한 인증서를 가져오십시오.

보안 레벨 3

여러 Hardware Management Console 및 시스템 관리자가 있는 경우 다음 단계를 완료하여 HMC의 보안을 향상시키십시오.

1. LDAP(Lightweight Directory Access Protocol) 또는 Kerberos와 같은 중앙 집중식 인증을 사용하십시오. LDAP 구성에 대한 자세한 정보는 HMC에서 LDAP를 구성하는 방법을 참조하십시오.
2. 서로 다른 Hardware Management Console 간의 사용자 데이터 복제를 사용으로 설정하십시오.
3. HMC가 강력한 암호만 사용하도록 HMC가 NIST SP 800-131A 모드에 있어야 합니다.
4. 방화벽에서 필요하지 않은 포트를 차단하십시오. 사용할 수 있는 HMC 포트에 대한 정보는 다음 표를 참조하십시오.

표 *29. HMC*와 상호작용하기 위해 사용자가 사용하는 포트

포트	설명	유형	프로토콜 버전(기본 모드)	프로토콜 버전(NIST 모드)
22	Open SSH	TCP	SSH v2.0	SSH v2.0
123	NTP	UDP	NTP	NTP
161	SNMP 에이전트	UDP	SNMP v3	SNMP v3
162	SNMP 트랩	UDP	SNMP v3	SNMP v3
427	SLP	UDP	해당사항 없음	해당사항 없음
443	HMC GUI 및 REST API	TCP	HTTPS(TLS 1.2, 1.1)	HTTPS(TLS 1.2)
657	RMC	TCP	RSCT(평문 + 해시 및 부호)	RSCT(평문 + 해시 및 부호)
2300	IBM i용 5250 터미널	TCP	평문	평문
2301	IBM i용 5250 보안 터미널	TCP	TLS 1.2	TLS 1.2
9900	FCS: HMC-HMC 검색	UDP	FCS	FCS
9920	FCS: HMC-HMC 통신	TCP	HTTPS(TLS 1.2)	HTTPS(TLS 1.2)
9960	GUI의 VTerm 애플릿	TCP	HTTPS(TLS 1.2, 1.1)	HTTPS(TLS 1.2)

표 *29. HMC*와 상호작용하기 위해 사용자가 사용하는 포트 *(계속)*				
포트	**설명**	**유형**	**프로토콜 버전(기본 모드)**	**프로토콜 버전(NIST 모드)**
12443	HMC REST API(레거시 포트)	TCP	HTTPS(HMC 버전 8.6.0 이하용 TLS 1.2, 1.1, 1.0)	HTTPS(TLS 1.2)
12347	RSCT 피어 도메인	UDP	RSCT(평문 + 해시 및 부호)	RSCT(평문 + 해시 및 부호)
12348	RSCT 피어 도메인	UDP	RSCT(평문 + 해시 및 부호)	RSCT(평문 + 해시 및 부호)

참고: 인트라넷에 노출되는 VTerm(포트 9960) 및 IBM i(포트 2301)에 대해 SSH(포트 22), HTTPS(포트 443 및 포트 12443), 5250 보안 터미널만 사용해야 합니다. 기타 모든 포트는 개인용 또는 격리된 네트워크에서 사용해야 합니다. 자원 모니터링 및 제어(RMC)(포트 657), FCS(포트 9900 및 포트 9920), RSCT 피어 도메인(포트 12347 및 포트 12348)에 대해 별도의 이더넷 포트 및 VLAN을 사용할 수 있습니다.

향상된 비밀번호 정책

HMC(Hardware Management Console)를 사용하여 로컬로 인증된 사용자에 대한 비밀번호 요구사항을 적용할 수 있습니다. 향상된 비밀번호 정책 기능을 사용하여 시스템 관리자는 비밀번호 제한사항을 설정할 수 있습니다. 향상된 비밀번호 정책은 HMC가 설치된 시스템에 적용됩니다.

시스템 관리자는 향상된 비밀번호 정책을 사용하여 모든 사용자에 대해 하나의 비밀번호 정책을 정의할 수 있습니다. HMC는 비밀번호 제한사항을 설정하기 위해 시스템 관리자가 활성화할 수 있는 일반 보안 비밀번호 정책을 제공합니다. 시스템 관리자는 일반 보안 정책 또는 새 사용자 정의 정책을 활성화하도록 선택할 수도 있습니다. HMC 일반 보안 비밀번호 정책은 시스템에서 제거할 수 없습니다. 다음 표에는 일반 보안 정책의 속성 및 기본값이 나열되어 있습니다.

표 *30. HMC* 일반 보안 비밀번호 정책의 비밀번호 속성		
속성	**설명**	**기본값**
`min_pwage`	비밀번호가 활성인 상태로 남아 있어야 하는 최소 일 수입니다.	1
`pwage`	비밀번호가 활성인 상태로 남아 있을 수 있는 최대 일 수입니다.	180
`min_length`	비밀번호의 최소 길이입니다.	8
`hist_size`	재사용할 수 없는, 이전에 저장된 비밀번호의 수입니다.	10
`warn_pwage`	비밀번호가 곧 만료되는 경우 사용자가 비밀번호 만료에 대해 경고를 받은 이후부터 비밀번호 만료까지 남은 일 수입니다.	7
`min_digits`	비밀번호에서 사용해야 하는 최소 자릿수입니다.	없음
`min_uppercase`	대문자의 최소 수입니다.	1
`min_lowercase`	소문자의 최소 수입니다.	6
`min_special_chars`	비밀번호에서 사용해야 하는 특수 문자의 최소 수입니다.	없음

HMC 일반 보안 비밀번호 정책에 대해 다음 항목을 고려하십시오.

- 정책은 **hscroot**, **hscpe** 및 **루트** 사용자 ID에는 적용되지 않습니다.

- 정책은 HMC에서 관리하는 로컬로 인증된 사용자에만 적용되며 LDAP 또는 Kerberos 사용자에게는 정책을 적용할 수 없습니다.
- HMC 일반 보안 비밀번호 정책 또는 사용자 정의 정책은 시스템 관리자가 비밀번호 재사용 제한사항을 설정하도록 허용합니다.
- HMC 일반 보안 비밀번호는 읽기 전용이며 HMC 일반 보안 비밀번호의 속성은 변경할 수 없습니다. 새 사용자 정의 비밀번호를 작성하여 비밀번호 제한사항을 설정할 수 있습니다.

다음 명령을 사용하여 HMC 일반 보안 비밀번호 정책을 구성할 수 있습니다.

mkpwdpolicy
모든 매개변수를 포함하는 파일에서 비밀번호 정책을 가져오거나 비밀번호 정책을 작성합니다.

lspwdpolicy
사용 가능한 모든 비밀번호 정책 프로파일을 나열하고 특정 매개변수를 검색합니다. 현재 활성인 비밀번호 정책을 볼 수도 있습니다.

rmpwdpolicy
기존 비활성 비밀번호 정책을 제거합니다.

참고: 활성인 중간 보안 정책 및 기본 읽기 전용 비밀번호 정책을 제거할 수 없습니다.

chpwdpolicy
비활성 비밀번호 정책의 매개변수를 변경합니다.

HMC를 보안 설정하는 동안 공통 문제점 해결

HMC를 보안 설정할 때 발생할 수 있는 일부 문제점을 해결하는 방법에 대해 학습합니다.

HMC(Hardware Management Console) 및 시스템 간의 연결을 보안 설정하는 방법

HMC는 FSP(Flexible Service Processor)를 통해 시스템에 연결합니다. 네트워크 클라이언트 프로토콜(NETC)이라고 하는 독점 2진 프로토콜이 FSP 및 Power 하이퍼바이저 모두를 관리하는 데 사용됩니다. 다음 표에는 HMC에서 사용하는 포트가 나열되어 있습니다.

표 *31. HMC*와 상호작용하는 데 사용되는 *FSP*의 포트

FSP의 포트	**설명**	**프로토콜 버전(기본 모드)**	**프로토콜 버전(NIST 모드)**
443	Advanced System Management Interface	HTTPS(TLS 1.2)	HTTPS(TLS 1.2)
30000	NETC	NETC(TLS 1.2). 이전 펌웨어의 지원을 위해 SSLv3으로 폴백합니다.	NETC(TLS 1.2)
30001	VTerm	NETC(TLS 1.2). 이전 펌웨어의 지원을 위해 SSLv3으로 폴백합니다.	NETC(TLS 1.2)

HMC를 잠그는 방법

인프라에 대한 보안을 강화하려는 경우 IPS(Intrusion Prevention System) 장치를 사용하거나 방화벽 뒤의 모든 Hardware Management Console 및 IBM Power Systems 서버를 추가할 수 있습니다. 또한 원격으로 사용하지 않거나 HMC를 잠그려는 경우 HMC에서 네트워크 서비스를 사용 안함으로 설정할 수 있습니다. HMC에서 네트워크 서비스를 사용 안함으로 설정하려면 다음 단계를 완료하십시오.

1. SSH 포트를 사용하여 원격 명령 실행을 사용 안함으로 설정하십시오.
2. 원격 가상 터미널(VTerm 포트)을 사용 안함으로 설정하십시오.
3. 원격 웹 액세스 (HMC 그래픽 사용자 인터페이스 및 REST API)를 사용 안함으로 설정하십시오.
4. 구성된 각 이더넷 포트에 대해 HMC 네트워크 설정을 사용하여 방화벽에서 포트를 차단하십시오.

NIST SP 800-131A 준수 모드에서 HMC를 설정하는 방법은 무엇입니까?

HMC 버전 8.1.0 이상에서 HMC를 준수 모드에서 설정하는 경우 NIST SP 800-131A에서 나열하는 강력한 암호만 지원됩니다. Transport Layer Security(TLS 1.2)를 지원하지 않는 POWER5 서버와 같은 이전 Power Systems 서버에 연결하지 못할 수 있습니다. 안전 모드 변경에 대한 자세한 정보는 HMC V8R8 NIST 모드를 참조하십시오.

HMC가 사용하는 암호를 보고 변경하는 방법은 무엇입니까?

HMC 버전 8.1.0 이상에서 HMC는 NIST 800-131A에 정의된 더 안전한 암호 세트를 지원합니다. 기본 모드에서 사용되는 암호는 강력합니다. HMC가 사용하는 암호화 암호에 대한 자세한 정보는 **lshmcencr** 명령을 실행하십시오. 기업 표준에 다른 암호 세트를 사용해야 하는 경우 **chhmcencr** 명령을 실행하여 암호화 암호를 수정하십시오.

HMC가 사용하는 암호화 암호를 나열하여 사용자 비밀번호를 암호화하려면 다음 명령을 실행하십시오.

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

HMC 웹 사용자 인터페이스 및 REST API가 현재 사용할 수 있는 암호화 암호를 나열하려면 다음 명령을 실행하십시오.

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

HMC SSH 인터페이스가 현재 사용할 수 있는 MAC 알고리즘 및 암호화 암호를 나열하려면 다음 명령을 실행하십시오.

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

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

HMC에서 인증서의 강도를 확인하는 방법은 무엇입니까?

HMC의 자체 서명 인증서는 강력한 2048비트 RSA 암호화가 있는 SHA256을 사용합니다. CA 서명 인증서를 사용 중인 경우 약한 1024비트 암호화를 사용 중이지 않은지 확인하십시오. HMC에 대해 다음 인증서를 사용할 수 있습니다.

- HMC 그래픽 사용자 인터페이스 및 REST API(포트 443 및 12443)에 대해 CA 서명 인증서를 사용할 수 있습니다.
- HMC 대 HMC 통신에 대해 포트 9920이 사용됩니다. 이 인증서를 사용자 고유의 인증서로 대체할 수 없습니다.

자체 서명 인증서(기본값) 또는 CA 서명 인증서 사이에서 선택하는 방법은 무엇입니까?

HMC는 설치 중에 인증서를 자동 생성합니다. 그러나 HMC에서 인증서 서명 요청(CSR)을 생성하고 인증 기관이 발행하는 새 인증서를 가져올 수 있습니다. 이 인증서를 HMC에 가져올 수 있습니다. 또한 HMC에 대해 도메인 이름을 획득해야 합니다. HMC의 인증서 관리에 대한 세부사항은 인증서 관리를 참조하십시오.

HMC를 감사하는 방법은 무엇입니까?

Hardware Management Console의 감사는 구성된 암호 및 다양한 HMC 사용자의 사용 활동에 초점을 맞춥니다. 다양한 HMC 사용자의 사용 활동을 보려면 다음 명령을 사용하십시오.

표 *32. HMC*가 사용하는 암호

목적	**명령**
비밀번호 암호화(글로벌 설정)	`lshmcencr -c passwd -t c`
각 사용자의 비밀번호 암호화	`lshmcusr -Fname:password_encryption`
SSH 암호	`lshmcencr -c ssh -t c`
SSH MAC	`lshmcencr -c sshmac -t c`

표 *32. HMC*가 사용하는 암호 *(계속)*	
목적	**명령**
HMC 그래픽 사용자 인터페이스 및 REST API에 사용되는 암호	`lshmcencr -c webui -t c`

다음 명령을 사용하여 HMC에서 사용하는 다양한 콘솔 및 서비스 가능 이벤트 정보를 모니터하십시오.

표 *33. HMC*에서 로그온된 사용자 및 콘솔 또는 서비스 가능 이벤트 정보를 보기 위한 명령	
정보	**명령**
GUI 사용자	`lslogon –r webui –u`
GUI 태스크	`lslogon –r webui –t`
CLI 사용자	`lslogon –r ssh –u`
CLI 태스크	`lslogon –r ssh –t`
HMC의 조작	`lssvcevents -t console -d <number of days>`
시스템의 조작	`lssvcevents –t hardware –m <managed system> -d <number of days>`

HMC의 중앙 집중식 모니터링: 다수의 Hardware Management Console이 있는 경우 모든 사용 데이터를 수집하도록 `rsyslog` 파일을 설정하십시오.

IBM이 HMC 보안 취약성을 수정하는 방법은 무엇입니까?

IBM에는 IBM PSIRT(Product Security Incident Response Team)라고 하는 보안 사고 대응 프로세스가 있습니다. IBM PSIRT(Product Security Incident Response Team)는 IBM 오퍼링과 관련된 보안 취약성 정보의 수집, 조사, 내부 협력을 관리하는 글로벌 팀입니다. HMC와 함께 제공되는 오픈 소스 및 IBM 구성요소는 활발하게 모니터되고 분석됩니다. IBM은 지원되는 모든 HMC 릴리스에 대해 임시 수정사항 및 보안 수정사항을 제공합니다.

HMC의 새 임시 수정사항을 추적하는 방법은 무엇입니까?

보안 공고에는 지원되는 HMC 버전의 취약성 및 임시 수정사항에 대한 정보가 포함되어 있습니다. HMC의 임시 수정사항을 추적하기 위해 다음을 수행할 수 있습니다.

- IBM Security Bulletin에서 최신 보안 공고를 검색하십시오.
- 알림을 위해 Twitter에서 @IBMPowereSupp를 팔로우하십시오.
- IBM 지원 센터의 이메일 알림에 등록하십시오.

보안 프로파일: 일반 개인정보 보호법률(GDPR) 및 PCI-DSS(Payment Card Industry Data Security Standard)

HMC(Hardware Management Console)가 사용자의 개인 정보를 처리하는 방법에 대해 학습합니다.

HMC(Hardware Management Console)는 카드 소지자 데이터를 저장하지 않는 폐쇄형 어플라이언스입니다. 그러므로 PCI-DSS가 정의하는 IT 보안의 요구사항 및 보안 평가 프로시저 서브세트만 HMC에 적용할 수 있습니다. IBM에서 분배하는 신뢰 코드만 HMC에 설치할 수 있습니다. 취약성이 IBM PSIRT 프로세스를 통해 알려지는 경우 임시 수정사항이 공개됩니다. 요구사항 및 권장사항은 다음 항목을 포함합니다.

GDPR 조회

표 *34. GDPR* 조회. 표는 GDPR과 관련된 질문에 대한 정보를 제공합니다.	
질문	**답변**
HMC에는 어떤 종류의 데이터가 저장됩니까?	HMC는 Power 하드웨어의 구성 정보, PowerVM 가상화 및 성능 지표 정보를 저장합니다.
HMC가 개인 데이터를 처리합니까?	콜홈 기능에 대한 연락처 정보를 제공할 수 있습니다. 콜홈 기능에 대한 연락처 정보 제공은 선택사항입니다.
HMC의 시스템 관리에 사용되는 사전 정의된 계정은 무엇입니까?	시스템 관리자는 *hscroot* 사용자 이름을 사용합니다.
HMC의 계정이 특정 사용자와 관련되어 있습니까?	아니요.
HMC에서 개인 데이터를 제공하는 것은 필수입니까?	아니요. 개인 데이터 정보를 제공하지 않아도 됩니다. 그러나 이 정보 제공은 선택사항입니다.
HMC 로그 파일에 개인 데이터 정보가 있습니까?	아니요.
개인 데이터를 완전히, 영구적으로 삭제할 수 있습니까?	예. 콜홈 기능을 구성 해제하십시오.

PCI-DSS 조회

표 *35. PCI-DSS* 조회. 표는 PCI-DSS와 관련된 질문에 대한 정보를 제공합니다.	
질문	**답변**
카드 소지자의 데이터를 보호하기 위해 방화벽 구성을 설치하고 유지보수하는 방법은 무엇입니까?	HMC는 카드 소지자 데이터를 저장하거나 액세스하지 않습니다. 그러나 HMC에는 방화벽 구성이 있으며 사용자는 특정 포트를 제어하고 사용할 수 있습니다.
시스템 비밀번호 및 기타 보안 매개변수에 대해 제공업체가 제공하는 기본값을 사용할 수 있습니까?	네트워크에 시스템을 설치하기 전에 *hscroot* 사용자의 사전 정의된 모든 비밀번호를 변경하십시오.
HMC가 저장된 카드 소지자 데이터를 보호하는 방법은 무엇입니까?	HMC는 카드 소지자 데이터를 저장하거나 액세스하지 않습니다.
데이터가 개방형 공용 네트워크에서 전송되는 경우 HMC가 카드 소지자의 데이터를 암호화하는 방법은 무엇입니까?	HMC는 카드 소지자 데이터를 저장하거나 액세스하지 않습니다.
바이러스 백신 소프트웨어 프로그램을 사용하고 정기적으로 업데이트하는 방법은 무엇입니까?	HMC는 폐쇄형 어플라이언스입니다. 그러므로 악성코드가 HMC를 감염시킬 수 없습니다.
보안 시스템 및 애플리케이션을 개발하고 유지보수하는 방법은 무엇입니까?	IBM Fix Central 웹 사이트에서 사용자의 시스템에 필요한 패치를 수동으로 설치해야 합니다. IBM에서 분배하는 신뢰 코드만 HMC에 설치할 수 있습니다.
HMC는 카드 소지자 데이터에 대한 액세스를 제한합니까?	HMC는 카드 소지자 데이터를 저장하거나 액세스하지 않습니다.
컴퓨터에 대한 액세스 권한이 있는 각 사용자에 고유 ID를 지정하는 방법은 무엇입니까?	공유 ID가 없는지 확인하고 비밀번호 정책을 따라 이 요구사항을 구현할 수 있습니다.
카드 소지자의 데이터에 대한 물리적 액세스를 제한하는 방법은 무엇입니까?	HMC는 카드 소지자 데이터를 저장하거나 액세스하지 않습니다.
네트워크 자원 및 카드 소지자 데이터에 대한 액세스를 추적하고 모니터하는 방법은 무엇입니까?	HMC는 카드 소지자 데이터를 저장하거나 액세스하지 않습니다.

표 *35. PCI-DSS* 조회. 표는 PCI-DSS와 관련된 질문에 대한 정보를 제공합니다. *(계속)*	
질문	**답변**
HMC가 시스템 및 프로세스의 보안을 테스트하는 방법은 무엇입니까?	스캔 도구는 릴리스된 모든 HMC 버전에서 보안 스캔을 실행하는 데 사용됩니다. 스캔 도구는 다음을 포함합니다. *Qualys*, *Nessus*, *testssl*, *sslscan*, *ASoC*.
직원 및 계약자에 대한 정보 보안을 포함하는 보안 정책을 유지보수하는 방법은 무엇입니까?	시스템 관리자는 원격 사용자 로그인을 사용 안함으로 설정하고, 요구사항 기반으로 사용자 로그인을 활성화하며, 액세스가 더 이상 필요하지 않은 경우에는 사용자 로그인을 비활성화합니다.

HMC 포트 위치

위치 코드를 사용하여 포트 위치를 찾을 수 있습니다. HMC 포트 위치 그림을 사용하면 서버에서 HMC 포트 위치로 위치 코드를 맵핑할 수 있습니다.

모델 9008-22L, 9009-22A 및 9223-22H HMC 포트 위치

이 다이어그램과 표를 사용하여 9008-22L, 9009-22A 및 9223-22H에서 HMC 포트를 맵핑할 수 있습니다.

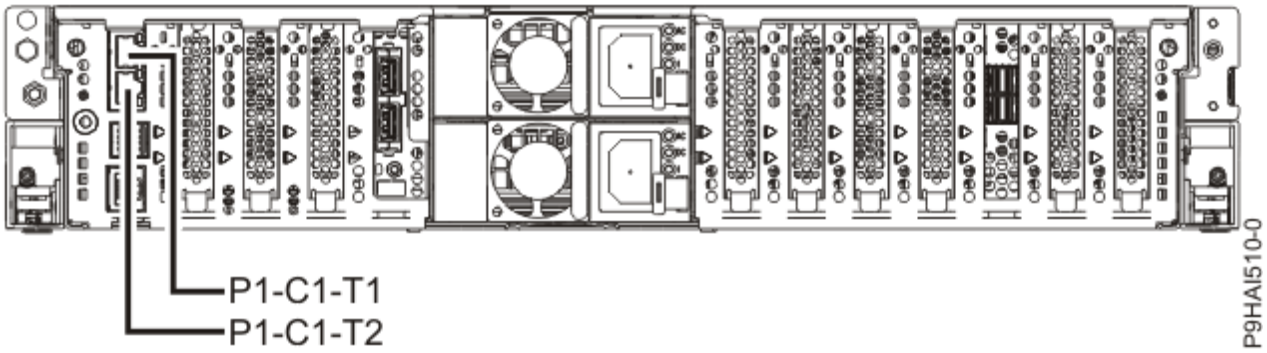


그림 *22. 9008-22L, 9009-22A* 및 *9223-22H HMC* 포트 위치

표 *36. 9008-22L, 9009-22A* 및 *9223-22H HMC* 포트 위치.		
포트	**실제 위치 코드**	**LED 식별**
HMC 포트 1	Un-P1-C1-T1	아니오
HMC 포트 2	Un-P1-C1-T2	아니오
9008-22L, 9009-22A, 9009-41A 및 9009-42A의 HMC 포트 위치에 대한 자세한 정보는 9008-22L, 9009-22A 또는 9223-22H의 부품 위치 및 위치 코드를 참조하십시오.		

모델 9009-41A, 9009-42A 및 9223-42H HMC 포트 위치

이 다이어그램과 표를 사용하여 9009-41A, 9009-42A 및 9223-42H에서 HMC 포트를 맵핑할 수 있습니다.

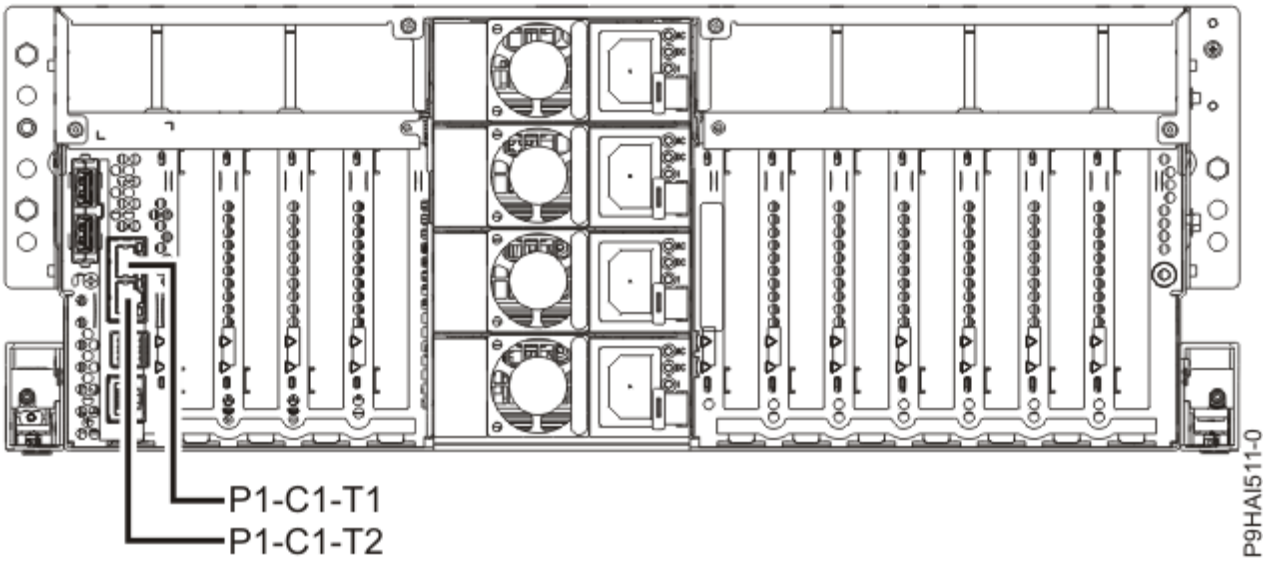


그림 *23. 9009-41A, 9009-42A* 및 *9223-42H HMC* 포트 위치

표 *37. 9009-41A, 9009-42A* 및 *9223-42H HMC* 포트 위치.		
포트	**실제 위치 코드**	**LED 식별**
HMC 포트 1	Un-P1-C1-T1	아니오
HMC 포트 2	Un-P1-C1-T2	아니오
9009-41A, 9009-42A 및 9223-42H의 HMC 포트 위치에 대한 자세한 정보는 9009-41A, 9009-42A 또는 9223-24H의 부품 위치 및 위치 코드를 참조하십시오.		

모델 9040-MR9 HMC 포트 위치

이 다이어그램과 표를 사용하여 9040-MR9에서 HMC 포트를 맵핑할 수 있습니다.

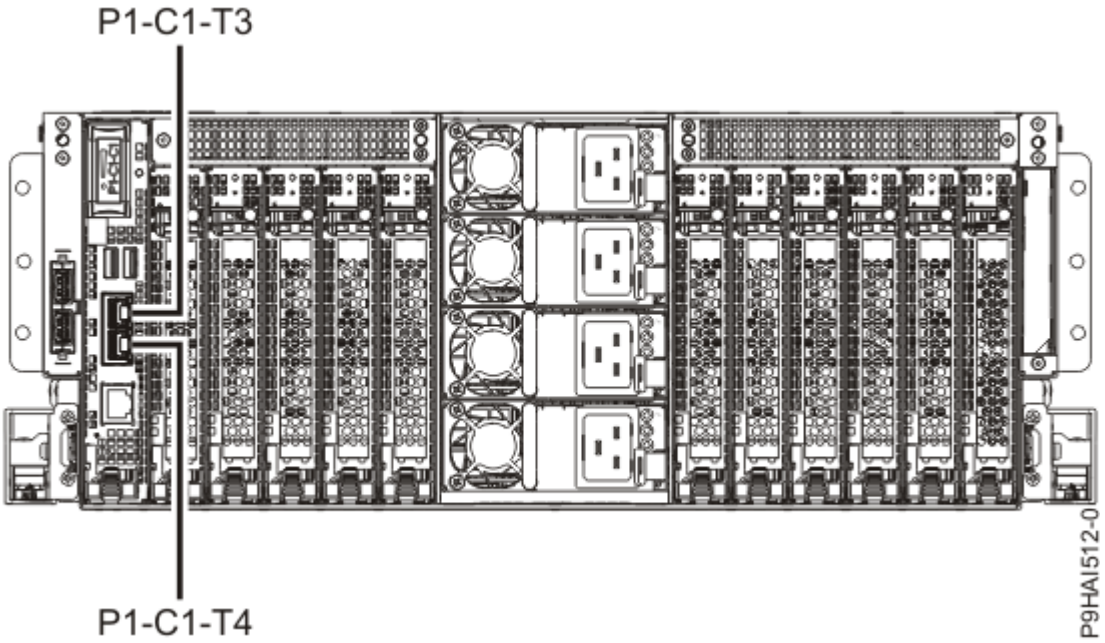


그림 *24. 9040-MR9 HMC* 포트 위치

표 *38. 9040-MR9 HMC* 포트 위치.		
포트	**실제 위치 코드**	**LED 식별**
HMC 포트 1	Un-P1-C1-T3	아니오
HMC 포트 2	Un-P1-C1-T4	아니오
9040-MR9의 HMC 포트 위치에 대한 자세한 정보는 부품 위치 및 위치 코드의 내용을 참조하십시오.		

모델 9080-M9S HMC 포트 위치

이 다이어그램과 표를 사용하여 9080-M9S에서 HMC 포트를 맵핑할 수 있습니다.

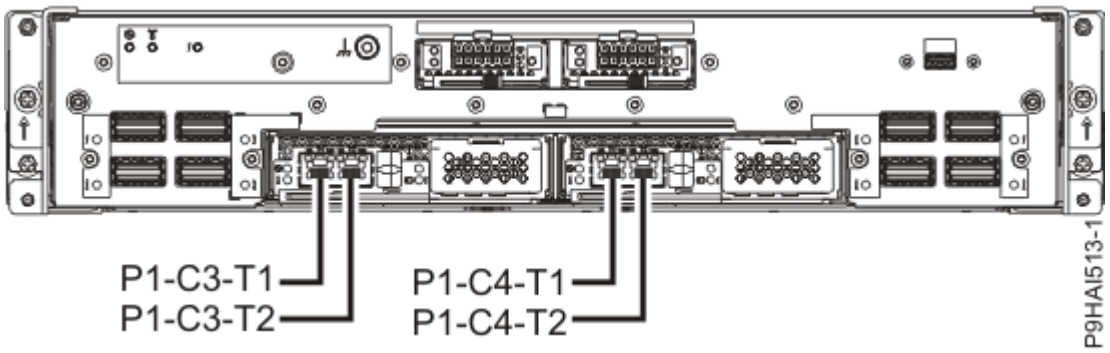


그림 *25. 9080-M9S HMC* 포트 위치

표 *39. 9080-M9S HMC* 포트 위치.		
포트	**물리적 포트 위치**	**LED 식별**
서비스 프로세서 카드 1 - HMC 포트 1	Un-P1-C3-T1	아니오
서비스 프로세서 카드 1 - HMC 포트 2	Un-P1-C3-T2	아니오
서비스 프로세서 카드 2 - HMC 포트 1	Un-P1-C4-T1	아니오
서비스 프로세서 카드 2 - HMC 포트 2	Un-P1-C4-T2	아니오
9080-M9S의 HMC 포트 위치에 대한 자세한 정보는 부품 위치 및 위치 코드의 내용을 참조하십시오.		

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 *10, 3IFC*
한국 아이.비.엠 주식회사
대표전화서비스*: 02-3781-7114*

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현상태대로" 제공합니다.일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

인용된 성능 데이터와 고객 예제는 예시 용도로만 제공됩니다. 실제 성능 결과는 특정 구성과 운영 조건에 따라 다를 수 있습니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

여기에 나오는 모든 IBM의 가격은 IBM이 제시하는 현 소매가이며 통지 없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보는 계획 수립 목적으로만 사용됩니다. 이 정보는 기술된 제품이 GA(General Availability)되기 전에 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 인물 또는 기업의 이름과 유사하더라도 이는 전적으로 우연입니다.

이 정보를 소프트카피로 확인하는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

IBM의 사전 서면 허가 없이는 이 문서의 그림과 스펙의 일부 또는 전체를 복제할 수 없습니다.

IBM은 명시된 특정 기계에서의 사용을 위해 본 정보를 준비했습니다. IBM은 이 정보의 기타 다른 용도에의 적합성에 대한 어떠한 진술도 제공하지 않습니다.

IBM의 컴퓨터 시스템에는 발견되지 않은 데이터 손상 또는 손실에 대한 가능성을 줄이도록 설계된 메카니즘이 포함되어 있습니다. 그러나 이 리스크를 제거할 수는 없습니다. 계획되지 않은 장애, 시스템 고장, 전력 동요나 정

전 또는 구성요소 고장을 겪은 사용자는 장애 또는 고장이 발생한 시점 또는 가까운 시점에 시스템에서 저장 또는 전송한 데이터 및 실행된 조작의 정확성을 검증해야 합니다. 추가로, 사용자는 민감하거나 중요한 운영 상의 해당 데이터를 이용하기 전에 독립적인 데이터 검증이 있음을 확인할 수 있는 절차를 설정해야 합니다. 사용자는 시스템 및 관련 소프트웨에 적용되는 업데이트된 정보와 수정 프로그램을 확인하기 위해 IBM의 지원 웹사이트를 주기적으로 확인해야 합니다.

승인 사항

본 제품은 어떠한 방법이든 공중 통신망의 인터페이스에 연결하기 위한 인증을 귀하의 국가에서 받지 않았을 수 있습니다. 그러한 연결 전에 법률이 요구하는 추가 인증이 필요할 수 있습니다. 궁금하신 사항은 IBM 담당자 또는 리셀러에게 문의하십시오.

IBM Power Systems 서버의 내게 필요한 옵션 기능

내게 필요한 옵션 기능은 거동이 불편하거나 시각 장애 등의 신체적 장애가 있는 사용자가 IT 컨텐츠를 사용할 수 있도록 해줍니다.

개요

IBM Power Systems 서버에는 다음과 같은 주요 내게 필요한 옵션 기능이 포함되어 있습니다.

- 키보드만으로 조작
- 스크린 리더를 사용한 조작

IBM Power Systems 서버는 US Section 508(www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) 및 WVAG(Web Content Accessibility Guidelines) 2.0(www.w3.org/TR/WCAG20/)을 준수하기 위해 최신 W3C 표준인 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/)을 사용합니다. 내게 필요한 옵션 기능을 활용하려면 IBM Power Systems 서버에서 지원하는 최신 웹 브라우저 및 최신 릴리스의 스크린 리더를 사용하십시오.

IBM Knowledge Center의 IBM Power Systems 서버 온라인 제품 문서의 경우 내게 필요한 옵션 기능을 사용할 수 있습니다. IBM Knowledge Center의 내게 필요한 옵션 기능은 IBM Knowledge Center 도움말의 내게 필요한 옵션 절(www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility)에서 설명합니다.

키보드 탐색

이 제품은 표준 탐색 키를 사용합니다.

인터페이스 정보

IBM Power Systems 서버 사용자 인터페이스에는 초당 2 - 55회의 속도로 깜박거리는 컨텐츠가 포함되어 있지 않습니다.

IBM Power Systems 서버 웹 사용자 인터페이스는 올바르게 컨텐츠를 렌더링하고 유용한 경험을 제공하기 위해 전적으로 캐스케이딩 스타일시트를 사용합니다. 이 애플리케이션은 고대비 모드를 포함하여 시력이 좋지 않은 사용자가 시스템 디스플레이 설정을 사용할 수 있는 적절한 방법을 제공합니다. 장치 또는 웹 브라우저 설정을 사용하여 글꼴 크기를 제어할 수 있습니다.

IBM Power Systems 서버 웹 사용자 인터페이스에는 애플리케이션의 기능 영역으로 신속히 이동하기 위해 사용할 수 있는 WAI-ARIA 탐색 랜드마크가 포함되어 있습니다.

공급업체 소프트웨어

IBM Power Systems 서버에는 IBM 라이센스 계약이 적용되지 않는 특정 공급업체 소프트웨어가 포함되어 있습니다. IBM은 이러한 제품의 내게 필요한 옵션 기능에 대해 어떠한 진술 또는 보증도 제공하지 않습니다. 해당 제품에 대한 내게 필요한 옵션 정보는 해당 공급업체에 문의하십시오.

내게 필요한 옵션 관련 정보

IBM에는 표준 IBM 지원 센터 및 지원 웹 사이트 외에도 다음과 같이 청각 장애가 있거나 청력이 좋지 않은 고객이 영업 및 지원 서비스에 액세스하기 위해 사용할 수 있는 TTY 전화 서비스도 있습니다.

TTY 서비스
800-IBM-3383(800-426-3383)
(북미 지역 내에서만 사용 가능함)

IBM에서 내게 필요한 옵션 기능에 도입할 내용에 대한 자세한 정보는 IBM 내게 필요한 옵션(www.ibm.com/able)을 참조하십시오.

개인정보처리방침 고려사항

SaaS(Software as a Service) 솔루션을 포함한 IBM 소프트웨어 제품(이하 "소프트웨어 오퍼링")은 제품 사용 정보를 수집하거나 최종 사용자의 경험을 개선하는 데 도움을 주거나 최종 사용자와의 상호 작용을 조정하거나 그 외의 용도로 쿠키나 기타 다른 기술을 사용할 수 있습니다. 많은 경우에 있어서, 소프트웨어 오퍼링은 개인 식별 정보를 수집하지 않습니다. IBM의 일부 소프트웨어 오퍼링은 귀하가 개인 식별 정보를 수집하도록 도울 수 있습니다. 본 소프트웨어 오퍼링이 쿠키를 사용하여 개인 식별 정보를 수집할 경우, 본 오퍼링의 쿠키 사용에 대한 특정 정보가 다음에 규정되어 있습니다.

이 소프트웨어 오퍼링은 배치된 구성에 따라 세션 관리 용도로 각 사용자의 사용자 이름 및 IP 주소를 수집하는 세션 쿠키를 사용할 수 있습니다. 쿠키를 사용하지 못하도록 할 수 있지만 이 경우 쿠키를 통해 사용 가능한 기능도 제거됩니다.

본 소프트웨어 오퍼링에 배치된 구성이 쿠키 및 기타 기술을 통해 최종 사용자의 개인 식별 정보 수집 기능을 고객인 귀하에게 제공하는 경우, 귀하는 통지와 동의를 위한 요건을 포함하여 이러한 정보 수집과 관련된 법률 자문을 스스로 구해야 합니다.

이러한 목적의 쿠키를 포함한 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인정보처리방침 주요 내용(http://www.ibm.com/privacy/kr/ko), IBM 온라인 개인정보처리방침(http://www.ibm.com/privacy/details/kr/ko) "쿠키, 웹 비콘 및 기타 기술" 및 "IBM 소프트웨어 제품 및 SaaS(Software-as-a Service) 개인정보처리방침"(http://www.ibm.com/software/info/product-privacy) 부분을 참조하십시오.

상표

IBM, IBM 로고 및 ibm.com은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

Red Hat, Red Hat "Shadow Man" 로고 및 모든 Red Hat 기반 상표 및 로고는 미국 또는 기타 국가에서 사용되는 Red Hat, Inc.의 상표 또는 등록상표입니다.

Microsoft 및 Windows는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

Java 및 모든 Java 기반 상표와 로고는 Oracle 및/또는 그 계열사의 상표 또는 등록상표입니다.

전자파 방출 주의사항

장비에 모니터를 연결할 때, 지정된 케이블을 사용하고 모니터와 함께 제공되는 간섭 억제 장치를 사용해야 합니다.

A등급 주의사항

다음의 A등급 문서는 피처 정보에서 EMC(Electromagnetic Compatibility) B등급으로 지정되지 않는 한 POWER9 프로세서 및 해당 피처가 있는 IBM 서버에 적용됩니다.

Federal Communications Commission(FCC) Statement

참고: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

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

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 800 225 5426
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Statement - Japan

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

The following is a summary of the VCCI Japanese statement in the box above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

（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

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格　JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

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

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

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

Electromagnetic Interference (EMI) Statement - People's Republic of China

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。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

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。

The following is a summary of the EMI Taiwan statement above.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

IBM Taiwan Contact Information:

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

한국방송통신위원회(KCC) 사용자안내문

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

Germany Compliance Statement

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

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

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

EN 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
Tel: 914-499-1900

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

Generelle Informationen:

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

Electromagnetic Interference (EMI) Statement - Russia

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

B등급 주의사항

다음의 B등급 문서는 기능 정보에서 전자파 장애(EMC) B등급으로 지정된 기능에 적용됩니다.

Federal Communications Commission(FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

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

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 800 225 5426
email: halloibm@de.ibm.com

VCCI Statement - Japan

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

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

（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

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

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

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

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

IBM Taiwan Contact Information

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

Germany Compliance Statement

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

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

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

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

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

Generelle Informationen:

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

이용 약관

다음 이용 약관에 따라 이 책을 사용할 수 있습니다.

적용: 본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용: 모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 개인적, 비상업적 용도로 복제할 수 있습니다. 귀하는 IBM 의 명시적 동의 없이 본 발행물 또는 그 일부를 배포 또는 전시하거나 2차적 저작물을 만들 수 없습니다.

상업적 사용: 모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 귀하 기업집단 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하의 기업집단 외에서는 IBM 의 명시적 동의 없이 2차적 저작물을 만들거나 이 책 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

권한: 본 허가에서 명시적으로 부여된 경우를 제외하고, 본 문서나 본 문서에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대한 어떠한 허가나 라이센스 또는 권한도 명시적 또는 묵시적으로 부여되지 않습니다.

IBM 은 이 책의 사용이 IBM의 이익을 해친다고 판단하거나 위에서 언급된 지시사항이 준수되지 안는다고 판단하는 경우 언제든지 부여한 허가를 철회할 수 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하는 경우에만 본 정보를 다운로드, 송신 또는 재송신할 수 있습니다.

IBM은 이 책의 내용에 대해 어떠한 보증도 제공하지 않습니다. 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 현 상태대로 제공합니다.