Power Systems

HMC Enhanced+ 인터페이스를 사용하여 *Hardware Management Console* 관리

IBM

Power Systems

HMC Enhanced+ 인터페이스를 사용하여 *Hardware Management Console* 관리

IBM

참고

이 정보 및 이 정보가 제공하는 제품을 사용하기 전에 반드시 107 페이지의 『주의사항』에 나오는 일반 정보를 읽으십시오.

이 개정판은 새 개정판에서 별도로 명시하지 않는 한 IBM Hardware Management Console 버전 8 릴리스 8.7.0 유지보수 레벨 0 및 모든 후속 릴리스와 수정사항에 적용됩니다.

목차

HMC Enhanced+ 인터페이스를 사용하여 HMC 관리

HMC Enhanced+ 인터페이스를 통해 HMC(Hardware Management Console)를 사용하는 방법을 학습합니다.

참고: HMC Enhanced + Tech 미리보기(Pre-GA) 인터페이스의 프로시저 및 기능은 HMC 버전 8.20과 함께 제공된 옵션이며, HMC 버전 8.30과 함께 제공된 HMC Enhanced+ 인터페이스와 동일합니다. 문서에서는 HMC Enhanced+만 참조되지만 해당 컨텐츠는 HMC Enhanced + Tech 미리보기(Pre-GA) 인터페이스에도 적용됩니다.

HMC Enhanced+ 인터페이스는 관리 시스템의 그래픽 보기가 있는 직관적인 인터페이스 작업 환경과 단순화된 탐색을 제공합니다. 콘솔에서 사용할 수 있는 태스크 및 웹 기반 사용자 인터페이스를 사용하여 탐색하는 방법에 대해 학습하십시오.

참고: HMC Enhanced 인터페이스의 기능은 HMC 버전 8.10.1 이상과 함께 제공된 옵션이며, 이제 HMC 버전 8.30과 함께 제공된 HMC Enhanced+ 인터페이스의 일부로 사용 가능합니다.

HMC Enhanced+ 인터페이스를 통한 HMC 관리의 새로운 기능

이 주제 콜렉션의 이전 업데이트 이후에 HMC Enhanced+ 인터페이스를 통한 HMC 관리의 새 정보 또는 크게 변경된 정보에 대해 읽으십시오.

2017년 8월

- HMC Classic 인터페이스는 HMC(Hardware Management Console) 버전 8.7.0 이상에서는 지원되지 않습니다. HMC Classic 인터페이스에서 이전에 사용 가능하던 기능을 이제는 HMC Enhanced+ 인터페이스에서 사용할 수 있습니다.
- 다음 주제가 추가되었습니다.
  - 30 페이지의 『파티션 가용성 우선순위』
  - 31 페이지의 『파티션 데이터 관리』
  - 31 페이지의 『시스템 프로파일 관리』
  - 30 페이지의 『워크로드 관리 그룹 보기』
  - 33 페이지의 『이용률 데이터』
  - 52 페이지의 『프레임에 대한 시스템 관리』
  - 64 페이지의 『시작 텍스트 작성』
  - 81 페이지의 『인증서 폐기 목록 관리』
  - 74 페이지의 『모든 시스템 계획』
- 다음 주제가 업데이트되었습니다.

- 93 페이지의 『서비스 정보 전송』
- 90 페이지의 『콜홈에 대한 이벤트 관리자』

2016년 10월

- 89 페이지의 『태스크 로그』 주제가 추가되었습니다.
- 4 페이지의 『웹 기반 사용자 인터페이스 사용』 주제가 업데이트되었습니다.

2016년 5월

- 93 페이지의 『서비스 정보 전송』 주제가 업데이트되었습니다.

2015년 10월

- 다음 주제가 추가되었습니다.
  - 35 페이지의 『SR-IOV 펌웨어 업데이트』
  - 60 페이지의 『네트워크 연결 테스트』
  - 59 페이지의 『네트워크 토폴로지 보기』
  - 66 페이지의 『Hardware Management Console 업데이트』
  - 71 페이지의 『OS 및 VIOS 이미지』
  - 77 페이지의 『사용자 프로파일 추가, 복사 또는 수정』
- 70 페이지의 『템플리트 및 OS 이미지』 주제가 업데이트되었습니다.

2015년 6월

- HMC Enhanced + Tech 미리보기(Pre-GA) 인터페이스의 프로시저 및 기능은 HMC 버전 8.20과 함께 제공된 옵션이며, HMC 버전 8.30과 함께 제공된 HMC Enhanced+ 인터페이스와 동일합니다. 문서에서는 HMC Enhanced+만 참조되지만 해당 컨텐츠는 HMC Enhanced + Tech 미리보기(Pre-GA) 인터페이스에도 적용됩니다.
- HMC Enhanced 인터페이스의 기능은 HMC 버전 8.10.1 이상과 함께 제공된 옵션이며, 이제 HMC 버전 8.30과 함께 제공된 HMC Enhanced+ 인터페이스의 일부로 사용 가능합니다.
- 78 페이지의 『사용자 특성』 및 20 페이지의 『세션 처리』 주제가 추가되었습니다.
- 23 페이지의 『전원 관리』 주제가 업데이트되었습니다.

2014년 11월

- POWER8® 프로세서를 포함하는 IBM® Power Systems™ 서버에서 HMC 버전 8, 릴리스 2 이상의 HMC Enhanced + Tech 미리보기(Pre-GA) 인터페이스에 대한 정보가 추가되었습니다.

HMC 소개

이 절에서는 HMC(Hardware Management Console)의 일부 개념 및 기능을 간략하게 설명하고 해당 기능에 액세스하는 데 사용되는 사용자 인터페이스를 소개합니다.

HMC를 사용하여 서버를 구성하고 관리할 수 있습니다. 하나의 HMC가 여러 서버를 관리할 수 있으며 듀얼 HMC는 동일한 시스템을 관리하여 중복 지원을 제공할 수 있습니다. 일관성 있는 기능을 보장하기 위해 각 HMC에는 HMC Licensed Machine Code 버전 8, 릴리스 3이 사전 설치되어 있습니다.

참고: 가상화는 IBM Power® System S824L(8247-42L) 서버에서 지원되지 않습니다.

유연성과 사용 가능성을 제공하기 위해 여러 구성으로 HMC를 구현할 수 있습니다.

DHCP 서버로서의 HMC

관리하는 시스템에 사설 네트워크를 통해 연결된 HMC는 시스템의 서비스 프로세서에 대한 DHCP 서버가 될 수 있습니다. 또한 HMC는 개방형 네트워크를 통해 시스템을 관리할 수도 있습니다. 이 개방형 네트워크에서는 관리 시스템의 서비스 프로세서 IP 주소가 고객이 제공하는 DHCP 서버를 통해 지정되거나 ASMI(Advanced System Management Interface)를 사용하여 수동으로 지정됩니다.

물리적 근접성

HMC 버전 7 이전에는 하나 이상의 로컬 HMC가 물리적으로 관리 시스템 근처에 있어야 했습니다. 버전 7 및 HMC의 웹 브라우저 인터페이스를 사용하는 경우에는 이를 준수할 필요가 없습니다.

중복 또는 듀얼 HMC

하나 또는 두 개의 HMC가 서버를 관리할 수 있습니다. 두 개의 HMC가 하나의 시스템을 관리하는 경우 이들은 피어이며, 각 HMC는 관리 시스템을 제어하는 데 사용될 수 있습니다. 하나의 HMC를 관리 시스템의 HCM 포트 또는 서비스 네트워크에 연결하는 것이 가장 좋습니다. 네트워크는 독립적으로 구성됩니다. 각 HMC는 서비스 네트워크에 대한 DCHP 서버가 될 수 있습니다. 네트워크가 독립적이기 때문에 두 개의 고유하고 라우팅 가능하지 않은 IP 범위에서 IP 주소를 제공하도록 DHCP 서버를 설정해야 합니다.

동일한 서버를 관리하는 중복 또는 듀얼 HMC의 버전 및 릴리스 레벨은 서로 다르지 않아야 합니다. 예를 들어, 버전 7 릴리스 7.1.0의 HMC와 버전 7 릴리스 3.5.0의 HMC는 동일한 서버를 관리할 수 없습니다. HMC의 버전 및 릴리스 레벨은 동일해야 합니다.

서버가 더 높은 버전의 관리 콘솔에 연결되면 파티션 구성이 최신 버전으로 업그레이드됩니다. 파티션 구성이 업그레이드된 후 낮은 레벨의 관리 콘솔은 데이터를 올바르게 해석할 수 없습니다. 서버가 높은 버전의 관리 콘솔에서 관리된 후 낮은 버전의 콘솔로 돌아가려면 먼저 서버를 초기화해야 합니다. 이전 레벨에서 수행된 백업을 복원하거나 파티션을 다시 작성할 수 있습니다. 서버가 초기화되지 않으면 낮은 레벨의 HMC 버전에 따라 다음 결과 중 하나가 발생할 수 있습니다.

- 버전 7 릴리스 7.8.0 이상의 HMC는 **버전 불일치** 연결 오류와 **저장 영역 버전 불일치** 참조 코드를 보고합니다.
- 버전 7 릴리스 7.7.0 이하의 HMC는 **완료되지 않음** 또는 **복구** 서버 상태를 보고할 수 있습니다. 또한 파티션 구성 손상이 발생할 수 있습니다.

사전 정의된 사용자 ID 및 비밀번호

사전 정의된 사용자 ID와 비밀번호가 HMC에 포함되어 있습니다. 시스템의 보안을 위해 hscroot의 사전 정의된 비밀번호를 즉시 변경해야 합니다.

HMC에 포함되어 있는 사전 정의된 사용자 ID 및 비밀번호는 다음과 같습니다.

표 *1.* 사전 정의된 *HMC* 사용자 *ID* 및 비밀번호

사용자 ID	비밀번호	용도
hscroot	abc123	hscroot 사용자 ID 및 비밀번호는 처음으로 HMC에 로그인할 때 사용됩니다. 대소문자를 구분하며 수퍼 관리자 역할의 구성원만 사용할 수 있습니다.
root	passw0rd	root 사용자 ID 및 비밀번호는 서비스 제공자가 유지보수 프로시저를 수행할 때 사용됩니다. HMC에 로그인할 때는 사용할 수 없습니다.

웹 기반 사용자 인터페이스 사용

웹 기반 사용자 인터페이스를 사용하여 HMC(Hardware Management Console) 또는 관리 자원에 대한 태스크를 수행할 수 있습니다.

이 사용자 인터페이스는 여러 주요 구성요소(제목 표시줄, 탐색 영역, 컨텐츠 분할창, 메뉴 팟 및 도크 팟)로 구성됩니다.

제목 표시줄: 작업영역 창의 맨 위에 있으며, 제품, 로그인한 사용자, 도움말 옵션 및 로고를 식별합니다.

탐색 영역: 창의 왼쪽 부분에 있으며, 시스템 선택 및 HMC에 대한 태스크 실행을 위한 기본 탐색 링크를 포함합니다.

컨텐츠 분할창: 창의 오른쪽 부분에 있으며, 탐색 영역의 현재 선택사항을 기반으로 정보를 표시합니다. 예를 들어, 탐색 영역에서 **모든 시스템**이 선택된 경우, 컨텐츠 분할창에는 사용 가능한 모든 시스템이 표시됩니다.

창의 왼쪽 부분에 있는 메뉴 팟은 시스템을 선택한 후 표시되며, 공통으로 사용되는 HMC 태스크와 자원 및 특성의 보기에 대한 빠른 액세스를 제공합니다.

창의 오른쪽 부분에 있는 도크 팟은 사용자가 선택한 HMC 태스크를 고정하는 데 사용할 수 있는 고정 기능을 표시합니다. 이 기능을 사용하여 해당 태스크에 빠르게 액세스할 수 있습니다.

탐색 분할창과 작업 분할창을 구분하는 경계선 위에서 마우스 포인터가 양방향 화살표로 바뀔 때까지 마우스 포인터를 움직여서 HMC 작업영역의 분할창 크기를 조정할 수 있습니다. 포인터 모양이 변하면 마우스 왼쪽 단추를 누른 채로 마우스 포인터를 왼쪽 또는 오른쪽으로 끄십시오. 단추를 놓으면 탐

색 분할창 또는 작업 분할창의 크기가 더 커지거나 더 작아집니다. 태스크 패드에서 자원 테이블을 구분하는 작업 분할창 경계 내에서도 이를 수행할 수 있습니다.

참고: HMC의 모든 기능을 사용하려면 팝업 창이 사용으로 설정되어야 합니다.

메뉴 옵션의 개요

HMC(Hardware Management Console)에서 사용 가능한 메뉴 옵션 및 연관된 태스크에 대해 학습합니다.

이 절에서 설명하는 메뉴 옵션 및 태스크는 HMC Enhanced+ 인터페이스에서 사용 가능합니다.

표 *2. HMC* 메뉴 옵션

메뉴	하위 메뉴	옵션/태스크
 **자원**	모든 시스템	모든 시스템 보기
	모든 파티션	모든 파티션 보기
	모든 Virtual I/O Server	모든 Virtual I/O Server 보기
	모든 프레임	모든 프레임 보기
	모든 전원 엔터프라이즈 풀	모든 전원 엔터프라이즈 풀 보기
	모든 공유 스토리지 풀 클러스터	모든 공유 스토리지 풀 클러스터 보기
	모든 그룹	모든 그룹 보기
 **HMC 관리**	콘솔 설정	설치 안내 마법사 실행
		네트워크 토폴로지 보기
		네트워크 연결 테스트
		네트워크 설정 변경
		성능 관리 설정 변경
		날짜 및 시간 변경
		언어 및 로케일 변경
	콘솔 관리	관리 콘솔 종료 또는 다시 시작
		조작 스케줄
		라이센스 보기
		Hardware Management Console 업데이트
		설치 자원 관리
		Virtual I/O Server 이미지 저장소 관리
		매체 포맷
		관리 콘솔 데이터 백업
		관리 콘솔 데이터 복원
		업그레이드 데이터 저장
		데이터 복제 관리
	템플리트 라이브러리	시스템 및 파티션 라이브러리
	업데이트	사용할 수 없음(대신 Hardware Management Console 업데이트 옵션을 사용하십시오.)

표 2. *HMC* 메뉴 옵션 (계속)

메뉴	하위 메뉴	옵션/태스크
사용자 및 보안 	사용자 및 역할	사용자 비밀번호 변경
		사용자 프로파일 및 액세스 관리
		사용자 및 태스크 관리
		태스크 및 자원 역할 관리
	시스템 및 콘솔 보안	인증서 관리
		LDAP 관리
		KDC 관리
		원격 명령 실행 사용
		원격 조작 사용
		원격 가상 터미널 사용
서비스 가능성 	콘솔 이벤트 로그	콘솔 이벤트 보기 창
	서비스 가능 이벤트 관리자	서비스 가능 이벤트 관리자 창
	콜홈에 대한 이벤트 관리자	콜홈에 대한 이벤트 관리자 창
	서비스 관리	서비스 가능 이벤트 작성
		원격 연결 관리
		원격 지원 요청 관리
		덤프 관리
		서비스 정보 전송
		서비스 정보 스케줄
		매체 포맷
		관리 콘솔 추적 수행
		관리 콘솔 로그 보기
		구성요소 로그 보기
		Electronic Service Agent 설정 마법사
		사용자 권한 부여
		Electronic Service Agent 사용
		아웃바운드 연결 관리
		인바운드 연결 관리
		고객 정보 관리
		서비스 가능 이벤트 알림 관리
		연결 모니터링 관리

태스크 및 역할

각 HMC 사용자는 다른 역할의 구성원일 수 있습니다. 이러한 각 역할을 사용하면 사용자는 HMC의 여러 부분에 액세스하고 관리 시스템에서 여러 태스크를 수행할 수 있습니다. HMC 역할은 사전 정의되거나 사용자 정의됩니다.

이 절에서 논의된 역할은 HMC 사용자를 나타냅니다. 논리 파티션에서 실행 중인 운영 체제에는 고유의 사용자 및 역할 세트가 있습니다. HMC 사용자를 작성할 때 해당 사용자에게 태스크 역할을 지정

해야 합니다. 각 태스크 역할을 사용하면 사용자는 HMC 인터페이스에서 사용 가능한 태스크에 대한 액세스 레벨을 다양화할 수 있습니다. 각 HMC 사용자 역할이 수행할 수 있는 태스크에 대한 자세한 정보는 『HMC 태스크, 사용자 역할, ID 및 연관된 명령』의 내용을 참조하십시오.

개별 HMC 사용자에게 관리 시스템 및 논리 파티션을 지정할 수 있습니다. 이를 통해 관리 시스템 A에는 액세스하지만 관리 시스템 B에는 액세스하지 못하는 사용자를 작성할 수 있습니다. 각 관리 자원 액세스 그룹을 관리 자원 역할이라고 합니다.

HMC의 기본값인 **사전 정의된** HMC 역할은 다음과 같습니다.

표 *3.* 사전 정의된 *HMC* 역할

역할	설명	HMC 사용자 ID
운영자	운영자는 일별 시스템 조작에 책임이 있습니다.	**hmcoperator**
수퍼 관리자	수퍼 관리자는 HMC 시스템의 루트 사용자(또는 관리자) 역할을 합니다. 수퍼 관리자에게는 대부분의 HMC 시스템에 액세스하고 수정할 수 있는 무제한의 권한이 있습니다.	**hmcsuperadmin**
제품 엔지니어	제품 엔지니어는 상황 지원에는 도움이 되지만 HMC 사용자 관리 기능에는 액세스할 수 없습니다. 사용자 시스템에 대한 지원 액세스를 제공하려면 제품 엔지니어 역할이 있는 사용자 ID를 작성하고 관리해야 합니다.	**hmcpe**
서비스 담당자	서비스 담당자는 사용자를 방문하여 시스템을 설치, 구성 또는 수리하는 직원입니다.	**hmcservicerep**
뷰어	뷰어는 HMC 정보를 볼 수 있지만 구성 정보를 변경할 수는 없습니다.	**hmcviewer**
클라이언트 라이브 업데이트	클라이언트 라이브 업데이트 역할은 관리 시스템의 파티션에서 AIX® 라이브 업데이트 기능을 사용 중일 때 사용하도록 마련되었습니다. 클라이언트 라이브 업데이트 사용자에게는 AIX에서 라이브 업데이트를 수행하는 데 필요한 정도로 제한된 권한이 있습니다.	**hmcclientliveupdate**

사전 정의된 HMC 역할을 수정하여 **사용자 정의** HMC 역할을 작성할 수 있습니다. 사용자 정의 HMC 역할 작성은 특정 사용자에게 특정 태스크 권한을 부여하거나 제한하는 데 유용합니다.

HMC 태스크, 사용자 역할, ID 및 연관된 명령

이 절에서 논의되는 역할은 HMC 사용자를 참조합니다. 논리 파티션에서 실행되는 운영 체제에는 고유의 사용자 및 역할 세트가 있습니다.

각 HMC 사용자에게는 연관된 태스크 역할과 자원 역할이 있습니다. 태스크 역할은 사용자가 수행할 수 있는 조작을 정의합니다. 자원 역할은 태스크를 수행하기 위한 시스템 및 파티션을 정의합니다. 사용자는 태스크 역할 또는 자원 역할을 공유할 수 있습니다. HMC는 다섯 개의 사전 정의된 태스크 역할과 함께 설치됩니다. 사전 정의된 단일 자원 역할을 사용하여 모든 자원에 액세스할 수 있습니다. 운영자는 사용자 정의된 태스크 역할, 사용자 정의된 자원 역할 및 사용자 정의된 사용자 ID를 추가할 수 있습니다.

일부 태스크에는 연관된 명령이 있습니다. HMC 명령행에 액세스하는 방법에 대한 자세한 정보는 103 페이지의 『HMC 원격 명령행 사용』을 참조하십시오.

일부 태스크는 명령행만 사용하여 수행할 수 있습니다. 해당 태스크의 목록은 18 페이지의 표 9의 내용을 참조하십시오.

태스크 정보를 찾을 위치에 대한 자세한 정보는 다음 표를 참조하십시오.

표 *4. HMC* 태스크 그룹

HMC 태스크와 해당 사용자 역할, ID 및 명령	**연관된 표**
HMC 관리	표 5
서비스 관리	11 페이지의 표 6
시스템 관리	12 페이지의 표 7
제어판 기능	17 페이지의 표 8

이 표에서는 HMC 관리 태스크, 명령 및 각 HMC 관리 태스크와 연관된 기본 사용자 역할을 설명합니다.

표 *5. HMC* 관리 태스크, 명령 및 기본 사용자 역할

HMC 인터페이스 태스크 및 연관된 명령	**사용자 역할 및 ID**			
	운영자 (hmcoperator)	**수퍼 관리자 (hmcsuperadmin)**	**뷰어 (hmcviewer)**	**서비스 담당자 (hmcservicerep)**
67 페이지의 『관리 콘솔 데이터 백업』 bkconsdata	X	X		X
63 페이지의 『날짜 및 시간 변경』 chhmc lshmc	X	X		X
63 페이지의 『언어 및 로케일 변경』 chhmc lshmc	X	X	X	X

표 5. *HMC* 관리 태스크, 명령 및 기본 사용자 역할 *(계속)*

HMC 인터페이스 태스크 및 연관된 명령	**사용자 역할 및 ID**			
	운영자 (hmcoperator)	**수퍼 관리자 (hmcsuperadmin)**	**뷰어 (hmcviewer)**	**서비스 담당자 (hmcservicerep)**
61 페이지의 『네트워크 설정 변경』 chhmc lshmc	X	X		X
75 페이지의 『사용자 비밀번호 변경』 chhmcusr	X	X	X	X
83 페이지의 『KDC 관리』 chhmc lshmc getfile rmfile		X		
82 페이지의 『LDAP 관리』 lshmcldap chhmcldap		X		
59 페이지의 『설치 안내 마법사 실행』		X		
원격 하드웨어 관리 콘솔 실행	X	X	X	X
HMC 화면 잠금	X	X	X	X
로그오프 또는 연결 끊기	X	X	X	X
80 페이지의 『인증서 관리』		X		
69 페이지의 『데이터 복제 관리』	X	X		
71 페이지의 『설치 자원 관리』	X	X		
79 페이지의 『태스크 및 자원 역할 관리』 chaccfg lsaccfg mkaccfg rmaccfg		X		

표 5. *HMC* 관리 태스크, 명령 및 기본 사용자 역할 *(계속)*

HMC 인터페이스 태스크 및 연관된 명령	**사용자 역할 및 ID**			
	운영자 (hmcoperator)	**수퍼 관리자 (hmcsuperadmin)**	**뷰어 (hmcviewer)**	**서비스 담당자 (hmcservicerep)**
75 페이지의 『사용자 프로파일 및 액세스 관리』 chhmcusr lshmcusr mkhmcusr rmhmcusr		X		
79 페이지의 『사용자 및 태스크 관리』 lslogon termtask	X	X	X	X
5250 콘솔 열기	X	X		X
88 페이지의 『원격 명령 실행 사용』 chhmc lshmc	X	X		X
88 페이지의 『원격 조작 사용』 chhmc lshmc	X	X	X	X
88 페이지의 『원격 가상 터미널 사용』	X	X		X
68 페이지의 『관리 콘솔 데이터 복원』	X	X		X
68 페이지의 『업그레이드 데이터 저장』 saveupgdata	X	X		X
65 페이지의 『조작 스케줄』	X	X		
64 페이지의 『시스템 종료 또는 다시 시작』 hmcshutdown	X	X		X
36 페이지의 『서비스 가능 이벤트 관리자』 lssvcevents	X	X		X
66 페이지의 『라이센스 보기』	X	X	X	X

이 표에서는 서비스 관리 태스크, 명령 및 기본 사용자 역할에 대해 설명합니다.

표 6. 서비스 관리 태스크, 명령 및 기본 사용자 역할

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할 및 ID			
	운영자(hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
37 페이지의 『서비스 가능 이벤트 작성』		X		X
90 페이지의 『서비스 가능 이벤트 관리자』 chsvcevent lssvcevents		X		X
91 페이지의 『원격 연결 관리』	X	X		X
92 페이지의 『원격 지원 요청 관리』	X	X	X	X
67 페이지의 『매체 포맷』	X	X		X
92 페이지의 『덤프 관리』 dump cpdump getdump lsdump startdump lsfru	X	X		X
93 페이지의 『서비스 정보 전송』 chsacfg lssacfg	X	X		
95 페이지의 『Electronic Service Agent 사용』	X	X		X
95 페이지의 『아웃바운드 연결 관리』	X	X		X
97 페이지의 『인바운드 연결 관리』	X	X		X
97 페이지의 『고객 정보 관리』	X	X		X
94 페이지의 『사용자 권한 부여』		X		
98 페이지의 『서비스 가능 이벤트 알림 관리』 chsacfg lssacfg	X	X		X
98 페이지의 『연결 모니터링 관리』	X	X	X	X
94 페이지의 『Electronic Service Agent 설정 마법사』		X		X

이 표에서는 시스템 관리 태스크, 명령 및 기본 사용자 역할에 대해 설명합니다.

표 7. 시스템 관리 태스크, 명령 및 기본 사용자 역할

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
21 페이지의 『기타 특성』 lshwres	X	X	X	X
lsled	X	X	X	X
lslparmigr	X	X	X	X
lssyscfg	X	X	X	X
chhwres	X	X	X	X
chsyscfg	X	X	X	X
migrlpar	X	X	X	X
optmem	X	X		X
lsmemopt	X	X	X	X
비밀번호 업데이트 chsyspwd		X		
기본 사용자 인터페이스 설정 변경	X	X	X	X
조작				
23 페이지의 『전원 끄기』 chsysstate	X	X		X
44 페이지의 『활성화』 chsysstate	X	X		X
50 페이지의 『현재 구성 저장』 chsysstate	X	X		X
44 페이지의 『다시 시작』 chsysstate	X	X		X
45 페이지의 『종료』 chsysstate	X	X		X
chlparstate	X	X		X
LED 상태: 주의 LED 비활성화 27 페이지의 『주의 LED』 chled	X	X		
LED 상태: LED 식별 27 페이지의 『주의 LED』	X	X	X	X
LED 상태: LED 테스트 27 페이지의 『주의 LED』	X	X	X	X
24 페이지의 『조작 스케줄』	X	X		

표 7. 시스템 관리 태스크, 명령 및 기본 사용자 역할 (계속)

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
26 페이지의 『ASM 인터페이스 실행』 asmmenu	X	X		X
26 페이지의 『재빌드』 chsysstate	X	X		
23 페이지의 『전원 관리』 chpwrmgmt lspwrmgmt		X		
46 페이지의 『삭제』 rmsyscfg	X	X		X
48 페이지의 『이동성』 lslparmigr migrlpar	X	X		X
49 페이지의 『프로파일 관리』 chsyscfg lssyscfg mksyscfg rmsyscfg chsysstate	X	X		X
23 페이지의 『조작』	X	X	X	X
구성				
30 페이지의 『템플리트에서 파티션 작성』		X		
30 페이지의 『템플리트에서 시스템 배치』		X		
30 페이지의 『구성을 템플리트로 캡처』		X		
44 페이지의 『템플리트 라이브러리』		X		
49 페이지의 『사용자 정의 그룹 관리』	X	X		X
49 페이지의 『프로파일 관리』 chsyscfg chsysstate lssyscfg mksyscfg rmsyscfg	X	X	X	X

표 7. 시스템 관리 태스크, 명령 및 기본 사용자 역할 (계속)

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
현재 구성 저장 50 페이지의 『현재 구성 저장』 mksyscfg	X	X		
연결				
28 페이지의 『서비스 프로세서 상태』 lssysconn	X	X	X	X
28 페이지의 『연결 다시 설정 또는 제거』 rmsysconn	X	X		
29 페이지의 『다른 HMC 연결 끊기』		X		
하드웨어(정보)				
39 페이지의 『하드웨어』	X	X	X	X
업데이트				
34 페이지의 『라이센스가 부여된 내부코드 변경』 lslic updlic		X		X
35 페이지의 『시스템 준비 상태 확인』 updlic		X		X
34 페이지의 『시스템 정보 보기』 lslic		X		X
HMC 업데이트 updhmc lshmc		X		X
서비스 가능성				
50 페이지의 『서비스 가능 이벤트 관리자』 chsvcevent lssvcevents		X		X
37 페이지의 『서비스 가능 이벤트 작성』		X		X
51 페이지의 『참조 코드 히스토리』 lsrefcode	X	X	X	X
51 페이지의 『제어판 기능』 lssyscfg	X	X		
39 페이지의 『FRU 추가』		X		X

표 7. 시스템 관리 태스크, 명령 및 기본 사용자 역할 (계속)

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
40 페이지의 『격납장치 추가』		X		X
40 페이지의 『FRU 교환』		X		X
40 페이지의 『FRU 제거』		X		X
41 페이지의 『격납장치 제거』		X		X
39 페이지의 『IO 장치 전원 켜기/끄기』		X		X
38 페이지의 『덤프 관리』 dump cpdump getdump lsdump startdump lsfru	X	X		X
38 페이지의 『VPD 수집』	X	X	X	X
39 페이지의 『유형, 모델, 피처』		X		
41 페이지의 『FSP 장애 복구 설정』 chsyscfg lssyscfg		X		
42 페이지의 『FSP 장애 복구 시작』 chsysstate		X		
CoD(Capacity on Demand)				
CoD 코드 입력 chcod		X		
히스토리 로그 보기 lscod	X	X	X	X
프로세서: 용량 설정 보기 lscod	X	X	X	X
프로세서 CUoD: 코드 정보 보기 lscod	X	X	X	X
프로세서: 온/오프 CoD: 관리 chcod		X		
프로세서: 온/오프 CoD: 용량 설정 보기 lscod	X	X	X	X

표 7. 시스템 관리 태스크, 명령 및 기본 사용자 역할 (계속)

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
프로세서: 온/오프 CoD: 청구 정보 보기 lscod	X	X	X	X
프로세서: 온/오프 CoD: 코드 정보 보기 lscod	X	X	X	X
프로세서: 평가판 CoD: 중지 chcod		X		
프로세서: 평가판 CoD: 용량 설정 보기 lscod	X	X	X	X
프로세서: 평가판 CoD: 코드 정보 보기 lscod	X	X	X	X
프로세서: 예약 CoD: 관리 chcod		X		
프로세서: 예약 CoD: 용량 설정 보기 lscod	X	X	X	X
프로세서: 예약 CoD: 코드 정보 보기 lscod	X	X	X	X
프로세서: 예약 CoD: 공유 프로세서 이용률 보기 lscod	X		X	X
PowerVM®(이전에는 Advanced POWER® Virtualization이라고 함): 활성 코드 입력 chcod		X		
PowerVM: 히스토리 로그 보기 lscod	X	X	X	X
PowerVM: 코드 정보 보기 lscod	X	X	X	X
엔터프라이즈 인에이블먼트: 활성 코드 입력 chcod		X		
엔터프라이즈 인에이블먼트: 히스토리 로그 보기 lscod	X	X	X	X
엔터프라이즈 인에이블먼트: 코드 정보 보기 lscod	X	X	X	X

표 7. 시스템 관리 태스크, 명령 및 기본 사용자 역할 (계속)

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어 (hmcviewer)	서비스 담당자 (hmcservicerep)
기타 고급 기능: 활성 코드 입력 chcod		X		
기타 고급 기능: 히스토리 로그 보기 lscod	X	X	X	X
기타 고급 기능: 코드 정보 보기 lscod	X	X	X	X
프로세서: 관리 chcod		X		
프로세서: 용량 설정 보기 lscod	X	X	X	X
프로세서: 코드 정보 보기 lscod	X	X	X	X
메모리: 관리 chcod		X		
메모리: 용량 설정 보기 lscod	X	X	X	X
메모리: 코드 정보 보기 lscod	X	X	X	X

이 표에서는 제어판 기능 태스크, 명령 및 기본 사용자 역할에 대해 설명합니다.

표 8. 제어판 기능 태스크, 명령 및 사용자 역할

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어(hmcviewer)	서비스 담당자 (hmcservicerep)
서비스 가능성				
(21) 전용 서비스 도구 활성화 chsysstate	X	X		
(65) 원격 서비스 사용 안함 chsysstate	X	X		
(66) 원격 서비스 사용 chsysstate	X	X		

표 *8.* 제어판 기능 태스크, 명령 및 사용자 역할 *(계속)*

HMC 인터페이스 태스크 및 연관된 명령	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어(hmcviewer)	서비스 담당자 (hmcservicerep)
(67) 디스크 장치 IOP 다시 설정/다시 로드 chsysstate	X	X		
(68) 동시 유지보수 도메인 전원 끄기	X	X		
(69) 동시 유지보수 도메인 전원 켜기	X	X		
(70) IOP 제어 스토리지 덤프 chsysstate	X	X		

이 표에서는 HMC UI 태스크와 연관되지 않은 명령에 대해 설명하고 각 명령을 수행할 수 있는 기본 사용자 역할을 정의합니다.

표 *9.* 명령행 태스크, 연관된 명령 및 사용자 역할

명령행 태스크	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어(hmcviewer)	서비스 담당자 (hmcservicerep)
로컬로 인증된 HMC 사용자의 비밀번호를 암호화하기 위해 HMC에서 사용되는 암호화 변경 또는 HMC 웹 UI에서 사용할 수 있는 암호화 변경 chhmcencr		X		
로컬로 인증된 HMC 사용자의 비밀번호를 암호화하기 위해 HMC에서 사용되는 암호화 나열 또는 HMC 웹 UI에서 사용할 수 있는 암호화 나열 chhmcfs	X	X	X	
HMC 파일 시스템에서 공간 해제 chhmcfs	X	X		
HMC 파일 시스템 정보 나열 lshmcfs	X	X	X	X
HMC에서 이동식 매체의 준비 상태 테스트 ckmedia	X	X		X
원격 사이트에서 HMC 업그레이드에 필요한 파일 얻기 getupgfiles	X	X		X
HMC에서 화면 캡처 제공 hmcwin	X	X	X	X

표 9. 명령행 태스크, 연관된 명령 및 사용자 역할 (계속)

명령행 태스크	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어(hmcviewer)	서비스 담당자 (hmcservicerep)
SSH 명령 사용법 로그 logssh	X	X	X	X
관리 시스템의 파티션 구성 데이터 지우기 또는 덤프 lpcfgop		X		
관리 프레임 또는 관리 프레임에 포함된 시스템의 환경 정보 나열 lshwinfo	X	X	X	X
관리 프레임에서 잠금을 소유한 HMC 나열 lslock	X	X	X	X
관리 프레임에서 HMC 잠금 해제 강제 실행 rmlock		X		
HMC에서 사용할 수 있는 스토리지 매체 장치 나열 lsmediadev	X	X	X	X
SSH 인증 키 관리 mkauthkeys	X	X	X	X
HMC 서브시스템 및 시스템 자원 모니터링 monhmc	X	X	X	X
HMC에서 관리 시스템에 대해 수집된 이용률 데이터 제거 rmlparutil	X	X		X
사용자가 HMC에서 제한된 모드로 텍스트 파일을 편집할 수 있도록 허용 rnvi	X	X	X	X
DLPAR 실패 후 하드웨어 자원 복원 rsthwres		X		
HMC에서 업그레이드 데이터 복원 rstupgdata	X	X		X
HMC에서 원격 시스템으로 파일 전송 sendfile	X	X	X	X
chsvc	X	X		X

표 9. 명령행 태스크, 연관된 명령 및 사용자 역할 (계속)

명령행 태스크	사용자 역할/ID			
	운영자 (hmcoperator)	수퍼 관리자 (hmcsuperadmin)	뷰어(hmcviewer)	서비스 담당자 (hmcservicerep)
lssvc	X	X	X	X
chstat	X	X		X
lsstat	X	X	X	X
chpwdpolicy		X		
lspwdpolicy	X	X	X	X
mkpwdpolicy		X		
rmpwdpolicy		X		
expdata		X		

세션 처리

HMC Enhanced+ 인터페이스에서 세션 제한사항에 대해 학습합니다.

세션 제한사항

HMC Enhanced+ 인터페이스는 HMC Classic 인터페이스와 같은 연결이 끊어진 세션을 지원하지 않습니다. HMC Enhanced+ 인터페이스에서 세션 로그오프와 세션 연결 끊기는 둘 다 세션 로그오프로 간주됩니다. 즉, 동일한 세션에 다시 연결하여 이전 세션에서 시작한 태스크를 재개할 수 없습니다. HMC Enhanced+ 인터페이스를 통한 모든 로그인은 새 세션을 작성합니다.

1. HMC Enhanced+ 인터페이스에서 장기 실행 태스크를 시작한 후 세션에서 로그오프하는 경우, 장기 실행 태스크는 백그라운드에서 계속 실행됩니다. 그러나 다시 로그인하면 새 세션이 작성되며, 이전 태스크의 진행상태를 추적하는 데 도움이 되는 태스크 진행상태 패널을 더 이상 사용할 수 없습니다. 이 시나리오에서는 이전 세션에서 시작된 태스크의 진행상태를 확인해야 하는 경우 각 명령행 인터페이스(CLI)를 실행하거나 관리 자원의 상태를 확인하거나 콘솔 이벤트 로그를 확인할 수 있습니다.

   참고: HMC Classic 인터페이스를 사용하여 이러한 제한사항을 회피하도록 장기 실행 태스크를 수행할 수 있습니다. 장기 실행 태스크의 일부 예에는 다음 태스크가 포함됩니다.

   서버에 대한 시스템 관리:

   - 시스템 계획 배치
   - 코드 업데이트
   - 하드웨어 - 긴급 복구 또는 업그레이드 준비

   파티션에 대한 시스템 관리:

   - 테라바이트 순서로 큰 장치에 DLPAR 메모리
   - LPM(Live Partition Mobility)

- 일시중단 또는 재개

HMC 관리:

- 관리 콘솔 데이터 백업
- 관리 콘솔 데이터 복원
- 업그레이드 데이터 저장

2. 확인 제한시간 설정에 지정된 시간 내에 재인증하는 데 실패하는 경우, 현재 세션에서 자동으로 로그오프됩니다.
3. 유휴 제한시간 사용자 특성 태스크는 HMC Enhanced+ 인터페이스에서 작동하지 않습니다. HMC Enhanced+ 인터페이스는 유휴 제한시간 설정에 대해 기본값 **0**을 사용합니다. 이 설정에 대해 다른 값을 설정하는 경우, 값이 무시됩니다.

   참고: 세션, 유휴 및 확인 제한시간 특성은 사용자에 대해 설정되며, 동일한 HMC에서 사용자에 따라 다를 수 있습니다.

서버에 대한 시스템 관리

시스템 관리는 서버, 논리 파티션 및 프레임을 관리하기 위한 태스크를 표시합니다. 이러한 태스크를 사용하여 서버를 설정 및 구성하고 서버의 현재 상태를 보고 문제점을 해결하고 솔루션을 적용할 수 있습니다.

이러한 태스크는 관리 시스템이 선택될 때 나열됩니다. 메뉴 팟에 나열되는 태스크는 작업 영역의 선택에 따라 변경됩니다.

기타 특성

선택한 관리 시스템의 특성을 표시합니다. 이 정보는 시스템 및 파티셔닝 계획과 자원 할당에 유용합니다.

이 특성에는 다음 탭이 포함됩니다.

일반 **일반** 탭에는 시스템의 이름, 일련 번호, 모델 및 유형, 상태, 주의 LED 상태, 서비스 프로세서 버전, 최대 파티션 수, 지정된 서비스 파티션(지정된 경우) 및 전원 끄기 정책 정보가 표시됩니다.

프로세서

프로세서 탭에는 설치된 처리 장치, 구성 해제된 처리 장치, 사용 가능한 처리 장치, 구성 가능한 처리 장치, 가상 프로세서당 최소 처리 장치 수 및 최대 공유 프로세서 풀 수를 포함하여 관리 시스템의 프로세서에 대한 정보가 표시됩니다.

메모리

메모리 탭에는 설치된 메모리, 구성 해제된 메모리, 사용 가능한 메모리, 구성 가능한 메모리,

메모리 영역 크기, 파티션 사용에 사용 가능한 현재 메모리 및 시스템 펌웨어 현재 메모리를 포함하여 관리 시스템의 메모리에 대한 정보가 표시됩니다. 또한 이 탭에서는 최대 메모리 풀 수도 설명합니다.

I/O **I/O** 탭에는 관리 시스템의 물리적 I/O 자원이 표시됩니다. I/O 슬롯 및 파티션 지정, 어댑터 유형 및 슬롯 LP 한계 정보가 표시됩니다. 물리적 I/O 자원 정보는 장치별로 그룹화됩니다.

- **슬롯** 열에는 각 자원의 물리적 I/O 특성이 표시됩니다.
- **I/O 풀** 열에는 시스템에 있는 모든 I/O 풀과 풀에 속한 파티션이 표시됩니다.
- **소유자** 열에는 현재 물리적 I/O를 소유한 사용자가 표시됩니다. 이 열의 값은 다음 값 중 하나일 수 있습니다.
  - SR-IOV(Single Root I/O Virtualization) 어댑터가 공유 모드에 있으면 이 열에 **하이퍼바이저**가 표시됩니다.
  - SR-IOV 어댑터가 전용 모드에 있을 때 어댑터가 전용 물리적 I/O로서 파티션에 지정되지 않으면 **지정되지 않음**이 표시됩니다.
  - SR-IOV 어댑터가 전용 모드에 있을 때 어댑터가 전용 물리적 I/O로서 논리 파티션에 지정되면 논리 파티션 이름이 표시됩니다.
- **슬롯 LP 한계** 열에는 SR-IOV 공유 모드에서 슬롯 또는 어댑터가 지원하는 논리 포트 수가 표시됩니다.

마이그레이션

관리 시스템이 파티션 마이그레이션 가능한 경우 **마이그레이션** 탭에 파티션 마이그레이션 정보가 표시됩니다.

전원 공급 매개변수

전원 공급 매개변수 탭에서는 다음 필드의 값을 변경하여 다음 다시 시작에 대한 전원 공급 매개변수를 변경할 수 있습니다. 해당 변경사항은 관리 시스템이 다음에 다시 시작할 때만 유효합니다.

기능 **기능** 탭에는 이 서버의 런타임 기능이 표시됩니다. 서버가 가상 신뢰 플랫폼 모듈(vTPM), 가상 서버 네트워크(VSN), 동적 플랫폼 최적화(DPO) 및 SR-IOV 가능을 지원하는지 확인할 수 있습니다.

고급 **고급** 탭에는 사용 가능한 대용량 페이지 메모리, 구성 가능한 대용량 페이지 메모리, 현재 페이지 크기 및 현재 최대 대용량 페이지 메모리를 포함하여 관리 시스템의 대용량 페이지 메모리 기능이 표시됩니다. 대용량 페이지 테이블 지원을 사용하여 시스템의 메모리 할당을 변경하려면 요청된 대용량 페이지 메모리(페이지 수) 필드를 원하는 메모리로 설정하십시오. 대용량 페이지 메모리에 대해 요청된 값을 변경하려면 시스템의 전원을 꺼야 합니다.

배리어 동기화 레지스터(BSR) 옵션은 배열 정보를 표시합니다.

프로세서 성능 옵션은 TurboCore 모드와 시스템 파티션 프로세서 한계(SPPL)를 표시합니다. 다음 TurboCore 모드와 다음 SPPL 값을 설정할 수 있습니다. SPPL은 전용 프로세서 파티션과 공유 프로세서 파티션 둘 다에 적용됩니다.

메모리 미러링 옵션은 현재 미러링 모드 및 현재 시스템 펌웨어 미러링 상태를 표시합니다. 다음 미러링 모드를 설정할 수 있습니다. 또한 메모리 최적화 도구도 실행할 수 있습니다.

VTPM 설정을 볼 수 있습니다.

조작

조작에는 작동 중인 관리 시스템에 대한 태스크가 포함됩니다.

전원 끄기

관리 시스템을 종료하십시오. 관리 시스템의 전원을 끄면 시스템의 전원이 다시 켜질 때까지 모든 파티션이 사용 불가능하게 됩니다.

관리 시스템의 전원을 끄기 전에 모든 논리 파티션이 종료되었고 논리 파티션의 상태가 실행 중에서 활성화되지 않음으로 변경되었는지 확인하십시오. 논리 파티션 종료에 대한 자세한 정보는 45 페이지의 『종료』의 내용을 참조하십시오.

관리 시스템의 전원을 끄기 전에 관리 시스템의 모든 논리 파티션을 종료하지 않으면 관리 시스템 자체에서 전원이 꺼지기 전에 각 논리 파티션을 종료합니다. 이 경우 관리 시스템의 전원을 끄는 데 상당한 시간이 지연될 수 있습니다(특히 논리 파티션이 응답하지 않는 경우). 또한 논리 파티션이 비정상 종료될 수도 있으며 그 결과 데이터가 유실되고 논리 파티션을 다시 활성화하는 경우 더 오래 지연될 수 있습니다.

다음 옵션 중에서 선택하십시오.

정상 전원 끄기

정상 전원 끄기 모드는 시스템의 조작을 제어된 방식으로 종료합니다. 시스템 종료 동안 활성 작업을 실행 중인 프로그램은 정리(작업 끝 처리)를 수행할 수 있습니다.

빠른 전원 끄기

빠른 전원 끄기 모드는 모든 활성 작업을 즉시 중지하여 시스템을 종료합니다. 해당 작업을 실행 중인 프로그램은 정리를 수행할 수 없습니다. 긴급하거나 위험한 상황 때문에 시스템을 종료해야 하는 경우 이 옵션을 사용하십시오.

전원 관리

절전 모드를 사용으로 설정하여 관리 시스템의 프로세서 소비전력을 줄일 수 있습니다.

절전 모드를 사용으로 설정하려면 다음을 수행하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 컨텐츠 분할창에서 절전 모드를 사용할 수 있도록 할 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **조작**을 펼치십시오.
4. **전원 관리**를 클릭하십시오.

5. **사용**을 클릭하십시오.
6. 다음 절전 모드 옵션 중에서 선택하십시오.
   - **절전 모드 사용 안함**: 절전 모드를 사용 안함으로 설정합니다. 프로세서 클럭 빈도는 명목 값으로 설정되며, 시스템에서 사용되는 전력은 명목 레벨에 남아 있습니다.
   - **정적 절전 모드 사용**: 프로세서 클럭 빈도와 전압을 고정 값으로 낮춰서 소비전력을 줄입니다. 이 옵션은 또한 예측 가능한 성능을 제공하면서 시스템의 소비전력을 줄입니다.
   - **동적 절전(선호되는 전원) 모드 사용**: 프로세서 사용에 따라 프로세서 빈도가 달라집니다. 사용량이 많은 기간에는 프로세서 빈도가 허용되는 최대값으로 설정되며, 이 값은 명목 빈도보다 클 수 있습니다. 또한 프로세서 사용량이 중간이거나 적은 기간에는 빈도가 명목 빈도보다 낮아집니다.
   - **동적 절전(선호되는 성능) 모드 사용**: 프로세서 사용에 따라 프로세서 빈도가 달라집니다. 사용량이 중간이거나 많은 기간에는 프로세서 빈도가 허용되는 최대값으로 설정되며, 이 값은 명목 빈도보다 클 수 있습니다. 또한 프로세서 사용량이 적은 기간에는 빈도가 명목 빈도보다 낮아집니다.
   - **고정 최대 빈도 모드 사용**: 사용자가 지정할 수 있는 고정 값으로 프로세서 빈도가 설정됩니다. 이 옵션을 사용하면 프로세서 빈도의 최대 한계 및 시스템의 소비전력을 설정할 수 있습니다.

   참고: 절전 모드를 사용하면 프로세서 빈도가 변경되고 프로세서 사용량이 변경되고 소비전력이 변경되고 성능이 달라집니다.

조작 스케줄

운영자 지원 없이 관리 시스템에서 특정 조작을 수행할 스케줄을 작성하십시오.

스케줄된 조작은 시스템 조작의 자동, 지연 또는 반복 처리가 필요한 상황에 유용합니다. 스케줄된 조작은 조작을 수행하기 위한 운영자의 지원 없이 지정된 시간에 시작됩니다. 스케줄은 단일 조작에 대해 설정되거나 여러 번 반복될 수 있습니다.

예를 들어, 관리 시스템에 대한 전원 켜기 또는 끄기 조작을 스케줄할 수 있습니다.

스케줄된 조작 태스크는 각 조작에 대해 다음 정보를 표시합니다.
- 조작의 오브젝트인 프로세서
- 스케줄된 날짜
- 스케줄된 시간
- 조작
- 남은 반복 수

스케줄된 조작 창에서 다음을 수행할 수 있습니다.
- 나중에 실행할 조작 스케줄
- 일정한 간격으로 반복할 조작 정의
- 이전에 스케줄된 조작 삭제
- 현재 스케줄된 조작의 세부사항 보기

- 지정된 시간 범위 내에서 스케줄된 조작 보기
- 날짜, 조작 또는 관리 시스템을 기준으로 스케줄된 조작 정렬

조작이 한 번 발생하도록 스케줄하거나 조작이 반복되도록 스케줄할 수 있습니다. 조작이 발생할 시간 및 날짜를 제공해야 합니다. 조작을 반복하려는 경우 다음을 선택하도록 요청됩니다.
- 조작이 발생할 요일(선택사항)
- 각 발생 사이의 시간 간격(필수)
- 총 반복 수(필수)

관리 시스템에 대해 스케줄할 수 있는 조작은 다음과 같습니다.

시스템 프로파일에서 활성화
선택한 시스템에서 선택한 시스템 프로파일의 활성화를 스케줄하기 위한 조작을 스케줄합니다.

프로파일 데이터 백업
관리 시스템의 프로파일 데이터를 백업하기 위한 조작을 스케줄합니다.

관리 시스템 전원 끄기
관리 시스템의 시스템 전원 끄기 조작을 일정한 간격으로 스케줄합니다.

관리 시스템 전원 공급
관리 시스템의 시스템 전원 공급 조작을 일정한 간격으로 스케줄합니다.

유틸리티 CoD 프로세서 관리
유틸리티 CoD 프로세서가 사용되는 방법을 관리하기 위한 조작을 스케줄합니다.

유틸리티 CoD 프로세서 분 사용 한계 관리
유틸리티 CoD 프로세서 사용에 대한 한계를 작성합니다.

공유 프로세서 풀 수정
공유 프로세서 풀을 수정하기 위한 조작을 스케줄합니다.

파티션을 다른 풀로 이동
파티션을 다른 프로세서 풀로 이동하기 위한 조작을 스케줄합니다.

관리 시스템의 절전 모드 변경
관리 시스템의 절전 모드를 변경하기 위한 조작을 스케줄합니다.

동적 플랫폼 최적화 모니터/수행
동적 플랫폼 최적화를 수행하고 이메일 알림 경보를 사용자에게 보내기 위한 조작을 스케줄합니다.

관리 시스템에서 조작을 스케줄하려면 다음을 수행하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 컨텐츠 분할창에서 하나 이상의 관리 시스템을 선택하십시오.

3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **조작**을 펼치십시오.
4. **조작 스케줄**을 클릭하십시오.
5. 스케줄된 조작 창의 메뉴 표시줄에서 **옵션**을 클릭하여 다음 레벨의 옵션을 표시하십시오.
   - 스케줄된 조작을 추가하려면 **옵션**을 클릭한 후 **새로 작성**을 클릭하십시오.
   - 스케줄된 조작을 삭제하려면 삭제할 조작을 선택하고 **옵션**을 가리킨 후 **삭제**를 클릭하십시오.
   - 스케줄된 조작의 목록을 선택된 오브젝트의 현재 스케줄로 업데이트하려면 **옵션**을 가리킨 후 **새로 고치기**를 클릭하십시오.
   - 스케줄된 조작을 보려면 보려는 조작을 선택하고 **보기**를 가리킨 후 **스케줄 세부사항...**을 클릭하십시오.
   - 스케줄된 조작의 시간을 변경하려면 보려는 조작을 선택하고 **보기**를 가리킨 후 **새 시간 범위...**를 클릭하십시오.
   - 스케줄된 조작을 정렬하려면 **정렬**을 가리킨 후 표시되는 정렬 카테고리 중 하나를 클릭하십시오.
6. HMC 작업영역으로 돌아가려면 **조작**을 가리킨 후 **종료**를 클릭하십시오.

ASM 인터페이스 실행

HMC(Hardware Management Console)는 시스템의 ASMI(Advanced System Management Interface)에 직접 연결할 수 있습니다.

ASMI는 서버의 조작(예: 자동 전원 다시 시작)을 관리하고 서버에 대한 정보(예: 오류 로그 및 필수 제품 데이터)를 볼 수 있는 서비스 프로세서에 대한 인터페이스입니다.

ASMI(Advanced System Management Interface)에 연결하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 컨텐츠 분할창에서 하나 이상의 관리 시스템을 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **조작**을 펼치십시오.
4. **ASM 인터페이스 실행**을 선택하십시오.

재빌드

관리 시스템에서 구성 정보를 추출하여 HMC(Hardware Management Console)에서 정보를 재빌드할 수 있습니다.

이 태스크는 실행 중인 서버의 조작을 중단시키지 않습니다.

관리 시스템을 재빌드하면 HMC에서 관리 시스템에 대한 정보가 업데이트됩니다. 관리 시스템 재빌드는 관리 시스템이 완료되지 않음 상태인 경우에 유용합니다. 완료되지 않음 상태는 HMC가 관리 시스템에서 논리 파티션, 프로파일 또는 자원에 대한 전체 정보를 수집할 수 없음을 의미합니다.

관리 시스템 재빌드는 HMC 창을 새로 고치는 것과 다릅니다. 관리 시스템을 재빌드할 때 HMC는 관리 시스템에서 정보를 추출합니다. HMC가 관리 시스템을 재빌드하는 동안에는 다른 태스크를 시작할 수 없습니다. 이 프로세스를 완료하는 데에는 몇 분이 소요될 수 있습니다.

비밀번호 변경

선택한 관리 시스템에서 HMC(Hardware Management Console) 액세스 비밀번호 변경

비밀번호가 변경된 후 이 관리 시스템에 액세스할 모든 다른 HMC의 HMC 액세스 비밀번호를 업데이트해야 합니다.

현재 비밀번호를 입력하십시오. 그런 다음, 새 비밀번호를 입력한 후 확인을 위해 다시 입력하십시오.

주의 LED

시스템 주의 LED 정보를 보고 특정 LED를 켜서 시스템 구성요소를 식별하고 관리 시스템의 모든 LED를 테스트하십시오.

시스템은 시스템의 다양한 구성요소(예: 격납장치 또는 FRU(Field Replaceable Unit))를 식별하는 데 도움이 되는 몇 가지 LED를 제공합니다. 이러한 이유로 이를 식별 LED라고 합니다. 각 LED는 해당 구성요소의 위 또는 근처에 있습니다. LED는 구성요소 자체나 구성요소의 운반 장치(예: 메모리 카드, 팬, 메모리 모듈 또는 프로세서)에 있습니다. LED는 녹색 또는 황색입니다. 녹색 LED는 다음 중 하나를 표시합니다.

- 전원이 켜져 있습니다.
- 링크에서 활동 중입니다. (시스템이 정보를 보내거나 받는 중일 수 있습니다.)

황색 LED는 결함을 나타내거나 상태를 식별합니다. 시스템 또는 시스템의 구성요소 중 하나에 황색 LED가 켜져 있거나 깜박이면 문제점을 식별하고 적절한 조치를 수행하여 시스템을 정상 상태로 복원하십시오.

다음 유형의 식별 LED를 활성화하거나 비활성화할 수 있습니다.

격납장치 식별 LED

어댑터를 특정 드로어(격납장치)에 추가하려면 드로어의 머신 유형, 모델 및 일련 번호(MTMS)를 알아야 합니다. 새 어댑터가 필요한 드로어의 MTMS가 올바른지 판별하기 위해 드로어의 LED를 활성화하고 MTMS가 새 어댑터가 필요한 드로어에 해당하는지 확인할 수 있습니다.

지정된 격납장치와 연관된 FRU에 대한 식별 LED

특정 I/O 어댑터에 케이블을 연결하려는 경우 FRU(Field Replaceable Unit)인 어댑터에 대한 LED를 활성화하고 케이블을 연결할 위치를 물리적으로 확인할 수 있습니다. 이는 여러 개의 어댑터가 있고 포트가 열려 있는 경우에 특히 유용합니다.

시스템 주의 LED 또는 논리 파티션 LED를 비활성화할 수 있습니다. 예를 들어, 문제점의 우선순위가 높지 않음을 판별하고 나중에 문제점을 수리하도록 결정할 수 있습니다. 그러나 다른 문제점이 발생하는 경우에는 경보를 받으려고 하므로 다른 문제점이 발생하면 다시 활성화될 수 있도록 시스템 주의 LED를 비활성화해야 합니다.

다음 옵션 중에서 선택하십시오.

주의 LED 끄기
이 태스크에서 시스템 주의 LED를 비활성화할 수 있습니다.

주의 LED 식별
선택된 격납장치에 포함된 모든 위치 코드에 대한 현재 식별 LED 상태를 표시합니다. 이 태스크에서는 LED에 대해 작동할 단일 위치 코드 또는 여러 위치 코드를 선택할 수 있으며, 해당 단추를 선택하여 LED를 활성화하거나 비활성화할 수 있습니다.

주의 LED 테스트
선택된 시스템에 대해 LED 램프 테스트를 시작합니다. 모든 LED가 몇 분 동안 활성화됩니다.

연결

서비스 프로세서 또는 프레임에 대한 HMC(Hardware Management Console) 연결 상태를 보거나, 해당 연결을 다시 설정하거나, 선택한 관리 시스템에 다른 HMC를 연결하거나, 다른 HMC의 연결을 끊을 수 있습니다.

작업 영역에서 관리 시스템을 선택한 경우, 해당 관리 시스템과 관련된 태스크는 다음과 같습니다. 프레임을 선택한 경우, 태스크는 해당 프레임에 적용됩니다.

서비스 프로세서 상태

관리 시스템의 서비스 프로세서에 대한 HMC(Hardware Management Console) 연결 상태에 대한 정보를 보십시오.

관리 시스템에 있는 서비스 프로세서에 대한 서비스 프로세서 연결 상태를 표시하려면 다음을 수행하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 서비스 프로세서 연결 상태를 보려는 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **조작**을 펼치십시오.
4. **서비스 프로세서 상태**를 선택하십시오.

연결 다시 설정 또는 제거

HMC(Hardware Management Console) 인터페이스에서 관리 시스템을 다시 설정하거나 제거하십시오.

연결을 다시 설정하거나 제거하려면 다음을 수행하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 다시 설정하거나 제거할 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **조작**을 펼치십시오.
4. **연결 다시 설정 또는 제거**를 선택하십시오.
5. 옵션을 선택하고 **확인**을 클릭하십시오.

다른 HMC 연결 끊기

선택된 HMC(Hardware Management Console)와 관리 서버 사이의 연결을 끊을 수 있습니다.

다른 HMC의 연결을 끊으려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 다른 HMC의 연결을 끊으려는 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **조작**을 펼치십시오.
4. **다른 HMC 연결 끊기**를 선택하십시오.
5. 목록에서 HMC를 선택하고 **확인**을 클릭하십시오.

시스템 템플리트

시스템 템플리트는 시스템 특성, 공유 프로세서 풀, 예약 스토리지 풀, 공유 메모리 풀, 호스트 이더넷 어댑터 및 SR-IOV 어댑터와 같은 자원의 구성 세부사항을 포함합니다. 별도의 태스크를 사용하여 이전에 구성한 많은 시스템 설정을 템플리트에서 시스템 배치 마법사에서 사용할 수 있습니다. 예를 들어, 마법사를 사용하여 시스템 템플리트에서 시스템을 배치할 때 Virtual I/O Server, 가상 네트워크 브릿지 및 가상 스토리지 설정을 구성할 수 있습니다.

템플리트 라이브러리에는 공통 사용 시나리오 기반의 구성 설정을 포함하는 사전 정의된 시스템 템플리트가 포함됩니다. 사전 정의된 시스템 템플리트는 즉시 사용할 수 있습니다.

또한 사용자 환경에 특정한 구성 설정을 포함하는 사용자 정의 시스템 템플리트를 작성할 수 있습니다. 사전 정의된 템플리트를 복사한 후 사용자 요구에 맞게 이를 변경하여 사용자 정의 템플리트를 작성할 수 있습니다. 또는 기존 시스템의 구성을 캡처하고 세부사항을 템플리트에 저장할 수 있습니다. 그런 다음, 동일한 구성이 필요한 다른 시스템에 해당 템플리트를 배치할 수 있습니다.

템플리트에서 시스템 배치

HMC(Hardware Management Console)의 템플리트 라이브러리에서 사용 가능한 시스템 템플리트를 사용하여 시스템을 배치할 수 있습니다. 템플리트에서 시스템 배치 마법사는 선택한 시스템의 배치를 완료하는 데 필요한 대상 시스템 특정 정보를 제공하도록 안내합니다.

템플리트에서 파티션 작성

HMC(Hardware Management Console)의 템플리트 라이브러리에서 사용 가능한 파티션 템플리트를 사용하여 파티션을 작성할 수 있습니다. 템플리트에서 파티션 작성 마법사는 배치 프로세스 및 구성 단계를 안내합니다.

구성을 템플리트로 캡처

실행 중인 서버의 구성 세부사항을 캡처하고 HMC(Hardware Management Console)를 사용하여 해당 정보를 사용자 정의 시스템 템플리트로 저장할 수 있습니다. 이 기능은 동일한 구성으로 여러 서버를 배치하려는 경우에 유용합니다. 사전 정의된 템플리트를 사용하려는 경우에는 이 태스크를 완료할 필요가 없습니다.

레거시

HMC(Hardware Management Console)에서 사용 가능한 **레거시** 태스크를 볼 수 있습니다.

작업 영역에서 관리 시스템을 선택하는 경우, 해당 관리 시스템과 연관된 **레거시** 태스크는 다음과 같습니다.

파티션 가용성 우선순위

이 태스크를 사용하여 이 관리 시스템에서 각 논리 파티션의 파티션 가용성 우선순위를 지정할 수 있습니다.

관리 시스템은 프로세서가 실패할 때 파티션 가용성 우선순위를 사용합니다. 프로세서가 논리 파티션에서 실패하며 미지정 프로세서를 관리 시스템에서 사용할 수 없는 경우, 논리 파티션은 보다 낮은 파티션 가용성 우선순위로 논리 파티션의 교체 프로세서를 확보할 수 있습니다. 이 태스크는 프로세서 실패 이후 보다 높은 파티션 가용성 우선순위를 지닌 논리 파티션의 계속적인 실행을 허용합니다.

파티션을 선택하고 목록에서 가용성 우선순위를 선택하여 파티션의 파티션 가용성 우선순위를 변경할 수 있습니다.

파티션 우선순위 지정에 대한 추가 정보가 필요하면 온라인 도움말을 사용하십시오.

워크로드 관리 그룹 보기

관리 시스템에 대해 지정된 워크로드 관리 그룹의 상세 보기를 표시합니다.

각 그룹은 총 프로세서 수, 공유 모드 처리를 사용하는 파티션의 처리 단위 및 그룹의 파티션에 할당된 총 메모리 용량을 표시합니다.

시스템 프로파일 관리

시스템 프로파일은 HMC(Hardware Management Console)가 특정 구성의 관리 시스템에서 논리 파티션을 시작하는 데 사용하는 파티션 프로파일의 순서화된 목록입니다.

시스템 프로파일을 활성화할 때 관리 시스템은 지정된 순서대로 시스템 프로파일의 각 파티션 프로파일을 활성화하려고 시도합니다. 시스템 프로파일을 사용하면 관리 시스템을 활성화하거나 관리 시스템을 하나의 전체 논리 파티션 구성 세트에서 다른 전체 논리 파티션 구성 세트로 변경하는 데 도움이 됩니다.

사용자는 과다 할당된 자원의 파티션 프로파일이 있는 시스템 프로파일을 작성할 수 있습니다. HMC를 사용하여 현재 사용 가능한 시스템 자원 및 전체 시스템 자원에 대해 시스템 프로파일의 유효성을 검증할 수 있습니다. 시스템 프로파일의 유효성을 검증하면 I/O 장치 및 처리 자원이 과다 할당되지 않도로 보장되며, 이는 시스템 프로파일이 활성화될 수 있는 가능성을 높여줍니다. 유효성 검증 프로세스는 시스템 프로파일의 모든 파티션 프로파일을 활성화하는 데 필요한 메모리의 양을 추정합니다. 시스템 프로파일이 유효성 검증을 통과할 수는 있지만 활성화되기에는 충분한 메모리가 없습니다.

이 태스크를 사용하여 다음 태스크를 완료하십시오.

- 새 시스템 프로파일을 작성합니다.
- 시스템 프로파일의 사본을 작성합니다.
- 관리 시스템에서 사용 가능한 자원에 대해 시스템 프로파일에 지정된 자원의 유효성을 검증합니다. 유효성 검증 프로세스는 시스템 프로파일의 임의의 논리 파티션이 이미 활성인지 여부와 관리 시스템의 커미트되지 않은 자원이 파티션 프로파일에 지정된 최소 자원을 충족할 수 있는지 여부를 표시합니다.
- 시스템 프로파일의 특성을 봅니다. 이 태스크에서 기존 시스템 프로파일을 보거나 변경할 수 있습니다.
- 시스템 프로파일을 삭제합니다.
- 시스템 프로파일을 활성화합니다. 시스템 프로파일을 활성화할 때 관리 시스템은 시스템 프로파일에 지정된 순서대로 파티션 프로파일을 활성화하려고 시도합니다.

시스템 프로파일 관리에 대한 추가 정보가 필요하면 온라인 도움말을 사용하십시오.

파티션 데이터 관리

파티션 프로파일은 논리 파티션에 대해 가능한 구성을 지정하는 HMC의 레코드입니다. 파티션 프로파일을 활성화하는 경우, 관리 시스템은 파티션 프로파일의 구성 정보를 사용하여 논리 파티션을 시작하려고 시도합니다.

파티션 프로파일은 논리 파티션에 대해 원하는 시스템 자원 및 논리 파티션이 보유할 수 있는 시스템 자원의 최대/최소 양을 지정합니다. 파티션 프로파일 내에 지정된 시스템 자원에는 프로세서, 메모리 및 I/O 자원이 포함되어 있습니다. 파티션 프로파일이 논리 파티션에 대한 특정 운영 설정을 지정할 수도 있습니다. 예를 들어, 파티션 프로파일이 활성화되면 다음 번에 관리 시스템의 전원을 켤 때 논리 파티션의 자동 시작이 설정되도록 파티션 프로파일을 설정할 수 있습니다.

HMC로 관리되는 관리 시스템의 각 논리 파티션에는 최소한 하나 이상의 파티션 프로파일이 있습니다. 논리 파티션에 대해 자원 스펙이 상이한 파티션 프로파일을 추가로 작성할 수 있습니다. 다수의 파티션 프로파일을 작성하는 경우에는 논리 파티션의 임의의 파티션 프로파일을 기본 파티션 프로파일이 되도록 지정할 수 있습니다. 특정 파티션 프로파일이 활성화되도록 선택하지 않은 경우, HMC는 기본 프로파일을 활성화합니다. 한 번에 하나의 파티션 프로파일만 활성화할 수 있습니다. 논리 파티션에 대해 다른 파티션 프로파일을 활성화하려면 다른 파티션 프로파일을 활성화하기 전에 우선 논리 파티션을 종료해야 합니다.

파티션 프로파일은 파티션 ID 및 프로파일 이름으로 식별됩니다. 파티션 ID는 관리 시스템에서 작성되는 각각의 논리 파티션을 식별하는 데 사용되는 정수이며, 프로파일 이름은 각 논리 파티션에 대해 작성되는 파티션 프로파일을 식별합니다. 논리 파티션의 각 파티션 프로파일의 프로파일 이름은 고유해야 하지만, 단일 관리 시스템에서는 서로 다른 논리 파티션에 대해 하나의 프로파일 이름을 사용할 수 있습니다. 예를 들어, 논리 파티션 1은 프로파일 이름이 "normal"인 파티션 프로파일을 둘 이상 보유할 수 없지만 관리 시스템에서는 각 논리 파티션에 대해 이름이 "normal"인 프로파일을 작성할 수 있습니다.

파티션 프로파일을 작성할 때 HMC는 시스템에서 사용 가능한 모든 자원을 표시합니다. HMC는 다른 파티션 프로파일이 이러한 자원의 일부를 사용 중인지 여부를 확인하지 않습니다. 따라서 사용자가 자원을 과다 할당할 가능성이 있습니다. 프로파일이 활성화될 때 시스템은 사용자가 프로파일에 할당한 자원을 할당하려고 시도합니다. 자원을 과다 할당하는 경우에는 파티션 프로파일이 활성화되지 않습니다.

예를 들어, 관리 시스템에 4개의 프로세서가 있다고 가정합니다. 파티션 1 프로파일 A에 3개의 프로세서가 있으며 파티션 2 프로파일 B에 2개의 프로세서가 있습니다. 이러한 두 파티션 프로파일을 동시에 활성화하려고 시도하는 경우, 프로세서 자원이 과다 할당되었으므로 파티션 2 프로파일 B의 활성화에 실패합니다.

논리 파티션을 종료하고 파티션 프로파일을 사용하여 논리 파티션을 다시 활성화하는 경우, 파티션 프로파일은 파티션 프로파일의 자원 스펙으로 논리 파티션의 자원 스펙을 덮어씁니다. 동적 논리 파티션을 사용하여 논리 파티션에 가해진 자원 변경사항은 파티션 프로파일을 사용하는 논리 파티션을 다시 활성화할 때 유실됩니다. 이는 논리 파티션에 대한 동적 논리 파티션 변경을 실행 취소하고자 할 때 필요합니다. 그러나 이는 관리 시스템을 종료할 때 논리 파티션이 보유한 자원 스펙을 사용하는 논리 파티션을 다시 활성화하고자 하는 경우에는 필요하지 않습니다. 따라서 최신 자원 스펙으로 파티션 프로파일을 최신 상태로 유지하십시오. 사용자는 논리 파티션의 현재 구성을 파티션 프로파일로서 저장할 수 있습니다. 이 태스크를 수행하면 파티션 프로파일을 수동으로 변경해야 할 필요가 없습니다.

해당 파티션 프로파일이 최신 상태가 아닌 논리 파티션을 종료하는 경우 및 관리 시스템이 시작될 때 논리 파티션이 자동으로 시작되도록 설정된 경우에는 파티션 자동 시작 전원 공급 모드를 사용하여 전체 관리 시스템을 다시 시작함으로써 해당 논리 파티션의 자원 스펙을 그대로 유지할 수 있습니다. 논리 파티션이 자동으로 시작되는 경우, 논리 파티션은 관리 시스템이 종료될 때 논리 파티션이 보유하던 자원 스펙을 그대로 보유합니다.

파티션 데이터 관리 태스크를 사용하여 다음 태스크를 완료할 수 있습니다.

- 파티션 데이터를 복원합니다. 파티션 프로파일 데이터가 유실된 경우에는 세 가지 방법 중 하나로 복원 태스크를 사용하십시오.
  - 백업 파일에서 파티션 데이터를 복원합니다. 선택된 백업 파일이 작성된 후에 수행된 프로파일 수정사항은 유실됩니다.
  - 최근 프로파일 활동 및 백업 파일의 병합된 데이터를 복원합니다. 정보가 충돌하는 경우에는 백업 파일의 데이터가 최근 프로파일 활동에 우선합니다.
  - 백업 파일 및 최근 프로파일 활동의 병합된 데이터를 복원합니다. 정보가 충돌하는 경우에는 최근 프로파일 활동의 데이터가 백업 파일에 우선합니다.
- 파티션 데이터를 초기화합니다. 관리 시스템에 대한 파티션 데이터를 초기화하면 현재 정의된 시스템 프로파일, 파티션 및 파티션 프로파일이 모두 삭제됩니다.
- 파티션 프로파일을 파일에 백업합니다.
- 파티션 데이터를 파일에 백업합니다.

파티션 데이터 관리에 대한 추가 정보가 필요하면 온라인 도움말을 사용하십시오.

이용률 데이터

특정 관리 시스템 또는 HMC이 관리하는 모든 시스템에 대한 자원 이용률 데이터를 수집하도록 HMC(Hardware Management Console)를 설정할 수 있습니다.

HMC는 메모리 및 프로세서 자원에 대한 이용률 데이터를 수집합니다. 이 데이터를 사용하여 경향을 분석하고 자원 조정을 수행할 수 있습니다. 데이터는 이벤트라고 하는 레코드에 수집됩니다. 이벤트는 다음 시간에 작성됩니다.

- 주기적 간격으로(30초, 1분, 5분, 30분, 1시간, 매일 및 매월).
- 자원 이용률에 영향을 주는 시스템 레벨과 파티션 레벨 상태 및 구성 변경사항을 작성할 때.
- HMC에서 로컬 시간을 시작, 종료하고 변경할 때.

관리 시스템에 대해 이용률 데이터를 표시하려면 우선 관리 시스템에 대한 이용률 데이터를 수집하도록 HMC를 설정해야 합니다.

샘플링 속도 변경 태스크를 사용하면 샘플링 속도를 사용, 설정하고 변경하거나 샘플링 콜렉션을 사용 안할 수 있습니다.

업데이트

시스템 정보 보기, Hardware Management Console(HMC)에서 라이센스가 부여된 내부코드(LIC) 관리 또는 시스템 준비 확인을 위한 태스크를 표시합니다.

시스템 정보 보기

HMC(Hardware Management Console)에서 선택된 시스템에 대한 정보를 표시합니다.

네트워크 토폴로지를 보려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 시스템 정보를 표시할 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **업데이트**를 펼치십시오.
4. **시스템 정보 보기**를 선택하십시오.
5. 목록에서 LIC 저장소를 선택하고 **확인**을 클릭하십시오.
6. 이 태스크를 완료한 후 **닫기**를 클릭하십시오.

HMC의 시스템 정보 보기에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

라이센스가 부여된 내부코드 변경

HMC(Hardware Management Console)에서 라이센스가 부여된 내부코드를 변경하십시오.

현재 릴리스 또는 새 릴리스에 라이센스가 부여된 내부코드를 변경할 수 있습니다.

라이센스가 부여된 내부코드의 변경을 보려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 시스템 정보를 표시할 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **업데이트**를 펼치십시오.
4. **라이센스가 부여된 내부코드 변경**을 선택하십시오.

   참고: 라이센스가 부여된 내부코드 변경 마법사를 클릭하여 안내되는 관리 시스템, 전원 및 I/O 라이센스가 부여된 내부코드(LIC)의 업데이트를 수행하십시오. **시스템 정보 보기**를 클릭하여 검색 가능한 레벨을 포함하는 현재 LIC 레벨을 검사하십시오. **고급 기능 선택**을 클릭하여 더 많은 옵션과 추가 대상 선택으로 관리 시스템 및 전원 LIC를 업데이트하십시오.
5. 목록에서 조치를 선택하고 **확인**을 클릭하십시오.
6. 이 태스크를 완료한 후 **닫기**를 클릭하십시오.

HMC의 라이센스가 부여된 내부코드 변경에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

시스템 준비 상태 확인

HMC(Hardware Management Console)에서 선택된 시스템의 라이센스가 부여된 내부코드 준비 상태를 확인하십시오.

시스템 준비 상태를 확인하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 시스템 정보를 표시할 서버를 선택하십시오.
3. 메뉴 팟에서 **시스템 조치**를 펼친 후 **업데이트**를 펼치십시오.
4. **시스템 준비 상태 확인**을 선택하십시오.
5. 이 태스크를 완료한 후 **확인**을 클릭하십시오.

HMC의 시스템 준비 상태 확인을 위한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

SR-IOV 펌웨어 업데이트

HMC(Hardware Management Console)에서 SR-IOV 어댑터의 드라이버 펌웨어를 업데이트하십시오.

참고: 어댑터는 공유 모드여야 합니다.

SR-IOV 어댑터의 펌웨어를 업데이트하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 시스템 정보를 표시할 서버를 선택하십시오.
3. **메뉴 팟**에서 **시스템 조치**를 펼친 후 **업데이트**를 펼치십시오.
4. **SR-IOV 펌웨어 업데이트**를 선택하십시오.
5. 어댑터를 선택하거나 마우스 오른쪽 단추로 클릭하여 컨텍스트 메뉴를 표시하십시오.
6. 시작할 펌웨어 업데이트의 유형을 선택하십시오.

   참고: 어댑터 드라이버 펌웨어를 업데이트하거나 어댑터 드라이버와 어댑터 펌웨어를 둘 다 업데이트할 수 있습니다. 어댑터 또는 어댑터 드라이버 펌웨어의 업데이트 조작 중에 어댑터에 구성된 논리 포트에서 네트워크 트래픽의 일시적인 중단을 경험할 수 있습니다. 각 어댑터를 업데이트하는 데에는 2 - 5분이 소요됩니다. 업데이트는 연속적으로 수행됩니다.
7. 이 태스크를 완료한 후 **닫기**를 클릭하십시오.

SR-IOV 어댑터의 드라이버 또는 펌웨어 업데이트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

서비스 가능성

HMC의 문제점 분석은 자동으로 오류 조건을 발견하고 수리 서비스가 필요한 문제점을 사용자에게 보고합니다.

이러한 문제점은 사용자에게 서비스 가능 이벤트로 보고됩니다. 선택된 시스템에 대한 특정 이벤트를 보려면 **서비스 가능 이벤트 관리자** 태스크를 사용하십시오. 그러나 문제점이 발생했음을 알아채거나 문제점이 시스템에 영향을 미치고 있다고 의심하지만 문제점 분석이 이를 사용자에게 보고하지 않은 경우에는 **서비스 가능 이벤트 작성** 태스크를 사용하여 문제점을 서비스 제공자에게 보고하십시오.

시스템에 대해 사용할 수 있는 서비스 가능성 태스크를 열려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 서비스 가능성 태스크를 관리할 서버를 선택하십시오.
3. 메뉴 팟에서 **서비스 가능성**을 펼친 후 **서비스 가능성**을 클릭하십시오.
4. 목록에서 수행할 서비스 가능성 태스크를 선택하십시오.

서비스 가능 이벤트 관리자

관리 시스템의 문제점은 HMC에 서비스 가능 이벤트로 보고됩니다. 문제점을 보거나, 문제점 데이터를 관리하거나, 서비스 제공자에게 이벤트를 콜홈하거나, 문제점 복구를 수행할 수 있습니다.

보려는 서비스 가능 이벤트에 대한 기준을 설정하려면 다음을 수행하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 서비스 가능 이벤트를 관리할 서버를 선택하십시오.
3. 메뉴 팟에서 **서비스 가능성**을 펼친 후 **서비스 가능성**을 클릭하십시오.
4. **서비스 가능 이벤트 관리자**를 클릭하십시오.
5. 이벤트 기준, 오류 기준 및 FRU 기준을 제공하십시오.
6. **확인**을 클릭하십시오.
7. 결과를 필터링하지 않으려면 **모두**를 선택하십시오.

서비스 가능 이벤트 개요 창에 기준과 일치하는 모든 이벤트가 표시됩니다. 압축 테이블 보기에 표시되는 정보는 다음을 포함합니다.

- 문제점 번호
- PMH 번호
- 참조 코드 - 참조 코드를 클릭하면 보고된 문제점에 대한 설명과 문제점을 수정하는 데 사용할 수 있는 조치가 표시됩니다.
- 문제점의 상태

- 문제점이 마지막으로 보고된 시간
- 문제점의 실패 MTMS

전체 테이블 보기에는 보고 MTMS, 처음 보고된 시간, 서비스 가능 이벤트 텍스트를 포함하여 좀 더 자세한 정보가 포함되어 있습니다.

서비스 가능 이벤트를 선택하고 **선택됨** 드롭 다운 메뉴를 사용하여 다음을 수행할 수 있습니다.
- **이벤트 세부사항 보기**: 이 이벤트와 연관된 FRU(Field Replaceable Unit) 및 이에 대한 설명을 표시합니다.
- **이벤트 복구**: 사용 가능한 경우 안내되는 복구 프로시저를 실행합니다.
- **이벤트 콜홈**: 이벤트를 서비스 제공자에게 보고합니다.
- **이벤트 문제점 데이터 관리**: 이 이벤트와 연관된 데이터 및 로그를 보거나 콜홈하거나 매체에 오프로드합니다.
- **이벤트 닫기**: 문제점이 해결된 후 주석을 추가하고 이벤트를 닫습니다.

서비스 가능 이벤트 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

서비스 가능 이벤트 작성

이 태스크는 HMC(Hardware Management Console)에서 발생한 문제점(예: 마우스가 작동하지 않음)을 서비스 제공자에게 보고하거나 사용자가 문제점 보고를 테스트할 수 있도록 합니다.

문제점 제출은 원격 지원 기능(RSF)을 사용하도록 이 Hardware Management Console을 사용자 정의했는지 여부와 이 Hardware Management Console에 서비스를 자동으로 호출할 수 있는 권한이 있는지 여부에 따라 달라집니다. 해당하는 경우 문제점 정보 및 서비스 요청이 모뎀 전송을 통해 서비스 제공자에게 자동으로 전송됩니다.

Hardware Management Console에 대한 문제점을 보고하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **서비스 가능 이벤트 작성**을 클릭하십시오.
3. **서비스 가능 이벤트 작성** 창에 표시된 목록에서 문제점 유형을 선택하십시오.
4. **문제점 설명** 입력 필드에 문제점에 대한 간략한 설명을 입력한 후 **서비스 요청**을 클릭하십시오.

문제점 보고 창에서 문제점 보고를 테스트하려면 다음을 수행하십시오.

1. **자동 문제점 보고 테스트**를 선택하고 **문제점 설명** 입력 필드에 테스트임을 입력하십시오.
2. **서비스 요청**을 클릭하십시오. 문제점이 Hardware Management Console의 서비스 제공자에게 보고됩니다. 문제점을 보고할 때 **문제점 보고** 창에 사용자가 제공하는 정보와 콘솔을 식별하는 시스템 정보가 서비스 제공자에게 전송됩니다.

문제점 보고 또는 문제점 보고 작동 여부 테스트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

덤프 관리

HMC가 관리하는 시스템의 시스템 덤프, 서비스 프로세서 덤프 및 전력 서브시스템 덤프를 관리하십시오.

시스템 덤프

시스템 장애 또는 수동 요청 이후 서버 하드웨어 및 펌웨어의 데이터 콜렉션입니다. 다음 레벨의 지원 담당자 또는 서비스 제공자의 지시에 따라서만 시스템 덤프를 수행하십시오.

서비스 프로세서 덤프

실패, 외부 다시 설정 또는 수동 요청 후 서비스 프로세서의 데이터 콜렉션입니다.

전력 서브시스템 덤프

대용량 전원 제어 서비스 프로세서의 데이터 콜렉션입니다. 특정 모델의 관리 시스템에만 적용할 수 있습니다.

덤프 관리 태스크를 사용하여 다음을 수행할 수 있습니다.

- 시스템 덤프, 서비스 프로세서 덤프 또는 전력 서브시스템 덤프를 시작합니다.
- 덤프를 시작하기 전에 덤프 유형에 대한 덤프 기능 매개변수를 수정합니다.
- 덤프를 삭제합니다.
- 덤프를 매체에 복사합니다.
- FTP를 사용하여 덤프를 다른 시스템에 복사합니다.
- 자세한 분석을 위해 콜홈 기능을 사용하여 덤프를 콜홈하여 덤프를 서비스 제공자(예: IBM 원격 지원 센터)에게 다시 전송합니다.
- 덤프가 진행될 때 덤프의 오프로드 상태를 봅니다.

덤프 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

VPD 수집

VPD(Vital Product Data)를 이동식 매체에 복사하십시오.

관리 시스템에는 내부에 저장된 VPD가 있습니다. VPD는 설치된 메모리 크기 및 설치된 프로세서 수와 같은 정보로 구성됩니다. 이러한 레코드는 원격 서비스 및 서비스 담당자가 사용할 수 있는 가치 있는 정보를 제공하여 관리 시스템의 펌웨어 및 소프트웨어를 최신 상태로 유지하는 데 도움이 될 수 있습니다.

참고: VPD를 수집하려면 하나 이상의 운영 파티션이 있어야 합니다. 자세한 정보는 논리 파티셔닝을 참조하십시오.

VPD 파일의 정보를 사용하여 관리 시스템에 대한 다음 유형의 주문을 완료할 수 있습니다.

- 영업 기능 설치 또는 제거
- 모델 업그레이드 또는 다운그레이드
- 기능 업그레이드 또는 다운그레이드

이 태스크를 사용하는 경우, 사용자 또는 사용자의 서비스 제공자가 사용할 수 있도록 이 정보를 이동식 매체(디스켓 또는 메모리 키)로 보낼 수 있습니다.

VPD 수집에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

유형, 모델, 피처

격납장치의 모델, 유형, 머신 일련 번호(MTMS) 또는 구성 ID를 편집하거나 표시하십시오.

확장 장치의 MTMS 값 또는 구성 ID를 교체 프로시저 동안 편집해야 할 수 있습니다.

MTMS 편집에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

하드웨어

관리 시스템에서 하드웨어를 추가, 교환 또는 제거하십시오. 설치된 FRU 또는 격납장치 목록과 해당 위치를 표시하십시오. FRU 또는 격납장치를 선택하고 장치를 추가, 교환 또는 제거하기 위한 단계별 프로시저를 실행하십시오.

시스템에 대해 사용할 수 있는 하드웨어 태스크를 열려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 하드웨어 태스크를 관리할 서버를 선택하십시오.
3. 메뉴 팟에서 **서비스 가능성**을 펼친 후 **서비스 가능성**을 클릭하십시오.
4. 목록에서 수행할 하드웨어 태스크를 선택하십시오.

IO 장치 전원 켜기/끄기:

IO 장치의 전원을 켜거나 끄려면 **IO 장치 전원 켜기/끄기** 태스크를 사용하십시오.

전원 도메인에 있는 장치 또는 슬롯만 전원을 켜거나 끌 수 있습니다. HMC가 제어할 수 없는 위치 코드에 대해서는 해당 전원 켜기/끄기 단추를 사용할 수 없습니다.

FRU 추가:

FRU(Field Replaceable Unit)를 찾고 추가하십시오.

FRU를 추가하려면 다음을 수행하십시오.

1. 드롭 다운 목록에서 격납장치 유형을 선택하십시오.
2. 목록에서 FRU 유형을 선택하십시오.
3. **다음**을 클릭하십시오.
4. 표시된 목록에서 위치 코드를 선택하십시오.
5. **추가**를 클릭하십시오.

6. **프로시저 실행**을 클릭하십시오.
7. FRU 설치 프로세스를 완료한 후 **완료**를 클릭하십시오.

FRU 교환:

하나의 FRU를 다른 FRU로 교환하려면 **FRU 교환** 태스크를 사용하십시오.

FRU를 교환하려면 다음을 수행하십시오.

1. 드롭 다운 목록에서 설치된 격납장치 유형을 선택하십시오.
2. 이 격납장치에 대해 표시된 FRU 유형 목록에서 FRU 유형을 선택하십시오.
3. **다음**을 클릭하여 FRU 유형의 위치 목록을 표시하십시오.
4. 특정 FRU의 위치 코드를 선택하십시오.
5. **추가**를 클릭하여 FRU 위치를 **보류 중인 조치**에 추가하십시오.
6. **프로시저 실행**을 선택하여 **보류 중인 조치**에 나열된 FRU 교체를 시작하십시오.
7. 설치를 완료하면 **완료**를 클릭하십시오.

FRU 제거:

관리 시스템에서 FRU를 제거하려면 **FRU 제거** 태스크를 사용하십시오.

FRU를 제거하려면 다음을 수행하십시오.

1. 드롭 다운 목록에서 격납장치를 선택하여 선택한 격납장치에 현재 설치되어 있는 FRU 유형 목록을 표시하십시오.
2. 이 격납장치에 대해 표시된 FRU 유형 목록에서 FRU 유형을 선택하십시오.
3. **다음**을 클릭하여 FRU 유형의 위치 목록을 표시하십시오.
4. 특정 FRU의 위치 코드를 선택하십시오.
5. **추가**를 클릭하여 FRU 위치를 **보류 중인 조치**에 추가하십시오.
6. **프로시저 실행**을 선택하여 **보류 중인 조치**에 나열된 FRU 제거를 시작하십시오.
7. 제거 프로시저를 완료한 후 **완료**를 클릭하십시오.

격납장치 추가:

격납장치를 찾고 추가하십시오.

격납장치를 추가하려면 다음을 수행하십시오.

1. 격납장치 유형을 선택한 후 **추가**를 클릭하십시오.
2. **프로시저 실행**을 클릭하십시오.
3. 격납장치 설치 프로세스를 완료한 후 **완료**를 클릭하십시오.

격납장치 제거:

격납장치를 제거하려면 **격납장치 제거** 태스크를 사용하십시오.

격납장치를 제거하려면 다음을 수행하십시오.

1. 격납장치 유형을 선택한 후 **추가**를 클릭하여 선택한 격납장치 유형의 위치 코드를 **보류 중인 조치**에 추가하십시오.
2. **프로시저 실행**을 클릭하여 선택한 시스템에서 **보류 중인 조치**에서 식별된 격납장치 제거를 시작하십시오.
3. 격납장치 제거 프로세스를 완료한 후 **완료**를 클릭하십시오.

MES 열기:

HMC(Hardware Management Console)의 MES 조작 활성 또는 비활성에 대해 MES 주문 번호 및 해당 상태를 보십시오.

목록에 새 번호를 추가하려면 MES 주문 번호 추가를 사용하십시오. 주문 번호를 추가하려면 다음 단계를 완료하십시오.

1. **MES 주문 번호 추가**를 클릭하십시오.
2. 새 MES 주문 번호를 입력하십시오.
3. **확인**을 클릭하십시오.

MES 닫기:

열린 모든 MES 주문 번호 및 해당 상태를 보십시오.

MES를 닫으려면 MES 주문 번호 닫기를 사용하십시오. MES를 닫으려면 다음 단계를 완료하십시오.

1. 테이블에서 열린 MES 주문 번호를 선택하십시오.
2. **확인**을 클릭하십시오.

FSP 장애 복구 설정:

관리 시스템의 기본 서비스 프로세서가 실패하는 경우, 보조 서비스 프로세서를 설정하십시오.

FSP 장애 복구는 서비스 프로세서 하드웨어 고장으로 인한 고객 가동 중단을 줄이도록 설계되었습니다. 중복 서비스 프로세서가 현재 시스템 구성에 대해 지원되는 경우, 선택한 관리 시스템에 대해 FSP 장애 복구를 설정하려면 **설정**을 선택하십시오.

FSP 장애 복구를 설정하려면 다음 단계를 완료하십시오.

1. 컨텐츠 분할창의 **FSP 장애 복구** 아래에서 **설정**을 클릭하십시오.
2. **확인**을 클릭하여 선택한 시스템의 자동 장애 복구를 사용으로 설정하십시오.

FSP 장애 복구 시작:

관리 시스템의 기본 서비스 프로세서가 실패하는 경우, 보조 서비스 프로세서를 시작하십시오.

FSP 장애 복구는 서비스 프로세서 하드웨어 고장으로 인한 고객 가동 중단을 줄이도록 설계되었습니다. 선택한 관리 시스템에 대해 FSP 장애 복구를 시작하려면 **시작**을 선택하십시오.

FSP 장애 복구를 시작하려면 다음 단계를 완료하십시오.

1. 컨텐츠 분할창의 **FSP 장애 복구** 아래에서 **시작**을 클릭하십시오.
2. **확인**을 클릭하여 선택한 시스템의 자동 장애 복구를 시작하십시오.

토폴로지 다이어그램

파티션의 토폴로지 다이어그램을 보는 방법을 학습합니다.

HMC(Hardware Management Console)를 사용하여 파티션의 토폴로지 다이어그램을 볼 수 있습니다.

CoD(Capacity on Demand)

관리 서버에 설치되어 있는 비활성 프로세서 또는 메모리를 활성화하십시오.

CoD(Capacity on Demand)를 사용하면 프로세서 및 메모리를 중단 없이 활성화할 수 있습니다. 또한 CoD(Capacity on Demand)는 간헐적 성능 요구를 충족시키기 위해 임시로 용량을 활성화하고, 시험적으로 추가 용량을 활성화하고, 필요에 따라 조작을 지원하기 위해 용량에 액세스할 수 있는 옵션을 제공합니다.

PowerVM

HMC(Hardware Management Console)에서 PowerVM 기능을 사용하여 IBM Power Systems 서버의 시스템 레벨 가상화 기능을 관리할 수 있습니다.

PowerVM 태스크를 사용하여 Virtual I/O Server(VIOS), 가상 네트워크 및 가상 스토리지와 같은 시스템과 연관된 가상 자원을 관리할 수 있습니다. 워크로드의 변화에 따라 또는 성능 향상을 위해 관리 시스템 레벨에서 PowerVM 기능을 관리할 수 있습니다.

PowerVM 기능에는 다음 태스크가 포함됩니다.

- Virtual I/O Server 관리
- 가상 네트워크 관리
- 가상 스토리지 관리
- SR-IOV 어댑터, 호스트 이더넷 어댑터(HEA) 및 호스트 채널 어댑터(HCA) 관리
- 예약 프로세서 풀 관리
- 공유 프로세서 풀 관리
- 공유 메모리 풀 관리

파티션에 대한 시스템 관리

시스템 관리는 서버, 논리 파티션 및 프레임을 관리하기 위해 수행할 수 있는 태스크를 표시합니다. 이러한 태스크를 사용하여 파티션을 설정 및 구성하고 파티션의 현재 상태를 보고 문제점을 해결하고 솔루션을 적용할 수 있습니다.

다음 태스크 세트는 파티션이 선택되어 메뉴 팟 또는 컨텐츠 분할창에 표시될 때 표시됩니다. 메뉴 팟에 나열되는 태스크는 작업 영역의 선택에 따라 변경됩니다.

기타 특성

기타 특성 태스크는 선택된 파티션의 특성을 표시합니다. 이 정보는 자원 할당 및 파티션 관리에 유용합니다. 이러한 특성에는 다음이 포함됩니다.

일반 **일반** 탭에는 파티션의 이름, ID, 환경, 상태, 자원 구성, 운영 체제, 파티션을 시작할 때 사용되는 현재 프로파일, 파티션을 일시중단할 수 있는지 여부 및 파티션이 있는 시스템이 표시됩니다.

하드웨어

하드웨어 탭에는 파티션에 있는 프로세서, 메모리 및 I/O의 현재 사용법이 표시됩니다.

참고: 운영 체제 및 하이퍼바이저가 가상 프로세서당 0.05 프로세서의 최소 자격을 지원할 때 최소, 최대 및 원하는 처리 장치 수를 지원되는 가장 낮은 값인 0.05로 설정할 수 있습니다.

가상 어댑터

가상 어댑터 탭에는 가상 어댑터의 현재 구성이 표시됩니다. 가상 어댑터를 사용하면 파티션 사이에서 자원을 공유할 수 있습니다. 이 탭에서는 파티션에서 가상 어댑터를 보고 작성하고 편집할 수 있습니다.

SR-IOV 논리 포트

SR-IOV 논리 포트 탭은 파티션에 구성된 논리 포트를 표시합니다(보기 전용).

설정 **설정** 탭은 파티션의 부트 모드 및 키잠금 위치를 표시합니다. 또한 파티션에 대한 현재 서비스 및 지원 설정도 표시됩니다.

기타 **기타** 탭에는 파티션의 워크로드 관리 그룹(적용 가능한 경우) 및 파티션의 전원 제어 파티션이 표시됩니다.

기본 프로파일 변경

파티션의 기본 프로파일을 변경하십시오.

드롭 다운 목록에서 새 기본 프로파일로 설정할 프로파일을 선택하십시오.

파티션 템플리트

파티션 템플리트는 물리적 어댑터, 가상 네트워크 및 스토리지 구성과 같은 파티션 자원에 대한 세부사항을 포함합니다. HMC(Hardware Management Console)에서 사용자가 직접 작성한 사용자 정의 템플리트나 템플리트 라이브러리에서 사용할 수 있는 빠른 시작 템플리트에서 클라이언트 파티션을 작성할 수 있습니다.

구성을 템플리트로 캡처

실행 중인 서버의 구성 세부사항을 캡처하고 HMC(Hardware Management Console)를 사용하여 해당 정보를 사용자 정의 시스템 템플리트로 저장할 수 있습니다. 이 기능은 동일한 구성으로 여러 서버를 배치하려는 경우에 유용합니다. 사전 정의된 템플리트를 사용하려는 경우에는 이 태스크를 완료할 필요가 없습니다.

템플리트 라이브러리

템플리트 라이브러리에 있는 템플리트에 액세스하려면 **템플리트 라이브러리** 옵션을 사용하십시오.

템플리트 라이브러리에서 사용할 수 있는 템플리트에 대해 보기, 수정, 배치, 작성, 캡처, 복사, 가져오기, 내보내기 또는 삭제를 수행할 수 있습니다.

조작

조작에는 파티션 조작을 위한 태스크가 포함됩니다.

파티션에 대해 사용할 수 있는 조작 태스크를 열려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 파티션**을 선택하십시오.
2. 조작 태스크를 관리할 파티션을 선택하십시오.
3. 메뉴 팟에서 **조작**을 펼치십시오.
4. 목록에서 수행할 조작 태스크를 선택하십시오.

활성화

활성화되지 않음 상태에 있는 관리 시스템의 파티션을 활성화하려면 **활성화** 태스크를 사용하십시오.

파티션을 활성화하려면 프로파일 목록에서 파티션 프로파일을 선택하고 **확인**을 클릭하십시오. VSI(Virtual Station Interface) 프로파일을 구성하는 동안 실패를 무시하려면 **고급** 탭에서 **VSI 프로파일 없음** 선택란을 선택하십시오.

참고: HMC 버전 7.7 이상에서는 DVD, 저장된 이미지 또는 NIM(Network Installation Management) 서버를 사용하여 HMC에서 로컬 파티션에 VIOS(Virtual I/O Server)를 설치할 수 있습니다.

다시 시작

선택한 논리 파티션을 다시 시작하십시오.

IBM i 논리 파티션의 경우, 운영 체제의 명령행에서 IBM i 논리 파티션을 다시 시작할 수 없는 경우에만 이 창을 사용하십시오. 이 창을 사용하여 IBM i 논리 파티션을 다시 시작하면 비정상 IPL이 발생합니다.

많은 클라이언트 파티션에 대해 PSP(Paging Service Partition) 역할을 하는 VIOS 파티션을 다시 시작하도록 선택하는 경우, VIOS 파티션을 종료하기 전에 클라이언트 파티션을 종료해야 함을 나타내는 경고가 표시됩니다.

다음 옵션 중 하나를 선택하십시오. 운영 체제 옵션과 운영 체제 즉시 옵션은 RMC(Resource Monitoring and Control)가 작동 중이고 구성된 경우에만 사용할 수 있습니다.

덤프 HMC가 논리 파티션을 종료하고 메인 스토리지 또는 시스템 메모리 덤프를 시작합니다. AIX 및 Linux 논리 파티션의 경우, HMC는 논리 파티션에도 종료됨을 알립니다. IBM i 논리 파티션의 경우에는 프로세서가 즉시 중지됩니다. 종료가 완료된 후 논리 파티션은 즉시 다시 시작됩니다. (IBM i 논리 파티션은 여러 번 다시 시작되어 덤프 정보를 저장할 수 있습니다.) 운영 체제의 일부가 정지되고 분석을 위해 논리 파티션의 덤프를 원하는 경우 이 옵션을 사용하십시오.

운영 체제

HMC가 논리 파티션에 대해 shutdown -r 명령을 실행하여 정상적으로 논리 파티션을 종료합니다. 이 조작 중에 논리 파티션은 필요한 모든 종료 활동을 수행합니다. 종료가 완료된 후 논리 파티션은 즉시 다시 시작됩니다. 이 옵션은 AIX 논리 파티션에만 사용할 수 있습니다. 즉시 : HMC가 논리 파티션을 즉시 종료합니다. HMC는 모든 활성 작업을 즉시 종료합니다. 이러한 작업에서 실행 중인 프로그램은 작업 정리를 수행할 수 없습니다. 데이터가 부분적으로 업데이트된 경우, 이 옵션을 사용하면 원하지 않는 결과가 발생할 수 있습니다. 제어된 종료가 실패한 후에만 이 옵션을 사용하십시오.

운영 체제 즉시

HMC가 논리 파티션에 대해 shutdown -Fr 명령을 실행하여 논리 파티션을 즉시 종료합니다. 이 조작 중에 논리 파티션은 다른 사용자 및 다른 종료 활동에 메시지를 전달하지 않습니다. 종료가 완료된 후 논리 파티션은 즉시 다시 시작됩니다. 이 옵션은 AIX 논리 파티션에만 사용할 수 있습니다.

덤프 재시도

HMC가 논리 파티션에서 메인 스토리지 또는 시스템 메모리 덤프를 재시도합니다. 덤프가 완료되면 논리 파티션이 종료된 후 다시 시작됩니다. 이전에 시도한 덤프 옵션이 성공하지 못한 경우에만 이 옵션을 사용하십시오. 이 옵션은 IBM i 논리 파티션에만 사용할 수 있습니다.

종료

선택한 논리 파티션을 종료하십시오.

IBM i 논리 파티션의 경우, 운영 체제의 명령행에서 IBM i 논리 파티션을 종료할 수 없는 경우에만 이 창을 사용하십시오. 이 창을 사용하여 IBM i 논리 파티션을 종료하면 비정상 IPL이 발생합니다.

많은 클라이언트 파티션에 대해 PSP(Paging Service Partition) 역할을 하는 VIOS 파티션을 종료하도록 선택하는 경우, VIOS 파티션을 종료하기 전에 클라이언트 파티션을 종료해야 함을 나타내는 경고가 표시됩니다.

다음 옵션 중에서 선택하십시오.

지연 HMC가 지연된 전원 끄기 순서를 사용하여 논리 파티션을 종료합니다. 이 옵션을 사용하면 논리 파티션 시간이 작업을 종료하고 데이터를 디스크에 쓸 수 있습니다. 논리 파티션이 미리 지정된 시간 내에 종료할 수 없는 경우에는 비정상적으로 종료되며 다음에 다시 시작할 때에는 평상시보다 시간이 더 오래 걸릴 수 있습니다.

즉시 HMC가 논리 파티션을 즉시 종료합니다. HMC는 모든 활성 작업을 즉시 종료합니다. 이러한 작업에서 실행 중인 프로그램은 작업 정리를 수행할 수 없습니다. 데이터가 부분적으로 업데이트된 경우, 이 옵션을 사용하면 원하지 않는 결과가 발생할 수 있습니다. 제어된 종료가 실패한 후에만 이 옵션을 사용하십시오.

운영 체제

HMC가 논리 파티션에 대해 shutdown 명령을 실행하여 정상적으로 논리 파티션을 종료합니다. 이 조작 중에 논리 파티션은 필요한 모든 종료 활동을 수행합니다. 이 옵션은 AIX 논리 파티션에만 사용할 수 있습니다.

운영 체제 즉시

HMC가 논리 파티션에 대해 shutdown -F 명령을 실행하여 논리 파티션을 즉시 종료합니다. 이 조작 중에 논리 파티션은 다른 사용자 및 다른 종료 활동에 메시지를 전달하지 않습니다. 이 옵션은 AIX 논리 파티션에만 사용할 수 있습니다.

삭제

선택한 파티션을 삭제하려면 **삭제** 태스크를 사용하십시오.

삭제 태스크는 선택된 파티션 및 해당 파티션과 연관된 모든 파티션 프로파일을 관리 시스템에서 삭제합니다. 파티션을 삭제하면 해당 파티션에 현재 지정되어 있는 모든 하드웨어 자원을 다른 파티션에서 사용할 수 있게 됩니다.

조작 스케줄

운영자 지원 없이 논리 파티션에서 특정 조작을 수행할 스케줄을 작성하십시오.

스케줄된 조작은 시스템 조작의 자동, 지연 또는 반복 처리가 필요한 상황에 유용합니다. 스케줄된 조작은 조작을 수행하기 위한 운영자의 지원 없이 지정된 시간에 시작됩니다. 스케줄은 단일 조작에 대해 설정되거나 여러 번 반복될 수 있습니다.

예를 들어, 논리 파티션에서 자원을 제거하거나 하나의 논리 파티션에서 다른 논리 파티션으로 자원을 이동하는 조작을 스케줄할 수 있습니다.

스케줄된 조작 태스크는 각 조작에 대해 다음 정보를 표시합니다.

- 조작의 오브젝트인 프로세서

- 스케줄된 날짜
- 스케줄된 시간
- 조작
- 남은 반복 수

스케줄된 조작 창에서 다음을 수행할 수 있습니다.
- 나중에 실행할 조작 스케줄
- 일정한 간격으로 반복할 조작 정의
- 이전에 스케줄된 조작 삭제
- 현재 스케줄된 조작의 세부사항 보기
- 지정된 시간 범위 내에서 스케줄된 조작 보기
- 날짜, 조작 또는 관리 시스템을 기준으로 스케줄된 조작 정렬

조작이 한 번 발생하도록 스케줄하거나 조작이 반복되도록 스케줄할 수 있습니다. 조작이 발생할 시간 및 날짜를 제공해야 합니다. 조작을 반복하려는 경우 다음을 선택하도록 요청됩니다.
- 조작이 발생할 요일(선택사항)
- 각 발생 사이의 시간 간격(필수)
- 총 반복 수(필수)

논리 파티션에 대해 스케줄할 수 있는 조작은 다음과 같습니다.

LPAR에서 활성화
선택한 프로파일에서 선택한 논리 파티션의 활성화를 위한 조작을 스케줄합니다.

동적 재구성
자원(프로세서 또는 수 메가바이트의 메모리)을 추가, 제거 또는 이동하기 위한 조작을 스케줄합니다.

운영 체제 종료(파티션에서)
선택한 논리 파티션의 종료를 스케줄합니다.

HMC에서 조작을 스케줄하려면 다음을 수행하십시오.
1. 탐색 영역에서 **시스템 관리**를 클릭하십시오.
2. 작업 분할창에서 하나 이상의 파티션을 선택하십시오.
3. 태스크 패드에서 **조작** 태스크 카테고리를 선택한 후 **조작 스케줄**을 클릭하십시오. 스케줄된 조작 사용자 정의 창이 열립니다.
4. 스케줄된 조작 사용자 정의 창의 메뉴 표시줄에서 **옵션**을 클릭하여 다음 레벨의 옵션을 표시하십시오.
   - 스케줄된 조작을 추가하려면 **옵션**을 클릭한 후 **새로 작성**을 클릭하십시오.
   - 스케줄된 조작을 삭제하려면 삭제할 조작을 선택하고 **옵션**을 가리킨 후 **삭제**를 클릭하십시오.
   - 스케줄된 조작의 목록을 선택된 오브젝트의 현재 스케줄로 업데이트하려면 **옵션**을 가리킨 후 **새로 고치기**를 클릭하십시오.

- 스케줄된 조작을 보려면 보려는 조작을 선택하고 **보기**를 가리킨 후 **스케줄 세부사항**을 클릭하십시오.
- 스케줄된 조작의 시간을 변경하려면 보려는 조작을 선택하고 **보기**를 가리킨 후 **새 시간 범위**를 클릭하십시오.
- 스케줄된 조작을 정렬하려면 **정렬**을 가리킨 후 표시되는 정렬 카테고리 중 하나를 클릭하십시오.

5. HMC 작업영역으로 돌아가려면 **조작**을 가리킨 후 **종료**를 클릭하십시오.

이동성

이동성 태스크를 사용하여 파티션을 다른 서버로 마이그레이션하고 마이그레이션의 요구사항을 충족하는지 확인하고 파티션이 올바르지 않은 상태인 경우 복구할 수 있습니다.

마이그레이션:

파티션을 다른 관리 시스템으로 마이그레이션하십시오.

파티션을 다른 시스템으로 마이그레이션하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘 을 클릭한 후 **모든 시스템**을 선택하십시오.
2. 컨텐츠 분할창에서 서버를 선택하십시오.
3. 메뉴 팟에서 **파티션**을 펼치고 다른 시스템으로 마이그레이션할 파티션을 선택하십시오.
4. **조작 > 이동성 > 마이그레이션**을 선택하십시오. 파티션 마이그레이션 마법사가 열립니다.
5. 파티션 마이그레이션 마법사의 단계를 완료하고 **완료**를 클릭하십시오.

유효성 검증:

소스 시스템에서 목적지 시스템으로 파티션을 이동하기 위한 설정의 유효성을 검증하십시오.

설정을 유효성 검증하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘 을 클릭한 후 **모든 시스템**을 선택하십시오.
2. 컨텐츠 분할창에서 서버를 선택하십시오.
3. 메뉴 팟에서 **파티션**을 펼치고 다른 시스템으로의 마이그레이션 설정을 유효성 검증할 파티션을 선택하십시오.
4. **조작 > 이동성 > 유효성 검증**을 선택하십시오. 파티션 마이그레이션 유효성 검증 창이 열립니다.
5. 필드에 정보를 채우고 **유효성 검증**을 클릭하십시오.

복구:

완료되지 않은 마이그레이션에서 이 파티션을 복구하십시오.

완료하지 않은 마이그레이션에서 이 파티션을 복구하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 시스템**을 선택하십시오.
2. 컨텐츠 분할창에서 서버를 선택하십시오.
3. 메뉴 팟에서 **파티션**을 펼치고 복구할 파티션을 선택하십시오.
4. **조작 > 이동성 > 복구**를 선택하십시오. 마이그레이션 복구 창이 열립니다.
5. 필요에 따라 정보를 완료하고 **복구**를 클릭하십시오.

구성

구성에는 파티션을 구성하기 위한 태스크가 포함됩니다.

프로파일 관리

선택한 파티션의 프로파일을 작성, 편집, 복사, 삭제 또는 활성화하려면 **프로파일 관리** 태스크를 사용하십시오.

파티션 프로파일에는 파티션의 자원 구성이 포함됩니다. 프로파일을 편집하여 프로파일의 프로세서, 메모리 및 어댑터 지정을 수정할 수 있습니다.

논리 파티션의 기본 파티션 프로파일은 다른 파티션 프로파일을 선택하지 않은 경우 논리 파티션을 활성화하는 데 사용되는 파티션 프로파일입니다. 먼저 다른 파티션 프로파일을 기본 파티션 프로파일로 지정하지 않으면 기본 파티션 프로파일을 삭제할 수 없습니다. 기본 프로파일은 상태 열에 정의됩니다.

선택한 파티션 프로파일의 정확한 사본을 작성하려면 **복사**를 선택하십시오. 그러면 파티션 프로파일을 복사하고 필요에 따라 사본을 변경하여 서로 거의 동일한 여러 개의 파티션 프로파일을 작성할 수 있습니다.

사용자 정의 그룹 관리

그룹은 오브젝트의 논리 콜렉션으로 구성됩니다. 그룹 기반으로 상태를 보고할 수 있으며 이를 통해 선호하는 방법으로 시스템을 모니터할 수 있습니다. 또한 그룹을 중첩(그룹 안에 포함된 그룹)하여 계층 구조 또는 토폴로지 보기를 제공할 수 있습니다.

하나 이상의 사용자 정의 그룹이 HMC(Hardware Management Console)에 이미 정의되어 있을 수 있습니다. 기본 그룹은 **구성** 아래의 **사용자 정의 그룹** 노드 아래에 나열됩니다. 기본 그룹은 **모든 파티션** 및 **모든 오브젝트**입니다. **사용자 정의 그룹 관리** 태스크를 사용하여 다른 그룹을 작성하고, 작성된 그룹을 삭제하고, 작성된 그룹에 추가하고, 패턴 일치 방법을 사용하여 그룹을 작성하거나 작성된 그룹에서 삭제할 수 있습니다.

사용자 정의 그룹 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

현재 구성 저장

새 프로파일 이름을 입력하여 논리 파티션의 현재 구성을 새 파티션 프로파일에 저장하십시오.

이 프로시저는 동적 논리 파티셔닝을 사용하여 논리 파티션의 구성을 변경하고 논리 파티션을 다시 시작할 때 변경사항을 유지하려는 경우에 유용합니다. 논리 파티션을 처음으로 활성화한 후 언제든지 이 프로시저를 수행할 수 있습니다.

서비스 가능성

HMC의 문제점 분석은 자동으로 오류 조건을 발견하고 수리 서비스가 필요한 문제점을 사용자에게 보고합니다.

이러한 문제점은 사용자에게 서비스 가능 이벤트로 보고됩니다. 선택된 시스템에 대한 특정 이벤트를 보려면 **서비스 가능 이벤트 관리자** 태스크를 사용하십시오. 그러나 문제점이 발생했음을 알아채거나 문제점이 시스템에 영향을 미치고 있다고 의심하지만 문제점 분석이 이를 사용자에게 보고하지 않은 경우에는 **서비스 가능 이벤트 작성** 태스크를 사용하여 문제점을 서비스 제공자에게 보고하십시오.

서비스 가능 이벤트 관리자

관리 파티션의 문제점은 HMC에 서비스 가능 이벤트로 보고됩니다. 문제점을 보거나, 문제점 데이터를 관리하거나, 서비스 제공자에게 이벤트를 콜홈하거나, 문제점 복구를 수행할 수 있습니다.

보려는 서비스 가능 이벤트에 대한 기준을 설정하려면 다음을 수행하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 서버**를 선택하십시오.
2. 서비스 가능 이벤트를 관리할 서버를 선택하십시오.
3. 메뉴 팟에서 **서비스 가능성**을 펼친 후 **서비스 가능성**을 클릭하십시오.
4. **서비스 가능 이벤트 관리자**를 클릭하십시오.
5. 이벤트 기준, 오류 기준 및 FRU 기준을 제공하십시오.
6. **확인**을 클릭하십시오.
7. 결과를 필터링하지 않으려면 **모두**를 선택하십시오.

서비스 가능 이벤트 개요 창에 기준과 일치하는 모든 이벤트가 표시됩니다. 압축 테이블 보기에 표시되는 정보는 다음을 포함합니다.

- 문제점 번호
- PMH 번호
- 참조 코드 - 참조 코드를 클릭하면 보고된 문제점에 대한 설명과 문제점을 수정하는 데 사용할 수 있는 조치가 표시됩니다.
- 문제점의 상태

- 문제점이 마지막으로 보고된 시간
- 문제점의 실패 MTMS

전체 테이블 보기에는 보고 MTMS, 처음 보고된 시간, 서비스 가능 이벤트 텍스트를 포함하여 좀 더 자세한 정보가 포함되어 있습니다.

서비스 가능 이벤트를 선택하고 **선택됨** 드롭 다운 메뉴를 사용하여 다음을 수행할 수 있습니다.
- **이벤트 세부사항 보기**: 이 이벤트와 연관된 FRU(Field Replaceable Unit) 및 이에 대한 설명을 표시합니다.
- **이벤트 복구**: 사용 가능한 경우 안내되는 복구 프로시저를 실행합니다.
- **이벤트 콜홈**: 이벤트를 서비스 제공자에게 보고합니다.
- **이벤트 문제점 데이터 관리**: 이 이벤트와 연관된 데이터 및 로그를 보거나 콜홈하거나 매체에 오프로드합니다.
- **이벤트 닫기**: 문제점이 해결된 후 주석을 추가하고 이벤트를 닫습니다.

서비스 가능 이벤트 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

참조 코드 히스토리

선택된 논리 파티션에 대해 생성된 참조 코드를 보려면 **참조 코드 히스토리** 태스크를 사용하십시오. 참조 코드는 하드웨어 또는 운영 체제 문제점의 원인을 판별하는 데 도움을 주는 진단 지원입니다.

기본적으로 논리 파티션이 생성한 최근 참조 코드만 표시됩니다. 추가 참조 코드를 보려면 보려는 참조 코드 수를 **히스토리 보기**에 입력하고 **이동**을 클릭하십시오. 창에 해당 수의 최신 참조 코드와 함께 각 참조 코드가 생성된 날짜 및 시간이 표시됩니다. 이 창은 논리 파티션에 대해 저장된 최대 참조 코드 수까지 표시할 수 있습니다.

제어판 기능

이 태스크는 선택된 IBM i 파티션에 대해 사용 가능한 가상 제어판 기능을 표시합니다. 태스크는 다음과 같습니다.

(21) 전용 서비스 도구 활성화
파티션에서 전용 서비스 도구(DST)를 시작합니다.

(65) 원격 서비스 사용 안함
파티션에서 원격 서비스를 비활성화합니다.

(66) 원격 서비스 사용
파티션에서 원격 서비스를 활성화합니다.

(68) 동시 유지보수 도메인 전원 끄기
동시 유지보수 전원 도메인 전원을 끕니다.

(69) 동시 유지보수 도메인 전원 켜기
동시 유지보수 전원 도메인 전원을 켭니다.

프레임에 대한 시스템 관리

프레임을 설정 및 구성하고 프레임의 현재 상태를 보고 문제점을 해결하고 솔루션을 적용하십시오.

특성

선택된 프레임 특성을 표시합니다.

프레임 특성에는 다음 특성이 포함되어 있습니다.

일반 **일반** 탭에는 프레임 이름과 번호, 상태, 유형, 모델, 일련 번호가 표시됩니다.

관리 시스템

관리 시스템 탭에는 프레임에 포함된 모든 관리 시스템과 이의 케이지 번호가 표시됩니다. 케이지는 관리 시스템, I/O 장치 및 대용량 전원 어셈블리(BPA)를 보유하는 격납장치의 일부입니다.

I/O 장치

I/O 장치 탭에는 프레임에 포함된 모든 I/O 장치와 이의 케이지 번호 및 지정된 관리 시스템이 표시됩니다. 케이지는 관리 시스템, I/O 장치 및 BPA를 보유하는 격납장치의 일부입니다. 시스템 열에서 **소유되지 않음**을 표시하면 대응되는 I/O 장치가 관리 시스템에 지정되지 않았음을 의미합니다.

조작

관리 프레임에 관한 태스크를 수행합니다.

프레임 초기화

관리 프레임을 초기화합니다.

이 조작 태스크는 하나 이상의 프레임이 선택된 경우에 사용될 수 있습니다. 이 태스크는 먼저 선택된 관리 프레임 내에서 소유되지 않은 I/O 장치의 전원을 켠 후에 선택된 관리 프레임 내에서 관리 시스템의 전원을 켭니다. 초기화 프로세스를 완료하는 데는 수 분이 걸릴 수 있습니다.

참고: 이미 전원이 켜져 있는 관리 시스템에는 영향을 주지 않습니다. 이는 시스템 전원이 꺼진 후에 다시 켜지지 않습니다.

모든 프레임 초기화

모든 프레임을 초기화합니다.

이 조작 태스크는 관리 프레임이 선택되지 않았으며 탐색 영역의 **프레임** 탭이 강조 표시된 경우에 사용할 수 있습니다. 이 태스크는 먼저 각 관리 프레임 내에서 소유되지 않은 I/O 장치의 전원을 켠 후에 각 관리 프레임 내에서 관리 시스템의 전원을 켭니다.

참고: HMC에 연결될 때 프레임에는 이미 전원이 켜져 있습니다. 프레임 초기화로 프레임의 전원이 켜지지는 않습니다.

재빌드

HMC 인터페이스에서 프레임 정보를 업데이트합니다.

프레임 업데이트 또는 재빌드는 프레임 정보의 새로 고치기와 매우 유사하게 작동됩니다. 프레임 재빌드는 HMC의 작업 분할창에서 시스템 상태 표시기가 미완료로 표시될 때 유용합니다. 미완료 표시기는 HMC가 프레임 내의 관리 시스템에서 전체 자원 정보를 수집할 수 없음을 의미합니다.

수 분이 소요되는 이 프로세스가 진행될 때는 HMC에서 다른 태스크를 수행할 수 없습니다.

비밀번호 변경

선택된 관리 프레임에서 HMC(Hardware Management Console) 액세스 비밀번호를 변경합니다.

비밀번호가 변경되면 이 관리 프레임에 액세스할 다른 모든 HMC에 대해 HMC 액세스 비밀번호를 업데이트해야 합니다.

현재 비밀번호를 입력하십시오. 그런 다음, 새 비밀번호를 입력한 후 확인을 위해 다시 입력하십시오.

IO 장치 전원 켜기/끄기

HMC(Hardware Management Console) 인터페이스를 사용하여 IO 장치의 전원을 끕니다.

전원 도메인에 상주하는 장치 또는 슬롯의 전원만 끄기가 가능합니다. HMC가 제어할 수 없는 위치 코드에 대해서는 해당 전원 켜기/끄기 단추를 사용할 수 없습니다.

구성

구성에는 프레임을 구성하기 위한 태스크가 포함되어 있습니다. 구성 태스크를 사용하여 사용자 정의 그룹을 관리할 수 있습니다.

사용자 정의 그룹 관리

그룹 기반으로 상태를 보고할 수 있으며 이를 통해 선호하는 방법으로 시스템을 모니터할 수 있습니다.

또한 그룹을 중첩(그룹 안에 포함된 그룹)하여 계층 구조 또는 토폴로지 보기를 제공할 수 있습니다.

하나 이상의 사용자 정의된 그룹이 이미 HMC에 정의되어 있을 수 있습니다. 기본 그룹은 **서버 관리** 아래의 **사용자 정의 그룹** 노드 아래에 나열됩니다. 기본 그룹은 **모든 파티션** 및 **모든 오브젝트**입니다. **사용자 정의 그룹 관리** 태스크를 사용하여 다른 그룹을 작성하고, 작성된 그룹을 삭제하고, 작성된 그룹에 추가하고, 패턴 일치 방법을 사용하여 그룹을 작성하거나 작성된 그룹에서 삭제할 수 있습니다.

그룹 관련 작업에 대한 추가 정보가 필요하면 온라인 도움말을 사용하십시오.

연결

연결 태스크를 사용하면 프레임에 대한 HMC(Hardware Management Console) 연결 상태를 보거나 해당 연결을 재설정할 수 있습니다.

대용량 전원 어셈블리(BPA) 상태

대용량 전원 어셈블리 상태 태스크를 사용하면 HMC(Hardware Management Console)에서 대용량 전원 어셈블리의 A면과 B면으로의 연결 상태를 볼 수 있습니다. 일반적으로 HMC는 A면과 B면 중 하나에 연결되어 작동됩니다. 그러나 코드 업데이트 조작 및 일부 동시 유지보수 조작에서는 HMC가 두 면에 모두 연결되어야 합니다.

HMC는 다음을 표시합니다.

- IP 주소
- BPA 역할
- 연결 상태
- 연결 오류 코드

상태가 "연결됨"이 아닌 경우, 연결 상태는 다음 상태 중 하나일 수 있습니다.

시작 중/알 수 없음
: 프레임에 포함되어 있는 대용량 전원 어셈블리(BPA) 중 하나를 시작하는 중입니다. 다른 BPA의 상태는 판별할 수 없습니다.

대기/대기
: 프레임에 포함된 BPA가 둘 다 대기 상태입니다. 대기 상태의 BPA는 정상적으로 작동 중입니다.

대기/시작 중
: 프레임에 포함된 BPA 중 하나가 정상적으로 작동 중(대기 상태)입니다. 다른 BPA는 시작하는 중입니다.

대기/사용 불가능
: 프레임에 포함된 BPA 중 하나는 정상적으로 작동 중(대기 상태)이지만 다른 BPA는 정상적으로 작동되지 않습니다.

프레임 번호 보류 중
: 프레임 번호에 대한 변경이 진행 중입니다. 프레임이 이 상태인 경우에는 어떤 조작도 수행할 수 없습니다.

인증 실패
: 프레임에 대한 HMC 액세스 비밀번호가 올바르지 않습니다. 프레임에 대해 올바른 비밀번호를 입력하십시오.

인증 보류 중 - 비밀번호 업데이트 필요
: 프레임 액세스 비밀번호가 설정되지 않았습니다. HMC에서 보안 인증 및 액세스 제어를 사용하려면 프레임에 대한 필수 비밀번호를 설정해야 합니다.

연결되지 않음
: HMC가 프레임에 연결할 수 없습니다.

미완료

HMC가 관리 프레임에서 모든 필수 정보를 가져오는 데 실패했습니다. 프레임이 정보에 대한 요청에 응답하지 않습니다.

재설정

HMC 및 선택된 관리 프레임 간의 연결을 재설정합니다.

관리 프레임과의 연결을 재설정하면 연결이 끊긴 후에 다시 연결됩니다. 관리 프레임이 연결되지 않음 상태이며 HMC 및 관리 프레임 둘 모두에서 네트워크 설정이 올바른지 확인한 경우에는 관리 프레임과의 연결을 재설정하십시오.

서비스 가능성

HMC(Hardware Management Console)에서 문제점 분석은 자동으로 오류 상태를 발견하며 수리를 위해 서비스가 필요한 문제점을 사용자에게 보고합니다.

이러한 문제점은 사용자에게 서비스 가능 이벤트로 보고됩니다. 사용자는 선택된 시스템에 대한 특정 이벤트를 보고 FRU(Field Replaceable Unit)를 추가, 제거하거나 교환할 수 있습니다. **서비스 가능 이벤트 관리자** 태스크를 사용하여 선택된 프레임에 대한 특정 이벤트를 볼 수 있습니다.

프레임에 사용할 수 있는 서비스 가능성 태스크를 열려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **자원** 아이콘  을 클릭한 후 **모든 프레임**을 선택하십시오.
2. 서비스 가능성 태스크를 관리할 프레임을 선택하십시오.
3. 메뉴 팟에서 **서비스 가능성**을 펼친 후 **서비스 가능성**을 클릭하십시오.
4. 목록에서 수행할 서비스 가능성 태스크를 선택하십시오.

서비스 가능 이벤트 관리자

관리 프레임의 문제점은 서비스 가능 이벤트로서 HMC(Hardware Management Console)에 보고됩니다. 문제점을 보거나, 문제점 데이터를 관리하거나, 서비스 제공자에게 이벤트를 콜홈하거나, 문제점 복구를 수행할 수 있습니다.

보고자 하는 서비스 가능 이벤트에 대한 기준을 설정하려면 다음을 수행하십시오.

1. 메뉴 팟에서 **서비스 가능 이벤트 관리자**를 여십시오.
2. 이벤트 기준, 오류 기준 및 FRU 기준을 제공하십시오.
3. **확인**을 클릭하십시오.
4. 결과를 필터링하지 않으려면 **모두**를 선택하십시오.

서비스 가능 이벤트 개요 창에 기준과 일치하는 모든 이벤트가 표시됩니다. 압축 테이블 보기에 표시되는 정보에는 다음 필드가 포함됩니다.

- 문제점 번호

- PMH 번호
- 참조 코드 - **참조** 코드를 클릭하면 보고된 문제점에 대한 설명과 문제점 해결을 위해 취할 수 있는 조치가 표시됩니다.
- 문제점의 상태
- 문제점이 마지막으로 보고된 시간
- 문제점의 실패 MTMS

전체 테이블 보기에는 보고 MTMS, 처음 보고된 시간, 서비스 가능 이벤트 텍스트를 포함하여 좀 더 자세한 정보가 포함되어 있습니다.

서비스 가능 이벤트를 선택하고 다음 태스크를 완료하십시오.
- **이벤트 세부사항 보기**: 이 이벤트와 연관된 FRU 및 해당 설명입니다.
- **이벤트 복구**: 사용 가능한 경우 안내되는 복구 프로시저를 실행합니다.
- **이벤트 콜홈**: 이벤트를 서비스 제공자에게 보고합니다.
- **이벤트 문제점 데이터 관리**: 이 이벤트와 연관된 데이터 및 로그를 보거나 콜홈하거나 매체에 오프로드합니다.
- **이벤트 닫기**: 문제점이 해결된 후 주석을 추가하고 이벤트를 닫습니다.

서비스 가능 이벤트 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

하드웨어

이 태스크를 사용하여 관리 프레임에서 하드웨어를 추가, 교환하거나 제거할 수 있습니다. 하드웨어 태스크에서 사용자는 설치된 FRU 또는 격납장치 및 해당 위치의 목록을 표시할 수 있습니다. FRU 또는 격납장치를 선택하고 장치를 추가, 교환 또는 제거하기 위한 단계별 프로시저를 실행하십시오.

FRU 추가:

FRU 추가 태스크를 사용하여 FRU를 찾고 추가할 수 있습니다.

FRU를 추가하려면 다음 단계를 완료하십시오.

1. 드롭 다운 목록에서 격납장치 유형을 선택하십시오.
2. FRU 유형을 선택하십시오.
3. **다음**을 클릭하십시오.
4. 위치 코드를 선택하십시오.
5. **추가**를 클릭하여 선택된 격납장치 위치를 보류 중 조치에 추가하십시오.
6. **프로시저 실행**을 클릭하여 보류 중 조치에서 식별된 격납장치 위치에 선택된 FRU 유형의 추가를 시작하십시오.
7. FRU 설치 프로세스를 완료한 후 **완료**를 클릭하십시오.

격납장치 추가:

격납장치 추가 태스크를 사용하여 격납장치 위치를 찾고 이를 추가할 수 있습니다.

격납장치를 추가하려면 다음 단계를 완료하십시오.

1. 격납장치 유형을 선택한 후 **추가**를 클릭하여 선택한 격납장치 유형의 위치 코드를 **보류 중인 조치**에 추가하십시오.
2. **보류 중 조치**에서 식별된 격납장치를 선택된 시스템에 추가하기 시작하려면 **프로시저 실행**을 클릭하십시오.
3. 격납장치 설치 프로세스를 완료한 후 **완료**를 클릭하십시오.

FRU 교환:

하나의 FRU를 다른 FRU와 교환합니다.

FRU를 교환하려면 다음 단계를 완료하십시오.

1. 설치된 격납장치 유형을 선택하십시오.
2. FRU 유형을 선택하십시오.
3. **다음**을 클릭하십시오.
4. 특정 FRU의 위치 코드를 선택하십시오.
5. **추가**를 클릭하십시오.
6. **프로시저 실행**을 선택하십시오.
7. 설치가 완료되면 **완료**를 클릭하십시오.

격납장치 교체:

하나의 격납장치를 다른 격납장치로 교체합니다.

격납장치를 교체하려면 다음 단계를 완료하십시오.

1. 설치된 격납장치를 선택한 후에 **추가**를 클릭하여 선택한 격납장치의 위치 코드를 **보류 중 조치**에 추가하십시오.
2. **프로시저 실행**을 클릭하여 선택된 시스템의 **보류 중 조치**에서 식별되는 격납장치의 교체를 시작하십시오.
3. 격납장치 교체 프로세스가 완료되면 **완료**를 클릭하십시오.

FRU 제거:

관리 시스템에서 FRU를 제거합니다.

FRU를 제거하려면 다음 단계를 완료하십시오.

1. 드롭 다운 목록에서 격납장치를 선택하십시오.
2. 이 격납장치에 대해 표시된 FRU 유형의 목록에서 FRU 유형을 선택하십시오.

3. **다음**을 클릭하십시오.
4. 특정 FRU의 위치 코드를 선택하십시오.
5. **추가**를 클릭하십시오.
6. **프로시저 실행**을 선택하십시오.
7. 제거 프로시저가 완료되면 **완료**를 클릭하십시오.

격납장치 제거:

HMC(Hardware Management Console)로 식별된 격납장치를 제거합니다.

격납장치를 제거하려면 다음 단계를 완료하십시오.

1. 격납장치 유형을 선택한 후 **추가**를 클릭하십시오.
2. **프로시저 실행**을 클릭하십시오.
3. 격납장치 제거 프로세스가 완료되면 **완료**를 클릭하십시오.

Power 엔터프라이즈 풀에 대한 시스템 관리

Power 엔터프라이즈 풀에 대한 시스템 관리는 사용자가 수행할 수 있는 Power 엔터프라이즈 풀 태스크를 표시합니다.

Power 엔터프라이즈 풀 오퍼링을 사용하여 다음 조작을 수행할 수 있습니다.

- 서버에 프로세서 또는 메모리 추가
- 서버에서 프로세서 또는 메모리 제거
- 풀 구성 업데이트
- 풀에 서버 추가
- 풀에서 기존 서버 제거
- 풀에 프로세서 또는 메모리 추가
- 다음 Power 엔터프라이즈 풀 정보 보기:
  - 풀 멤버십 정보
  - 풀 자원 정보
  - 풀 호환 정보
  - 풀 히스토리 로그

HMC 관리 태스크

HMC 관리 아래의 HMC(Hardware Management Console)에서 사용 가능한 태스크에 대해 학습합니다.

이러한 태스크를 열려면 7 페이지의 『HMC 태스크, 사용자 역할, ID 및 연관된 명령』의 내용을 참조하십시오.

참고: 사용자 ID에 지정된 태스크 역할에 따라 사용자에게 액세스 권한이 없는 태스크가 있을 수 있습니다. 태스크 목록 및 해당 태스크에 액세스할 수 있도록 허용된 사용자 역할에 대해서는 8 페이지의 표 5의 내용을 참조하십시오.

설치 안내 마법사 실행

이 태스크는 마법사를 사용하여 시스템 및 HMC를 설치합니다.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **설치 안내 마법사 실행**을 클릭하십시오.
3. **설치 안내 마법사 실행 - 시작** 창에서 특정 전제조건을 충족시키는 것이 좋습니다. 이에 대한 정보는 **설치 안내 마법사 실행 - 시작** 창에서 **전제조건**을 클릭하십시오. 이를 완료하면 마법사가 시스템 및 HMC를 설정하는 데 필요한 다음 태스크로 안내합니다. 각 태스크를 완료하면 **다음**을 클릭하여 진행하십시오.
   a. HMC 날짜 및 시간 변경
   b. HMC 비밀번호 변경
   c. 추가 HMC 사용자 작성
   d. HMC 네트워크 설정 구성(이 태스크는 원격으로 **설치 안내 마법사 실행**에 액세스하는 경우 수행할 수 없습니다.)
   e. 담당자 정보 지정
   f. 연결 정보 구성
   g. 사용자에게 Electronic Service Agent™ 소프트웨어 도구를 사용할 수 있는 권한 부여 및 문제점 이벤트의 알림 구성
4. 마법사의 모든 태스크를 완료한 후 **완료**를 클릭하십시오.

네트워크 토폴로지 보기

이 태스크를 사용하여 HMC(Hardware Management Console) 내의 다양한 네트워크 노드 간 연결을 보고 ping할 수 있습니다.

네트워크 토폴로지를 보려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 토폴로지 보기**를 클릭하십시오.
3. **네트워크 토폴로지 보기** 창에서 현재 노드와 저장된 노드를 ping할 수 있습니다.
4. 이 태스크를 완료한 후 **닫기**를 클릭하십시오.

네트워크 토폴로지 보기에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

네트워크 연결 테스트

이 태스크를 사용하여 HMC(Hardware Management Console)의 네트워크 프로토콜에 대한 네트워크 진단 정보를 볼 수 있습니다.

네트워크 연결을 테스트하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 연결 테스트**를 클릭하십시오.
3. **네트워크 연결 테스트** 창에서 다음 탭에 대해 작업할 수 있습니다.

   Ping TCP/IP 주소 또는 이름을 ping할 수 있습니다.

   인터페이스
   현재 구성된 네트워크 인터페이스의 통계를 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   이더넷 설정
   현재 구성된 이더넷 카드의 설정을 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   주소 구성된 네트워크 인터페이스의 TCP/IP 주소를 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   라우트
   커널 IP 및 IPv6 라우팅 테이블과 해당 네트워크 인터페이스를 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   ARP ARP(Address Resolution Protocol) 연결의 내용을 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   소켓 TCP/IP 소켓에 대한 정보를 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   TCP TCP(Transmission Control Protocol) 연결에 대한 정보를 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   IP 테이블
   IP(Internet Protocol) 패킷 필터 규칙에 대한 정보를 테이블 형식으로 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.

   UDP UDP(User Datagram Protocol) 통계에 대한 정보를 표시합니다. 현재 표시된 정보를 최신 정보로 업데이트하려면 **새로 고치기**를 클릭하십시오.
4. 이 태스크를 완료한 후 **취소**를 클릭하십시오.

네트워크 연결 테스트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

네트워크 설정 변경

이 태스크를 통해 HMC에 대한 현재 네트워크 정보를 보고 네트워크 설정을 변경할 수 있습니다.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **네트워크 설정 변경**을 클릭하십시오.
3. **네트워크 설정 변경** 창에서 다음 탭에 대해 작업할 수 있습니다.

   식별 HMC의 호스트 이름 및 도메인 이름을 포함합니다.

   콘솔 이름

   네트워크에 있는 다른 콘솔에 대해 사용자의 콘솔을 식별하는 이름인 사용자의 HMC 사용자 이름입니다. 이 이름은 짧은 호스트 이름입니다. 예: hmc1.

   도메인 이름

   도메인 이름 서비스(DNS)가 IP 주소로 변환할 수 있는 이름입니다. 예를 들어, DNS는 도메인 이름 www.example.com을 198.105.232.4로 변환할 수 있습니다. (긴 호스트 이름은 콘솔 이름과 기간과 도메인 이름으로 구성됩니다. 예: hmc.endicott.yourcompany.com.)

   콘솔 설명

   사용자 전용입니다. 예를 들어, 고객 재무에 대한 기본 HMC입니다.

   LAN 어댑터

   요약된 모든 표시 가능한 근거리 통신망(LAN) 어댑터 목록입니다. 해당 항목 중 하나를 선택하고 **세부사항...** 을 클릭하면 주소 지정, 라우팅, 기타 LAN 어댑터 특성 및 방화벽 설정을 변경할 수 있는 창이 열립니다.

   이름 서비스

   콘솔 네트워크 설정을 구성하기 위해 DNS 및 도메인 접미부 값을 지정하십시오.

   라우팅

   콘솔 네트워크 설정을 구성하기 위한 라우팅 정보 및 기본 게이트웨이 정보를 지정하십시오.

   게이트웨이 주소는 모든 네트워크에 대한 라우트입니다. 기본 게이트웨이 주소(정의된 경우)는 대상 스테이션이 소스와 동일한 서브넷에 없는 경우 이 HMC에 데이터를 보낼 위치를 알려줍니다. 시스템이 동일한 서브넷(일반적으로 건물 또는 건물 내 구역)의 모든 스테이션에 도달할 수 있지만 영역 외부에서는 통신할 수 없는 경우, 일반적으로 기본 게이트웨이가 잘못 구성되었기 때문입니다.

   특정 LAN을 **게이트웨이 장치**로 지정하거나 "모두"를 선택할 수 있습니다.

   '라우팅됨' 사용을 선택하여 라우팅된 디먼을 시작할 수 있으며 이를 통해 라우팅된 디먼을 실행하고 HMC에서 라우팅 정보를 내보낼 수 있습니다.

4. 이 태스크를 완료한 후 **확인**을 클릭하십시오.

참고: 작성한 변경의 유형에 따라 네트워크 또는 콘솔이 자동으로 다시 시작되거나 콘솔이 자동으로 다시 부팅됩니다.

네트워크 설정 사용자 정의에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

성능 모니터링 설정 변경

성능 및 용량 모니터 도구는 가상화된 서버 자원에 대한 할당 및 사용 데이터를 수집합니다. 이 도구는 그래프 및 표 형식으로 데이터를 표시하며 이러한 그래프와 표는 성능 및 용량 모니터 홈 페이지에서 볼 수 있습니다. 성능 및 용량 모니터는 HMC(Hardware Management Console) 버전 8 릴리스 1 이상에서 사용 가능합니다.

성능 및 용량 모니터는 데이터를 수집하고 용량 보고 및 성능 모니터링을 제공합니다. 이 정보를 사용하여 사용 가능한 용량 및 자원이 과도하게 사용되는지 또는 충분히 이용되고 있지 않은지 여부를 판별할 수 있습니다. 또한 그래프와 표를 해석하면 용량을 계획하고 문제점을 해결하는 데 유용할 수 있습니다. 성능 및 용량 모니터 도구에 대한 자세한 정보는 성능 및 용량 모니터 사용을 참조하십시오.

성능 및 용량 모니터는 데이터 콜렉션을 사용하도록 선택하는 서버에서만 데이터를 캡처합니다.

데이터 콜렉션을 사용으로 설정하려면 다음 단계를 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **성능 모니터링 설정 변경**을 클릭하십시오.
3. 1 - 366 범위의 숫자를 입력하여 성능 데이터를 저장할 일 수를 지정하십시오. 또는 **성능 데이터 스토리지** 아래에 있는 **성능 데이터 저장 일 수** 옆의 위로 또는 아래로 화살표를 클릭할 수도 있습니다.

   참고: 기본적으로 HMC는 180일 동안 데이터를 저장합니다. 그러나 HMC가 데이터를 저장하는 최대 일 수를 366일로 지정할 수 있습니다.
4. 데이터를 수집하려는 서버의 이름 옆에 있는 **콜렉션** 열에서 토글 스위치를 클릭하십시오. 또는 **모두 켜짐**을 클릭하여 사용자 환경에서 HMC가 관리하는 모든 서버에 대한 데이터 콜렉션을 사용으로 설정할 수도 있습니다.

   참고: 스토리지 공간이 제한되어 있기 때문에 사용자 환경에 있는 모든 서버에서 데이터를 수집하지 못할 수 있습니다. 예상 스토리지 공간이 부족할 수 있다고 HMC가 판별하면 HMC는 더 많은 서버에서 데이터를 수집할 수 없도록 합니다.
5. **확인**을 클릭하여 변경사항을 적용하고 창을 닫으십시오. 이제 성능 및 용량 모니터 홈 페이지에 액세스하면 수집된 데이터를 검토할 수 있습니다.

날짜 및 시간 변경

배터리 작동 HMC 클럭의 시간 및 날짜를 변경하고 NTP(Network Time Protocol) 서비스에 대한 시간 서버를 추가 또는 제거하십시오.

이 태스크는 다음과 같은 상황에서 사용하십시오.

- HMC에서 배터리가 교체된 경우
- 시스템이 물리적으로 다른 표준 시간대로 이동된 경우

참고: 시간 설정은 선택한 시간대의 일광 절약 시간에 대해 자동으로 조정됩니다.

날짜 및 시간을 변경하려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **날짜 및 시간 변경**을 클릭하십시오.
3. **콘솔 날짜 및 시간 사용자 정의** 탭을 클릭하십시오.
4. 날짜 및 시간 정보를 입력하십시오.
5. **확인**을 클릭하십시오.

시간 서버 정보를 변경하려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **날짜 및 시간 변경**을 클릭하십시오.
3. **NTP 구성** 탭을 클릭하십시오.
4. 시간 서버에 대해 적절한 정보를 제공하십시오.
5. **확인**을 클릭하십시오.

HMC의 날짜 및 시간 변경에 대한 추가 정보나 NTP(Network Time Protocol) 서비스에 대한 시간 서버 추가 또는 제거에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

언어 및 로케일 변경

이 태스크는 HMC의 언어 및 위치를 설정합니다. 언어를 선택한 후 해당 언어와 연관된 로케일을 선택할 수 있습니다.

언어 및 로케일 설정은 국가나 지역의 고유한 언어, 문자 세트 및 기타 설정(예: 날짜, 시간, 숫자 및 통화 단위의 형식)을 결정합니다. **언어 및 로케일 변경** 창에서 작성된 변경사항은 HMC 자체의 언어 및 로케일에만 적용됩니다. HMC에 원격으로 액세스하면 브라우저의 언어 및 로케일 설정으로 브라우저가 HMC 인터페이스를 표시하는 데 사용하는 설정이 결정됩니다.

HMC에서 언어 및 로케일을 변경하려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **언어 및 로케일 변경**을 클릭하십시오.
3. **언어 및 로케일 변경** 창에서 적용 가능한 언어 및 로케일을 선택하십시오.
4. **확인**을 클릭하여 변경사항을 적용하십시오.

HMC의 언어 및 로케일 변경에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

시작 텍스트 작성

시작 메시지를 작성하고 표시하거나, 사용자가 HMC(Hardware Management Console)에 로그온하기 전에 나타나는 경고 메시지를 표시합니다.

이 태스크의 메시지 입력 영역에 입력하는 텍스트는 처음 콘솔에 액세스한 이후 **시작** 창에 나타납니다. 이 텍스트를 사용하여 시스템에 적용되는 특정 회사 정책이나 보안 제안사항에 대해 사용자에게 알릴 수 있습니다.

시작 텍스트를 작성하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 설정**을 선택하십시오.
2. 컨텐츠 분할창에서 **시작 텍스트 작성**을 클릭하십시오.
3. 텍스트 상자에 표시할 시작 텍스트를 입력하십시오.

   참고: 최대 8192자까지 허용됩니다.
4. **확인**을 클릭하십시오.

이 태스크에 대한 자세한 정보를 보려면 온라인 도움말을 사용하십시오.

시스템 종료 또는 다시 시작

이 태스크를 사용하여 콘솔을 시스템 종료(콘솔 전원 끄기)하거나 다시 시작할 수 있습니다.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **시스템 종료 또는 다시 시작**을 클릭하십시오.
3. **시스템 종료 또는 다시 시작** 창에서 다음을 수행할 수 있습니다.
   - 시스템 종료가 발생한 후 HMC를 자동으로 다시 시작하려면 **HMC 다시 시작**을 선택하십시오.
   - HMC를 자동으로 다시 시작하지 않으려면 **HMC 다시 시작**을 선택하지 마십시오.

4. 시스템 종료를 진행하려면 **확인**을 클릭하고 그렇지 않으면 **취소**를 클릭하여 태스크를 종료하십시오.

HMC 시스템 종료 또는 다시 시작에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

조작 스케줄

운영자 지원 없이 HMC 자체에서 특정 조작을 수행할 스케줄을 작성하십시오.

스케줄된 조작은 시스템 조작의 자동, 지연 또는 반복 처리가 필요한 상황에 유용합니다. 스케줄된 조작은 조작을 수행하기 위한 운영자의 지원 없이 지정된 시간에 시작됩니다. 스케줄은 단일 조작에 대해 설정되거나 여러 번 반복될 수 있습니다.

예를 들어, 중요한 HMC 정보를 DVD에 백업하는 조작이 한 번 발생하도록 스케줄하거나 반복 스케줄을 설정할 수 있습니다.

스케줄된 조작 태스크는 각 조작에 대해 다음 정보를 표시합니다.
- 조작의 오브젝트인 프로세서
- 스케줄된 날짜
- 스케줄된 시간
- 조작
- 남은 반복 수

스케줄된 조작 창에서 다음을 수행할 수 있습니다.
- 나중에 실행할 조작 스케줄
- 일정한 간격으로 반복할 조작 정의
- 이전에 스케줄된 조작 삭제
- 현재 스케줄된 조작의 세부사항 보기
- 지정된 시간 범위 내에서 스케줄된 조작 보기
- 날짜, 조작 또는 관리 시스템을 기준으로 스케줄된 조작 정렬

조작이 한 번 발생하도록 스케줄하거나 반복되도록 스케줄할 수 있습니다. 조작이 발생할 시간 및 날짜를 제공해야 합니다. 조작이 반복되도록 스케줄되면 다음을 선택하도록 요청됩니다.
- 조작이 발생할 요일(선택사항)
- 각 발생 사이의 시간 간격(필수)
- 총 반복 수(필수)

HMC에 대해 스케줄할 수 있는 조작은 다음과 같습니다.

중요한 콘솔 데이터 백업

HMC의 중요한 콘솔 하드 디스크 정보를 백업하기 위한 조작을 스케줄합니다.

HMC에서 조작을 스케줄하려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **조작 스케줄**을 클릭하십시오.
3. **조작 스케줄** 창의 메뉴 표시줄에서 **옵션**을 클릭하여 다음 레벨의 옵션을 표시하십시오.
   - 스케줄된 조작을 추가하려면 **옵션**을 가리킨 후 **새로 작성**을 클릭하십시오.
   - 스케줄된 조작을 삭제하려면 삭제할 조작을 선택하고 **옵션**을 가리킨 후 **삭제**를 클릭하십시오.
   - 스케줄된 조작의 목록을 선택된 오브젝트의 현재 스케줄로 업데이트하려면 **옵션**을 가리킨 후 **새로 고치기**를 클릭하십시오.
   - 스케줄된 조작을 보려면 보려는 조작을 선택하고 **보기**를 가리킨 후 **스케줄 세부사항**을 클릭하십시오.
   - 스케줄된 조작의 시간을 변경하려면 보려는 조작을 선택하고 **보기**를 가리킨 후 **새 시간 범위**를 클릭하십시오.
   - 스케줄된 조작을 정렬하려면 **정렬**을 가리킨 후 표시되는 정렬 카테고리 중 하나를 클릭하십시오.
4. HMC 작업영역으로 돌아가려면 **옵션**을 가리킨 후 **종료**를 클릭하십시오.

조작 스케줄에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

라이센스 보기

이 HMC에 대해 사용자가 동의한 라이센스가 부여된 내부코드를 보십시오.

언제든지 라이센스를 볼 수 있습니다. 라이센스를 보려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **라이센스 보기**를 클릭하십시오.
3. 자세한 정보를 보려면 라이센스 링크를 클릭하십시오.

   참고: 이 목록은 독립된 라이센스 계약에 따라 제공되는 프로그램 및 코드를 포함하지 않습니다.
4. **확인**을 클릭하십시오.

Hardware Management Console 업데이트

HMC(Hardware Management Console)의 내부 코드를 업데이트하는 방법과 시스템 정보 및 시스템 준비 상태를 보는 방법을 학습합니다.

HMC를 업데이트하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Hardware Management Console 업데이트**를 클릭하십시오. **HMC 수정 서비스 설치 마법사**가 열립니다.
3. **다음**을 클릭하여 업데이트 프로세스를 시작하십시오.
4. 마법사의 단계에 따라 업데이트 조작을 완료하십시오.
5. 이 태스크를 완료한 후 **완료**를 클릭하십시오.

Hardware Management Console 업데이트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

매체 포맷

이 태스크는 디스켓 또는 USB 2.0 플래시 드라이브 메모리 키를 포맷합니다.

사용자 지정 레이블을 공급하여 디스켓을 포맷할 수 있습니다.

디스켓 또는 USB 2.0 플래시 드라이브 메모리 키를 포맷하려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **매체 포맷**을 클릭하십시오.
3. **매체 포맷** 창에서 포맷하려는 매체의 유형을 선택한 후 **확인**을 클릭하십시오.
4. 매체가 올바르게 삽입되었는지 확인한 후 **포맷**을 클릭하십시오. **매체 포맷** 진행 창이 표시됩니다. 매체가 포맷되면 **매체 포맷 완료** 창이 표시됩니다.
5. **확인**을 클릭한 후 **닫기**를 클릭하여 태스크를 종료하십시오.

디스켓 또는 USB 2.0 플래시 드라이브 메모리 키 포맷에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

관리 콘솔 데이터 백업

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

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

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

HMC를 사용하여 다음과 같은 중요한 데이터를 모두 백업할 수 있습니다.

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

참고: 제품 CD에서 HMC의 재설치와 함께 아카이브된 데이터만 사용하십시오.

HMC 중요 데이터를 백업하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **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. **확인**을 클릭하여 백업 프로세스를 계속하십시오.

HMC 데이터 백업에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

관리 콘솔 데이터 복원

이 태스크는 HMC의 중요한 백업 데이터를 복원할 원격 저장소를 선택하는 데 사용됩니다.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **관리 콘솔 데이터 복원**을 클릭하십시오.
3. **관리 콘솔 데이터 복원** 창에서 **원격 NFS(Network File System) 서버에서 복원**, **원격 FTP(File Transfer Protocol) 서버에서 복원**, **원격 SFTP(Secure Shell File Transfer Protocol) 서버에서 복원** 또는 **원격 이동식 매체에서 복원**을 클릭하십시오.
4. 계속하려면 **다음**을 클릭하고, 변경하지 않고 태스크를 종료하려면 **취소**를 클릭하십시오.

이 HMC의 중요한 백업 데이터 복원에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

업그레이드 데이터 저장

이 태스크는 마법사를 사용하여 업그레이드 데이터를 선택한 매체에 저장합니다. 이 데이터는 현재 소프트웨어 레벨을 실행하는 동안 작성되거나 사용자 정의된 파일로 구성됩니다. 이 데이터를 선택한 매체에 저장하는 것은 HMC 소프트웨어 업그레이드 전에 수행됩니다.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **업그레이드 데이터 저장**을 클릭하십시오.

3. **업그레이드 데이터 저장** 창에서 이 마법사가 데이터를 저장하는 데 필요한 단계를 안내합니다. 데이터를 저장할 매체의 유형을 선택한 후 **다음**을 클릭하여 태스크 창을 통해 진행하십시오.
4. 태스크를 완료한 후 **완료**를 클릭하십시오.

업그레이드 데이터 저장에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

데이터 복제 관리

이 태스크는 사용자 정의된 데이터 복제를 사용 또는 사용 안함으로 설정합니다. 사용자 정의된 데이터 복제를 사용하면 다른 HMC가 이 HMC에서 사용자 정의된 콘솔 데이터를 얻거나 이 HMC로 데이터를 전송할 수 있습니다.

다음 유형의 데이터를 구성할 수 있습니다.

- 고객 정보 데이터
  - 관리자 정보(예: 고객 이름, 주소 및 전화번호)
  - 시스템 정보(예: 관리자 이름, 주소 및 시스템의 전화)
  - 계정 정보(예: 고객 번호, 엔터프라이즈 번호 및 영업 지방 사무소)
- 그룹 데이터
  - 모든 사용자 정의 그룹 정의
- 모뎀 구성 데이터
  - 원격 지원을 위한 모뎀 구성
- 아웃바운드 연결 데이터
  - RSF에 대한 로컬 모뎀 구성
  - 인터넷 연결 사용
  - 외부 시간 소스에 대한 구성

참고: 사용자 정의 가능 콘솔 데이터는 특정 HMC 및 이와 연관된 허용 가능한 사용자 정의 가능 데이터 유형이 구성된 후에만 다른 HMC에서 승인됩니다.

데이터 복제를 관리하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **데이터 복제 관리**를 클릭하십시오.
3. **데이터 복제 관리** 창에서 수행할 적절한 옵션을 선택하십시오.

사용자 정의 가능 데이터 복제 사용 또는 사용 안함 설정에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

템플리트 및 OS 이미지

시스템 템플리트는 시스템 특성, 공유 프로세서 풀, 예약 스토리지 풀, 공유 메모리 풀, 호스트 이더넷 어댑터, SR-IOV(Single Root I/O Virtualization) 어댑터, Virtual I/O Server, 가상 네트워크 및 가상 스토리지와 같은 자원의 구성 세부사항을 포함합니다. 별도의 태스크를 사용하여 이전에 구성한 많은 시스템 설정을 템플리트에서 시스템 배치 마법사에서 사용할 수 있습니다. 예를 들어, 마법사를 사용하여 시스템 또는 파티션 템플리트에서 시스템을 배치할 때 Virtual I/O Server, 가상 네트워크 브릿지 및 가상 스토리지 설정을 구성할 수 있습니다.

템플리트 라이브러리에는 공통 사용 시나리오 기반의 구성 설정을 포함하는 사전 정의된 시스템 템플리트가 포함됩니다. 사전 정의된 시스템 템플리트는 즉시 사용할 수 있습니다. 템플리트 라이브러리에서 사용할 수 있는 템플리트에 대해 보기, 수정, 배치, 복사, 가져오기, 내보내기 또는 삭제를 수행할 수 있습니다.

또한 사용자 환경에 특정한 구성 설정을 포함하는 사용자 정의 시스템 템플리트를 작성할 수 있습니다. 사전 정의된 템플리트를 복사한 후 사용자 요구에 맞게 이를 변경하여 사용자 정의 템플리트를 작성할 수 있습니다. 또는 기존 시스템의 구성을 캡처하고 세부사항을 템플리트에 저장할 수 있습니다. 그런 다음, 동일한 구성이 필요한 다른 시스템에 해당 템플리트를 배치할 수 있습니다.

템플리트 라이브러리에 액세스하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **템플리트 및 OS 이미지**를 선택하십시오.
2. **템플리트 및 OS 이미지** 창에서 다음에 액세스할 수 있습니다.
   - **시스템 템플리트**
   - **파티션 템플리트**
   - **OS 및 VIOS 이미지**
3. 이 태스크를 완료한 후 **닫기**를 클릭하십시오.

시스템 템플리트

시스템 템플리트는 공유 프로세서 풀, 예약 스토리지 풀, 공유 메모리 풀, 물리적 I/O 어댑터, 호스트 이더넷 어댑터, SR-IOV(Single Root I/O Virtualization) 어댑터, Virtual I/O Server(VIOS), 가상 네트워크 및 가상 스토리지와 같은 자원에 대한 구성 정보를 포함합니다.

사용자 환경에 특정한 구성 설정을 포함하는 사용자 정의 시스템 템플리트를 작성할 수 있습니다. 또한 사전 정의된 템플리트를 복사한 후 사용자 요구에 맞게 이를 변경하여 사용자 정의 템플리트를 작성할 수도 있습니다. 또는 기존 시스템의 구성을 캡처하고 세부사항을 템플리트에 저장할 수 있습니다. 그런 다음, 동일한 구성이 필요한 다른 시스템에 해당 템플리트를 배치할 수 있습니다. 템플리트에 대한 세부사항을 보려면 템플리트 이름을 클릭하십시오. 템플리트의 보기, 편집, 복사, 삭제, 배치 또는 내보내기를 수행하려면 목록에서 시스템 템플리트를 선택하십시오.

시스템 템플리트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

파티션 템플리트

파티션 템플리트는 물리적 어댑터, 가상 네트워크 및 스토리지 구성과 같은 파티션 자원에 대한 세부사항을 포함합니다.

사용자 환경에 특정한 구성 설정을 포함하는 사용자 정의 파티션 템플리트를 작성할 수 있습니다. 또한 사전 정의된 템플리트를 복사한 후 사용자 요구에 맞게 이를 변경하여 사용자 정의 템플리트를 작성할 수도 있습니다. 또는 기존 시스템의 구성을 캡처하고 세부사항을 템플리트에 저장할 수 있습니다. 그런 다음, 동일한 구성이 필요한 다른 시스템에 해당 템플리트를 배치할 수 있습니다. 템플리트에 대한 세부사항을 보려면 템플리트 이름을 클릭하십시오. 템플리트의 보기, 편집, 복사, 삭제, 배치 또는 내보내기를 수행하려면 목록에서 파티션 템플리트를 선택하십시오.

파티션 템플리트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

OS 및 VIOS 이미지

HMC(Hardware Management Console)가 액세스할 수 있고 사용할 수 있는 운영 환경에 대한 VIOS 이미지 및 설치 자원을 정의하십시오.

다음 태스크에 액세스할 수 있습니다.

설치 자원 관리:

HMC의 운영 환경을 위한 설치 자원을 추가 또는 제거할 수 있습니다.

HMC를 사용하여 하나 이상의 논리 파티션에 하나 이상의 운영 환경을 설치하기 위한 정보가 포함된 시스템 계획을 배치할 수 있습니다. 운영 환경을 시스템 계획 배치의 일부로 설치하려면 HMC가 해당 운영 환경에 대한 설치 자원에 액세스할 수 있고 이를 사용할 수 있어야 합니다.

운영 환경의 설치 자원은 특정 릴리스 및 수정 레벨의 특정 운영 환경 버전에 대한 설치 파일의 필수 세트입니다. 설치 자원은 HMC의 로컬 하드 드라이브 또는 HMC가 액세스할 수 있는 NIM(Network Installation Management) 서버에 있을 수 있습니다.

로컬 설치 자원을 정의하고 작성하려면 다음 전제조건을 충족해야 합니다.

- 특정 운영 환경 버전 및 수정 레벨에 대해 하나의 로컬 설치 자원만 정의할 수 있습니다. 예를 들어, AIX 5.3용의 로컬 설치 자원과 AIX 6.1용의 다른 로컬 설치 자원을 정의할 수 있지만 동일한 AIX 버전 및 수정 레벨에 대해서는 두 개의 로컬 설치 자원을 정의할 수 없습니다. 이 제한사항은 나열된 모든 운영 환경에 적용됩니다.
- HMC에는 운영 환경에 대한 설치 파일의 필수 세트에 필요한 충분한 하드 디스크 여유 공간이 있어야 합니다. HMC는 HMC가 기본 저장 덤프용으로 사용하는 동일한 로컬 하드 드라이브 위치에 설치 자원을 작성합니다. 따라서 기본 저장 덤프가 일부 유형의 HMC 오류를 해결하는 데 필요하기 때문에 잠재적인 기본 저장 덤프 문제점을 피하려면 일정한 크기의 하드 드라이브 여유 공간을

유지하는 것이 좋습니다. 일반 기본 저장 덤프는 평균 4GB - 8GB이므로 HMC를 위한 로컬 설치 자원을 정의하고 작성하는 경우 이러한 덤프를 위해 10GB 이상의 하드 드라이브 여유 공간을 유지할 것을 고려하십시오.

- HMC 로컬 하드 드라이브에 복사할 수 있는 운영 환경을 위한 설치 매체가 있어야 합니다. 필요한 매체 유형은 설치할 운영 환경의 유형에 따라 다릅니다. CD 또는 DVD를 Red Hat 및 SLES(SUSE Linux Enterprise Server) 운영 환경의 설치 이미지 소스로 사용할 수 있습니다. 그러나 AIX 및 Virtual I/O Server 운영 환경에 대해서는 DVD만 설치 이미지 소스로 사용할 수 있습니다.

원격 NIM 서버 설치 자원을 정의하는 경우 HMC가 설치 자원에 액세스하여 사용할 수 있도록 보장하려면 여러 전제조건을 충족해야 합니다.

- 운영 환경에 필요한 전체 설치 파일 세트가 고유하게 이름 지정된 NIM 자원 그룹 내의 NIM 서버에 있어야 합니다.

  참고: AIX 및 Virtual I/O Server 운영 환경에 대해서만 원격 자원을 정의할 수 있습니다.
- 각 설치 자원이 다른 NIM 이름 지정된 자원 그룹 내에 있는 경우, 특정 운영 환경 버전 및 수정 레벨에 대해 여러 원격 설치 자원을 정의할 수 있습니다.
- NIM 서버의 완전한 호스트 이름을 알고 있어야 합니다.
- 필수 운영 환경 설치 파일 세트가 포함된 자원 그룹 이름을 알고 있어야 합니다.
- NIM 서버에 액세스할 수 있고 시스템 계획 배치 중에 운영 환경 설치 파일을 사용하도록 HMC를 설정해야 합니다. HMC는 NIM 서버에 액세스할 수 있는 SSH(Secure Shell)를 사용하여 SSH(Secure Shell) 명령을 실행할 수 있어야 합니다. 따라서, 다음 단계를 완료하여 HMC가 NIM 서버에 적절한 암호 키를 제공할 수 있도록 해야 합니다.
  1. HMC 명령 프롬프트를 열고 `ssh-keygen -t rsa -f /home/hscroot/ssh_keys` 명령을 실행하여 ssh 연결을 사용하려면 HMC에 필요한 RSA 키를 생성하고 이 키를 HMC HOME 디렉토리의 액세스 가능한 파일에 저장하십시오. 이 명령은 필요한 RSA 키를 포함하는 **ssh_keys** 및 **ssh_keys.pub**의 두 파일을 작성합니다. **ssh_keys** 파일에는 HMC가 ssh 연결을 설정하는 데 필요한 개인 키가 포함되며, 이 파일은 `/home/hscroot` 서브디렉토리에 있어야 합니다. **ssh_keys.pub** 파일에는 NIM 서버가 HMC로 ssh 연결을 완료해야 하는 개인 키가 포함됩니다.
  2. 원격 NIM 서버에서 **/home/hscroot/ssh_keys.pub** 파일의 컨텐츠를 NIM 서버의 **/.ssh/authorized_keys** 파일에 추가하거나 복사하십시오.

참고: NIM 서버에 정의된 원격 클라이언트는 파티션의 운영 환경 설치 후에도 설치 후 관리를 위해 동일한 위치에 남아 있습니다. 시스템의 짧은 호스트 이름이 이 원격 클라이언트를 식별합니다.

사용자가 HMC에 대해 정의하고 작성하는 각 설치 자원을 시스템 계획 배치 마법사의 **운영 환경 설치 사용자 정의** 단계에서 선택에 사용할 수 있습니다. 이 단계를 수행할 때 선택한 파티션에 사용하려는 설치 자원이 사용 불가능한 경우, **새 설치 자원**을 클릭하여 설치 자원 관리 창을 열어서 새 설치 자원을 정의하고 작성할 수 있습니다.

설치 자원 관리 태스크를 열려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **템플리트 및 OS 이미지**를 선택하십시오.
2. **템플리트 및 OS 이미지** 창에서 **OS 및 VIOS 이미지** 탭을 선택한 후 **설치 자원 관리**를 클릭하십시오.
3. **설치 자원 관리** 창의 사용 가능한 옵션에서 적절한 태스크를 선택하십시오.
4. 태스크를 진행하려면 **확인**을 클릭하십시오. 그렇지 않으면 **취소**를 클릭하여 태스크를 종료하십시오.

Virtual I/O Server 이미지 저장소 관리:

HMC 버전 7.7 이상에서는 HMC에서 DVD, 저장된 이미지 또는 NIM(Network Installation Management) 서버의 VIOS(Virtual I/O Server) 이미지를 저장할 수 있습니다. 저장된 VIOS 이미지는 VIOS 설치에 사용될 수 있습니다. VIOS 이미지를 설치하려면 HMC 수퍼 관리자(hmcsuperadmin) 여야 합니다.

VIOS 이미지 저장소를 관리하거나 가져오려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **템플리트 및 OS 이미지**를 선택하십시오.
2. **템플리트 및 OS 이미지** 창에서 **OS 및 VIOS 이미지** 탭을 선택한 후 **Virtual I/O Server 이미지 저장소 관리**를 클릭하십시오.
3. Virtual I/O Server 이미지 저장소 창에서 **새 Virtual I/O Server 이미지 가져오기**를 클릭하십시오.
4. 새 Virtual I/O Server 이미지 가져오기 창에서 DVD 또는 파일 시스템에서 VIOS 이미지를 가져오도록 선택하십시오.
   - DVD의 VIOS 이미지를 HMC로 가져오려면 다음 단계를 완료하십시오.
     a. Virtual I/O Server 이미지 가져오기 창에서 **관리 콘솔 DVD**를 선택하십시오.
     b. **이름** 필드에 DVD에서 가져올 VIOS 이미지 이름을 입력하십시오.
     c. **확인**을 클릭하십시오.
   - NFS(Network File System), FTP(File Transfer Protocol) 또는 SFTP(Secure Shell File Transfer Protocol)에서 VIOS 이미지를 가져오려면 다음 단계를 완료하십시오.
     a. Virtual I/O Server 이미지 가져오기 창에서 **파일 시스템**을 선택하십시오.
     b. **원격 NFS 서버**, **원격 FTP 서버** 또는 **원격 SFTP 서버**를 선택하십시오.
     c. 필요한 세부사항을 입력한 후 **확인**을 클릭하십시오.

모든 시스템 계획

시스템 계획은 단일 관리 시스템의 논리 파티션 구성에 대한 스펙입니다.

테이블에는 관리 시스템을 구성하는 데 사용될 수 있는 모든 시스템 계획이 나열되어 있습니다. 자체 시스템 계획을 작성하거나 기존 시스템 계획을 가져올 수 있습니다.

시스템 계획 작성

이 HMC(Hardware Management Console)가 관리하는 시스템에 대한 새 시스템 계획을 작성할 수 있습니다. 새 시스템 계획에는 계획을 작성하는 데 사용된 관리 시스템의 논리 파티션 및 파티션 프로파일에 대한 스펙이 포함되어 있습니다.

1. **작성**을 클릭하십시오.
2. 사용 가능한 목록에서 관리 시스템을 선택하고 **시스템 계획 이름** 및 **계획 설명** 필드를 채우십시오.
3. 원하는 옵션을 선택하십시오.
4. **작성**을 클릭하십시오.

시스템 계획 가져오기

시스템 계획 파일을 HMC(Hardware Management Console)로 가져올 수 있습니다. 새 시스템 계획에는 계획을 작성하는 데 사용된 관리 시스템의 논리 파티션 및 파티션 프로파일에 대한 스펙이 포함되어 있습니다.

1. **가져오기**를 클릭하십시오.
2. HMC로 시스템 계획 파일을 가져오기 위한 소스를 선택하십시오.
3. **가져오기**를 클릭하십시오.

시스템 계획 내보내기

시스템 계획 파일을 HMC(Hardware Management Console)에서 내보낼 수 있습니다.

1. 목록에서 시스템 계획을 선택하고 **조치** → **내보내기**를 클릭하십시오.
2. HMC로 시스템 계획 파일을 내보내기 위한 소스를 선택하십시오.
3. **내보내기**를 클릭하십시오.

시스템 계획 배치

HMC가 관리하는 하나 이상의 시스템에 시스템 계획 파일을 배치할 수 있습니다. 시스템 계획이 배치되는 관리 시스템에는 시스템 계획의 하드웨어와 동일한 하드웨어가 있어야 합니다.

1. 목록에서 시스템 계획을 선택하고 **조치** > **배치**를 클릭하십시오.
2. **시스템 계획 배치** 마법사의 지시사항을 따르십시오.

시스템 계획 삭제

HMC(Hardware Management Console)에서 시스템 계획 파일을 삭제할 수 있습니다.

1. 목록에서 시스템 계획을 선택하고 **조치** > **삭제**를 클릭하십시오.

새로 고치기

테이블을 새로 고쳐서 사용 가능한 시스템 계획에 대한 최근 변경사항을 볼 수 있습니다.

1. 최신 데이터로 테이블을 업데이트하려면 **새로 고치기**를 클릭하십시오.

이 태스크에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

사용자 및 보안 태스크

HMC에서 **사용자 및 보안** 태스크에 대해 사용 가능한 태스크를 설명합니다.

참고: 사용자 ID에 지정된 태스크 역할에 따라 사용자에게 액세스 권한이 없는 태스크가 있을 수 있습니다. 태스크 목록 및 해당 태스크에 액세스할 수 있도록 허용된 사용자 역할에 대해서는 *7* 페이지의 『HMC 태스크, 사용자 역할, ID 및 연관된 명령』의 내용을 참조하십시오.

사용자 비밀번호 변경

이 태스크를 통해 HMC에 로그온하는 데 사용되는 기존 비밀번호를 변경할 수 있습니다. 비밀번호는 콘솔에 로그인하기 위한 사용자 ID 및 사용자 권한을 확인합니다.

비밀번호를 변경하려면 다음을 수행하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **사용자 비밀번호 변경**을 클릭하십시오.
3. **사용자 비밀번호 변경** 창에서 현재 비밀번호를 지정하고 사용할 새 비밀번호를 지정한 후, 제공된 필드에 확인을 위해 새 비밀번호를 다시 지정하십시오.
4. **확인**을 클릭하여 변경을 진행하십시오.

비밀번호 변경에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

사용자 프로파일 및 액세스 관리

HMC에 로그온하는 시스템 사용자를 관리하십시오. 사용자 프로파일은 사용자 ID, 서버 인증 방법, 권한 및 텍스트 설명의 조합입니다. 권한은 사용자에게 액세스 권한이 있는 오브젝트에 대해 사용자 프로파일에 지정된 권한 레벨을 표시합니다.

사용자는 HMC에서 로컬 인증을 사용하거나 Kerberos 원격 인증을 사용하거나 LDAP 인증을 사용하여 인증될 수 있습니다. HMC에서 Kerberos 인증 설정에 대한 자세한 정보는 83 페이지의 『KDC 관리』의 내용을 참조하십시오. LDAP 인증에 대한 자세한 정보는 82 페이지의 『LDAP 관리』의 내용을 참조하십시오.

보안상의 이유로, 원격으로 인증된 Kerberos 또는 LDAP 사용자는 로컬 콘솔을 잠글 수 없습니다.

로컬 인증을 사용하는 경우 사용자 ID 및 비밀번호를 사용하여 HMC에 로그인하기 위한 사용자의 권한을 확인합니다. 사용자 ID는 영문자로 시작하고 1 - 32자로 구성되어야 합니다. 비밀번호에 적용되는 규칙은 다음과 같습니다.

- 영숫자 문자로 시작해야 합니다.
- 7자 이상을 포함해야 하지만 이 한계는 시스템 관리자가 변경할 수 있습니다.
- 문자는 표준 7비트 ASCII 문자여야 합니다.
- 비밀번호에 사용할 수 있는 올바른 문자는 A - Z, a - z, 0 - 9 및 특수 문자(~ ! @ # $ % ^ & * ( ) _ + - = { } [ ] \ : " ; ')입니다.

Kerberos 인증을 사용하는 경우 Kerberos 원격 사용자 ID를 지정하십시오.

LDAP 인증을 선택한 경우에는 추가 정보가 필요하지 않습니다.

사용자 프로파일에는 사용자에게 지정된 태스크 역할 및 관리 자원 역할이 포함됩니다. 관리 자원 역할은 관리 오브젝트 또는 오브젝트 그룹에 대한 권한을 지정하고 태스크 역할은 관리 오브젝트 또는 오브젝트 그룹에 대해 수행할 사용자의 액세스 레벨을 정의합니다. 사용 가능한 기본 관리 자원 역할, 태스크 역할 또는 **태스크 및 자원 역할 관리** 태스크를 사용하여 작성한 사용자 정의 역할의 목록에서 선택할 수 있습니다.

모든 HMC 태스크 및 각 태스크를 수행할 수 있는 사전 정의된 기본 사용자 ID의 목록에 대해서는 7 페이지의 『HMC 태스크, 사용자 역할, ID 및 연관된 명령』의 내용을 참조하십시오.

기본 관리 자원 역할은 다음과 같습니다.

- 모든 시스템 자원

기본 태스크 역할은 다음과 같습니다.

- hmcservicerep(서비스 담당자)
- hmcviewer(뷰어)
- hmcoperator(운영자)
- hmcpe(제품 엔지니어)
- hmcsuperadmin(수퍼 관리자)

사용자 프로파일을 추가하거나 사용자 정의하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **사용자 프로파일 및 액세스 관리**를 클릭하십시오.
3. 다음 단계 중 하나를 완료하십시오.
   - **사용자 프로파일** 창에서 새 사용자 ID를 작성하는 경우, 메뉴 표시줄에서 **사용자**를 가리키고 해당 메뉴가 표시되면 **추가**를 클릭하십시오. **사용자 추가** 창이 표시됩니다.
   - **사용자 프로파일** 창에서 기존 프로파일과 동일한 속성으로 사용자 ID를 작성하는 경우, 메뉴 표시줄에서 **사용자**를 가리키고 해당 메뉴가 표시되면 **복사**를 클릭하십시오. **사용자 복사** 창이 표시됩니다.

     참고: 일부 사용자 프로파일(예: 기본 ID)은 사전 정의되어 있으며 해당 권한을 변경할 수 없습니다. 그러나 기본 사용자 프로파일(예: 운영자)을 복사한 후 그 결과인 새 사용자 프로파일을 수정할 수 있습니다. 새로 정의된 사용자는 원래 복사된 사용자 프로파일보다 더 큰 권한을 가질 수 없습니다.
   - **사용자 프로파일** 창에서 사용자 ID를 삭제하는 경우, 메뉴 표시줄에서 **사용자**를 가리키고 해당 메뉴가 표시되면 **제거**를 클릭하십시오. **사용자 제거** 창이 표시됩니다.
   - **사용자 프로파일** 창에 사용자 ID가 있는 경우, 목록에서 사용자 ID를 선택한 후 메뉴 표시줄에서 **사용자**를 가리키고 해당 메뉴가 표시되면 **수정**을 클릭하십시오. **사용자 수정** 창이 표시됩니다.
     - 제한시간 및 비활성 값을 지정하려면 **사용자 수정** 창에서 **사용자 특성**을 클릭하십시오.
4. 창의 필드를 완료하거나 변경하고, 완료한 후 **확인**을 클릭하십시오.

사용자 프로파일의 작성, 수정, 복사 또는 제거와 제한시간 및 비활성 값 수정에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

사용자 프로파일 추가, 복사 또는 수정

사용자 프로파일을 추가, 복사 또는 수정하는 방법을 학습합니다.

Kerberos 또는 LDAP(Lightweight Directory Access Protocol)을 통해 원격으로 인증하는 사용자는 적절하게 설정된 프로파일이 있어야 합니다. 원격으로 인증하는 각 Kerberos 또는 LDAP 사용자의 사용자 프로파일에서 로컬 인증 대신 해당 인증 유형을 사용하도록 설정해야 합니다. Kerberos 또는 LDAP 원격 인증을 사용하도록 설정된 사용자는 HMC에 로컬로 로그인하는 경우에도 항상 해당 인증 유형을 사용합니다.

참고: Kerberos 인증을 사용하려면 **KDC 구성** 태스크를 사용하여 KDC(Key Distribution Center) 서버를 구성해야 합니다. LDAP 인증을 사용하려면 **LDAP 구성** 태스크를 사용하여 LDAP 서버를 구성해야 합니다. 모든 사용자가 Kerberos 또는 LDAP 원격 인증을 사용하도록 설정할 필요는 없습니다. 해당 사용자가 로컬 인증만 사용할 수 있도록 일부 사용자 프로파일을 설정할 수 있습니다.

사용자 프로파일 추가, 복사 또는 수정 창에서 다음 속성을 수정할 수 있습니다.

- **사용자 ID**: 작성 또는 관리할 사용자 프로파일의 사용자 ID를 입력하십시오. 사용자 이름은 영문자로 시작하고 1 - 32자로 구성되어야 합니다.
- **설명**: 사용자 자신의 레코드를 위해 의미 있는 설명을 입력하십시오.
- **비밀번호**: 사용자 ID의 비밀번호를 입력하십시오.
- **비밀번호 확인**: 확인을 위해 비밀번호를 다시 입력하십시오.
- **비밀번호 만기 일 수**: 만기되기 전에 비밀번호가 유효한 일 수를 지정하십시오. **엄격한 비밀번호 규칙 적용** 선택란이 선택된 경우 이 필드를 사용할 수 있습니다.
- **관리 자원 역할**: 현재 사용 가능한 관리 자원 역할을 표시합니다. 이 사용자 ID의 액세스 권한을 정의하려면 하나 이상의 관리 자원 역할을 선택하십시오.
- **태스크 역할**: 현재 사용 가능한 태스크 역할을 표시합니다. 이 사용자 ID에 대해 하나의 태스크 역할을 선택하십시오.

사용자 프로파일의 작성, 수정, 복사 또는 제거와 제한시간 및 비활성 값 수정에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

사용자 특성

선택한 사용자의 제한시간 및 비활성 값을 지정하는 방법을 학습합니다.

다음 제한시간 및 비활성 태스크에 대한 시간의 양을 지정할 수 있습니다.

제한시간 값

- **세션 제한시간(분)**: 로그온 세션 중에 ID 확인을 위해 사용자에게 프롬프트를 표시하는 분 수를 지정합니다. 0이 아닌 값이 지정되면 지정된 시간에 도달한 후 사용자에게 비밀번호를 다시 입력하도록 프롬프트가 표시됩니다. **확인 제한시간(분)** 필드에 지정된 시간 내에 비밀번호를 다시 입력하지 않으면 세션의 연결이 끊어집니다.
- **확인 제한시간(분)**: **세션 제한시간(분)** 필드에 값이 지정된 경우, 프롬프트가 표시될 때 사용자가 비밀번호를 입력해야 하는 시간을 지정합니다. 지정된 시간 내에 비밀번호가 다시 입력되지 않으면 세션의 연결이 끊어집니다.
- **유휴 제한시간(분)**: 사용자의 세션이 유휴 상태일 수 있는 분 수를 지정합니다. 사용자가 지정된 시간 내에 세션과 상호작용하지 않으면 세션이 잠기고 화면 보호기가 시작됩니다. 화면의 아무곳이나 클릭하면 ID 확인을 위한 프롬프트가 사용자에게 표시됩니다.
- **비밀번호 변경 간 최소 시간(일)**: 사용자의 비밀번호 변경 사이에 경과해야 하는 최소 일 수를 지정합니다.

참고: 이 필드에 0이 표시되면 만기 시간이 없음을 나타내며, 이는 기본값입니다. 최대 525600분(1년에 해당)의 값을 지정할 수 있습니다.

비활성 값

- **비활성 시 사용 안함(일)**: 사용자가 비활성 최대 일 수에 도달한 후 일시적으로 사용 안함 상태가 되는 일 수를 지정합니다.
- **비활성 시 사용 안함 상태가 되지 않음**: 사용자 세션이 비활성 때문에 사용 안함 상태가 되지 않도록 지정하는 옵션입니다.
- **웹을 통한 원격 액세스 허용**: 관리 중인 사용자가 원격 웹 서버 액세스를 사용할 수 있도록 지정하는 옵션입니다.

사용자 및 태스크 관리

로그온한 사용자 및 해당 사용자가 실행 중인 태스크를 표시하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **사용자 및 태스크 관리**를 클릭하십시오.
3. 사용자 및 태스크 관리 창에 다음 정보가 표시됩니다.
   - 로그인한 사용자
   - 사용자가 로그인한 시간
   - 실행 중인 태스크 수
   - 사용자의 액세스 위치
   - 실행 중인 태스크에 대한 정보:
     - 태스크 ID
     - 태스크 이름
     - 대상(있는 경우)
     - 세션 ID
4. **로그온한 사용자** 목록에서 세션을 선택한 후 **로그오프** 또는 **연결 끊기**를 클릭하여 현재 실행 중인 세션에서 로그오프하거나 연결을 끊도록 선택하십시오.

   또는 **실행 중인 태스크** 목록에서 태스크를 선택한 후 **다음으로 전환** 또는 **종료**를 클릭하여 다른 태스크로 전환하거나 태스크를 종료하도록 선택할 수 있습니다.
5. 이 태스크를 완료한 후 **닫기**를 클릭하십시오.

태스크 및 자원 역할 관리

사용자 역할을 정의하고 사용자 정의하려면 이 태스크를 사용하십시오.

참고: 사전 정의된 역할(기본 역할)은 수정할 수 없습니다.

사용자 역할은 권한의 콜렉션입니다. 사용자 역할은 지정된 사용자 클래스에 허용되는 태스크 세트(태스크 역할)를 정의하도록 작성되거나 사용자가 관리할 수 있는 관리 오브젝트 세트(관리 자원 역할)를

정의하도록 작성될 수 있습니다. 사용자 역할을 정의하거나 사용자 정의하면 **사용자 프로파일 및 액세스 관리** 태스크를 사용하여 고유의 권한을 갖는 새 사용자를 작성할 수 있습니다.

사전 정의된 관리 자원 역할은 다음과 같습니다.
- 모든 시스템 자원

사전 정의된 태스크 역할은 다음과 같습니다.
- hmcservicerep(서비스 담당자)
- hmcviewer(뷰어)
- hmcoperator(운영자)
- hmcpe(제품 엔지니어)
- hmcsuperadmin(수퍼 관리자)

관리 자원 역할 또는 태스크 역할을 사용자 정의하려면 다음을 수행하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **태스크 및 자원 역할 관리**를 클릭하십시오.
3. **태스크 및 자원 역할 관리** 창에서 **관리 자원 역할** 또는 **태스크 역할**을 선택하십시오.
4. 역할을 추가하려면 메뉴 표시줄에서 **편집**을 클릭한 후 **추가**를 클릭하여 새 역할을 작성하십시오.

   또는

   기존 역할을 복사, 제거 또는 수정하려면 사용자 정의할 오브젝트를 선택하고 메뉴 표시줄에서 **편집**을 클릭한 후 **복사**, **제거** 또는 **수정**을 클릭하십시오.
5. 태스크를 완료한 후 **종료**를 클릭하십시오.

관리 자원 역할 및 태스크 역할 사용자 정의에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

인증서 관리

HMC에서 사용되는 인증서를 관리하려면 이 태스크를 사용하십시오. 이 태스크는 콘솔에서 사용되는 인증서에 대한 정보를 가져올 수 있는 기능을 제공합니다. 이 태스크를 사용하여 콘솔에서 사용할 새 인증서를 작성하고 인증서의 특성 값을 변경하고 기존 및 아카이브된 인증서 또는 서명 인증서에 대해 작업할 수 있습니다.

HMC에 대한 모든 원격 브라우저 액세스는 SSL(Secure Sockets Layer) 암호화를 사용해야 합니다. HMC에 대한 모든 원격 액세스에는 SSL 암호화가 필요하고 이 암호화에 대한 키를 제공하려면 인증서가 필요합니다. HMC는 이 암호화가 발생할 수 있는 자체 서명된 인증서를 제공합니다.

참고:

HMC의 자체 서명된 인증서는 2048비트 RSA 암호화를 사용합니다. 인증 기관(CA) 서명 인증서를 사용하는 경우에는 2048비트 암호화를 사용해야 합니다. 다음 단계를 완료하고 CA에서 서명을 선택하여 CA에서 서명한 새 2048비트 인증서를 작성할 수 있습니다.

인증서를 관리하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **인증서 관리**를 클릭하십시오.
3. 인증서에 대해 수행할 조치는 **인증서 관리** 창의 메뉴 표시줄을 사용하십시오.
   - 콘솔에 대한 새 인증서를 작성하려면 **작성**을 클릭한 후 **새 인증서**를 선택하십시오. 인증서를 자체 서명할 것인지 또는 인증 기관(CA)의 서명을 받을 것인지를 결정한 후 **확인**을 클릭하십시오.
   - 자체 서명된 인증서의 특성 값을 수정하려면 **선택됨**을 클릭한 후 **수정**을 선택하십시오. 적절하게 변경한 후 **확인**을 클릭하십시오.
   - 기존 및 아카이브된 인증서 또는 서명 인증서에 대해 작업하려면 **고급**을 클릭하십시오. 그런 다음, 다음 옵션을 선택할 수 있습니다.
     - 기존 인증서 삭제
     - 아카이브된 인증서에 대해 작업
     - 인증서 가져오기
     - 발행자 인증서 보기
4. 모든 변경사항을 적용하려면 **적용**을 클릭하십시오.

인증서 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

인증서 폐기 목록 관리

이 태스크를 사용하여 HMC(Hardware Management Console)에서 사용되는 인증서 폐기 목록을 작성, 수정, 삭제하고 이를 가져올 수 있습니다.

HMC에 액세스 중인 모든 원격 브라우저는 SSL(Secure Sockets Layer) 암호화를 사용해야 합니다. 이 암호화에 대한 키를 제공하려면 인증서가 필요합니다. HMC는 이 암호화가 발생할 수 있는 자체 서명된 인증서를 제공합니다.

인증서 폐기 목록을 관리하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.

2. 컨텐츠 분할창에서 **인증서 폐기 목록 관리**를 클릭하십시오.
3. 인증서로 수행할 조치에 대해 **인증서 폐기 목록 관리** 창의 메뉴 표시줄을 사용하십시오.
   - 콘솔에 대해 새 인증서 폐기 목록을 작성하려면 **가져오기**를 클릭한 후 **새 CRL**을 선택하십시오. 인증서 폐기 목록을 콘솔의 이동식 매체에서 가져오는지 또는 웹 브라우저를 실행 중인 시스템의 파일 시스템에서 가져오는지 여부를 판별하십시오.

     참고: 이동식 매체에서 목록을 가져오는 경우에는 인증서 폐기 목록 파일이 매체의 맨 위 디렉토리에 있어야 합니다.
   - 콘솔에서 인증서 폐기 목록을 수정하려면 테이블에서 인증서 폐기 목록을 선택하고 이를 알맞게 변경한 후 **적용**을 클릭하십시오.
   - 콘솔에서 인증서 폐기 목록을 삭제하려면 **선택됨**을 클릭한 후 **CRL 삭제**를 클릭하십시오. 인증서 폐기 목록을 선택한 후 **확인**을 클릭하십시오.
   - 기존 및 아카이브된 인증서 또는 서명 인증서에 대해 작업하려면 **고급**을 클릭하십시오.

인증서 폐기 목록의 관리에 대한 추가 정보가 필요하면 온라인 도움말을 사용하십시오.

LDAP 관리

LDAP(Lightweight Directory Access Protocol) 인증을 사용하도록 HMC를 구성하십시오.

참고: LDAP 인증을 사용하도록 HMC를 구성하기 전에 HMC와 LDAP 서버 사이에 작동 중인 네트워크 연결이 있는지 확인해야 합니다.

LDAP(Lightweight Directory Access Protocol) 인증을 사용하도록 HMC를 구성하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **시스템 및 콘솔 보안**을 선택하십시오.
2. 컨텐츠 분할창에서 **LDAP 관리**를 클릭하십시오. **LDAP 서버 정의** 창이 열립니다.
3. **LDAP 사용**을 선택하십시오.
4. 인증에 사용할 LDAP 서버를 정의하십시오(예: Microsoft Active Directory, Tivoli® 및 Open LDAP).
5. 인증된 사용자를 식별하는 데 사용되는 LDAP 속성을 정의하십시오. 기본값은 **uid**지만 사용자 자신의 속성을 사용할 수 있습니다. Microsoft Active Directory의 경우, **sAMAccountName**을 속성으로 사용하십시오.
6. LDAP 서버의 식별 이름 트리(검색 기반이라고도 함)를 정의하십시오.
7. **확인**을 클릭하십시오.

LDAP 인증을 사용하려면 로컬 인증 대신 LDAP 원격 인증을 사용하도록 각 원격 사용자의 프로파일을 구성해야 합니다.

KDC 관리

Kerberos 원격 인증을 위해 HMC(Hardware Management Console)에서 사용되는 KDC(Key Distribution Center) 서버를 보십시오.

이 태스크에서 다음을 수행할 수 있습니다.

- 기존 KDC 서버 보기
- 영역, 티켓 수명 및 클럭 오차를 포함한 기존 KDC 서버 매개변수 수정
- HMC에서 KDC 서버 추가 및 구성
- KDC 서버 제거
- 서비스 키 가져오기
- 서비스 키 제거

Kerberos는 비밀 키 암호화를 사용하여 클라이언트/서버 애플리케이션에 대한 강력한 인증을 제공하도록 설계된 네트워크 인증 프로토콜입니다.

Kerberos를 기반으로 클라이언트(일반적으로 사용자 또는 서비스)는 KDC로 티켓에 대한 요청을 보냅니다. KDC는 클라이언트에 대한 TGT(Ticket-Granting Ticket)를 작성하고 클라이언트의 비밀번호를 키로 사용하여 암호화한 후 암호화된 TGT를 다시 클라이언트로 전송합니다. 그러면 클라이언트는 비밀번호를 사용하여 TGT 복호화를 시도합니다. 성공적으로 TGT를 복호화하면(즉, 클라이언트가 올바른 비밀번호를 제공한 경우) 클라이언트는 클라이언트의 ID를 증명하는 복호화된 TGT를 보관합니다.

티켓은 사용 가능한 기간이 정해져 있습니다. Kerberos를 사용하려면 관련 호스트의 클럭이 동기화되어야 합니다. HMC 클럭이 KDC 서버의 클럭과 동기화되지 않으면 인증은 실패합니다.

Kerberos 영역은 Kerberos 원격 인증을 사용하는 관리 도메인, 사이트 또는 논리 네트워크입니다. 각 영역은 해당 영역의 사용자 및 서비스에 대한 정보를 포함하고 KDC 서버에 저장되어 있는 마스터 Kerberos 데이터베이스를 사용합니다. 또한 영역에는 해당 영역에 대한 마스터 Kerberos 데이터베이스의 사본을 읽기 전용으로 저장하고 있는 하나 이상의 슬레이브 KDC 서버가 있을 수 있습니다.

KDC 위조를 방지하기 위해 서비스 키를 사용하여 KDC에 인증하도록 HMC를 구성할 수 있습니다. 서비스 키 파일은 키 탭이라고도 합니다. Kerberos는 요청된 TGT가 HMC에 대한 서비스 키 파일을 발행한 KDC와 동일한 KDC에서 발행되었는지 확인합니다. 서비스 키 파일을 HMC로 가져오기 전에 HMC 클라이언트의 호스트 프린시펄에 대한 서비스 키를 생성해야 합니다.

참고: MIT Kerberos V5 *nix 배포의 경우, KDC에서 `kadmin` 유틸리티를 실행하고 `ktadd` 명령을 사용하여 서비스 키 파일을 작성하십시오. 다른 Kerberos 구현에서는 다른 프로세스를 사용하여 서비스 키를 작성해야 할 수 있습니다.

다음 소스 중 하나에서 서비스 키 파일을 가져올 수 있습니다.

- HMC에 현재 마운트되어 있는 이동식 매체(예: 광 디스크 또는 USB 대용량 스토리지 장치). 이 옵션을 HMC에서 원격이 아닌 로컬로 사용해야 하며 이 옵션을 사용하기 전에 이동식 매체를 HMC에 마운트해야 합니다.
- 보안 FTP를 사용하는 원격 사이트. SSH가 설치되어 실행 중인 원격 사이트에서 서비스 키 파일을 가져올 수 있습니다.

이 HMC에서 Kerberos 원격 인증을 사용하려면 다음을 완료하십시오.

- HMC에서 NTP(Network Time Protocol) 서비스를 사용으로 설정하고 동일한 NTP 서버에 대해 시간을 동기화하도록 HMC와 KDC 서버를 설정해야 합니다. **HMC 관리** 아이콘  에서 63 페이지의 『날짜 및 시간 변경』 태스크에 액세스하고 **콘솔 설정**을 선택하여 HMC에서 NTP 서비스를 사용으로 설정할 수 있습니다.
- 로컬 인증 대신 Kerberos 원격 인증을 사용하도록 각 원격 사용자의 사용자 프로파일을 설정해야 합니다. Kerberos 원격 인증을 사용하도록 설정된 사용자는 HMC에 로컬로 로그인한 경우에도 항상 Kerberos 원격 인증을 사용합니다.

  참고: 모든 사용자가 Kerberos 원격 인증을 사용하도록 설정할 필요는 없습니다. 해당 사용자가 로컬 인증만 사용할 수 있도록 일부 사용자 프로파일을 설정할 수 있습니다.
- 서비스 키 파일 사용은 선택사항입니다. 서비스 키 파일을 사용하기 전에 해당 파일을 HMC로 가져와야 합니다. 서비스 키가 HMC에 설치되는 경우, 영역 이름은 네트워크 도메인 이름과 같아야 합니다. 다음은 HMC 호스트 이름을 hmc1, DNS 도메인을 example.com, Kerberos 영역 이름을 EXAMPLE.COM이라고 가정할 때 kadmin.local 명령을 사용하여 Kerberos 서버에 서비스 키 파일을 작성하는 예제입니다.

  – `# kadmin_local kadmin.local: ktadd -k /etc/krb5.keytab host/hmc1.example.com@EXAMPLE.COM`

  Kerberos 서버에서 Kerberos ktutil 사용하여 서비스 키 파일 컨텐츠를 확인하십시오. 출력은 다음과 유사합니다.

  –
```
# ktutil

ktutil:  rkt /etc/krb5.keytab

ktutil: l

slot KVNO Principal

---- ---- ---------------------------------------------------------------------

 1    9      host/hmc1.example.com@EXAMPLE.COM

 2    9      host/hmc1.example.com@EXAMPLE.COM
```

- GSSAPI를 사용하여 비밀번호를 사용하지 않고 SSH(Secure Shell) 로그인을 수행할 수 있도록 HMC Kerberos 구성을 수정할 수 있습니다. 비밀번호를 사용하지 않고 Kerberos를 통해 HMC에 원격으로 로그인하려면 서비스 키를 사용하도록 HMC를 구성하십시오. 구성이 완료되면 `kinit -f` 프린시펄을 사용하여 원격 Kerberos 클라이언트 시스템에 전달 가능한 신임 정보를 확보하십시오. 그런 다음, 다음 명령을 실행하여 비밀번호를 입력하지 않고 HMC에 로그인하십시오. `$ ssh -o PreferredAuthentications=gssapi-with-mic` *user@host*

KDC를 관리하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **KDC 관리**를 클릭하십시오.
3. **KDC 관리** 창의 **조치** 드롭 다운 목록 아래에 있는 사용 가능한 옵션에서 적절한 태스크를 선택하십시오.
4. 태스크를 완료한 후 **확인**을 클릭하십시오.

KDC 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

KDC 서버 보기

HMC(Hardware Management Console)에서 기존 KDC(Key Distribution Center) 서버를 표시합니다.

HMC에서 기존 KDC 서버를 보려면 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오. 컨텐츠 분할창에서 **KDC 구성**을 클릭하십시오. 서버가 없고 NTP가 아직 사용으로 설정되지 않은 경우 경고 패널 메시지가 표시됩니다. HMC의 NTP 서비스를 사용으로 설정하고 원하는 대로 새 KDC 서버를 구성하십시오.

KDC 서버 수정

HMC(Hardware Management Console)에서 KDC(Key Distribution Center)를 수정하는 방법을 학습합니다.

기존 KDC(Key Distribution Center) 서버 매개변수를 수정하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **KDC 관리**를 클릭하십시오.

3. KDC 서버를 선택하십시오.
4. 수정할 값을 선택하십시오.
   - **영역**. 영역은 인증 관리 도메인입니다. 일반적으로 영역은 항상 대문자로 표시됩니다. DNS 도메인과 동일한 영역 이름(대문자)을 작성하는 것이 좋습니다. 사용자는 사용자가 영역의 인증 서버와 키를 공유하는 경우에만 해당 영역에 속합니다. 서비스 키 파일이 HMC에 설치된 경우 영역 이름은 네트워크 도메인 이름과 동일해야 합니다.
   - **티켓 수명**. 티켓 수명은 신임 정보의 수명을 설정합니다. 형식은 정수 뒤에 **s**(초), **m**(분), **h**(시간) 또는 **d**(일)가 지정됩니다. Kerberos 수명 문자열(예: *2d4h10m*)을 입력하십시오.
   - **클럭 오차**. 클럭 오차는 Kerberos가 메시지를 올바르지 않다고 간주하기 전에 HMC와 KDC 서버 사이에서 허용 가능한 최대 클럭 오차 크기를 설정합니다. 형식은 초 수를 나타내는 정수입니다.
5. **확인**을 클릭하십시오.

KDC 서버 추가

이 HMC(Hardware Management Console)에 KDC(Key Distribution Center) 서버를 추가하십시오.

새 KDC 서버를 추가하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **KDC 관리**를 클릭하십시오.
3. **조치** 드롭 다운 목록에서 **KDC 서버 추가**를 선택하십시오.
4. KDC 서버의 호스트 이름 또는 IP 주소를 입력하십시오.
5. KDC 서버 영역을 입력하십시오.
6. **확인**을 클릭하십시오.

KDC 서버 제거

HMC(Hardware Management Console)에서 Kerberos 인증은 모든 KDC(Key Distribution Center) 서버가 제거될 때까지 사용되는 상태로 남아 있습니다.

KDC 서버를 제거하려면 다음을 수행하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **KDC 관리**를 클릭하십시오.
3. 목록에서 KDC 서버를 선택하십시오.

4. **조치** 드롭 다운 목록에서 **KDC 서버 제거**를 선택하십시오.
5. **확인**을 클릭하십시오.

서비스 키 가져오기

서비스 키 파일을 HMC(Hardware Management Console)로 가져오려면 우선 서비스 파일이 HMC 호스트를 위한 Kerberos 서버에 작성되어야 합니다. 서비스 키 파일은 HMC 클라이언트의 호스트 프린시펄(예: `host/example.com@EXAMPLE.COM`)을 포함합니다. KDC 인증 외에 호스트 서비스 키 파일은 GSSAPI를 사용하여 비밀번호 없는 SSH(Secure Shell) 로그인을 사용으로 설정하는 데 사용됩니다.

참고: MIT Kerberos V5 *nix 배포의 경우, KDC에서 `kadmin` 유틸리티를 실행하고 `ktadd` 명령을 사용하여 서비스 키 파일을 작성하십시오. 다른 Kerberos 구현에서는 다른 프로세스를 사용하여 서비스 키를 작성해야 할 수 있습니다.

서비스 키를 가져오려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **KDC 관리**를 클릭하십시오.
3. **조치** 드롭 다운 목록에서 **서비스 키 가져오기**를 선택하십시오.
4. 다음 중 하나에서 선택하십시오.
   - **로컬** - 서비스 키가 HMC에 현재 마운트되어 있는 이동식 매체에 있어야 합니다. 이 옵션을 HMC에서 원격이 아닌 로컬로 사용해야 하며 이 옵션을 사용하기 전에 이동식 매체를 HMC에 마운트해야 합니다. 매체에 서비스 키 파일의 전체 경로를 지정하십시오.
   - **원격** - 서비스 키가 보안 FTP를 통해 HMC에서 사용 가능한 원격 사이트에 있어야 합니다. SSH(Secure Shell)가 설치되어 실행 중인 원격 사이트에서 서비스 키 파일을 가져올 수 있습니다. 원격 사이트에 사이트의 호스트 이름, 사이트에 대한 사용자 ID 및 비밀번호, 서비스 키 파일의 전체 경로를 지정하십시오.
5. **확인**을 클릭하십시오.

HMC가 다시 부팅될 때까지 서비스 키 파일의 구현은 적용되지 않습니다.

서비스 키 제거

HMC(Hardware Management Console)에서 서비스 키를 제거하는 방법을 학습합니다.

HMC에서 서비스 키를 제거하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.

2. 컨텐츠 분할창에서 **KDC 관리**를 클릭하십시오.
3. **조치** 드롭 다운 목록에서 **서비스 키 제거**를 선택하십시오.
4. **확인**을 클릭하십시오.

서비스 키를 제거한 후 HMC를 다시 부팅해야 합니다. 다시 부팅에 실패하면 로그인 오류가 발생할 수 있습니다.

원격 명령 실행 사용

이 태스크는 ssh 기능을 사용하여 원격 명령 실행을 사용으로 설정하는 데 사용됩니다.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **원격 명령 실행 사용**을 클릭하십시오.
3. **원격 명령 실행 사용** 창에서 **ssh 기능을 사용하여 원격 명령 실행 사용**을 선택하십시오.
4. **확인**을 클릭하십시오.

원격 조작 사용

이 태스크는 웹 브라우저를 통해 원격 워크스테이션에서 HMC에 액세스할 수 있도록 허용하는 데 사용됩니다.

HMC 원격 액세스를 사용하려면 다음을 수행하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **원격 조작 사용**을 클릭하십시오.
3. 원격 조작 드롭 다운 목록에서 **사용**을 선택한 후 **확인**을 클릭하십시오. 웹 브라우저를 사용하여 원격 워크스테이션에서 HMC에 액세스할 수 있습니다.

HMC에 대한 원격 액세스 허용에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

원격 가상 터미널 사용

원격 가상 터미널 연결은 다른 원격 HMC에서 논리 파티션으로의 터미널 연결입니다. 원격 클라이언트에 대한 원격 가상 터미널 액세스를 사용으로 설정하려면 이 태스크를 사용하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **원격 가상 터미널 사용**을 클릭하십시오.

3. **원격 가상 터미널 사용** 창에서 원격 가상 터미널 연결 사용을 선택하여 이 태스크를 사용할 수 있습니다.
4. **확인**을 클릭하여 변경사항을 활성화하십시오.

원격 터미널 연결 사용에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

서비스 가능성 태스크

HMC에서 **서비스 가능성** 태스크에 대해 사용 가능한 태스크를 설명합니다.

참고: 사용자 ID에 지정된 태스크 역할에 따라 사용자에게 액세스 권한이 없는 태스크가 있을 수 있습니다. 태스크 목록 및 해당 태스크에 액세스할 수 있도록 허용된 사용자 역할에 대해서는 7 페이지의 『HMC 태스크, 사용자 역할, ID 및 연관된 명령』의 내용을 참조하십시오.

태스크 로그

현재 실행 중이거나 HMC(Hardware Management Console)에서 완료된 모든 태스크를 보십시오.

태스크 로그를 보려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **태스크 로그**를 선택하십시오.
2. 태스크 로그에서 다음 탭을 볼 수 있습니다.
   - 태스크 이름: 태스크의 이름을 표시합니다.
   - 상태: 태스크의 현재 상태(실행 중 또는 완료됨)를 표시합니다.
   - 자원: 자원의 이름을 표시합니다.
   - 자원 유형: 자원의 유형을 표시합니다.
   - 이니시에이터: 태스크를 시작한 사용자의 이름을 표시합니다.
   - 시작 시간: 태스크가 시작된 시간을 표시합니다.
   - 기간: 태스크를 완료하는 데 걸린 시간을 표시합니다.

태스크 로그 보기에 대한 추가 정보는 온라인 도움말을 사용하십시오.

콘솔 이벤트 로그

HMC(Hardware Management Console)에서 발생하는 시스템 이벤트의 레코드를 보십시오. 시스템 이벤트는 프로세스가 발생하고 시작 및 종료하고 성공 또는 실패할 때 표시되는 개별 활동입니다.

콘솔 이벤트 로그를 보려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **콘솔 이벤트 로그**를 선택하십시오.

2. 다른 시간 범위로 변경하거나 이벤트가 요약에 표시되는 방법을 변경하려면 메뉴 표시줄을 사용하십시오. 또한 테이블 도구 모음의 **조치 선택** 메뉴 또는 테이블 아이콘을 사용하여 여러 가지로 변형된 테이블을 표시할 수 있습니다.
3. 이벤트 보기를 완료하였으면 메뉴 표시줄에서 **보기**를 선택한 후 **종료**를 클릭하십시오.

HMC 이벤트 보기에 대한 추가 정보는 온라인 도움말을 사용하십시오.

서비스 가능 이벤트 관리자

이 태스크를 사용하여 보려는 서비스 가능 이벤트 세트의 기준을 선택할 수 있습니다. 기준 선택을 완료하면 지정된 기준과 일치하는 서비스 가능 이벤트를 볼 수 있습니다.

보려는 서비스 가능 이벤트의 기준을 설정하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 가능 이벤트 관리자**를 선택하십시오.
2. **서비스 가능 이벤트 관리자** 창에서 이벤트 기준, 오류 기준 및 FRU 기준을 제공하십시오.
3. 보려는 서비스 가능 이벤트에 대해 원하는 기준을 지정하였으면 **확인**을 클릭하십시오.

이벤트 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

콜홈에 대한 이벤트 관리자

이 태스크를 사용하여 HMC에서 IBM으로 전송 중인 모든 데이터를 모니터하고 승인할 수 있습니다.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **콜홈에 대한 이벤트 관리자**를 선택하십시오.
2. **콜홈에 대한 이벤트 관리자** 창에서 **콘솔 관리**를 선택하여 등록된 관리 콘솔의 목록을 관리할 수 있습니다. **이벤트 기준**을 사용하여 승인 상태, 상태 및 원래 HMC를 지정함으로써 등록된 모든 관리 콘솔에 대해 사용 가능한 이벤트의 목록을 필터링할 수 있습니다. 기준을 사용하여 보기를 필터링할 수 있으며, 세부사항을 보고 파일을 보고 콜홈 조작을 수행할 이벤트를 선택할 수 있습니다.
3. **확인**을 클릭하여 콜홈에 대한 이벤트 관리자를 종료하고 필터 값을 저장하십시오.

이 태스크에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

서비스 가능 이벤트 작성

이 태스크는 HMC(Hardware Management Console)에서 발생한 문제점(예: 마우스가 작동하지 않음)을 서비스 제공자에게 보고하거나 사용자가 문제점 보고를 테스트할 수 있도록 합니다.

문제점 제출은 원격 지원 기능(RSF)을 사용하도록 이 Hardware Management Console을 사용자 정의했는지 여부와 이 Hardware Management Console에 서비스를 자동으로 호출할 수 있는 권한이 있는지 여부에 따라 달라집니다. 해당하는 경우 문제점 정보 및 서비스 요청이 모뎀 전송을 통해 서비스 제공자에게 자동으로 전송됩니다.

Hardware Management Console에 대한 문제점을 보고하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **서비스 가능 이벤트 작성**을 클릭하십시오.
3. **서비스 가능 이벤트 작성** 창에 표시된 목록에서 문제점 유형을 선택하십시오.
4. **문제점 설명** 입력 필드에 문제점에 대한 간략한 설명을 입력한 후 **서비스 요청**을 클릭하십시오.

문제점 보고 창에서 문제점 보고를 테스트하려면 다음을 수행하십시오.

1. **자동 문제점 보고 테스트**를 선택하고 **문제점 설명** 입력 필드에 테스트임을 입력하십시오.
2. **서비스 요청**을 클릭하십시오. 문제점이 Hardware Management Console의 서비스 제공자에게 보고됩니다. 문제점을 보고할 때 **문제점 보고** 창에 사용자가 제공하는 정보와 콘솔을 식별하는 시스템 정보가 서비스 제공자에게 전송됩니다.

문제점 보고 또는 문제점 보고 작동 여부 테스트에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

원격 연결 관리

HMC(Hardware Management Console)에서 원격 연결을 관리하는 방법을 학습합니다.

참고: 이 태스크를 사용하려면 HMC의 콜홈 서버 서비스를 사용으로 설정해야 합니다.

HMC는 원격 연결을 자동으로 관리합니다. HMC는 요청을 큐에 넣고 수신한 순서에 따라 처리합니다. 그러나 이 태스크를 사용하면 필요한 경우 큐를 수동으로 관리할 수 있습니다. 전송을 중지하거나 우선순위 요청을 다른 요청 앞으로 이동하거나 요청을 삭제할 수 있습니다.

원격 연결을 관리하려면 다음을 수행하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **원격 연결 관리**를 클릭하십시오.
3. **원격 연결 관리** 창에 전송 중인 요청의 목록과 전송 대기 중인 요청의 목록이 표시됩니다. 각 목록에서 요청을 선택하고 메뉴 표시줄에서 **옵션**을 클릭하여 사용 가능한 옵션을 표시할 수 있습니다. 옵션을 통해 다음을 수행할 수 있습니다.
   - 선택된 요청에 우선순위 지정(해당 요청을 큐의 맨 위로 이동)

- 선택된 요청 취소
- 모든 활성 요청(전송 중인 요청) 취소
- 모든 대기 중인 요청 취소
- 큐 보류(현재 활성 요청을 완료한 후 큐를 보류 상태로 설정)
- 큐 해제
- 창 닫기 및 종료

원격 연결 수동 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

원격 지원 요청 관리

HMC(Hardware Management Console)가 제출한 콜홈 요청을 보거나 관리하는 방법을 학습합니다.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **원격 지원 요청 관리**를 클릭하십시오.
3. **원격 지원 요청 관리** 창에 활성 요청 목록과 대기 중인 요청 목록이 표시됩니다. 각 목록에서 요청을 선택하고 메뉴 표시줄에서 **옵션**을 클릭하여 사용 가능한 옵션을 표시할 수 있습니다. 옵션을 통해 다음을 수행할 수 있습니다.
   - 모든 콜홈 서버 보기
   - 선택된 요청 취소
   - 모든 활성 요청 취소
   - 모든 대기 중인 요청 취소
   - 창 닫기 및 종료

원격 연결 수동 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

덤프 관리

HMC(Hardware Management Console)에서 선택된 시스템의 덤프 프로시저를 관리하는 방법을 학습합니다.

덤프를 관리하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **덤프 관리**를 클릭하십시오.
3. **덤프 관리** 창에서 덤프를 선택하고 다음 덤프 관련 태스크 중 하나를 수행하십시오.

   메뉴 표시줄의 **선택됨**에서는 다음을 수행할 수 있습니다.
   - 덤프를 매체에 복사합니다.
   - 덤프를 원격 시스템에 복사합니다.

- 콜홈을 사용하여 덤프를 서비스 제공자에게 전송합니다.
- 덤프를 삭제합니다.

메뉴 표시줄의 **조치**에서는 다음을 수행할 수 있습니다.
- 관리 시스템에 대해 하드웨어 및 서버 펌웨어의 덤프를 시작합니다.
- 서비스 프로세서의 덤프를 시작합니다.
- 대용량 전원 제어 서비스 프로세서의 덤프를 시작합니다.
- 덤프 유형에 대한 덤프 기능 매개변수를 수정합니다.

메뉴 표시줄의 **상태**에서는 덤프의 오프로드 진행 상태를 볼 수 있습니다.

4. 이 태스크를 완료한 후 **확인**을 클릭하십시오.

덤프 관리에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

서비스 정보 전송

서비스 제공자에게 즉시 서비스 정보를 전송하거나, 문제점 판별에 사용할 서비스 정보를 전송하는 시점을 스케줄합니다.

서비스 정보를 스케줄하거나 전송하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **서비스 정보 전송**을 클릭하십시오.
3. 컨텐츠 분할창에서 **데이터 스케줄 및 전송** 탭을 클릭하여 서비스 정보를 스케줄하십시오.

   참고: 또한 다음 탭을 클릭하여 전송할 데이터를 선택하고 FTP 연결을 구성하십시오.
   - **데이터 스케줄 및 전송**: 정보를 서비스 제공자에게 즉시 전송하거나 전송을 스케줄하십시오.
   - **FTP 연결 구성**: FTP를 사용하여 서비스 정보를 오프로드할 수 있도록 구성 데이터를 제공하십시오.
   - **문제점 보고서 전송**: 원하는 데이터와 데이터의 목적지를 선택하십시오.
4. 원하는 서비스 전송 유형을 정기적 전송 사용 또는 즉시 전송으로 선택하십시오.
   - **작동 테스트(하트비트) 정보 -- 항상 사용**: 문제점 이벤트 로그 파일을 전송합니다.
   - **하드웨어 서비스 정보(VPD)**: 이 HMC에 연결된 모든 관리 시스템의 VPD(Vital Product Data)를 전송합니다.
   - **소프트웨어 서비스 정보**: 파티션에서 실행 중인 모든 소프트웨어의 VPD를 전송합니다.
   - **성능 관리 정보**: 성능 관리 정보를 수집하여 전송합니다.
   - **액세스 키 정보 업데이트**: 액세스 키 정보를 확인하고 업데이트합니다.
5. 반복 전송을 스케줄할 간격(일) 및 시간을 선택하십시오. 정보를 즉시 전송하려면 **지금 전송**을 클릭하십시오.

6. **확인**을 클릭하십시오.

서비스 정보 스케줄에 대한 추가 정보는 온라인 도움말을 사용하십시오.

매체 포맷

이 태스크는 디스켓 또는 USB 2.0 플래시 드라이브 메모리 키를 포맷합니다.

사용자 지정 레이블을 공급하여 디스켓을 포맷할 수 있습니다.

디스켓 또는 USB 2.0 플래시 드라이브 메모리 키를 포맷하려면 다음을 수행하십시오.

1. 탐색 영역에서 **HMC 관리** 아이콘  을 클릭한 후 **콘솔 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **매체 포맷**을 클릭하십시오.
3. **매체 포맷** 창에서 포맷하려는 매체의 유형을 선택한 후 **확인**을 클릭하십시오.
4. 매체가 올바르게 삽입되었는지 확인한 후 **포맷**을 클릭하십시오. **매체 포맷** 진행 창이 표시됩니다. 매체가 포맷되면 **매체 포맷 완료** 창이 표시됩니다.
5. **확인**을 클릭한 후 **닫기**를 클릭하여 태스크를 종료하십시오.

디스켓 또는 USB 2.0 플래시 드라이브 메모리 키 포맷에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

Electronic Service Agent 설정 마법사

HMC(Hardware Management Console) 인터페이스를 사용하여 Electronic Service Agent 설정 마법사를 여는 방법을 학습합니다.

Electronic Service Agent 설정 마법사를 열려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Electronic Service Agent 설정 마법사**를 선택하십시오. Electronic Service Agent 마법사가 열립니다. 마법사의 지시사항에 따라 콜홈 태스크를 구성하십시오.

사용자 권한 부여

Electronic Service Agent에 대한 권한을 요청하십시오. Electronic Service Agent는 시스템을 사용자 ID와 연관시키고 Electronic Service Agent 기능을 통해 시스템 정보에 액세스할 수 있도록 허용합니다. 이 등록은 사용자의 운영 체제에서 AIX 또는 IBM i 운영 체제에 대한 서비스 프로세스를 자동화하는 경우에도 사용됩니다.

사용자 ID를 등록하려면 다음을 수행하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **사용자 권한 부여**를 클릭하십시오.
3. Electronic Service Agent에 등록된 사용자 ID를 제공하십시오. 사용자 ID가 필요한 경우, IBM 등록 웹 사이트(*https://www.ibm.com/account/profile*)에서 등록할 수 있습니다.
4. **확인**을 클릭하십시오.

eService 웹 사이트에 고객 사용자 ID를 등록하기 위한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

Electronic Service Agent 사용

이 태스크를 사용하여 관리 시스템의 콜홈 상태를 사용 또는 사용 안함으로 설정할 수 있습니다.

참고: 사용자 정의 가능 데이터 복제가 **데이터 복제 관리** 태스크를 통해 이 HMC에서 **사용**으로 설정된 경우, 이 태스크에 지정된 데이터는 네트워크에 구성된 다른 HMC의 자동 복제에 따라 변경될 수 있습니다. 데이터 복제에 대한 자세한 정보는 69 페이지의 『데이터 복제 관리』의 내용을 참조하십시오.

관리 시스템의 콜홈 상태를 사용으로 설정하면 서비스 가능 이벤트가 발생하는 경우 콘솔이 서비스 센터에 자동으로 접속합니다. 관리 시스템이 사용 안함으로 설정되면 서비스 담당자가 서비스 가능 이벤트에 대한 알림을 받지 못합니다.

시스템의 콜홈을 관리하려면 다음을 수행하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **Electronic Service Agent 사용**을 클릭하십시오.
3. **Electronic Service Agent 사용** 창에서 콜홈 상태를 사용 또는 사용 안함으로 설정할 시스템을 선택하십시오.
4. 태스크를 완료한 후 **확인**을 클릭하십시오.

Electronic Service Agent 사용에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

아웃바운드 연결 관리

HMC(Hardware Management Console)가 원격 서비스에 연결하는 데 사용할 아웃바운드 연결 수단을 사용자 정의하십시오.

참고: 사용자 정의 가능 데이터 복제가 **데이터 복제 관리** 태스크를 통해 이 HMC에서 **사용**으로 설정된 경우, 이 태스크에 지정된 데이터는 네트워크에 구성된 다른 HMC의 자동 복제에 따라 변경될 수 있습니다. 데이터 복제에 대한 자세한 정보는 69 페이지의 『데이터 복제 관리』의 내용을 참조하십시오.

로컬 모뎀, 인터넷, 인터넷 가상 사설망(VPN)을 통하거나 원격 패스스루(pass-through) 시스템을 통해 연결을 시도하도록 이 HMC를 구성할 수 있습니다. 원격 서비스는 자동화된 서비스 조작을 수행하기 위한 HMC와 IBM 서비스 지원 시스템 사이의 양방향 통신입니다. 연결은 HMC만 시작할 수 있습니다. IBM 서비스 지원 시스템은 HMC에 대한 연결을 시작할 수 없으며 시도할 수도 없습니다.

연결 정보를 사용자 정의하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **아웃바운드 연결 관리**를 클릭하십시오.
3. 태스크를 계속하기 전에 **아웃바운드 연결 관리** 창에서 **로컬 서버를 콜홈 서버로 사용**(선택 표시가 나타남)을 선택하십시오.

   참고: 먼저 이 태스크에서 사용자가 제공한 정보에 대해 설명된 조항에 **동의**해야 합니다. 그러면 로컬 HMC가 서비스 제공자의 콜홈 요청 원격 지원 기능에 연결할 수 있습니다.
4. 전화 걸기 정보 창에는 입력을 제공하기 위한 다음 탭이 표시됩니다.
   - 로컬 모뎀
   - 인터넷
   - 인터넷 VPN
   - 패스스루(pass-through) 시스템
5. 모뎀을 통한 연결을 허용하려면 **로컬 모뎀** 탭을 사용한 후 **서비스에 대해 로컬 모뎀 전화 걸기 허용**을 선택하십시오.
   a. 사용자의 위치에서 외부 회선에 도달하기 위해 전화를 걸 접두부가 필요한 경우, **모던 구성**을 클릭하고 **모뎀 설정 사용자 정의** 창에서 사용자의 위치에 필요한 **전화 걸기 접두부**를 입력하십시오. **확인**을 클릭하여 설정을 승인하십시오.
   b. 전화 번호를 추가하려면 **로컬 모뎀** 탭 페이지에서 **추가**를 클릭하십시오. 로컬 모뎀 전화 걸기가 허용되는 경우, 하나 이상의 전화번호가 구성되어 있어야 합니다.
6. 인터넷을 통한 연결을 허용하려면 **인터넷** 탭을 사용한 후 **서비스에 대해 기존 인터넷 연결 허용**을 선택하십시오.
7. 로컬 HMC에서 서비스 제공자의 원격 지원 기능에 연결하기 위해 기존 인터넷 연결을 통한 VPN 사용을 구성하려면 **인터넷 VPN** 탭을 사용하십시오.
8. HMC가 TCP/IP 주소 또는 호스트 이름을 사용하여 구성된 대로 패스스루 시스템을 사용할 수 있도록 하려면 **패스스루 시스템** 탭을 사용하십시오.
9. 필수 필드를 모두 완료한 후 **확인**을 클릭하여 변경사항을 저장하십시오.

아웃바운드 연결 정보 사용자 정의에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

인바운드 연결 관리

서비스 제공자가 일시적으로 사용자의 로컬 콘솔(예: HMC(Hardware Management Console)) 또는 관리 시스템의 파티션에 로그인할 수 있도록 허용하는 방법을 학습합니다.

인바운드 연결을 관리하려면 다음을 수행하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **인바운드 연결 관리**를 클릭하십시오.
3. **인바운드 연결 관리** 설정 창에서 다음을 수행하십시오.
   - 자동이 아닌 원격 서비스 세션을 시작하는 데 필요한 정보를 제공하려면 **원격 서비스** 탭을 사용하십시오.
   - 자동 원격 서비스 세션을 시작하기 위해 서비스 제공자로부터 수신되는 호출을 승인하는 데 필요한 정보를 제공하려면 **호출 응답** 탭을 사용하십시오.
4. **확인**을 클릭하여 선택을 계속하십시오.

인바운드 연결 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

고객 정보 관리

이 태스크를 사용하여 HMC(Hardware Management Console)의 고객 정보를 사용자 정의할 수 있습니다.

참고: 사용자 정의 가능 데이터 복제가 데이터 복제 관리 태스크를 통해 이 HMC에서 **사용**으로 설정된 경우, 이 태스크에 지정된 데이터는 네트워크에 구성된 다른 HMC의 자동 복제에 따라 변경될 수 있습니다. 데이터 복제에 대한 자세한 정보는 69 페이지의 『데이터 복제 관리』의 내용을 참조하십시오.

고객 정보 관리 창에는 입력을 제공하기 위한 다음 탭이 표시됩니다.

- 관리자
- 시스템
- 계정

고객 정보를 사용자 정의하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **고객 정보 관리**를 클릭하십시오.
3. **고객 정보 관리** 창에서 **관리자** 페이지에 적절한 정보를 제공하십시오.

   참고: 별표(*)가 있는 필드의 정보는 필수입니다.

4. **고객 정보 관리** 창에서 **시스템** 및 **계정** 탭을 선택하여 추가 정보를 제공하십시오.
5. 태스크를 완료한 후 **확인**을 클릭하십시오.

계정 정보 사용자 정의에 대한 추가 정보를 얻으려면 온라인 도움말을 사용하십시오.

서비스 가능 이벤트 알림 관리

이 태스크는 시스템에서 문제점 이벤트가 발생하는 경우 사용자에게 알려주는 이메일 주소를 추가하고 전자 서비스 에이전트로부터 시스템 이벤트의 알림을 수신할 방법을 구성합니다.

알림을 설정하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **서비스 가능 이벤트 알림 관리**를 클릭하십시오.
3. **서비스 가능 이벤트 알림 관리** 창에서 다음을 수행할 수 있습니다.
   - 시스템에서 문제점 이벤트가 발생하는 경우 알림을 받을 이메일 주소를 추가하려면 **이메일** 탭을 사용하십시오.
   - Hardware Management Console 애플리케이션 프로그램 인터페이스 이벤트에 대한 SNMP(Simple Network Management Protocol) 트랩 메시지를 보낼 위치를 지정하려면 **SNMP 트랩 구성** 탭을 사용하십시오.
4. 이 태스크를 완료한 후 **확인**을 클릭하십시오.

서비스 가능 이벤트 알림 관리에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

연결 모니터링 관리

연결 모니터링이 가동 중단을 발견하는 데 사용하고 선택된 시스템에 대해 연결 모니터링을 사용 또는 사용 안함으로 설정하는 타이머의 구성 방법을 학습하십시오.

시스템별 연결 모니터링 설정을 보고 권한이 있는 경우 이를 변경할 수 있습니다. HMC와 관리 시스템 사이에서 통신 문제가 발견되면 연결 모니터링은 서비스 가능 이벤트를 생성합니다. 연결 모니터링을 사용 안함으로 설정하면 선택된 시스템과 이 HMC 사이의 네트워킹 문제에 대해 서비스 가능 이벤트가 생성되지 않습니다.

연결을 모니터하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 **서비스 가능성** 아이콘  을 클릭한 후 **서비스 관리**를 선택하십시오.
2. 컨텐츠 분할창에서 **연결 모니터링 관리**를 클릭하십시오.
3. **연결 모니터링 관리** 창에서 필요한 경우 타이머 설정을 조정하고 서버를 사용 또는 사용 안함으로 설정하십시오.

4. 태스크를 완료한 후 **확인**을 클릭하십시오.

연결 모니터링에 대한 추가 정보가 필요한 경우 온라인 도움말을 사용하십시오.

원격 조작

HMC(Hardware Management Console)에 원격으로 연결하고 사용하십시오.

원격 조작은 HMC에서 명령행 인터페이스(CLI) 또는 로컬 HMC 운영자가 사용하는 GUI를 사용합니다. 다음과 같은 방법으로 조작을 원격으로 수행할 수 있습니다.

- 원격 HMC 사용
- 웹 브라우저를 사용하여 로컬 HMC에 연결
- HMC 원격 명령행 사용

원격 *HMC*는 서비스 프로세서와 다른 서브넷에 있는 HMC이므로 IP 멀티캐스트를 통해 서비스 프로세서를 자동으로 발견할 수 없습니다.

원격 HMC를 사용할지 또는 로컬 HMC에 연결된 웹 브라우저를 사용할지를 결정하려면 필요한 제어의 범위를 고려하십시오. 원격 HMC는 원격 HMC에서 직접 제어하는 특정 관리 오브젝트 세트를 정의하지만 로컬 HMC에 연결된 웹 브라우저는 로컬 HMC와 동일한 관리 오브젝트 세트를 제어합니다. 통신 연결 및 통신 속도는 추가 고려사항입니다. LAN 연결은 원격 HMC 또는 웹 브라우저 제어에 대한 승인 가능한 통신을 제공합니다.

원격 HMC 사용

원격 HMC는 완전한 HMC이므로 가장 완전한 기능 세트를 제공합니다. 관리 오브젝트 구성 프로세스만 로컬 HMC와 다릅니다.

완전한 HMC로서 원격 HMC의 설정 및 유지보수 요구사항은 로컬 Hardware Management Console과 동일합니다. 원격 HMC는 관리할 각 관리 오브젝트(서비스 프로세서)에 LAN TCP/IP를 통해 연결되어야 합니다. 따라서, 원격 HMC와 해당 관리 오브젝트 사이에 있을 수 있는 모든 고객 방화벽은 HMC에서 서비스 프로세서 통신이 발생하는 것을 허용해야 합니다. 원격 HMC는 또한 서비스와 지원을 위해 다른 HMC와 통신해야 할 수 있습니다. 표 10에는 통신을 위해 원격 HMC에서 사용하는 포트가 표시됩니다.

표 *10.* 통신을 위해 원격 *HMC*에서 사용하는 포트

포트	사용
udp 9900	HMC 대 HMC 검색
tcp 9920	HMC 대 HMC 명령

원격 HMC는 서비스 및 지원을 위해 IBM(또는 IBM에 연결할 수 있는 다른 HMC)에 연결되어야 합니다. IBM에 대한 연결은 인터넷 액세스(회사 방화벽을 거쳐) 형식이거나 제공된 모뎀을 사용하는 고

객 제공 교환식 전화 연결을 통한 전화 걸기 연결(95 페이지의 『아웃바운드 연결 관리』 참조) 형식일 수 있습니다. 원격 HMC는 로컬 HMC 또는 서비스 프로세서와의 통신을 위해 제공된 모뎀을 사용할 수 없습니다.

성능, 상태 정보의 사용 가능성, 서비스 프로세서의 제어 기능에 대한 액세스는 원격 HMC와 관리 오브젝트를 상호 연결하는 고객 네트워크의 신뢰성, 사용 가능성 및 응답성에 따라 다릅니다. 원격 HMC는 각 서비스 프로세서에 대한 연결을 모니터하고 유실된 연결 복구를 시도하고 복구할 수 없는 해당 연결을 보고할 수 있습니다.

원격 HMC에 대한 보안은 로컬 HMC와 동일한 방식으로 HMC 사용자 로그인 프로시저를 통해 제공됩니다. 로컬 HMC에서와 같이 원격 HMC와 각 서비스 프로세서 사이의 모든 통신은 암호화됩니다. 보안 통신을 위한 인증서가 제공되고, 사용자가 원하는 경우 변경할 수 있습니다.

원격 HMC에 대한 TCP/IP 액세스는 내부적으로 관리되는 방화벽을 통해 제어되고 HMC 관련 기능으로 제한됩니다.

웹 브라우저 사용

단일 로컬 HMC(Hardware Management Console)에 연결된 관리 오브젝트의 모니터링 및 제어가 때때로 필요한 경우 웹 브라우저를 사용하십시오. 웹 브라우저 사용의 예는 운영자 또는 시스템 프로그래머가 근무 시간 외에 집에서 모니터하는 경우입니다.

각 HMC에는 지정된 사용자 세트의 원격 액세스를 허용하도록 구성될 수 있는 웹 브라우저가 포함되어 있습니다. 웹 브라우저와 로컬 HMC 사이에 고객 방화벽이 있으면 포트가 액세스 가능해야 하고 이러한 포트에서 수신 요청을 허용하도록 방화벽을 설정해야 합니다. 표 11에서는 웹 브라우저가 HMC와 통신하는 데 필요한 포트에 대해 설명합니다.

표 *11.* 웹 브라우저가 *HMC*와 통신하기 위해 사용되는 포트

포트	**사용**
TCP 443	웹 서버 통신에 대한 보안 브라우저 액세스
TCP 8443	웹 서버 통신에 대한 보안 브라우저 액세스
TCP 9960	브라우저 애플릿 통신
TCP 12443[1]	원격 웹 브라우저 통신
[1]이 포트는 HMC 버전 7.8.0 이상에서 원격 액세스가 사용으로 설정된 경우 HMC 방화벽에서 열려 있습니다. 이 포트는 원격 클라이언트와 HMC 사이에 있는 방화벽에서도 열려 있어야 합니다.	

HMC가 웹 브라우저 액세스를 허용하도록 구성된 후 웹 브라우저는 사용 가능한 사용자에게 HMC에 대한 물리적 액세스가 필요한 기능(예: 로컬 디스켓 또는 DVD 매체를 사용하는 기능)을 제외하고 로컬 HMC의 모든 구성된 기능에 대한 액세스를 제공합니다. 원격 웹 브라우저 사용자에게 제공되는 사용자 인터페이스는 로컬 HMC의 사용자 인터페이스와 동일하며 로컬 HMC와 동일한 제한조건이 적용됩니다.

웹 브라우저는 LAN TCP/IP 연결을 사용하고 암호화된(HTTPS) 프로토콜만 사용하여 로컬 HMC에 연결될 수 있습니다. 웹 브라우저에 대한 로그온 보안은 HMC 사용자 로그인 프로시저를 통해 제공됩니다. 보안 통신을 위한 인증서가 제공되며, 사용자가 변경할 수 있습니다.

성능, 상태 정보의 사용 가능성, 관리 오브젝트의 제어 기능에 대한 액세스는 웹 브라우저와 로컬 HMC를 상호 연결하는 네트워크의 신뢰성, 사용 가능성 및 응답성에 따라 다릅니다. 웹 브라우저와 개별 관리 오브젝트는 직접 연결되어 있지 않으므로 웹 브라우저는 각 서비스 프로세서에 대한 연결을 모니터하지 않고 복구하지 않으며 유실된 연결을 보고하지 않습니다. 이러한 기능은 로컬 HMC에서 처리됩니다.

웹 브라우저 시스템은 서비스 또는 지원을 위해 IBM에 연결될 필요가 없습니다. 브라우저 및 시스템 레벨의 유지보수는 고객의 책임입니다.

HMC의 URL이 https://*xxx.xxx.xxx.xxx*(여기서 *xxx.xxx.xxx.xxx*는 IP 주소임) 형식을 사용하여 지정되고 Microsoft Internet Explorer가 브라우저로 사용되면 호스트 이름 불일치 메시지가 표시됩니다. 이 메시지를 피하기 위해 Firefox 브라우저가 사용되거나 호스트 이름이 **네트워크 설정 변경** 태스크를 사용하여 HMC에 대해 구성되고(61 페이지의 『네트워크 설정 변경』 참조) IP 주소 대신 이 호스트 이름이 URL에 지정됩니다. 예를 들어, https://*hostname.domain_name* 또는 https://*hostname* 형식을 사용할 수 있습니다(예: https://hmc1.ibm.com 또는 https://hmc1 사용).

웹 브라우저 사용 준비

웹 브라우저를 사용하여 HMC(Hardware Management Console)에 액세스하도록 준비하는 데 필요한 단계를 수행하십시오.

웹 브라우저를 사용하여 HMC에 액세스하려면 우선 다음 태스크를 완료해야 합니다.

- 지정된 사용자의 원격 제어를 허용하도록 HMC를 구성하십시오.
- LAN 기반 연결의 경우 제어할 HMC의 TCP/IP 주소를 알아두고 HMC와 웹 브라우저 간의 방화벽 액세스를 올바르게 설정하십시오.
- HMC 웹 액세스를 위해 액세스 관리자로부터 올바른 사용자 ID 및 비밀번호를 지정받으십시오.

웹 브라우저 요구사항

HMC(Hardware Management Console)를 모니터하고 제어하기 위해 웹 브라우저가 충족해야 하는 요구사항에 대해 학습합니다.

HMC 웹 브라우저 지원에는 HTML 2.0, JavaScript 1.0, JVM(Java™ Virtual Machine), JRE(Java Runtime Environment) 버전 7 및 HMC에 연결된 브라우저의 쿠키 지원이 필요합니다. 브라우저가 Java Virtual Machine으로 구성되었는지 여부를 판별하는 데 도움이 필요하면 지원 담당자에게 문의하십시오. 웹 브라우저는 HTTP 1.1을 사용해야 합니다. 프록시 서버를 사용 중인 경우, 프록시 연결에 대해 HTTP 1.1을 사용으로 설정해야 합니다. 또한 팝업 창이 사용 안함으로 설정된 브라우저가 실행 중인 경우에는 브라우저에 주소 지정된 모든 HMC에 대해 팝업 창을 사용으로 설정해야 합니다. 다음 브라우저가 테스트되었습니다.

Google Chrome

HMC 버전 8.1은 Google Chrome 버전 33을 지원합니다.

Microsoft Internet Explorer

HMC 버전 8.1은 Internet Explorer 9.0, Internet Explorer 10.0 및 Internet Explorer 11.0을 지원합니다.

참고: 성능 CEC 태스크는 Internet Explorer 9.0에서 지원되지 않습니다.

- 브라우저가 인터넷 프록시를 사용하도록 구성된 경우 로컬 IP 주소는 예외 목록에 포함됩니다. 자세한 정보는 네트워크 관리자를 참조하십시오. Hardware Management Console에 도달하기 위해 프록시를 계속 사용해야 하는 경우, 인터넷 옵션 창의 **고급** 탭 아래에서 **프록시 연결을 통해 HTTP 1.1 사용**을 사용으로 설정하십시오.

Mozilla Firefox

HMC 버전 8.1은 Mozilla Firefox 버전 17 및 Mozilla Firefox 버전 24 ESR(Extended Support Release)을 지원합니다. 창을 올리거나 내리고 기존 창을 이동하거나 크기 조정하는 JavaScript 옵션이 사용으로 설정되어 있는지 확인하십시오. 해당 옵션을 사용으로 설정하려면 브라우저의 옵션 대화 상자에서 **컨텐츠** 탭을 클릭하고 JavaScript 사용 옵션 옆에 있는 **고급**을 클릭한 후 창 올리기 또는 내리기 옵션 및 기존 창 이동 또는 크기 조정 옵션을 선택하십시오. 이러한 옵션을 사용하여 HMC 태스크 사이에서 쉽게 전환할 수 있습니다. 최신 Mozilla Firefox ESR 레벨에 대한 자세한 정보는 Security Advisories for Firefox ESR을 참조하십시오.

참고: HMC가 NIST SP 800-131a 안전 모드에 있는 동안 Mozilla Firefox를 사용하는 경우, 다음과 같은 제한사항이 적용됩니다.

- 원격 클라이언트에 대해서는 Mozilla Firefox를 사용할 수 없습니다.
- 로컬 콘솔을 사용할 수 없습니다.

기타 웹 브라우저 고려사항

HMC에 원격으로 연결된 경우 ASMI가 작동하려면 세션 쿠키를 사용해야 합니다. ASM 프록시 코드는 세션 정보를 저장하고 사용합니다.

Internet Explorer

1. **도구** > **인터넷 옵션**을 클릭하십시오.
2. **개인정보 보호정책** 탭을 클릭하고 **고급**을 선택하십시오.
3. **세션 쿠키 항상 허용**이 선택되었는지 여부를 판별하십시오.
4. 선택되지 않은 경우, **자동 쿠키 처리 대체** 및 **항상 세션 쿠키 허용**을 선택하십시오.
5. 퍼스트파티 쿠키 및 써드파티 쿠키의 경우 차단, 프롬프트 또는 허용을 선택하십시오. 프롬프트가 선호됩니다. 이 경우에는 사이트가 쿠키를 쓰려고 할 때마다 사용자에게 프롬프트가 표시됩니다. 일부 사이트에서는 쿠키 쓰기를 허용해야 합니다.

Firefox

1. **도구** > **옵션**을 클릭하십시오.

2. **쿠키** 탭을 클릭하십시오.
3. **사이트에 쿠키 설정 허용**을 선택하십시오.
4. 특정 사이트만 허용하려는 경우 **예외**를 선택하고 이 HMC를 추가하여 액세스를 허용하십시오.

HMC 원격 명령행 사용

HMC 그래픽 사용자 인터페이스에서 태스크를 수행하는 대신 명령행 인터페이스(CLI)를 사용할 수 있습니다.

다음과 같은 상황에서 명령행 인터페이스를 사용할 수 있습니다.

- 일관된 결과가 필요한 경우. 여러 관리 시스템을 관리해야 하는 경우 명령행 인터페이스를 사용하면 일관된 결과를 얻을 수 있습니다. 명령 순서를 스크립트에 저장하여 원격으로 실행할 수 있습니다.
- 자동화된 조작이 필요한 경우. 관리 시스템을 관리하는 일관된 방법을 개발한 후 다른 시스템의 일괄처리 애플리케이션(예: **cron** 디먼)에서 스크립트를 호출하여 조작을 자동화할 수 있습니다.

로컬 HMC에서는 터미널 창에서 명령행 인터페이스를 사용할 수 있습니다.

SSH 클라이언트와 HMC 간의 보안 스크립트 실행 설정

SSH(Secure Shell) 클라이언트와 HMC(Hardware Management Console) 사이의 스크립트 실행이 안전한지 확인해야 합니다.

HMC는 일반적으로 관리 시스템이 있는 기계실 내부에 배치되므로 HMC에 물리적으로 액세스할 수는 없을 수 있습니다. 이 경우 원격 웹 브라우저 또는 원격 명령행 인터페이스를 사용하여 HMC에 원격으로 액세스할 수 있습니다.

참고: SSH 클라이언트와 HMC 사이에서 스크립트가 자동으로 실행될 수 있도록 하려면 SSH 프로토콜이 이미 클라이언트의 운영 체제에 설치되어 있어야 합니다.

SSH 클라이언트와 HMC 사이에서 스크립트가 자동으로 실행될 수 있도록 하려면 다음을 수행하십시오.

1. 원격 명령 실행을 사용으로 설정하십시오. 자세한 정보는 88 페이지의 『원격 명령 실행 사용』의 내용을 참조하십시오.
2. 클라이언트의 운영 체제에서 SSH 프로토콜 키 생성기를 실행하십시오. SSH 프로토콜 키 생성기를 실행하려면 다음을 수행하십시오.
   a. 키를 저장하려면 $HOME/.ssh 디렉토리를 작성하십시오(RSA 또는 DSA 키를 사용할 수 있음).
   b. 공개 키 및 개인 키를 생성하려면 다음 명령을 실행하십시오.

      ```
      ssh-keygen -t rsa
      ```

      다음 파일이 $HOME/.ssh 디렉토리에 작성됩니다.

개인 키: id_rsa
공개 키: id_rsa.pub

그룹 및 기타 둘 다에 대한 쓰기 비트는 꺼져 있습니다. 개인 키에 600 권한이 있는지 확인하십시오.

3. 클라이언트의 운영 체제에서 다음 명령을 통해 ssh를 사용하고 **mkauthkeys** 명령을 사용하여 HMC에서 HMC 사용자의 authorized_keys2 파일을 업데이트하십시오.

```
ssh hmcuser@hmchostname "mkauthkeys -–add '<the contents of $HOME/ .ssh/id_rsa.pub>'
" "
```

HMC에서 키를 삭제하려면 다음 명령을 사용할 수 있습니다.

```
ssh hmcuser@hmchostname "mkauthkeys --remove 'joe@somehost' "
```

ssh를 통해 HMC에 액세스하는 모든 호스트에 대해 비밀번호 프롬프트를 사용으로 설정하려면 **scp** 명령을 사용하여 HMC에서 키 파일을 복사하십시오. `scp hmcuser@hmchostname:.ssh/authorized_keys2 authorized_keys2`

authorized_keys2 파일을 편집하고 이 파일에서 모든 행을 제거하십시오. 그런 다음 다시 HMC에 복사하십시오. `scp authorized_keys2 hmcuser@hmchostname:.ssh/authorized_keys2`

HMC 원격 명령 사용 및 사용 안함

HMC(Hardware Management Console)에 대한 원격 명령행 인터페이스 액세스를 사용 또는 사용 안함으로 설정할 수 있습니다.

원격 명령을 사용 또는 사용 안함으로 설정하려면 다음 단계를 완료하십시오.

1. 탐색 영역에서 관리 시스템을 선택하고 **사용자 및 보안** 아이콘  을 클릭한 후 **사용자 및 역할**을 선택하십시오.
2. 컨텐츠 분할창에서 **원격 명령 실행 사용**을 클릭하십시오.
3. **원격 명령 실행 사용** 창에서 다음을 수행할 수 있습니다.
   - 원격 명령을 사용하려면 **ssh 기능을 사용하여 원격 명령 실행 사용**을 선택하십시오.
   - 원격 명령을 사용하지 않으려면 **ssh 기능을 사용하여 원격 명령 실행 사용**이 선택되지 않았는지 확인하십시오.
4. **확인**을 클릭하십시오.

LAN 연결 웹 브라우저에서 HMC에 로그인

LAN 연결 웹 브라우저에서 원격으로 HMC(Hardware Management Console)에 로그인할 수 있습니다.

LAN 연결 웹 브라우저에서 HMC에 로그인하려면 다음 단계를 사용하십시오.

1. 웹 브라우저 PC가 원하는 HMC에 LAN으로 연결되어 있는지 확인하십시오.
2. 웹 브라우저에서 원하는 HMC의 URL을 ***https://hostname.domain_name***(예: https://hmc1.ibm.com) 또는 ***https://xxx.xxx.xxx.xxx*** 형식을 사용하여 입력하십시오.

   현재 웹 브라우저 세션에서 HMC에 처음 액세스하는 경우 인증서 오류가 수신될 수 있습니다. 이 인증서 오류는 다음과 같은 경우에 표시됩니다.

   - HMC에 포함된 웹 서버는 자체 서명 인증서를 사용하도록 구성되고 브라우저는 HMC를 인증서 발행자로서 신뢰하도록 구성되지 않았습니다.
   - HMC는 인증 기관(CA)이 서명한 인증서를 사용하도록 구성되고 브라우저는 이 CA를 신뢰하도록 구성되지 않았습니다.

   두 경우 모두 브라우저에 표시되는 인증서가 HMC에서 사용되는 인증서임을 알면 계속할 수 있으며 HMC에 대한 모든 통신은 암호화됩니다.

   브라우저 세션에 처음 액세스할 때 인증서 오류에 대한 알림을 수신하지 않으려면 HMC 또는 CA를 신뢰하도록 브라우저를 구성할 수 있습니다. 일반적으로 브라우저를 구성하려면 다음 방법 중 하나를 사용하십시오.

   - 브라우저가 영구적으로 인증서 발행자를 신뢰할 것임을 표시해야 합니다.
   - 인증서를 보고 신뢰할 수 있는 CA의 데이터베이스에 HMC에서 사용되는 인증서를 발행한 CA의 인증서를 설치합니다.

   인증서가 자체 서명된 경우, HMC 자체가 인증서를 발행한 CA로 간주됩니다.
3. 프롬프트가 표시되면 관리자가 지정한 사용자 이름 및 비밀번호를 입력하십시오.

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*

2바이트 문자 세트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이센스 사용자는 다음 주소로 문의하십시오.

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

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

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.

저작권 라이센스:

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 추가 비용 없이 이들 샘플 프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건하에서 완전히 테스트된 것은 아닙니다. 따라서 IBM은 이들 샘플 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 진술하지 않습니다. 본 샘플 프로그램은 일체의 보증 없이 "현상태대로" 제공됩니다. IBM은 귀하의 샘플 프로그램 사용과 관련되는 손해에 대해 책임을 지지 않습니다.

이러한 샘플 프로그램 또는 파생 제품의 각 사본이나 그 일부에는 반드시 다음과 같은 저작권 표시가 포함되어야 합니다.

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

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 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.

개인정보 보호정책 고려사항

SaaS(software as a service) 솔루션을 포함한 IBM 소프트웨어 제품("소프트웨어 오퍼링")은 제품 사용 정보를 수집하거나 일반 사용자 경험을 개선하거나 일반 사용자와의 상호작용을 조정하거나 기타 다른 목적을 위해 쿠키 또는 기타 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 개인정보 보호정책(http://www.ibm.com/privacy/kr/ko) 및 IBM 온라인 개인정보 보호정책(http://www.ibm.com/privacy/details/kr/ko)의 "쿠키, 웹 비콘 및 기타 기술" 및 "IBM 소프트웨어 제품 및 SaaS(Software-as-a Service)"(http://www.ibm.com/software/info/product-privacy)를 참조하십시오.

프로그래밍 인터페이스 정보

이 HMC(Hardware Management Console) 관리 서적에는 고객이 IBM Hardware Management Console 버전 8 릴리스 8.7.0 유지보수 레벨 0 서비스를 받기 위한 프로그램을 작성할 수 있도록 마련된 프로그래밍 인터페이스가 문서화되어 있습니다.

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.

Microsoft는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

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

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.

Printed in Korea