

Power Systems

安装和配置硬件管理控制台

IBM

Power Systems

安装和配置硬件管理控制台

IBM

注意

使用本资料及其支持的产品之前，请阅读第 vii 页的『安全声明』、第 163 页的『声明』、*IBM Systems Safety Notices Manual* (G229-9054) 以及 *IBM Environmental Notices and User Guide* (Z125-5823) 中的信息。

目录

安全声明	vii
安装和配置硬件管理控制台	1
有关安装和配置 HMC 的新增内容	1
安装和配置任务	2
安装和配置带有新服务器的新 HMC.	2
更新和升级 HMC 代码.	2
向现有安装添加另一 HMC.	3
安装 HMC	3
独立 HMC 布线	3
将 7310-CR4 HMC 安装到机架中	5
清点部件清单	6
确定位置.	7
在不使用机架安装模板的情况下标记位置	7
将滑轨安装到机架.	8
在滑轨上安装 HMC	11
安装电缆管理臂	13
机架安装式 HMC 布线	14
HMC 端口位置	15
将 7042-CR5 和 7042-CR6 安装到机架中	18
将 7042-CR7 和 7042-CR8 安装到机架中	23
将 7042-CR9 HMC 安装到机架中	33
将 7063-CR1 安装到机架中	41
有关安装机架安装式 7063-CR1 系统的先决条件	41
清点系统的清单	42
确定并标记 7063-CR1 系统在机架中的位置	42
使用固定导轨将 HMC 安装到机架中	43
将固定导轨连接到系统机箱和机架	44
将系统安装到机架并连接和布置电源线	45
使用滑轨将 HMC 安装到机架中	46
将滑轨连接至系统和机架	47
将系统安装到机架并连接和布置电源线	50
用电缆连接机架安装式 7063-CR1 HMC	51
配置 7063-CR1 HMC	52
安装 HMC 虚拟设备	53
在 x86 上安装 HMC 虚拟设备	54
使用 KVM 管理程序安装 HMC 虚拟设备	54
使用 Xen 虚拟机管理器安装 HMC 虚拟设备	54
使用 VMware ESXi 安装 HMC 虚拟设备	55
在 PowerVM (逻辑分区) 上安装 HMC 虚拟设备	55
将激活引擎用于 HMC 虚拟设备	56
设置激活引擎的配置概要文件	57
安装监视器和键盘	63
清点部件清单	65
在不使用机架安装模板的情况下标记位置	65
将监视器和键盘安装到机架中	65
安装控制台开关 (可选)	69
使用 HMC Classic 或 HMC Enhanced 界面配置 HMC	71
在 HMC 上选择网络设置	71
HMC 网络连接	71

HMC 网络连接的类型	71
决定要用于回拨服务器的连接方法	74
简化的连接	76
使用因特网 SSL 以连接至远程支持	76
选择因特网协议	76
因特网 SSL 地址列表	77
使用虚拟专用网连接至远程支持	77
VPN 服务器地址列表	78
使用电话和调制解调器连接至远程支持	78
使用多个回拨服务器	79
准备 HMC 配置	79
HMC 的安装前配置工作表	80
配置 HMC	87
通过指导式安装向导使用快速路径来配置 HMC	87
启动 HMC 并完成指导式安装向导中的步骤	87
复查您的配置	88
使用 HMC 菜单配置 HMC	88
启动 HMC	89
更改日期和时间	90
配置 HMC 网络类型	90
更改 HMC 防火墙设置	95
将路由条目配置为缺省网关	96
配置域名服务	96
配置域后缀	96
配置 HMC 以便它使用 LDAP 远程认证	97
配置 HMC 以便它使用密钥分发中心服务器进行 Kerberos 远程认证	97
配置 HMC 以便它可与服务和支持联系	98
配置回拨事件管理器	102
为受管系统设置密码	103
测试 HMC 与受管系统之间的连接	104
配置后步骤	104
备份重要的 HMC 数据	104
将整个 HMC 硬盘驱动器备份到远程系统	105
更新, 升级和迁移 HMC 机器代码	106
确定 HMC 机器代码版本和发行版	106
对连接至因特网的 HMC 获取并应用机器代码更新	106
步骤 1. 确保已连接至因特网	106
步骤 2. 查看现有 HMC 机器代码级别	107
步骤 3. 查看可用的 HMC 机器代码级别	107
步骤 4. 应用 HMC 机器代码更新	107
步骤 5. 验证 HMC 机器代码更新是否安装成功	107
使用 DVD 或 FTP 服务器获取并应用 HMC 的机器代码更新	108
步骤 1. 查看现有 HMC 机器代码级别	108
步骤 2. 查看可用的 HMC 机器代码级别	108
步骤 3. 获取 HMC 机器代码更新	108
步骤 4. 应用 HMC 机器代码更新	109
步骤 5. 验证 HMC 机器代码更新是否安装成功	109
升级 HMC 软件	109
步骤 1. 获取升级	109
步骤 2. 查看现有 HMC 机器代码级别	109
步骤 3. 备份受管系统的概要文件数据	110
步骤 4. 备份 HMC 数据	110
步骤 5. 记录当前 HMC 配置信息	110
步骤 6. 记录远程命令状态	111
步骤 7. 保存升级数据	111
步骤 8. 升级 HMC 软件	111

步骤 9. 验证 HMC 机器代码升级是否安装成功	112
使用网络升级图像从远程位置升级 HMC	112
使用 HMC 增强型+ 界面配置 HMC	113
在 HMC 上选择网络设置	113
HMC 网络连接	113
HMC 网络连接的类型	113
决定要用于回拨服务器的连接方法	116
使用因特网 SSL 以连接至远程支持	118
选择因特网协议	118
因特网 SSL 地址列表	118
使用虚拟专用网连接至远程支持	119
VPN 服务器地址列表	120
使用电话和调制解调器连接至远程支持	120
使用多个回拨服务器	120
准备 HMC 配置	121
HMC 的安装前配置工作表	122
配置 HMC	128
通过指导式安装向导使用快速路径来配置 HMC	128
启动 HMC 并完成指导式安装向导中的步骤	128
复查您的配置	129
使用 HMC 菜单配置 HMC	129
启动 HMC	130
更改日期和时间	131
配置 HMC 网络类型	131
更改 HMC 防火墙设置	137
将路由条目配置为缺省网关	138
配置域名服务	138
配置域后缀	139
配置 HMC 以便它使用 LDAP 远程认证	139
配置 HMC 以便它使用密钥分发中心服务器进行 Kerberos 远程认证	140
配置本地控制台以向服务和支持报告错误	141
配置回拨事件管理器	146
为受管系统设置密码	147
测试 HMC 与受管系统之间的连接	147
配置后步骤	148
备份重要的 HMC 数据	148
将整个 HMC 硬盘驱动器备份到远程系统	149
更新, 升级和迁移 HMC 机器代码	149
确定 HMC 机器代码版本和发行版	150
对连接至因特网的 HMC 获取并应用机器代码更新	150
步骤 1. 确保已连接至因特网	150
步骤 2. 查看现有 HMC 机器代码级别	151
步骤 3. 查看可用的 HMC 机器代码级别	151
步骤 4. 应用 HMC 机器代码更新	151
步骤 5. 验证 HMC 机器代码更新是否安装成功	151
使用 DVD 或 FTP 服务器获取并应用 HMC 的机器代码更新	152
步骤 1. 查看现有 HMC 机器代码级别	152
步骤 2. 查看可用的 HMC 机器代码级别	152
步骤 3. 获取 HMC 机器代码更新	152
步骤 4. 应用 HMC 机器代码更新	153
步骤 5. 验证 HMC 机器代码更新是否安装成功	153
升级 HMC 软件	153
步骤 1. 获取升级	153
步骤 2. 查看现有 HMC 机器代码级别	154
步骤 3. 备份受管系统的概要文件数据	154
步骤 4. 备份 HMC 数据	154

步骤 5. 记录当前 HMC 配置信息	155
步骤 6. 记录远程命令状态	155
步骤 7. 保存升级数据.	156
步骤 8. 升级 HMC 软件	156
步骤 9. 验证 HMC 机器代码升级是否安装成功	157
使用网络升级图像从远程位置升级 HMC	157
HMC 端口位置.	158
声明	163
IBM Power Systems 服务器的辅助功能选项功能部件	164
隐私声明注意事项	165
商标	165
电子辐射声明	165
A 类声明.	165
B 类声明	170
条款和条件	173

安全声明

可能会在本指南中各处都刊载安全声明。

- 可通过**危险声明**提醒用户注意可能使人致命或带来极端危险的情况。
- 可通过**警告声明**提醒用户注意因某些现有条件而可能给人带来危险的情况。
- 可通过**注意声明**提醒用户注意可能会导致程序、设备、系统或数据损坏的情况。

世界贸易安全信息

一些国家或地区要求以本地语言提供产品出版物中包含的安全信息。如果您所在的国家或地区有此要求，那么随产品包提供的的安全信息文档（例如，以打印文档、DVD 或作为产品的一部分显示）将随产品一起提供。此文档包含以本地语言提供的的安全信息，它引用了美国英语源出版物中的内容。使用美国英语出版物来安装、操作或维修此产品之前，必须先熟悉文档中的相关安全信息。如果您对美国英语出版物中的任何安全信息了解得不是很清楚，那么还可以参阅安全信息文档。

可以呼叫 IBM 热线 1-800-300-8751 来获取安全信息文档的替代物或其他副本。

德语版安全信息

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

激光器安全信息

IBM® 服务器可以使用基于光纤并利用了激光器或 LED 的 I/O 卡或功能部件。

符合激光器标准

IBM 服务器可安装在 IT 设备机架内部或外部。

危险：在系统中或周围工作时，请遵守以下预防措施：

电源线、电话线和通信电缆中的电压和电流存在危险。为了避免触电：

- 如果 IBM 提供了电源线，请仅使用 IBM 提供的电源线将电源连接至此部件。请勿将 IBM 提供的电源线用于任何其他产品。
- 不要打开或维护任何电源组合件。
- 在电暴期间，不要连接或断开任何电缆，或执行本产品的安装、维护或重新配置。
- 本产品可能配有多根电源线。要消除所有危险电压，请断开所有电源线。
 - 如果是交流电源，请断开交流电源的所有电源线。
 - 如果是含有直流配电面板 (PDP) 的机架，请断开客户的直流电源与 PDP 的连接。
- 将电源连接至产品时，确保正确连接所有电源线。
 - 对于有交流电源的机架，将所有电源线连接至正确布线并接地的电源插座。确保电源插座根据系统铭牌提供了正确的电压和相位旋转。
 - 如果是含有直流配电面板 (PDP) 的机架，请将客户的直流电源连接至 PDP。连接直流电源和直流电源返回连线时，确保使用正确的极性。
- 把任何将连接到本产品的设备连接至正确布线的电源插座。
- 尽可能只用一只手来连接或断开信号电缆。
- 当存在火烧、水浸或结构损坏的迹象时，不要打开任何设备。

- 在校正所有不安全的情况之前，不要尝试打开机器的电源。
- 假设存在一个电气安全隐患。那么在子系统安装过程中，请检查所有指定的连续电阻、接地和电源以确保机器符合安全要求。
- 如果存在任何不安全情况，那么请停止检查。
- 除非安装和配置过程中另有指示，否则，在打开设备盖板之前：断开已连接的交流电源线，关闭位于机架配电面板 (PDP) 中的适用断路器，并与所有远程通信系统、网络和调制解调器断开连接。

危险：

- 当在本产品或连接的设备上安装、移动或打开盖板时，请按以下过程中的描述来连接和断开电缆。

要断开电缆：

1. 关闭所有设备（除非另有指示）。
2. 如果是交流电源，请拔出电源插座中的电源线。
3. 如果是含有直流配电面板 (PDP) 的机架，请关闭位于 PDP 中的断路器，并断开客户的直流电源的供电。
4. 拔出连接器中的信号电缆。
5. 拔出设备中的所有电缆。

要连接电缆：

1. 关闭所有设备（除非另有指示）。
2. 将所有电缆连接到设备。
3. 将信号电缆连接到连接器。
4. 如果是交流电源，请将电源线连接到电源插座。
5. 如果是包含有直流配电面板 (PDP) 的机架，请恢复客户的直流电源的供电，并打开位于 PDP 中的断路器。
6. 打开设备。

系统周边可能存在锐利边缘、角落和接头。搬运设备的时候要小心，避免割伤、擦伤和夹伤。(D005)

(R001 第 1/2 部分)：

危险：在 IT 机架系统中或周围工作时，请遵守以下预防措施：

- 重型设备 - 如果操作不当，可能导致人员受伤或设备损坏。
- 始终降低机箱上的支撑垫。
- 始终在机箱上安装稳定支架。
- 为了避免由于不均匀的机械负载而导致的危险情况，始终将最重的设备安装在机箱底部。始终从机箱的底部开始安装服务器和可选设备。
- 不要将装有机架的设备用作支架或工作空间。不要在装有机架的设备顶部放置物件。此外，不要倚靠装有机架的设备，也不要使用这些设备来稳定身体姿势（例如，在梯子上工作时）。



- 每个机箱都可能有多根电源线。
 - 对于有交流电源的机架，在维护期间，当指示断开电源时，确保断开机箱中的所有电源线。
 - 如果是含有直流配电面板 (PDP) 的机架，在维护期间，当指示断开电源时，请关闭用于控制系统部件电源的断路器，或者断开客户的直流电源。
- 将安装在机箱中的所有设备连接到安装在同一机箱中的电源设备。不要将安装在一个机箱中的设备的电源线插入安装在不同机箱中的电源设备。

- 未正确布线的电源插座会使系统或连接到系统的设备上的金属部件带有危险电压。由客户负责确保电源插座已正确布线并接地以防止电击。

(R001 第 2/2 部分) :

警告:

- 对于所有装有机架的设备，如果机架的内部环境温度将超过本制造商建议的环境温度，那么不要将部件安装在该机架中。
- 不要将部件安装在通风不畅的机架中。确保流过部件周围的气流不会受阻或减弱。
- 应考虑设备与电源电路的连接，以便电路超载不会影响电源布线或过电流保护。为了提供与机架的正确电源连接，请参阅机架中设备上的铭牌以确定电源电路的总电源要求。
- (对于滑动屉式机柜。) 如果未将机架稳定支架与机架相连，那么不要拉出或安装任何屉式机柜或功能部件。不要同时拉出多个屉式机柜。如果您同时拉出多个屉式机柜，那么可能会导致机架不稳定。



- (对于固定屉式机柜。) 此屉式机柜是固定屉式机柜，如果本制造商未指定，那么不能移动它进行维护。如果尝试将该屉式机柜部分或全部移出机架，那么可能导致机架不稳定或导致屉式机柜掉出机架外。

注意：

重新安置机箱时，从机箱上部拆卸组件可以提高机架的稳定性。无论何时在房间或建筑物中重新安置组装好的机架式机箱，请遵循以下一般准则。

- 通过从机箱顶部开始拆卸设备来减少机箱的重量。尽可能将机箱恢复至接收时的配置。如果不知道此配置，那么必须遵循以下预防措施：
 - 拆卸 32U 位置（合规性标识 RACK-001）或 22U 位置（合规性标识 RR001）的所有设备。
 - 确保最重的设备安装在机箱底部。
 - 确保安装在机箱内 32U 层（合规性标识 RACK-001）或 22U 层（合规性标识 RR001）以下的设备之间没有空的 U 层，收到特别配置允许的情况除外。
- 如果要重新安置的机箱是机箱套件的一部分，那么从套件中拆离该机箱。
- 如果要重新安置的机箱随付了可拆卸的支架，那么在重新安置机箱之前必须重新装好支架。
- 检查您计划采用的路线，以消除可能的危险。
- 验证您选择的路线是否可以承受已装好组件的机箱的重量。请参阅随机箱附带的文档以了解已装好组件的机箱的重量。
- 验证所有门的大小是否至少为 760 x 230 毫米（30 x 80 英寸）。
- 确保所有设备、支架、屈式机柜、门和电缆安全可靠。
- 确保将四个支撑垫升到其最高位置。
- 确保移动时机箱上没有安装任何稳定支架。
- 不要使用倾斜度超过 10 度的斜坡。
- 当机箱到达新位置时，请完成以下步骤：
 - 降低四个支撑垫。
 - 在机箱上安装稳定支架。
 - 如果您从机箱中取出了任何设备，那么按从最低到最高的位置顺序将它们重新装入机箱。
- 如果需要进行长距离重新安置，那么将机箱恢复至接收时的配置。将机箱包装在原来的包装材料或等效材料中。并降低支撑垫以使脚轮升至离开托盘的位置并用螺钉将机箱与托盘固定在一起。

(r002)

(L001)



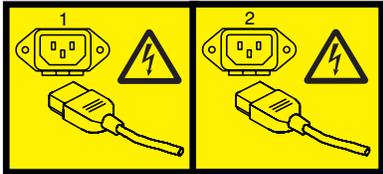
危险：任何贴有此标签的组件内部都存在危险的电压、电流或能量级别。请勿打开贴有此标签的任何外盖或隔板。(L001)

(L002)

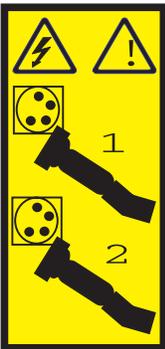


危险：不要将装有机架的设备用作支架或工作空间。(L002)

(L003)



或



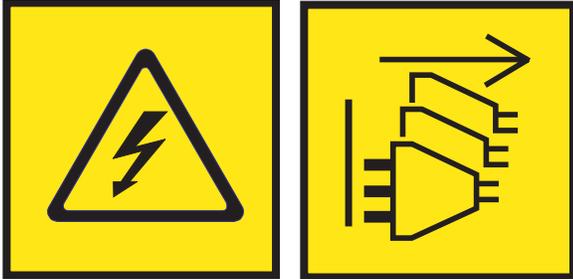
或



或



或



危险：多根电源线。本产品可能配有多根交流电源线或多根直流电源线。要消除所有危险电压，请断开所有电源线。(L003)

(L007)



警告：附近有高温表面。(L007)

(L008)



警告：附近有危险的活动部件。(L008)

所有激光器已在美国经过认证，符合 1 类激光器产品的 DHHS 21 CFR 子章节 J 中的要求。在美国以外的国家或地区，它们经认证符合 IEC 60825 标准，属于 1 类激光器产品。请查阅每个部件上的标签，以获取激光器认证编号和许可信息。

注意：

本产品可能包含以下其中一个或多个设备：**CD-ROM 驱动器、DVD-ROM 驱动器、DVD-RAM 驱动器**或属于 1 类激光器产品的激光器模块。注意以下信息：

- 不要取出盖板。取出激光器产品的盖板会导致暴露在危险的激光辐射中。该设备内部没有可维护的部件。
- 采用非此处指定的过程进行控制或调整可能会导致暴露在危险的辐射中。

(c026)

注意：

数据处理环境可能包含在具有激光器模块的系统链路中进行传送的设备，这些激光器模块在 1 类以上的功率级别下工作。因此，请不要直视光纤电缆的末端或打开的插座。虽然通过灯光从断开连接的光纤电缆的一端看到另一端来验证光纤电缆的连续电阻可能不会伤害眼睛，但此过程也是有潜在危险。因此，不建议通过灯光从一端看到另一端的方法来验证光纤电缆的连续电阻。要验证光纤电缆的连续电阻，请使用光学灯源和电源计量表。**(C027)**

注意：

本产品包含 1M 类激光器。请不要用光学仪器直接观察。**(c028)**

注意：

某些激光产品包含嵌入式 3A 类或 3B 类激光器二极管。注意以下信息：激光器在打开时会产生辐射。请不要凝视光束，不要用光学仪器直接观察，并避免直接暴露在光束中。**(c030)**

注意：

此电池含锂。为了避免可能发生爆炸，不要焚烧此电池或对此电池进行充电。

不要：

- ___ 投入或浸入水中
- ___ 高温超过 100°C (212°F)
- ___ 修复或拆卸

仅使用 IBM 认可的部件进行更换。按当地法规的指示回收或废弃此电池。在美国，IBM 提供了收集此电池的过程。有关信息，请拨打 1-800-426-4333。打电话时，请提供电池单元的 IBM 部件号。**(C003)**

注意：

关于 **IBM** 提供的供应商起重工具：

- 只有经过授权的人员才能对起重工具进行操作。
- 起重工具用于在机架高度对部件（负荷）进行操作，例如辅助、抬起、安装和卸下。它并非用于在有负荷的情况下在大坡度上执行运输工作，也并非意在取代指定的工具（例如，液压车、堆高车、叉车）以及此类相关的搬运做法）。如果这不可行，那么必须使用经过专门培训的人员或服务（例如，装配工或搬运工）。
- 使用起重工具之前，请阅读并完全理解起重工具操作员手册的内容。不阅读、理解、遵守安全规则，或者不遵循指示信息，可能导致财产损坏和/或人身伤害。如有疑问，请联系供应商的服务和支持人员。本地书面手册必须随机器一起提供，存放在防护套内。供应商的 **Web** 站点上提供了手册的最新版本。
- 在每次使用之前，请测试验证稳定装置的制动功能。请勿在稳定装置制动咬合的情况下过度用力移动或翻滚起重工具。
- 在平台升高时请勿移动起重工具，微小的定位调整除外。
- 请勿超过额定的负荷容量。请参阅“负荷容量表”，了解延伸平台中心处和边缘处的最大负荷。
- 仅当负荷正确位于平台中心时，才能抬高负荷。还要考虑到负荷的质心/重心 (**CoG**)，因此请勿将超过 **200 磅 (91 千克)** 的重量置于滑动平台架的边缘。
- 请勿将平台倾斜立管附件选件放置在平台的一角。在使用前，仅通过提供的硬件，将平台立管倾斜选件固定到主支架的全部四 (**4x**) 个位置。负荷物体设计为在没有相应外力的情况下滑上/滑下光滑平台，因此请注意不要推或倚靠在这些对象上。除非需要进行最终微调，否则请始终使立管倾斜选件保持平放。
- 请勿站在突出的负荷下方。
- 请勿使用不平整的表面，无论是上倾还是下倾（大坡度）。
- 请勿堆积负荷。
- 请勿在受到药物或酒精影响的情况下进行操作。
- 请勿将梯子靠在起重工具上。
- 存在翻倒危险。请勿推动负荷或者将负荷倚靠在升高的平台上。
- 请勿用作人员升降平台或台阶。不得骑在上面。
- 请勿站在起重工具上的任何位置。不可将其用作台阶。
- 请勿攀爬主柱。
- 请勿操作已损坏或者发生故障的起重工具机器。
- 在平台下存在遭到挤压的危险。仅当下方没有任何人员和障碍物的情况下才能降低负荷高度。在操作期间，请确保手脚不放在负荷下方。
- 不得使用叉式升降。不得使用托盘车、液压车或叉车抬起或移动起重工具裸机。
- 主柱高于平台。请注意天花板高度、电缆槽、消防喷淋头、灯和其他头顶物件。
- 请勿在升起负荷的情况下离开起重工具机器的岗位。
- 在移动设备时注意观察，确保双手、手指和衣物不处于负荷下方。
- 只能用手转动绞盘。如果单手无法轻松转动绞盘手柄，那么可能已过载。请勿继续转动绞盘使之超过平台行程顶部或低于底部。过度松开绞盘会使手柄脱离并损坏缆线。在降低高度、解旋的过程中请始终握住手柄。在松开绞盘手柄前，请始终确保绞盘可承受负荷。
- 绞盘事故可能导致严重伤害。不得用于移动人员。请确保在抬起设备时听到咬合声。在松开手柄前请确保绞盘已锁定到位。在操作此绞盘前，请阅读指示信息页面。不得允许绞盘自由松开。自由松开将导致缆线不平整地缠绕在绞盘卷筒上、损坏缆线并且可能导致严重伤害。 (**C048**)

NEBS（网络设备构建系统）GR-1089-CORE 的电源和布线信息

下列注释适用于已指明符合 NEBS（网络设备构建系统）GR-1089-CORE 的 IBM 服务器：

设备适合安装在下列各项中：

- 网络远程通信设施

- NEC（国家电气法规）适用的位置

此设备的建筑物内端口仅适合连接至建筑物内或未裸露的电线或电缆。此设备的建筑物内端口不得通过金属连接至已与 OSP（户外装置）或其电线相连的接口。这些接口设计为仅用作建筑物内接口（2 类或 4 类端口，如 GR-1089-CORE 中所述），并需要与裸露的 OSP 电缆隔离。添加主要保护装置并不足以防止这些接口与 OSP 电线进行金属连接。

注：所有以太网电缆均必须屏蔽，并且两端接地。

交流电系统不需要使用外部浪涌保护器（SPD）。

直流电系统采用已隔离的直流电回流（DC-I）设计。直流电电池回流终端不得连接至机架或机架地线。

直流电系统适合安装在共用等电位连接网络（CBN）中，如 GR-1089-CORE 中所述。

安装和配置硬件管理控制台

描述如何安装硬件管理控制台 (HMC) 硬件、将其连接至受管系统并配置它以供使用。您可以亲自执行这些任务，也可以联系服务供应商来为您执行这些任务。服务供应商可能会收取服务费用。

注：虚拟化在 IBM Power® System S824L (8247-42L) 服务器上不受支持。

有关安装和配置 HMC 的新增内容

了解“安装和配置 HMC”主题中自从本主题集合上一次更新以来的新增信息或重大更改的信息。

2017 年 8 月

- HMC Classic 界面在硬件管理控制台 (HMC) V8.7.0 或更高版本中不再受支持。以前通过 HMC Classic 界面提供的功能现在通过 HMC 增强型+ 界面提供。
- 添加了下列主题：
 - 第 41 页的『将 7063-CR1 安装到机架中』
 - 第 136 页的『配置 BMC 连接』
- 添加了第 41 页的『将 7063-CR1 安装到机架中』主题。

2016 年 10 月

- 更新了第 15 页的『HMC 端口位置』主题。

2016 年 5 月

- 添加了第 33 页的『将 7042-CR9 HMC 安装到机架中』主题。

2015 年 10 月

- 添加了第 53 页的『安装 HMC 虚拟设备』主题。
- 更新了以下主题：
 - 第 77 页的『因特网 SSL 地址列表』
 - 第 79 页的『准备 HMC 配置』

2015 年 6 月

- HMC Enhanced + 技术预览 (Pre-GA) 界面 (它是 HMC V8.2.0 随附的选件) 与 HMC V8.3.0 随附的 HMC 增强型+ 界面具有相同的过程和功能。文档中仅引用了 HMC 增强型+，但是该内容也适用于 HMC Enhanced + 技术预览 (Pre-GA) 界面。
- HMC Enhanced 界面 (它是 HMC V8.2.0 随附的选件) 的过程和功能现在是 HMC V8.3.0 随附的 HMC 增强型+ 界面的一部分。
- 添加了第 113 页的『使用 HMC 增强型+ 界面配置 HMC』部分。
- 更新了第 102 页的『配置回拨事件管理器』主题。

2014 年 10 月

- 添加了下列主题：
 - 第 23 页的『将 7042-CR7 和 7042-CR8 安装到机架中』

- 第 102 页的『配置回拨事件管理器』
- 更新了第 89 页的『启动 HMC』主题。

2014 年 6 月

- 针对包含 POWER8 处理器的 IBM Power Systems 服务器增加了信息。

安装和配置任务

了解与不同 HMC 安装和配置任务相关联的任务。

本节描述安装和配置 HMC 时必须执行的高级任务。可使用不同方法来安装和配置 HMC。查找最适合要执行的的任务的情境。

注：如果要管理基于 POWER8® 处理器的服务器，那么 HMC 必须为 V8.1.0。有关更多信息，请参阅第 106 页的『确定 HMC 机器代码版本和发行版』。

安装和配置带有新服务器的新 HMC

了解有关安装和配置带有新服务器的新 HMC 时必须执行的高级任务的更多信息。

表 1. 安装和配置带有新服务器的新 HMC 时需要执行的任务

任务	在何处查找相关信息
1. 收集信息并填写安装前配置工作表	第 80 页的『HMC 的安装前配置工作表』 第 79 页的『准备 HMC 配置』
2. 打开该硬件的包装。	
3. 连接 HMC 硬件的电缆。	第 3 页的『独立 HMC 布线』 第 14 页的『机架安装式 HMC 布线』
4. 按下电源按钮以开启 HMC。	
5. 登录并启动 HMC Web 应用程序。	
6. 访问指导式安装向导或使用 HMC 菜单来配置 HMC。	第 87 页的『通过指导式安装向导使用快速路径来配置 HMC』 第 88 页的『使用 HMC 菜单配置 HMC』
7. 将服务器连接至 HMC。	

更新和升级 HMC 代码

了解有关更新和升级 HMC 代码时必须执行的高级任务的更多信息。

如果已有 HMC 并且要更新或升级 HMC 代码，那么必须完成下列高级任务：

表 2. 更新或升级 HMC 代码时需要执行的任务

任务	在何处查找相关信息
1. 获取升级。	第 109 页的『升级 HMC 软件』
2. 查看现有 HMC 机器代码级别。	
3. 备份受管系统的概要文件数据。	
4. 备份 HMC 数据。	
5. 记录当前 HMC 配置信息。	
6. 记录远程命令状态。	
7. 保存升级数据。	
8. 升级 HMC 软件。	
9. 验证 HMC 机器代码升级是否安装成功	

向现有安装添加另一 HMC

了解有关向受管系统添加另一 HMC 时必须执行的高级任务的更多信息。

如果已有 HMC 和受管系统并且要向此配置添加另一 HMC，请执行以下操作：

表 3. 向现有安装添加另一 HMC 时需要执行的任务

任务	在何处查找相关信息
1. 确保 HMC 硬件支持 HMC V7 代码。	
2. 收集信息并填写安装前配置工作表。	第 80 页的『HMC 的安装前配置工作表』
3. 打开该硬件的包装。	
4. 连接 HMC 硬件的电缆。	『独立 HMC 布线』 第 14 页的『机架安装式 HMC 布线』
5. 按下电源按钮以开启 HMC。	
6. 登录 HMC。	
7. HMC 代码级别必须匹配。更改其中一个 HMC 上的代码以匹配另一个 HMC 上的代码。	第 106 页的『确定 HMC 机器代码版本和发行版』 第 109 页的『升级 HMC 软件』
8. 访问指导式安装向导或使用 HMC 菜单来配置 HMC。	第 88 页的『使用 HMC 菜单配置 HMC』
9. 使用回拨设置向导来配置此 HMC 以获取服务。	第 98 页的『配置 HMC 以便它可与服务和支持联系』
10. 将服务器连接至 HMC。	

安装 HMC

在配置 HMC 软件之前，必须设置 HMC 硬件。了解有关设置桌面 HMC 或机架安装式 HMC 的更多信息。

独立 HMC 布线

放置 HMC 并用电缆连接每个硬件组件。

您可以将独立 HMC 用电缆连接至受管系统。

1. 确保将 HMC 置于正确的位置。
2. 将监视器电缆连接到监视器接口，并拧紧螺钉。

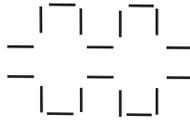
3. 将电源线连接到监视器。
4. 确保 HMC 上的电压选择开关设置为世界性区域使用的电压。电压选择开关是红色的，且位于电源接口附近。移动开关以便显示您所在地区使用的电压。
5. 将电源线插入到 HMC 中。
6. 将键盘和鼠标连接至 HMC。
7. 连接可选调制解调器：

注：在安装和配置 HMC 期间，当 HMC 执行例行的拨出过程时，调制解调器可能自动拨出。这是一种通常行为。

如果您要连接可选外置调制解调器，请执行以下操作：

注：可使用其他连接方法将错误信息发送至 IBM。

- a. 如果尚未连接外置调制解调器，那么请将调制解调器数据线连接至 HMC 外置调制解调器。
- b. 将调制解调器数据线连接至 HMC 上标有以下符号的系统端口：



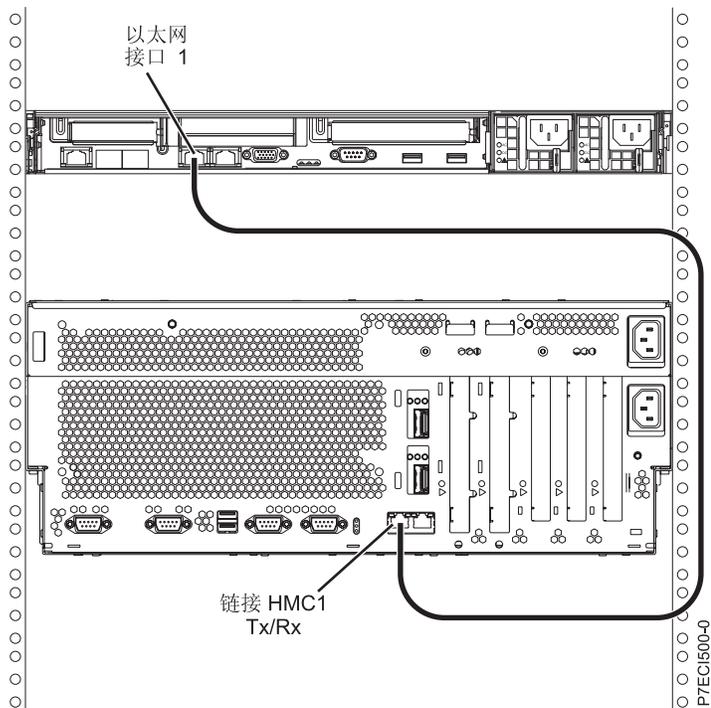
IPHA1522-0

- c. 使用电话线将外置调制解调器的 Line 端口连接到墙上的模拟信号电话插孔。

如果要连接至可选集成调制解调器，那么使用数据线将集成的 HMC 调制解调器连接至适当的数据源。例如，使用电话线将 HMC 调制解调器的 Line 端口连接到墙上的模拟信号插孔。

注：可使用其他连接方法将错误信息发送至 IBM。

8. 如果已安装受管系统，那么可在安装过程中通过同时观察 HMC 和受管系统以太网端口的绿色状态灯来验证以太网电缆连接是否处于活动状态。
9. 将 HMC 上的以太网连接器 **1** 连接至受管系统上的 **LINK HMC1** 端口。



10. 如果要将第二个 HMC 连接至受管服务器，那么将它连接至受管服务器上标有 **LINK HMC2** 的以太网端口。
11. 如果您使用的是外置调制解调器，那么将调制解调器电源线插入 HMC 调制解调器。
12. 将监视器、HMC 和 HMC 外置调制解调器的电源线插入到电源插座中。如果要将此 HMC 连接至新的受管系统，那么此时不要将该受管系统连接至电源。

接下来需要配置 HMC 软件。继续执行第 87 页的『配置 HMC』。

相关概念:

第 74 页的『决定要用于回拨服务器的连接方法』

了解有关使用回拨服务器时可使用的连接选项的更多信息。

第 71 页的『HMC 网络连接』

将 7310-CR4 HMC 安装到机架中

本节描述如何将 7310-CR4 HMC 安装到机架中。这是一个客户任务。

如果 HMC 用来管理任何基于 POWER7® 处理器的系统，那么该 HMC 必须为 CR3 或更高级别型号的机架安装式 HMC。

以下是 7310-CR4 的后视图：

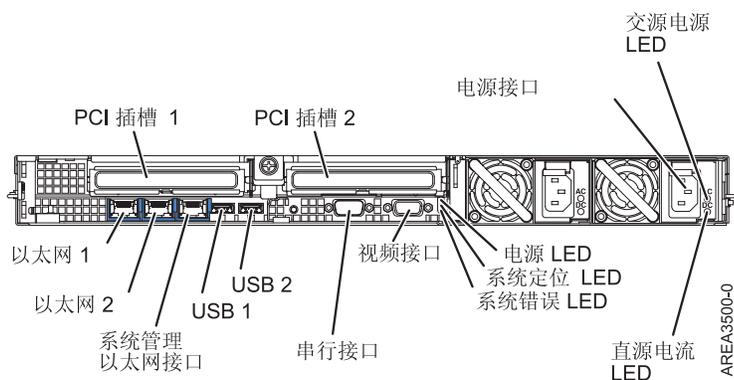


图 1. 7310-CR4 的后视图

要将 7310-CR4 HMC 安装到机架中，请完成以下步骤：

1. 清点部件清单。请参阅清点部件清单。
2. 找到机架安装硬件工具箱和随系统部件一起提供的系统导轨组合件。

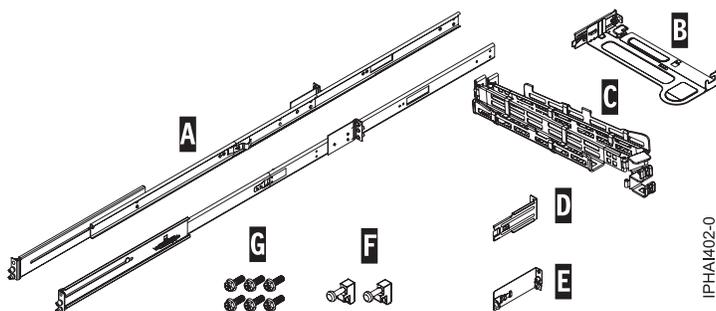


图 2. 导轨工具箱

表 4. 导轨工具箱部件

滑轨工具箱部件

- A 滑轨
- B 电缆管理臂安装托盘
- C 电缆管理臂
- D 电缆固定支架
- E 电缆固定托架和保护卡扣
- F 锁扣 (2)
- G 螺钉 (6)

要点：此系统部件的高度为 1 个 EIA 单位；您需要知道此信息才能完成安装。

清点部件清单

您可能需要清点部件清单。使用本节中的过程执行此任务。

如果您尚未清点部件清单，请清点之后再继续安装。

1. 找到附件箱中的工具清单。
2. 确保您已收到订购的所有部件。

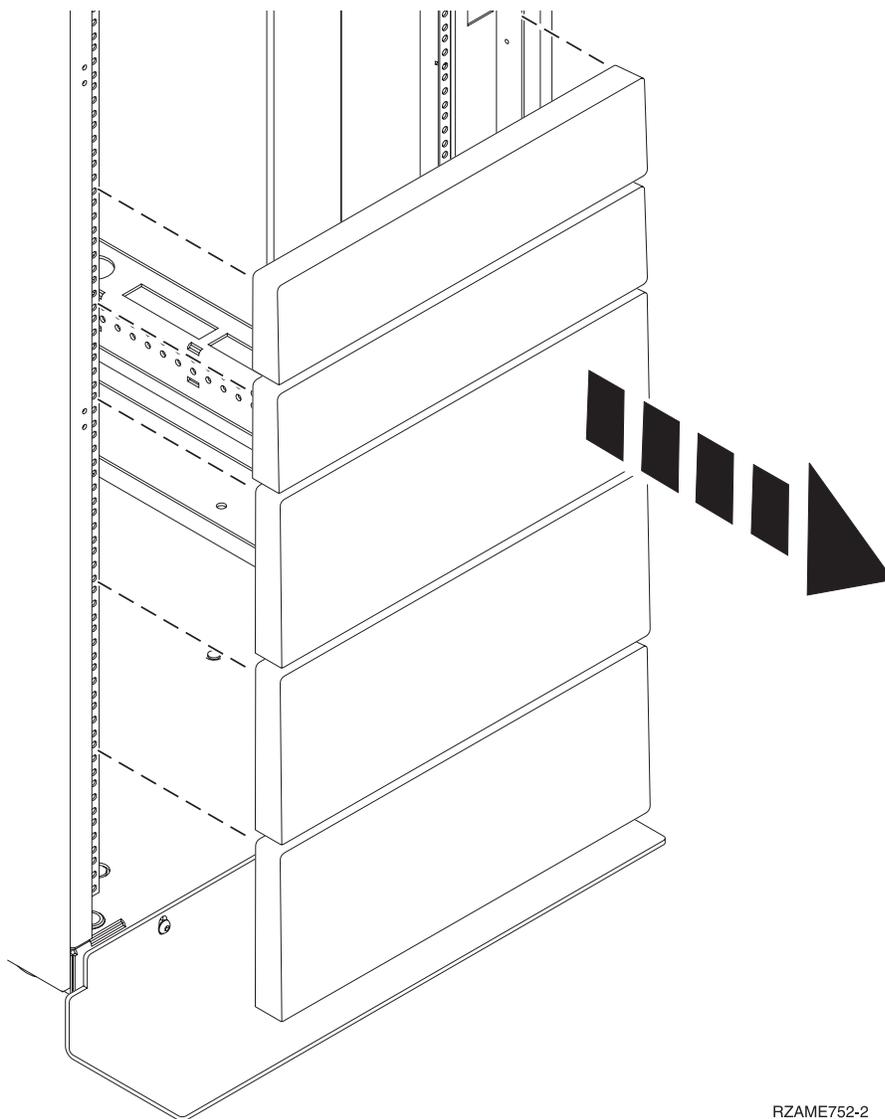
如果有不正确、遗漏或损坏的部件，请联系 IBM 经销商或 IBM 销售与支持。

确定位置

您可能需要确定将在机架的什么位置安装系统。本节包含一些过程，以便您可以执行这些任务。

将 HMC 安装到机架之前，请完成以下步骤：

1. 规划将放置部件的位置。请将较大和较重的部件放置在机架下部。
2. 如果机架包含填充板，那么请除去这些填充板，以便可以检修到计划放置部件的机架箱内部。



RZAME752-2

图 3. 除去填充板。

3. 如果有必要，请卸下机架的前门和后门。
4. 要遵循在没有模板的情况下标记位置的指示信息，请参阅在没有机架安装模板的情况下标记位置。

在不使用机架安装模板的情况下标记位置：

您可以在不使用模板的情况下标记位置。

本系统不包含机架安装模板。这些系统的高度为 1 个 EIA 单位。

要确定安装位置，请完成下列步骤：

1. 确定将系统放置在机架中。记录 EIA 位置。

注：机架上的一个 EIA 单位由三个孔组成。

2. 面向机架正面并从右边开始将一块提供的不干胶贴到 EIA 单位的顶部孔的旁边。

注：不干胶用于帮助标识机架上的位置。如果用完了不干胶，请使用其他标记工具来帮助标识孔位置，例如，胶带、记号笔或铅笔。如果您要安装滑轨，请在每个 EIA 单位的下部孔和中间孔上作标记或贴上不干胶。

3. 将另一块不干胶贴到该 EIA 单位上面的下部孔。

注：如果您要数孔，请从第一块不干胶标识的孔开始并向上数两个孔。将第二块不干胶贴到第三个孔旁边。

4. 对位于机架左边的相应孔重复步骤 1。
5. 移至机架后端。
6. 在右边，找到与机架前端标记的底部 EIA 单位对应的 EIA 单位。
7. 将一块不干胶贴到底部 EIA 单位上。
8. 将一块不干胶贴到该 EIA 单位的顶部孔上。
9. 标记机架左边的相应孔。

将滑轨安装到机架

了解如何将滑轨安装到机架。

要将滑轨安装到机架，请完成以下步骤：

1. 将标有 right 的右滑轨 (A) 插入机架右后端的机架安装凸缘 (B) 位置。两个导轨锁钉将穿过 EIA 单位上的底部孔和中间孔 (B)。

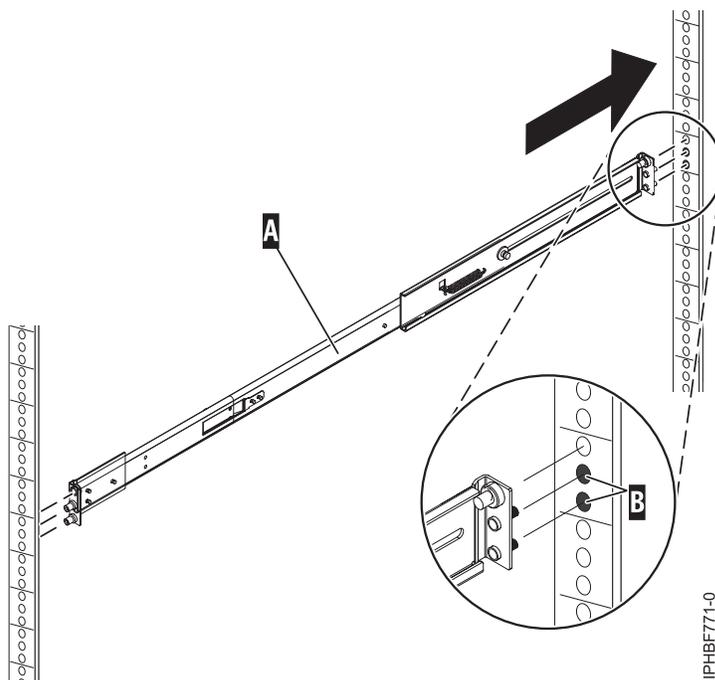


图 4. 将右滑轨安装到机架后端

2. 推送导轨 (A) 的端部，以压缩导轨上装有弹簧的机械装置，并将导轨插入机架右前端的安装凸缘 (B) 位置。导轨将松开，并且两个导轨锁钉将穿过 EIA 单位上的底部和中间孔 (B)。

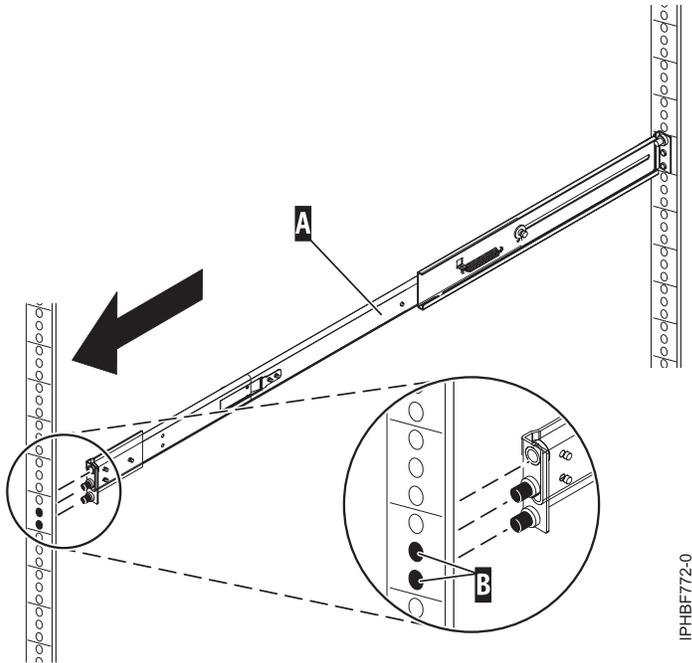


图 5. 将右滑轨安装到机架前端

3. 重复步骤 第 8 页的 1 - 2 以将标有 *left* 的左滑轨安装到机架中。
4. 从机架前端，将锁扣 (C) 放置在锁钉上。用手指将外加螺丝 (D) 拧入右滑轨 (A) 前端的顶部锁钉上。

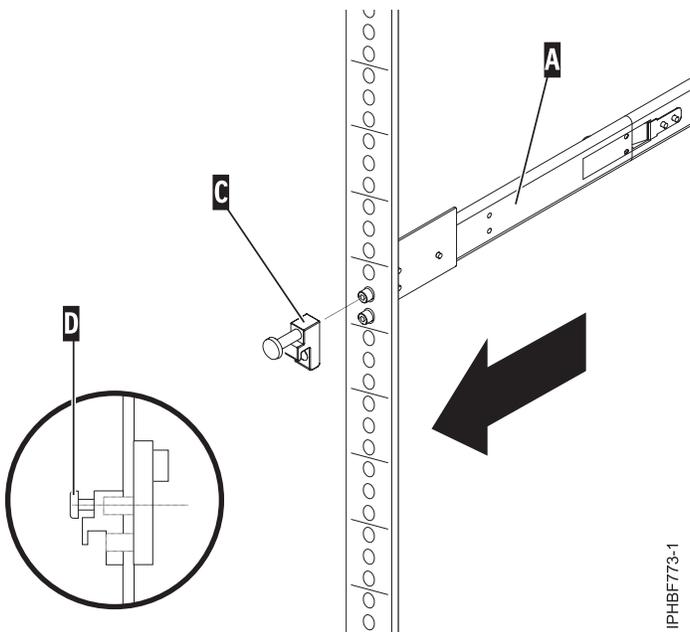


图 6. 将锁扣安装到导轨前端

5. 重复上一步以将锁扣安装在左滑轨的前端。
6. 移到机架背面。锁紧螺钉 (F) 以将电缆管理臂安装支架 (E) 连接到左导轨 (G) 的后端。

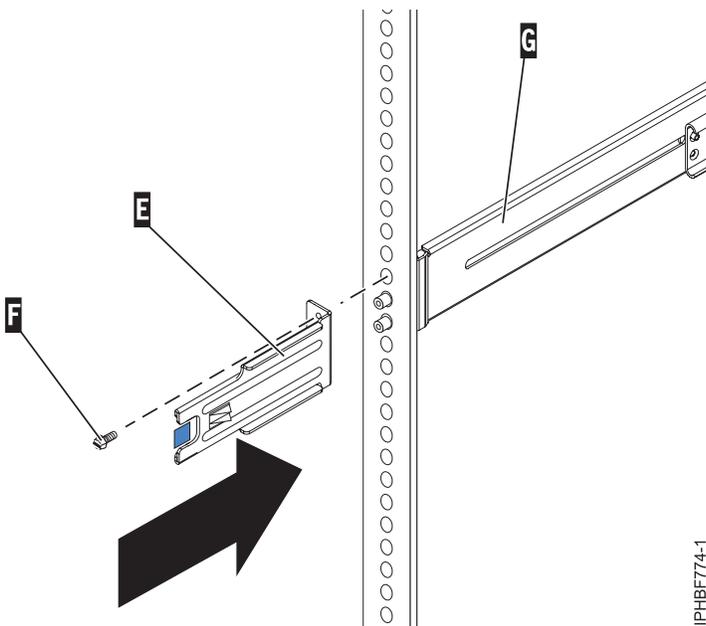


图 7. 将电缆管理支架连接到左导轨后端

7. 如果未计划传输此系统，请继续执行第 11 页的『在滑轨上安装 HMC』。如果打算运输此系统，请插入螺钉 (I) 以将电缆固定托架 (H) 连接到右导轨 (A) 后端。用手指拧紧该螺钉。

电缆固定托架可以用来在运输期间固定电缆管理臂。如果在安装电缆管理臂之后未取下该机械，那么您无法将系统从机架中滑出。

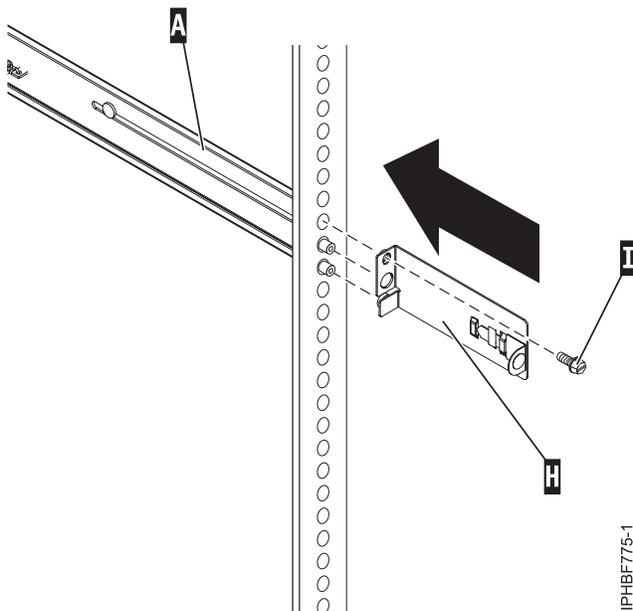


图 8. 将电缆固定托架连接到右导轨后端。

在滑轨上安装 HMC

您可能需要在滑轨上安装 HMC。使用本节中的过程执行此任务。

在滑轨上安装 HMC 之前，请确保已展开稳定器并且已将机架稳定支架连接到机架前端的底部，以防止在从机架中拉出导轨时机架向前倾倒。

要在滑轨组合件上安装 HMC，请完成以下步骤：

1. 从 HMC 的右边拆卸包含电源的搬运支架。要拆卸搬运支架，请将该支架向右边推，然后将它旋出 HMC。
2. 从机架前端，将滑轨完全伸长，直到将导轨锁定在伸长位置 **(A)**。

警告： 在将 HMC 安装到导轨上之前，必须安装导轨前端的锁扣和电缆管理臂支架。如果未安装这些部件，那么安装过程可能会导致导轨受压而变形，并且 HMC 可能跌出机架。

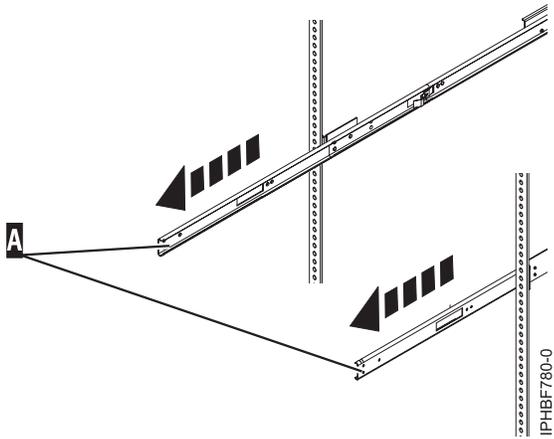


图 9. 伸长滑轨

要点：此部件的重量大约为 17 公斤（37 磅）。您在将 HMC 安装到机架时，一定要能够把握十足地支撑此重量。

3. 将 HMC 抬起至与导轨相同的高度，并将 HMC 后端的一组轮子 **(B)** 放置到导轨导槽之间。

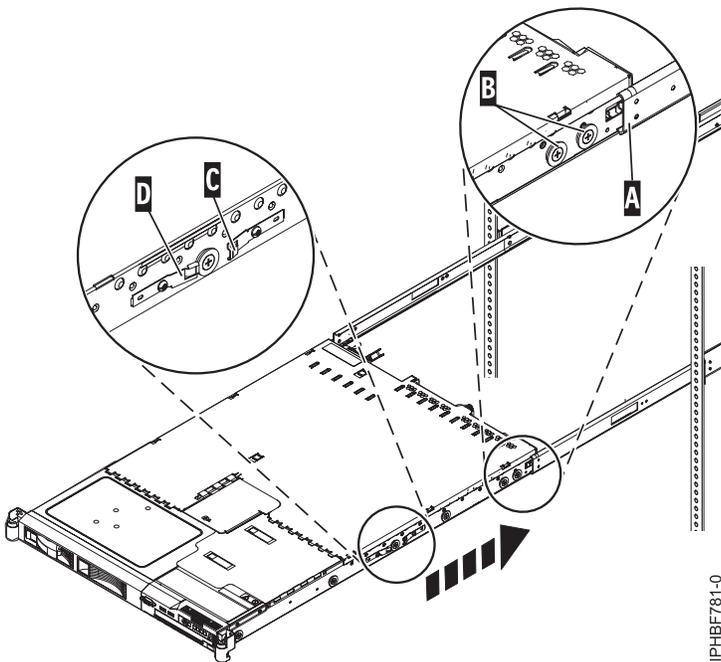


图 10. 在滑轨上安装 HMC。

4. 将 HMC 推入滑轨，直到滑钩 **(C)** 卡入锁定位置。这样将使系统锁定在滑轨上的服务位置。您会听到一声卡嗒声。
5. 在滑轨的两边按滑轨前端的释放插销 **(D)**。
6. 将 HMC 滑入和滑出机架，以验证 HMC 可以随意移动而没有被卡住。

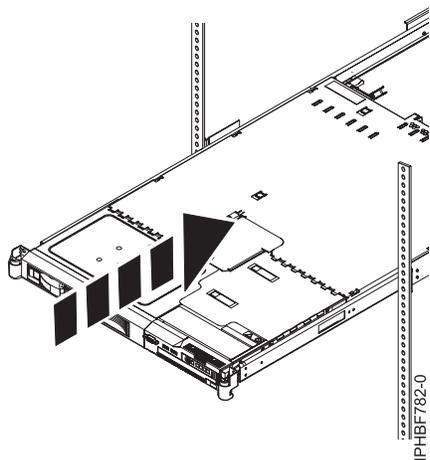


图 11. 将 HMC 滑入机架

要点: 在任何情况下, 都不要将 HMC 强行推入滑轨。如果 HMC 不能随意滑入机架, 请将 HMC 从导轨上完全拆卸下来。在将 HMC 从导轨上拆卸下来之后, 重新定位 HMC, 然后将 HMC 重新插入导轨。重复此过程, 直到 HMC 可以随意滑入机架。

7. 推送 HMC 直到机架撞锁 (F) 进入锁定位置。

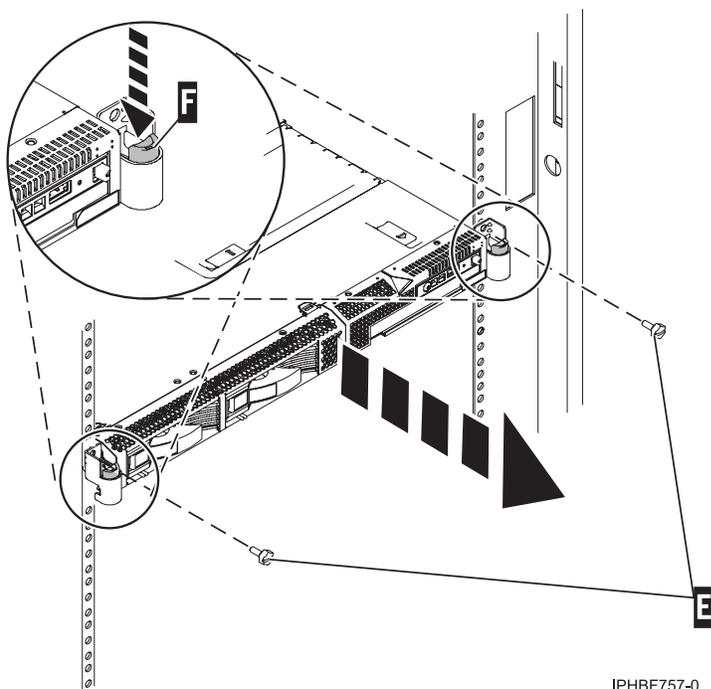


图 12. 机架撞锁和螺钉

8. 充分拧紧两条导轨各自在前端和后端安装的四个螺钉。
9. 如果将搬运机架, 请插入并拧紧两个机架保护螺钉 (E)。

安装电缆管理臂

您可能需要安装电缆管理臂。使用本节中的过程执行此任务。

要安装电缆管理臂, 请完成以下步骤:

1. 在机架的后端, 找到位于左边系统导轨组合件 (从机架背面看) 的固定后端部分的电缆管理臂凸缘 (A)。

2. 通过将电缆管理臂夹扣 (B) 推送到导轨上的锁定位置, 将该夹扣连接到导轨。

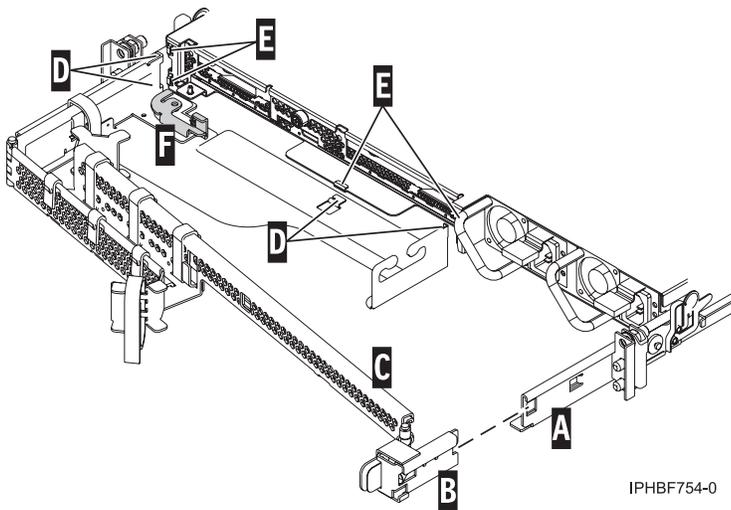


图 13. 电缆管理臂和系统部件。

3. 将电缆管理臂 (C) 的另一端连接到 HMC 的后端。将电缆管理臂上的卡扣 (D) 与 HMC 后端的槽口 (E) 对齐。
4. 将电缆管理臂滑向左边并将它固定。确保所有卡扣都已卡入槽口。
5. 将锁定杆 (F) 推入锁定位置。确保电缆管理臂 (C) 保持水平, 以便它不会随意移动。

机架安装式 HMC 布线

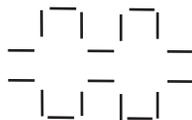
了解如何从物理上安装机架安装式 HMC。

1. 确保将 HMC 置于正确位置。
2. 将 HMC 安装到机架。有关更多信息, 请参阅第 5 页的『将 7310-CR4 HMC 安装到机架中』。将 HMC 安装到机架后, 请继续执行下一步。
3. 将电源线插入 HMC。
4. 连接键盘、监视器和鼠标。
5. 连接可选调制解调器:

如果您要连接外置调制解调器, 请执行以下步骤:

注: 可使用其他连接方法将错误信息发送至 IBM。有关更多信息, 请参阅第 74 页的『决定要用于回拨服务器的连接方法』。

- a. 如果要将外置调制解调器安装到机架, 请立即安装。
- b. 如果尚未连接外置调制解调器, 那么请将调制解调器数据线连接至 HMC 外置调制解调器。
- c. 将调制解调器数据线连接至 HMC 上标有以下符号的系统端口:



IPHAI522-0

- d. 使用电话线将外置调制解调器的 Line 端口连接到墙上的模拟信号电话插孔。

e. 将调制解调器电源线插入到 HMC 调制解调器中。

如果要连接至集成调制解调器，那么使用数据线将集成的 HMC 调制解调器连接至适当的数据源。例如，使用电话线将 HMC 调制解调器的 Line 端口连接到墙上的模拟信号插孔。

注：可使用其他连接方法将错误信息发送至 IBM。有关更多信息，请参阅第 74 页的『决定要用于回拨服务器的连接方法』。

6. 将以太网（或交叉）电缆从 HMC 连接至受管服务器。

注：要了解有关 HMC 网络连接的更多信息，请参阅第 71 页的『HMC 网络连接』。

7. 如果已安装受管系统，那么可在安装过程中通过同时观察 HMC 和受管系统以太网端口的绿色状态灯来验证以太网电缆连接是否处于活动状态。

8. 将 HMC 上的以太网端口连接至受管服务器上标有 **HMC1** 的以太网端口：

9. 如果要将第二个 HMC 连接至受管服务器，那么连接至受管服务器上标有 **HMC2** 的以太网端口。

10. 将监视器、HMC 和 HMC 外置调制解调器的电源线插入电源插座。

注：如果要将此 HMC 连接至新的受管系统，那么此时不要将该受管系统连接至电源。

接下来需要配置 HMC 软件。继续执行第 87 页的『配置 HMC』。

HMC 端口位置

您可以通过使用位置代码查找部件位置。使用 HMC 端口位置图将位置代码映射至服务器上的 HMC 端口位置。

型号 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置

使用以下图和表来映射 8247-21L、8247-22L、8284-21A 或 8284-22A 上的 HMC 端口。

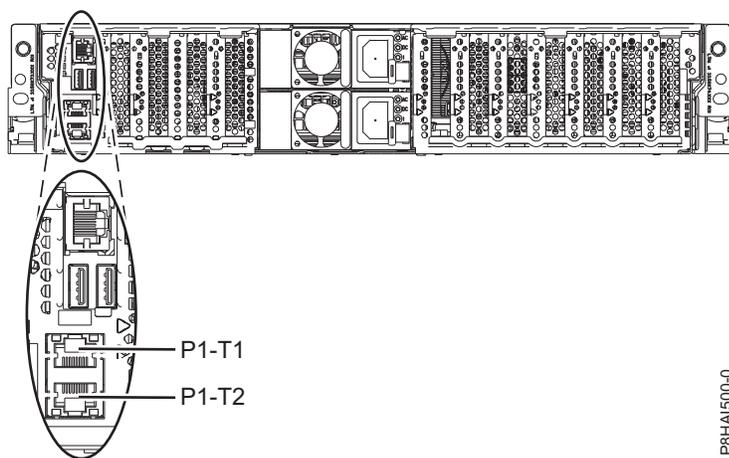


图 14. 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置

表 5. 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置

端口	物理位置码	标识 LED
HMC 端口 1	Un-P1-T1	否
HMC 端口 2	Un-P1-T2	否

表 5. 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置 (续)

端口	物理位置码	标识 LED
有关 8247-21L、8247-22L、8284-21A 或 8284-22A 上的 HMC 端口位置的更多信息，请参阅 8247-21L、8247-22L 或 8284-22A 的部件位置和位置码。		

型号 8247-42L、8286-41A 或 8286-42A HMC 端口位置

使用以下图和表来映射 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口。

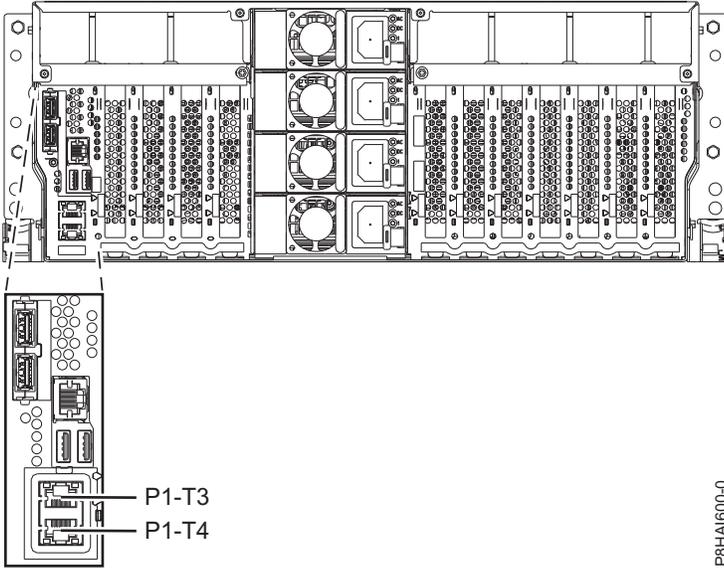


图 15. 机架视图 - 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口位置

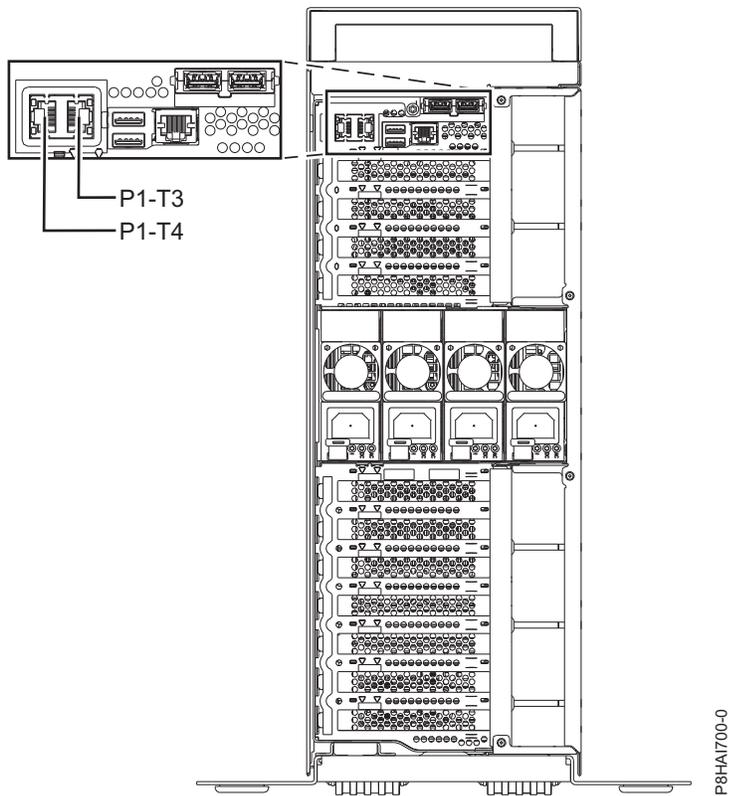


图 16. 关于 8286-41A 上 HMC 端口位置的塔式机柜视图

表 6. 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口位置

端口	物理位置码	标识 LED
HMC 端口 1	Un-P1-T3	否
HMC 端口 2	Un-P1-T4	否

有关 8247-42L、8286-41A 或 8286-42A 上 HMC 端口位置的更多信息，请参阅 8247-42L、8286-41A 或 8286-42A 的部件位置和位置码。

型号 9080-MHE、9080-MME、9119-MHE 和 9119-MME HMC 端口位置

使用以下图和表来映射 9080-MHE、9080-MME、9119-MHE 和 9119-MME 上的 HMC 端口。

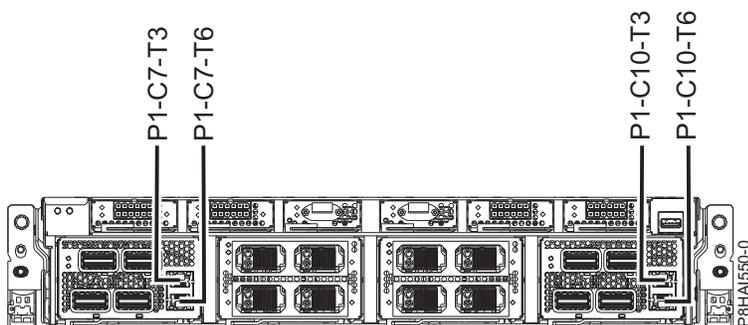


图 17. 9080-MHE、9080-MME、9119-MHE 和 9119-MME HMC 端口位置

表 7. 9080-MHE、9080-MME、9119-MHE 和 9119-MME HMC 端口位置

端口	物理位置码	标识 LED
服务处理器卡 1 - HMC 端口 1	Un-P1-C7-T3	否
服务处理器卡 1 - HMC 端口 2	Un-P1-C7-T6	否
服务处理器卡 2 - HMC 端口 1	Un-P1-C10-T3	否
服务处理器卡 2 - HMC 端口 2	Un-P1-C10-T6	否

有关 9080-MHE、9080-MME、9119-MHE 和 9119-MME 上的 HMC 端口位置的更多信息，请参阅 9080-MHE、9080-MME、9119-MHE 或 9119-MME 位置的部件位置和位置码。

型号 8408-44E 和 8408-E8E HMC 端口位置

使用以下图和表来映射 8408-44E 和 8408-E8E 上的 HMC 端口。

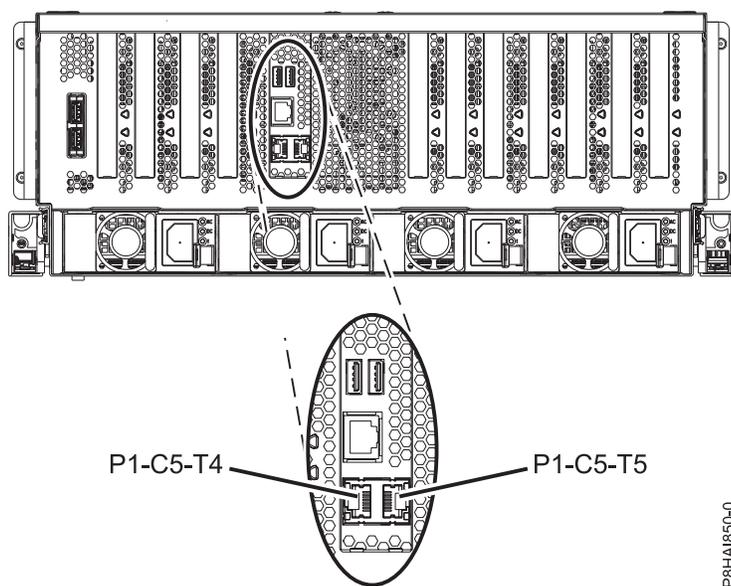


图 18. 8408-44E 和 8408-E8E HMC 端口位置

表 8. 8408-44E 和 8408-E8E HMC 端口位置

端口	物理位置码	标识 LED
HMC 端口 1	Un-P1-C5-T4	否
HMC 端口 2	Un-P1-C5-T5	否

有关 8408-44E 和 8408-E8E 上的 HMC 端口位置的更多信息，请参阅 8404-44E 和 8408-E8E 位置的部件位置和位置码。

将 7042-CR5 和 7042-CR6 安装到机架中

本节描述如何将 7042-CR5 和 7042-CR6 HMC 安装到机架中。

清点部件清单。下图显示在机架机柜中安装服务器所需的项。如果缺少或已损坏任何项，请与购买地点的服务人员联系。

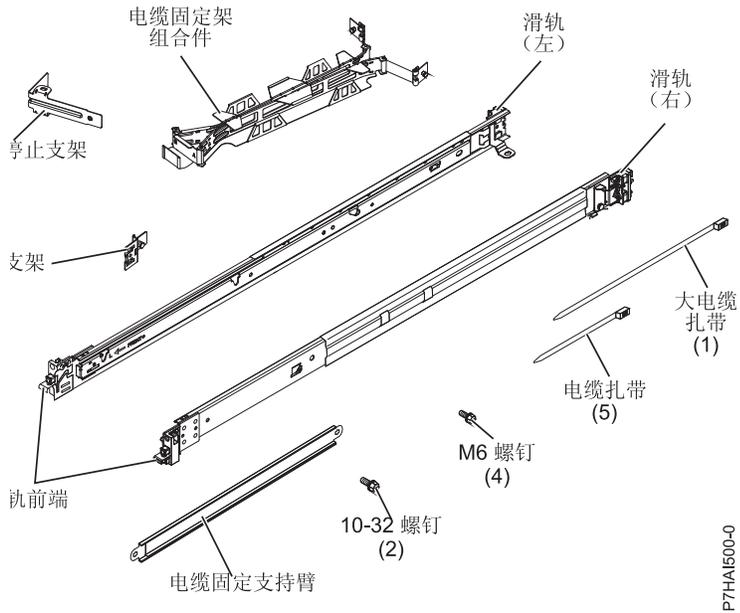


图 19. 部件清单

注：螺钉可用于装运，或用于在高震区域中维持额外稳定性。

要将 7042-CR5 或 7042-CR6 HMC 安装到机架中，请完成以下步骤：

1. 每个滑轨都标有 R (右) 或 L (左)。请选择其中一个滑轨并将前面的可移动卡扣 (1) 向上托起；然后，将前面的撞锁 (2) 拉出，以从前端导轨中滑出。如果翼形螺钉安装在滑轨 (3) 中，请将它除去。

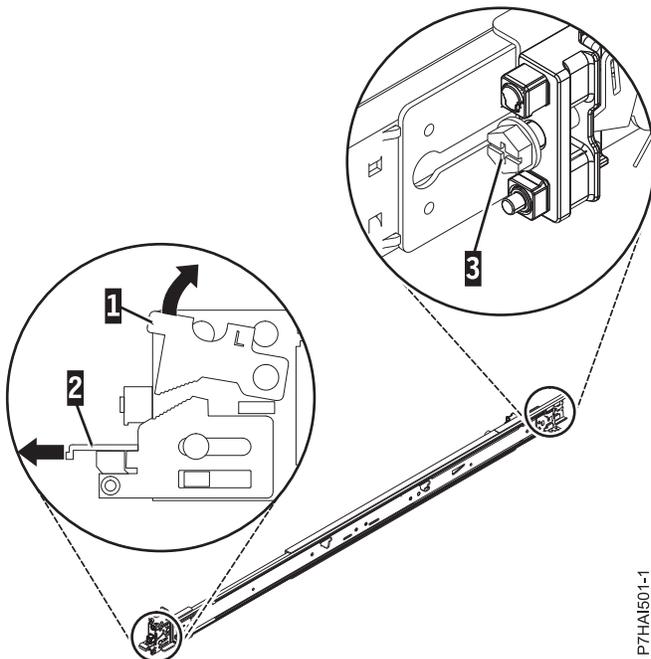


图 20. 滑轨和可移动卡扣

注：请确保可移动卡扣保持伸长，并且不会锁定在原位置。

- 将滑轨后端的三个锁钉与机架后端的所选 U 中的三个孔对齐。推送导轨，以便这些锁钉进入这些孔 (1) 中，并使滑轨 (2) 下坠，直到它锁定到位。

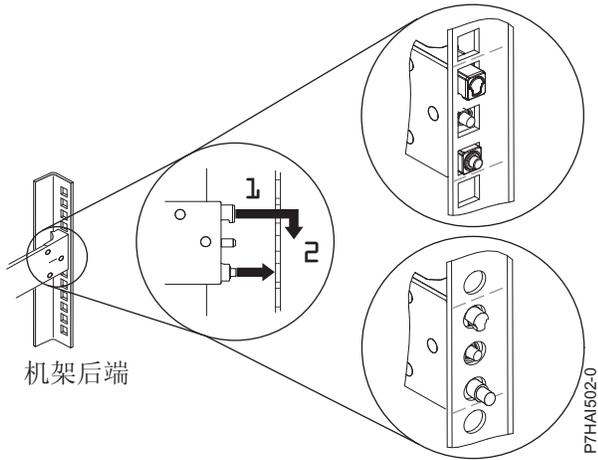


图 21. 使锁钉与机架后端中的孔对齐

- 将滑轨向前拉，并将导轨前端的两个锁钉 (1) 插入机架前端上的 U 中位置较低的两个孔中。使导轨就位，直到它锁定到位。尽力推送前面的撞锁 (2)。重复步骤 1 至 3 以将另一导轨安装到机架中。确保每个前面的撞锁都完全就位。

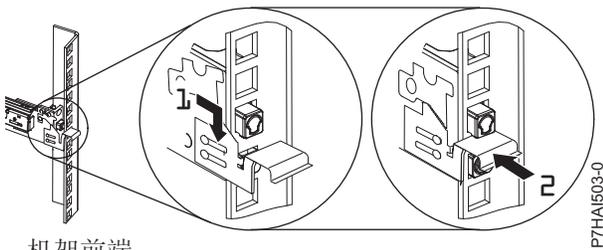


图 22. 机架前导轨和锁钉

- 将滑轨 (1) 向前拉，直到它们锁定到位（两次咔嚓声）。小心抬起服务器，并使它侧倾到滑轨上相应位置，以便服务器上后端的钉头 (2) 与滑轨上后端的插槽 (3) 对齐。使服务器向下滑动，直到后端的钉头滑进后端的两个插槽，然后缓慢地放低服务器 (4) 的前端，直到其他钉头滑进滑轨上的其他插槽。确保前面的撞锁 (5) 在这些钉头上方滑动。

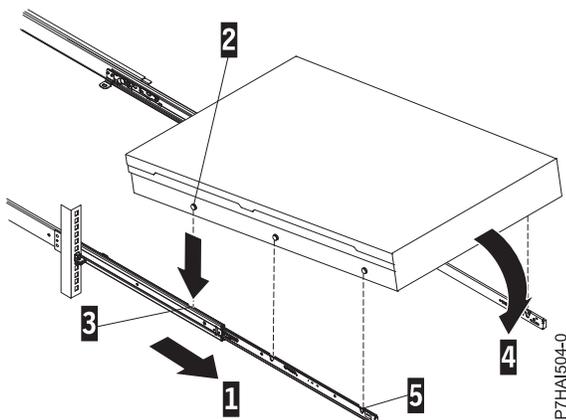


图 23. 滑轨伸长并且服务器钉头与导轨中的插槽对齐

5. 抬起滑轨上的蓝色释放插销 (1)，并将服务器 (2) 尽力推送到机架中，直到它锁定到位。

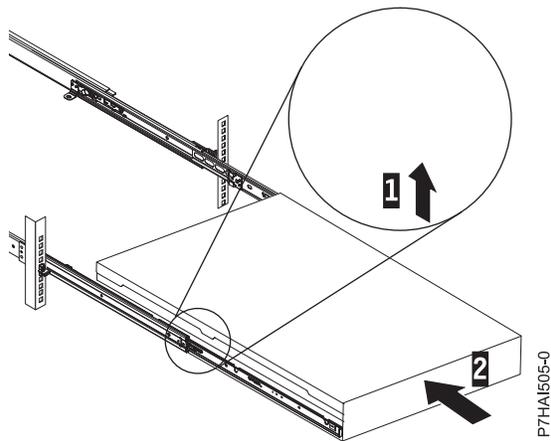


图 24. 释放插销和服务器

6. 电缆管理臂可以安装在服务器的任何一侧。下图显示在左侧安装电缆管理臂时的情况。要在右侧安装电缆管理臂，请遵循指示信息并在对侧上安装硬件。将支持臂 (1) 的一端连接至计划要连接电缆管理臂的滑轨，以便您可以使支持臂 (2) 的另一端朝机架旋转。

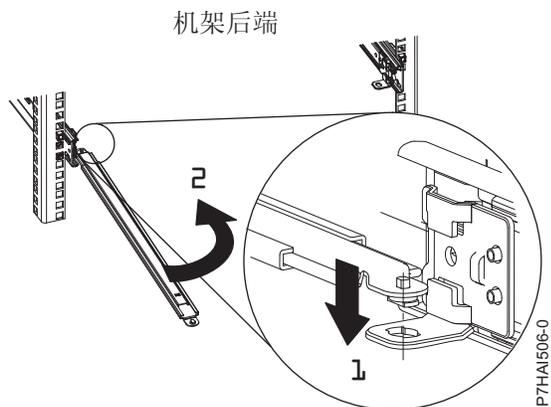


图 25. 支持臂连接

7. 将 L 形的电缆管理固定支架 (1) 安装在支持臂的未连接端。转动支架 (2) 以将它固定到支持臂。

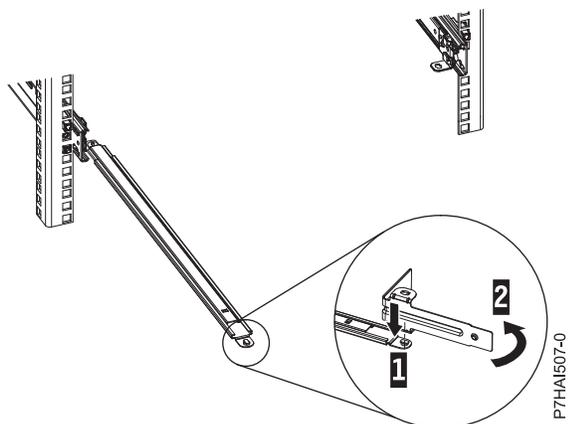


图 26. 固定到支持臂的电缆管理固定支架

8. 要将支持臂的另一侧连接至滑轨的后部，请将锁钉 (1) 拉出，然后将支架 (2) 滑入滑轨中。

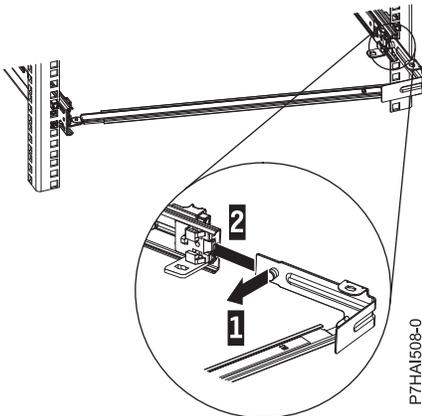


图 27. 锁钉伸长并且支架安装到滑轨中

9. 将安装支架锁钉 (1) 拉出并将安装支架 (2) 滑入您正在安装电缆管理臂的滑轨中。将该支架推送到滑轨中，直到带有弹簧的锁钉锁定到位。

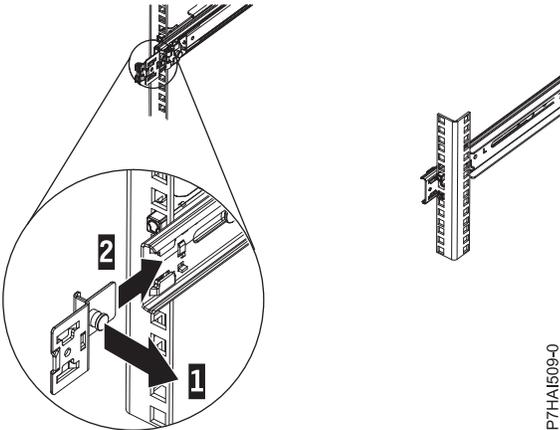


图 28. 安装支架锁钉伸长并且安装支架安装到滑轨中

10. 将电缆管理臂放置于支持臂上。将电缆管理臂锁钉 (1) 拉出，然后将电缆管理臂卡扣 (2) 滑入滑轨内部的插槽中。推送该卡扣，直到它锁定到位。将另一电缆管理臂锁钉 (3) 拉出，然后将电缆管理臂卡扣滑入滑轨外部的插槽 (4) 中。推送该卡扣，直到它锁定到位。

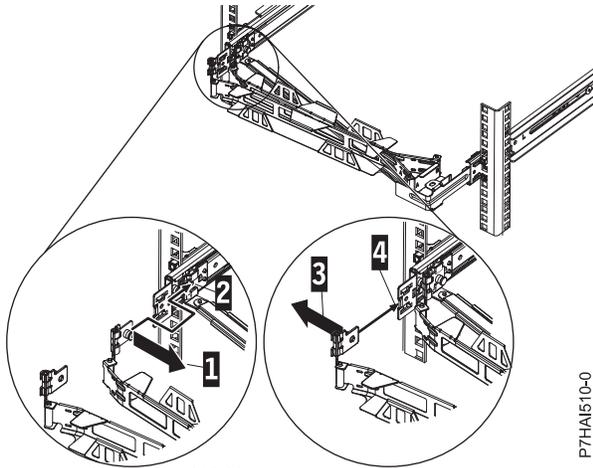


图 29. 电缆管理臂连接

11. 将电源线和其他电缆连接至服务器（需要时，包括键盘、监视器和鼠标电缆）的后端。对电缆管理臂 **(1)** 上的电缆和电源线进行线路规划，并通过电缆扎带或钩环固定器来对它们进行固定。

注：允许所有电缆中存在松弛情况，以避免当电缆管理臂移动时这些电缆中出现拉紧状态。

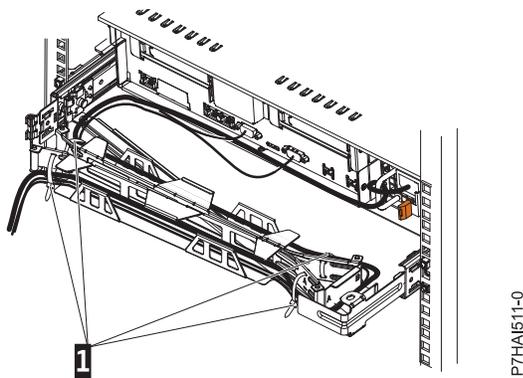


图 30. 电源线连接和路由

12. 将服务器滑入机架中，直到它锁定到位。

将 7042-CR7 和 7042-CR8 安装到机架中

了解如何将 7042-CR7 和 7042-CR8 硬件管理控制台 (HMC) 安装到机架中。

清点部件清单。以下各图显示了在机架式机箱中安装服务器时所需的物品。如果缺少或已损坏任何项，请与购买地点的服务人员联系。

电缆管理臂包装箱内物品

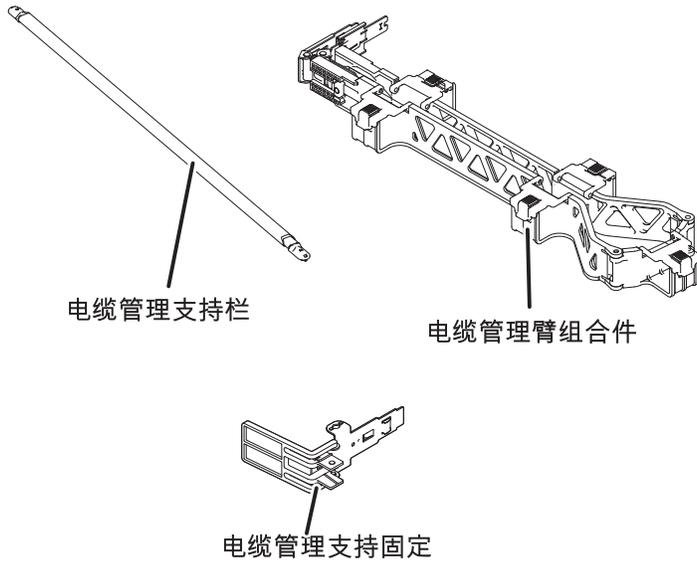


图 31. 电缆管理臂包装箱内物品

导轨箱内物品

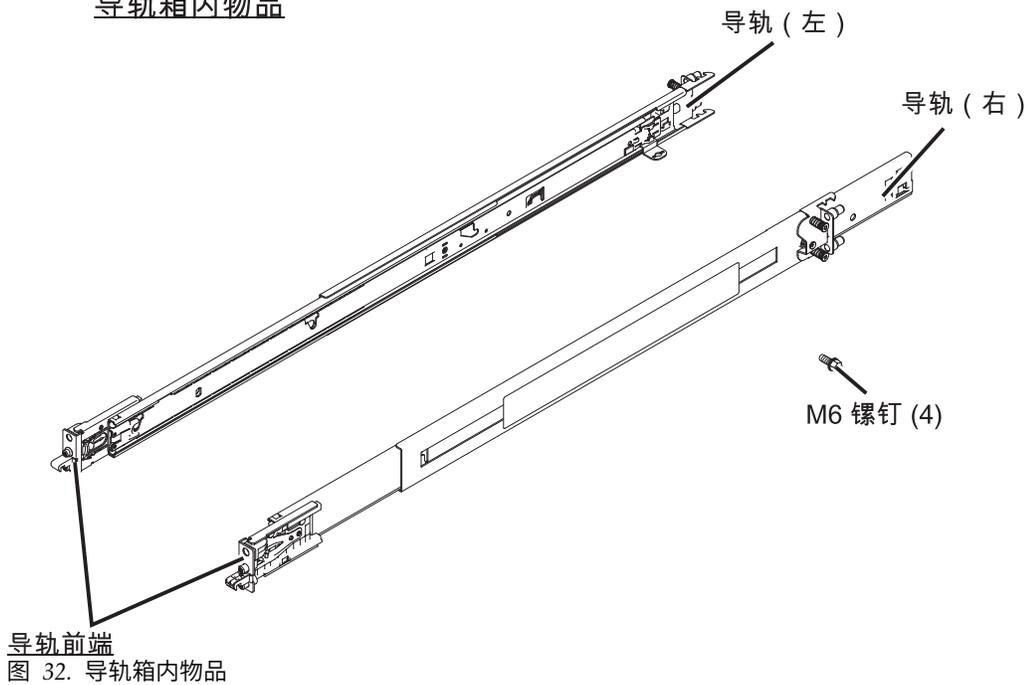


图 32. 导轨箱内物品

注：您需要使用滑轨箱和电缆管理臂箱来执行该安装。

要将 7042-CR7 或 7042-CR8 HMC 安装到机架中，请完成以下步骤：

1. 选择机架中可用的 1 单位或 2 单位空间（这取决于您正在安装的服务器）来安装服务器。

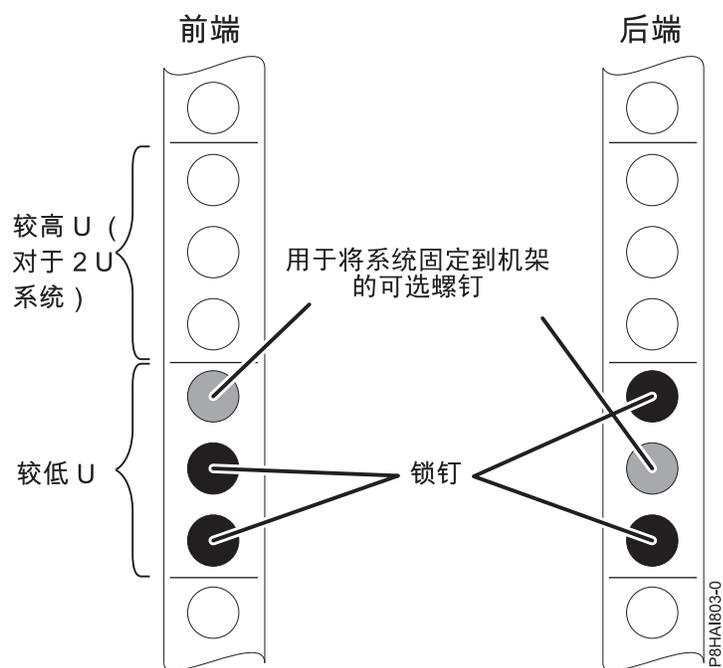


图 33. 识别机架空间

注：当您安装 2 单位服务器时，请确保将滑轨安装在机架中 2 U 区域的较低 U 中。

2. 每个滑轨都在其末端标记为左前/后端或右前/后端。选择其中一根滑轨，然后将后部支架一直往后拉，直至其锁定到位。

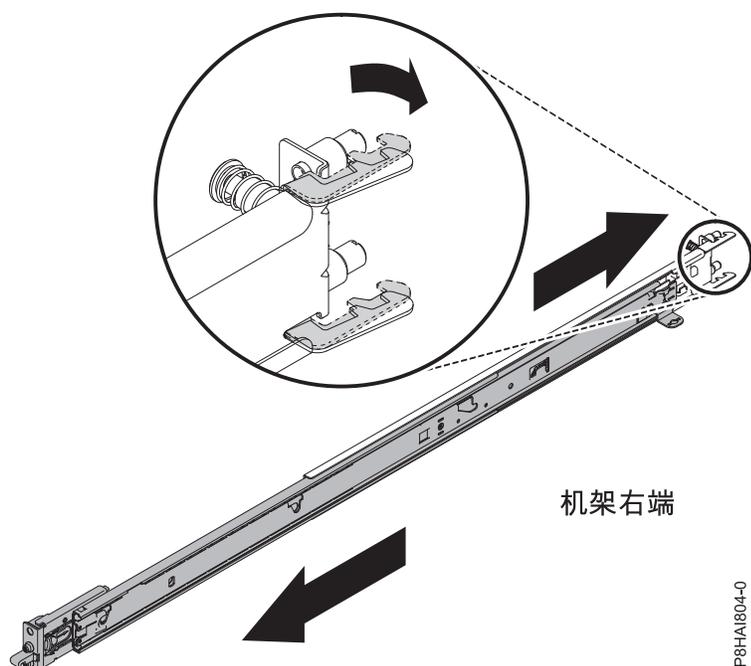


图 34. 滑轨和可移动卡扣

注：请确保可移动卡扣保持伸长，并且不会锁定在原位置。

3. 从机架前部，将机架后部所选 U 中滑轨后部的两个锁钉对齐。推送导轨以使锁钉进入孔中，然后将导轨滑入机架以将滑轨的后部锁定到机架中。

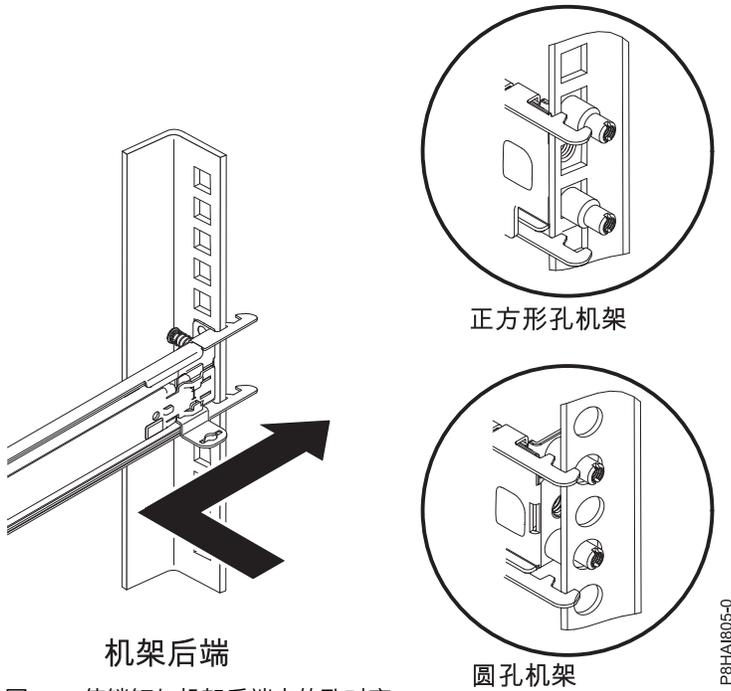


图 35. 使锁钉与机架后端中的孔对齐

注：如果要安装到 1 U 空间并且已将设备直接安装在此 1 U 空间上方或下方，那么必须伸长导轨以将导轨的后端滑入机架的后端。

4. 打开前部滑轨插销。如果在接收它们时将其关闭，请通过推入蓝色按钮并推送锁定架来打开插销。

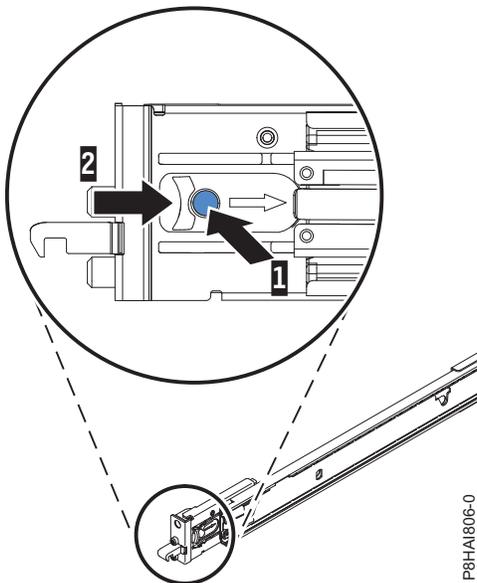


图 36. 前部滑轨插销

5. 向前拉动滑轨，并在机架 EIA 导轨前部的相应 U 空间中找到前部插销。调整导轨的长度。请确保前端已旋转到位，并且机架 EIA 导轨前部具有前部插销。

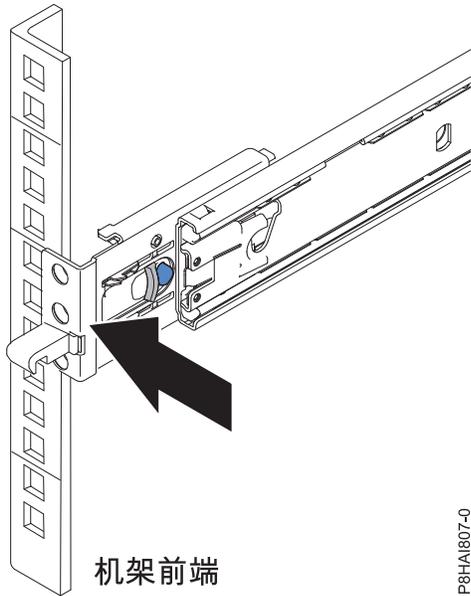


图 37. 机架前导轨和锁钉

P8HA1807-0

- 按蓝色按钮以使用锁钉合上支架。将滑轨上移和下移以确保导轨完全咬合。重复步骤 1 至 5 以将另一导轨安装到机架中。确保每个前部插销都完全咬合。

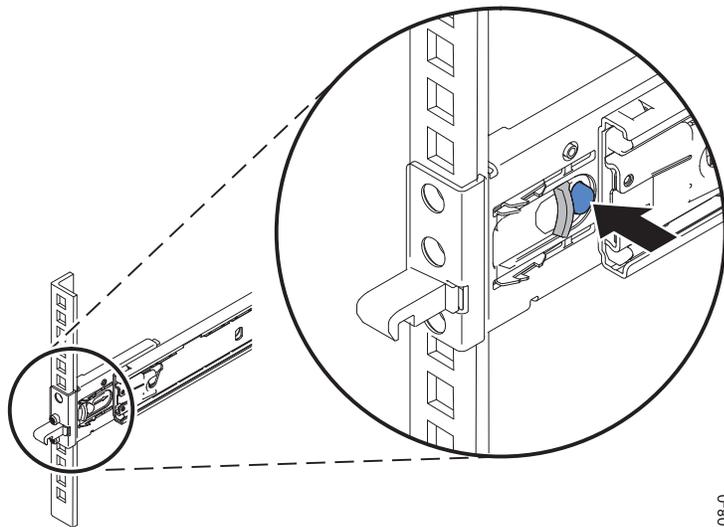


图 38. 机架前导轨和锁钉

P8HA1808-0

- 将滑轨 **(1)** 向前拉，直到它们锁定到位（两次咔嚓声）。小心抬起服务器，并使它侧倾到滑轨上相应位置，以便服务器上后端的钉头 **(2)** 与滑轨上后端的插槽对齐。放低服务器，直到后端的钉头滑进后端的两个插槽，然后缓慢地放低服务器 **(3)** 的前端，直到其他钉头进入滑轨上的其他插槽（听到咔嚓声两次）。确保前部插销覆盖前端钉头，以便系统固定到滑轨。

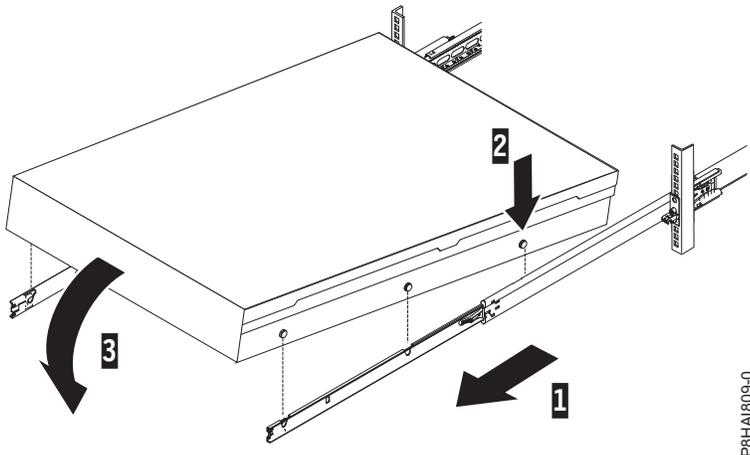


图 39. 滑轨伸长并且服务器钉头与导轨中的插槽对齐

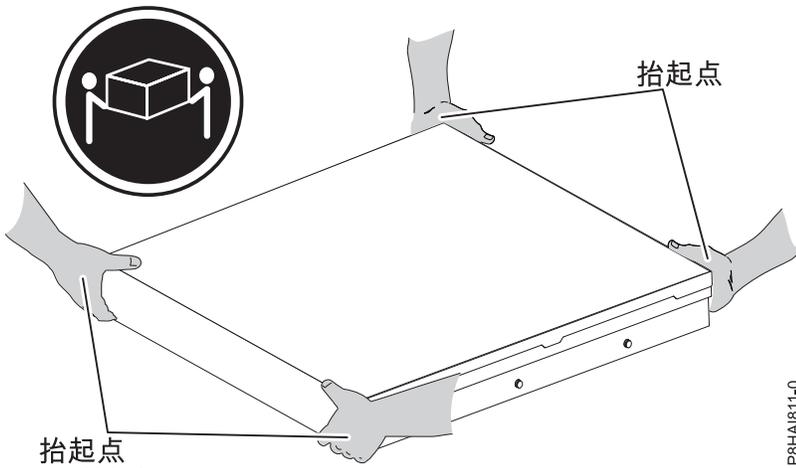


图 40. 抬起点

注：抬起时，请使用安全的做法。如果要安装 2 U 服务器，请确保由两个人抬起服务器。他们的手必须定位，如图 40 中所示。

8. 抬起滑轨上的锁定拉杆 (1)，并将服务器 (2) 尽力推送到机架中，直到它锁定到位。

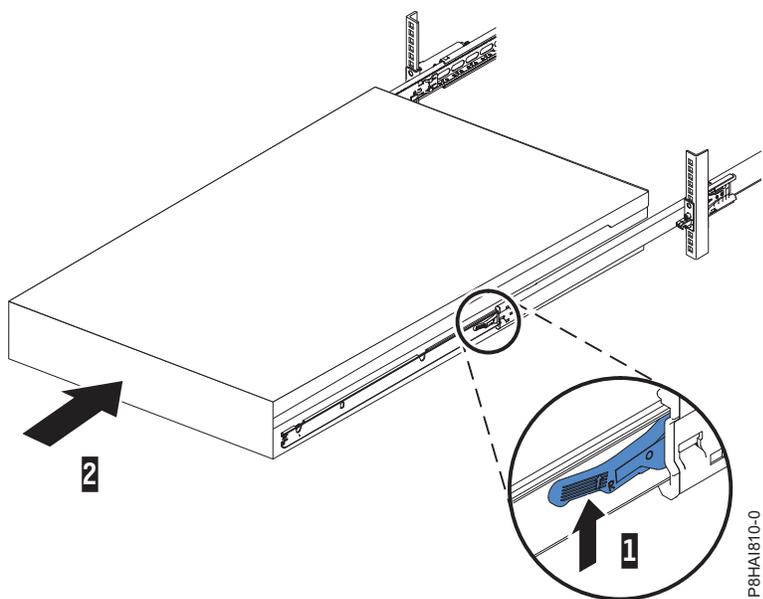


图 41. 释放插销和服务器

9. 电缆管理臂可以安装在服务器的任何一侧。下图显示在左侧安装电缆管理臂时的情况。要在右侧安装电缆管理臂，请遵循指示信息并在对侧上安装硬件。将支持臂 (1) 的一端连接至计划要连接电缆管理臂的滑轨，以便您可以使支持臂 (2) 的另一端朝机架旋转。

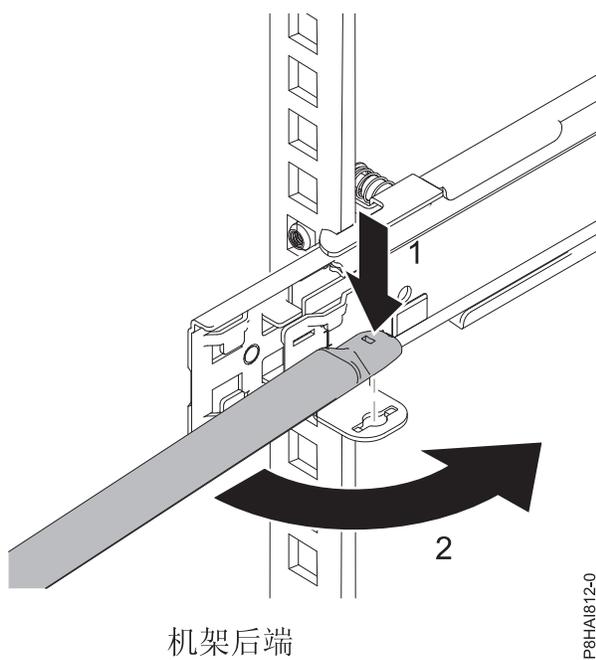


图 42. 支持臂连接

10. 将支持臂的另一端连接到电缆管理固定支架 (1)。转动支架 (2) 以将它固定到支持臂。

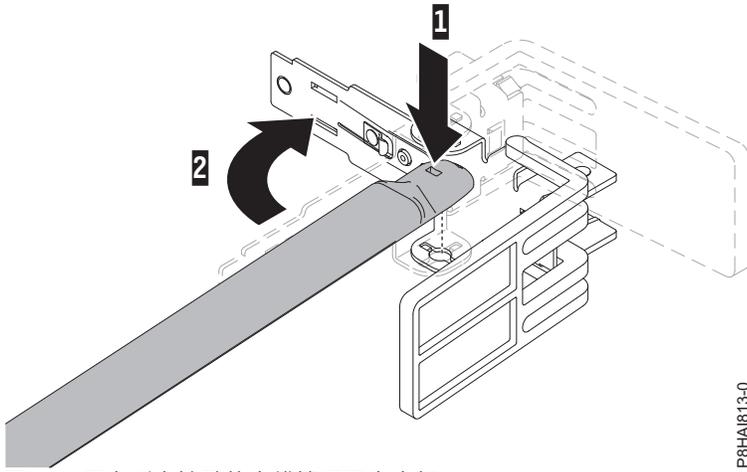


图 43. 固定到支持臂的电缆管理固定支架

P8HA1813-0

11. 电缆管理臂锁钉上印有大写字母 **I** 和 **O**，标识内部和外部锁钉。在支持臂未连接端上安装电缆管理固定支架（具有大写字母 **O**）。确保支持臂已安全地安装。

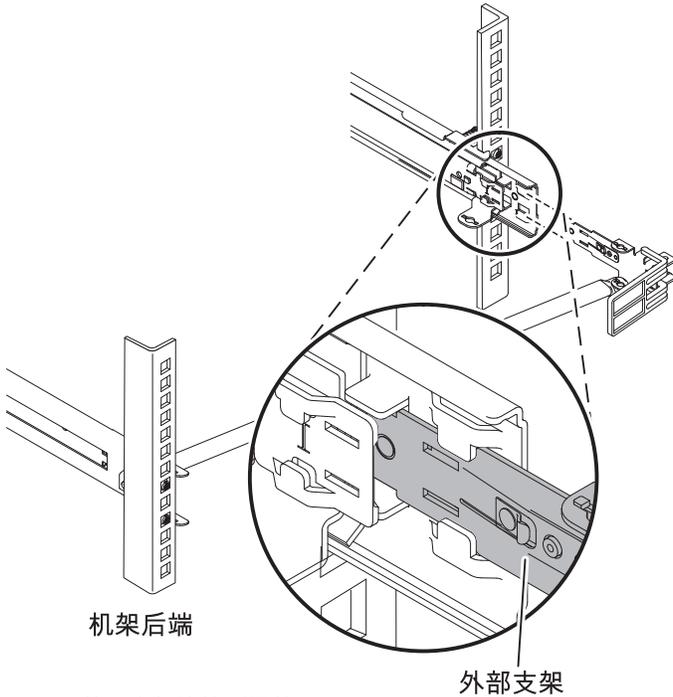


图 44. 将固定架连接到滑轨

P8HA1814-0

12. 将电缆管理臂放置在支持臂上。拉出电缆管理臂的内外侧锁钉，然后将电缆管理臂卡扣滑入滑轨内侧和外侧上的插槽中。推动卡扣直至其咬合到位。

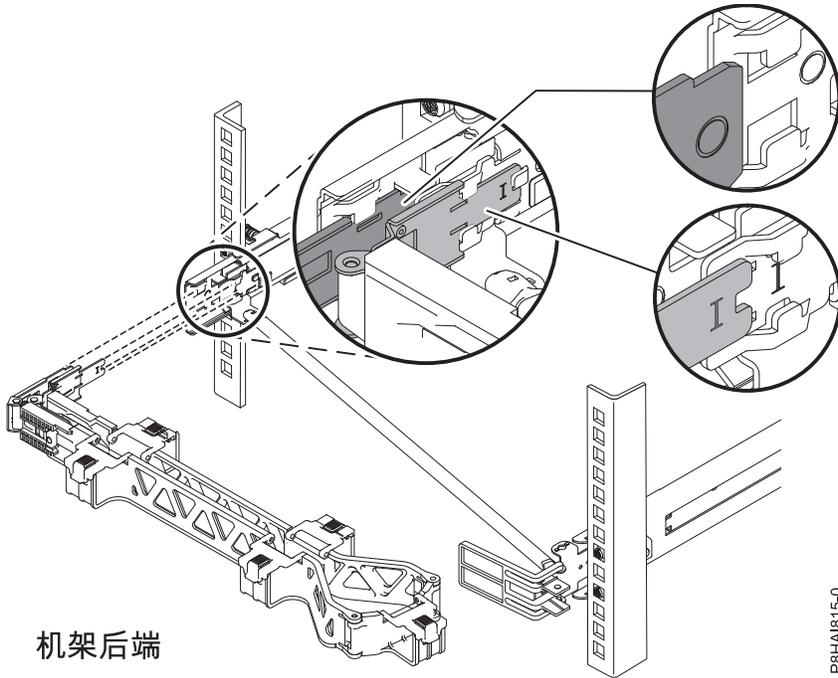


图 45. 电缆管理臂连接

13. 要使得电缆管理支持臂上的电缆管理臂旋紧和旋松更容易，可以向上推动卡扣来打开固定架，向下推动卡扣来关闭固定架。

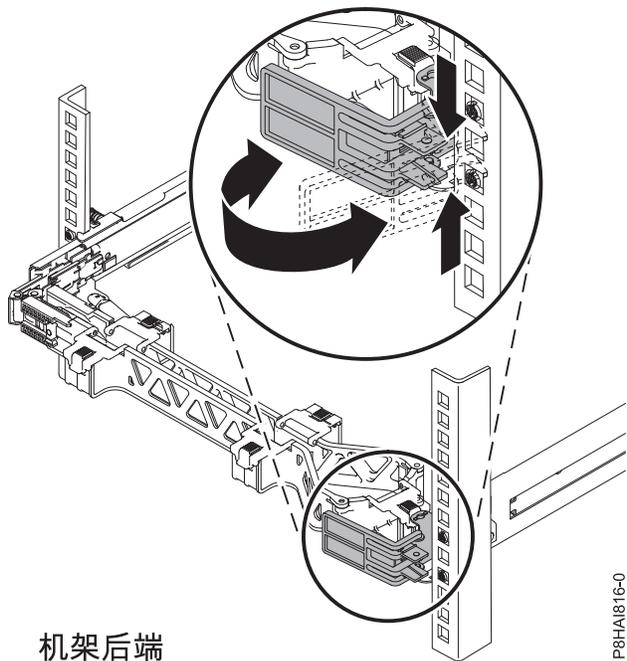


图 46. 电缆管理支持固定

14. 将电源线和其他电缆连接至服务器（需要时，包括键盘、监视器和鼠标电缆）的后端。将电缆与电源线路由在电缆管理臂上，并使用电缆扎带或钩环固定器将它们固定。

注：电缆皮带的位置可能与其他系统稍有不同。使用系统后端提供的电缆皮带固定电缆，防止它们下垂。

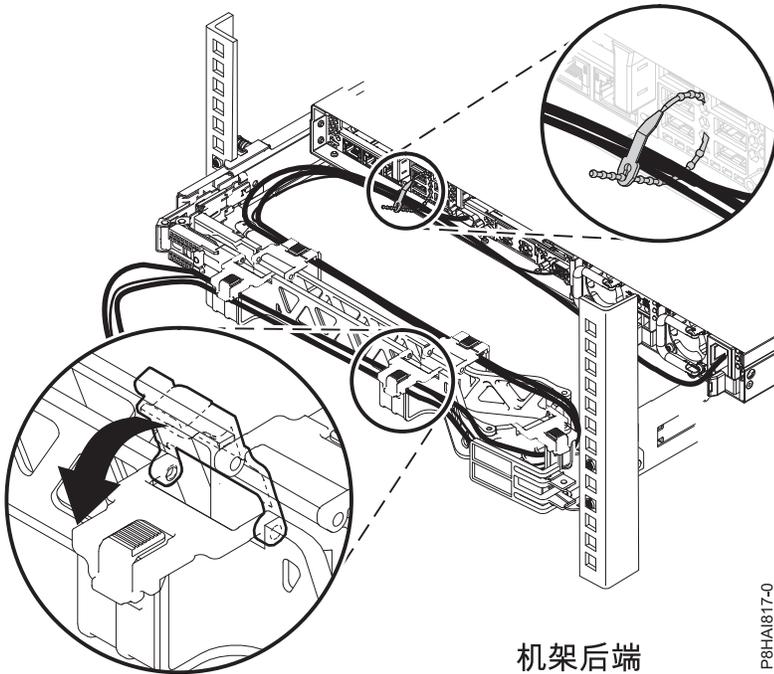


图 47. 电源线连接和电缆的路由路线

15. 必须使用钩环固定器捆绑电缆以便电缆管理臂可以进行适当的移动。

注：请确保电缆不会下垂到 U 空间的下方，这样它们不会缠到下方的系统。允许所有电缆中存在松弛情况，以避免当电缆管理臂移动时这些电缆中出现拉紧状态。

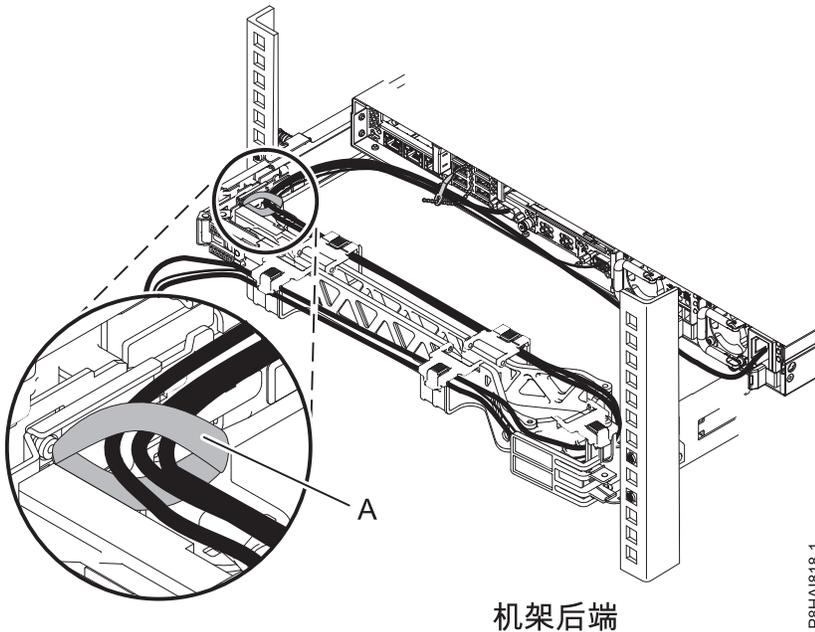
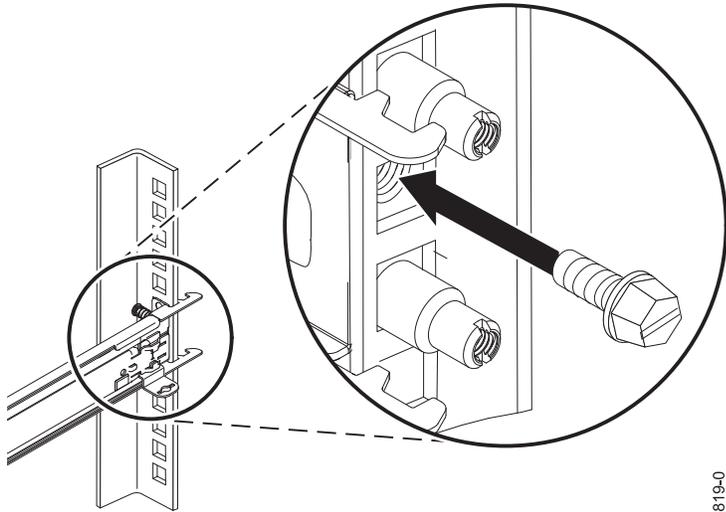


图 48. 钩环固定器

16. 如果要装运安装了系统的机架，或者您处于易振动的区域，请将 M6 镙钉插入滑轨的后端。使用电缆扎带将电缆管理臂的活动端固定到机架（如果需要）。



机架后端

图 49. 固定好服务器以进行装运

P8HA1819-0

将 7042-CR9 HMC 安装到机架中

了解如何将 7042-CR9 硬件管理控制台 (HMC) 安装到机架中。

清点部件清单。以下各图显示了在机架式机箱中安装服务器时所需的物品。如果缺少或已损坏任何项，请与购买地点的服务人员联系。

电缆管理臂包装箱内物品

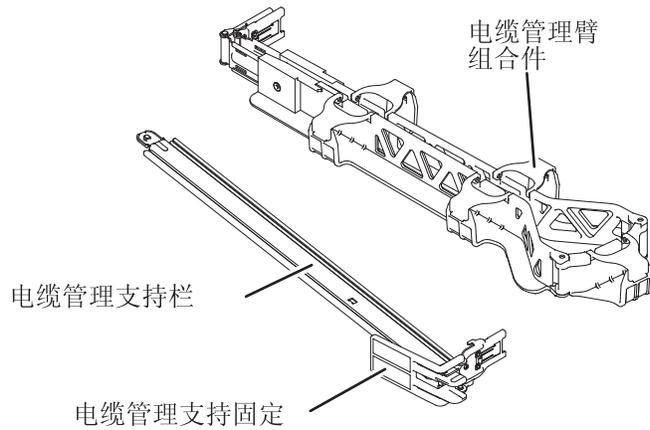
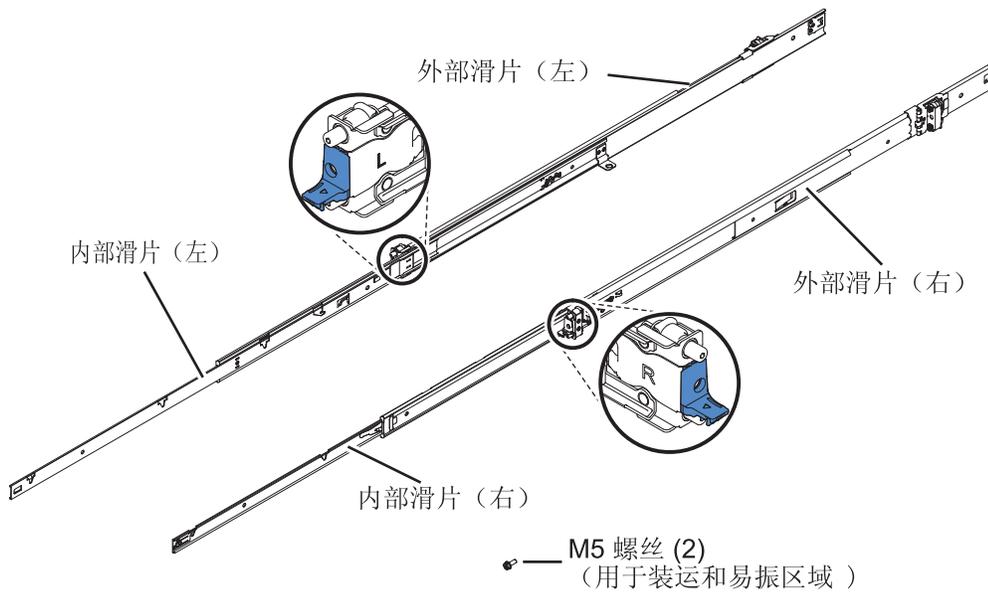


图 50. 电缆管理臂包装箱内物品

P8HA1750-0

导轨箱内物品



P8HA1751-0

图 51. 导轨箱内物品

注：该安装需要滑轨包装箱和电缆管理臂包装箱。

要将 7042-CR9 HMC 安装到机架中，请完成以下步骤：

1. 选择机架中的可用空间（取决于要安装的服务器）以安装服务器。

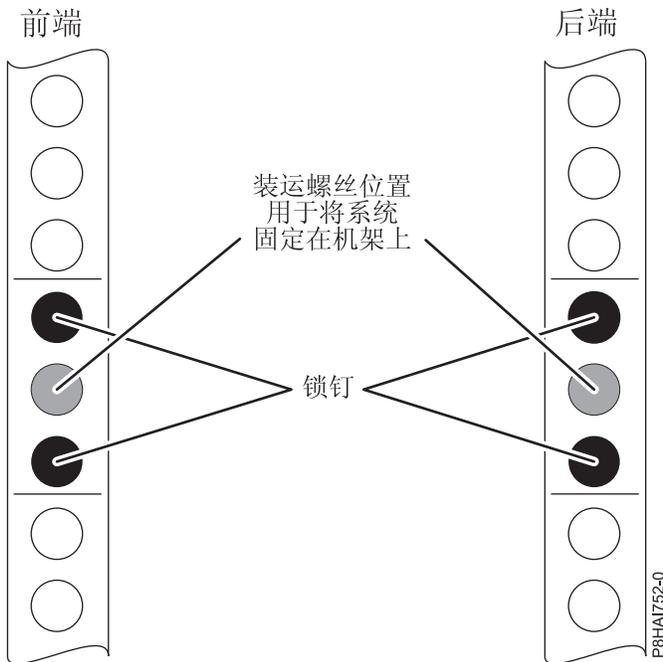


图 52. 识别机架空间

注：您需要 1 个单位 (1 U) 的空间，并且滑轨安装在 1 个单位空间的底部单位 (U) 中。

2. 将外部滑片伸长到尽头，直到听到发出咔嗒声。后部机架装配支架现在已旋转解锁位置。

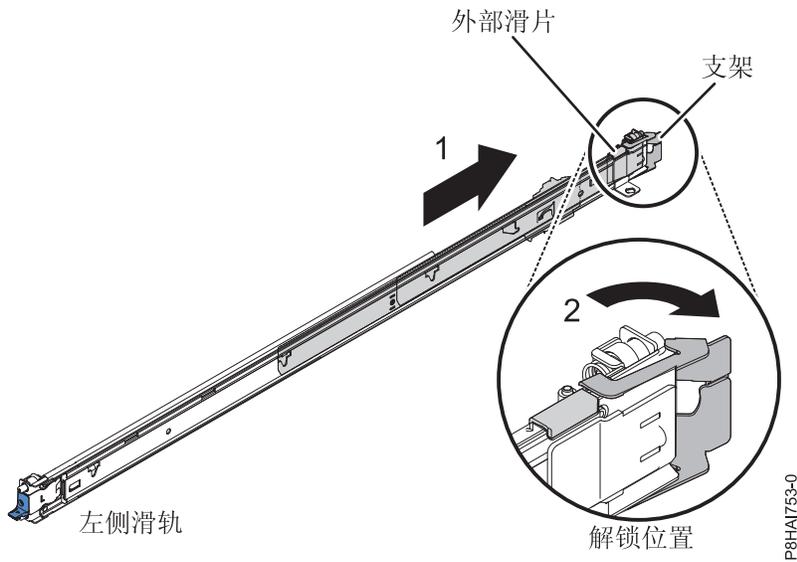


图 53. 滑轨和外部滑片

注：每个滑轨都在其末端标记为 **R**（右）或 **L**（左）。

3. 将外部滑轨组件的后端与机架后部的孔对齐。对齐锁钉，然后推动滑轨，使锁钉插入孔中。两个滑轨锁钉穿过 EIA 凸缘上的上下两个孔伸出。将滑轨向机架后部的方向推，直到后部机架装配支架锁定到位。

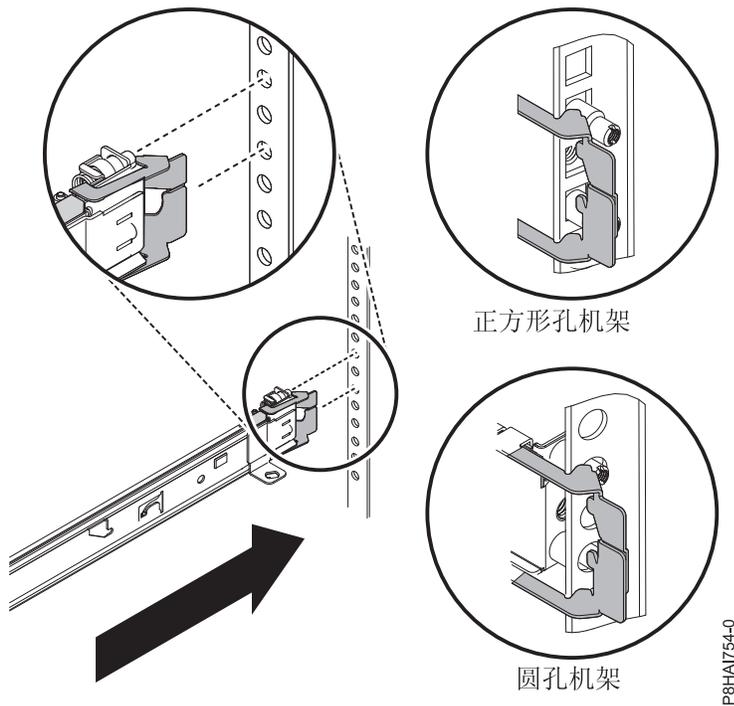
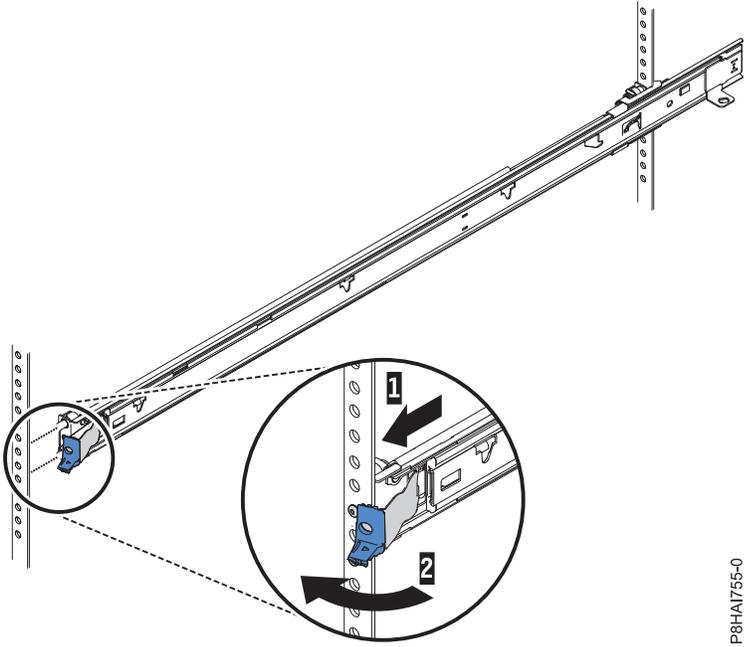


图 54. 使锁钉与机架后端中的孔对齐

4. 将前部滑锁旋转至打开位置，将外部滑轨组件的前端与机架前部的孔对齐。将锁钉与 EIA 凸缘中的孔对齐，将滑轨向前拉，使锁钉穿过这些孔。将前部滑锁旋转至闭合位置，以锁定滑轨前部。对其他外部滑片，重复步骤 2 至 4。



P8HA1755-0

图 55. 前部滑轨插销

- 按释放插销 (1)。移动机架机箱时，或者将机架机箱安装在易振区域中时，请拧紧服务器前部的外加 M5 螺丝 (2)。

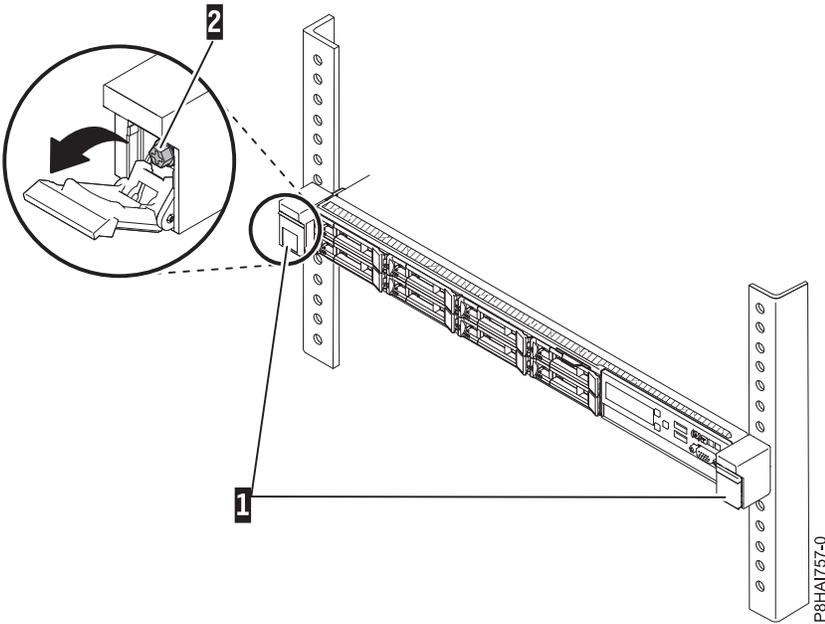


图 56. 机架前导轨和锁钉

- 将滑轨 (1) 向前拉，直到它们锁定到位（两次咔嚓声）。小心抬起服务器，并使它侧倾到滑轨上相应位置，以便服务器上后端的钉头 (2) 与滑轨中的插槽对齐。放低服务器，直到后端的钉头滑进后端的两个插槽，然后缓慢地放低服务器 (3) 的前端，直到其他钉头滑进滑轨上的其他插槽。确保前部插销覆盖前端钉头，以便系统固定到滑轨。

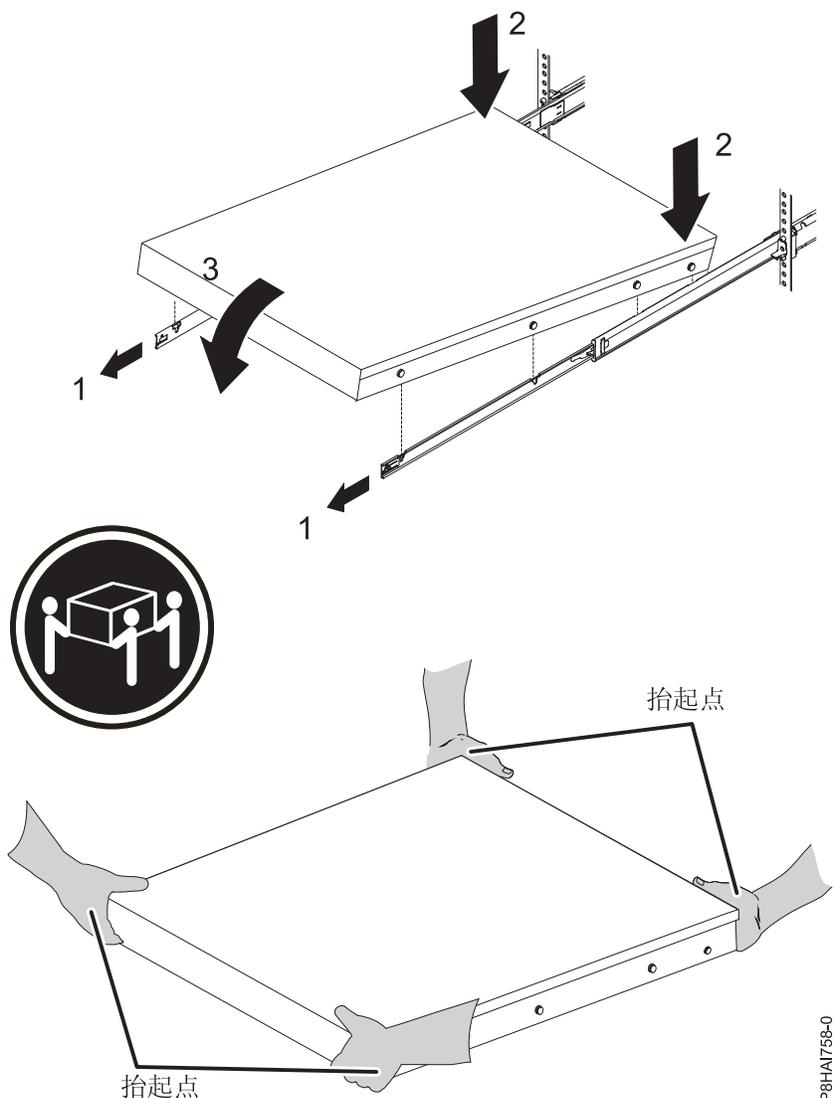


图 57. 滑轨伸长并且服务器钉头与导轨中的插槽对齐和抬起点

注：抬起时，请使用安全的做法。如果要安装 1 U 服务器，请确保由两个人抬起服务器。他们的手必须定位，如图 57 中所示。

7. 抬起滑轨上的锁定拉杆 (1)，并将服务器 (2) 尽力推送到机架中，直到它锁定到位。

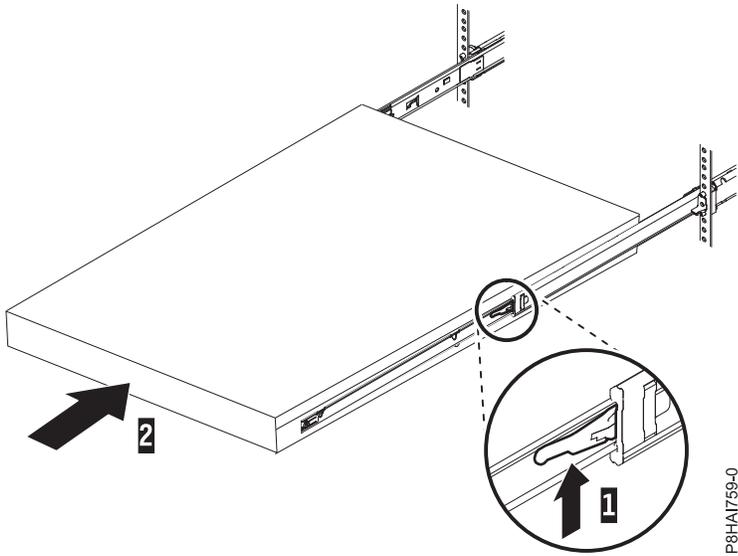


图 58. 释放插销和服务器

8. 电缆管理臂可以安装在服务器的任何一侧。图 59 显示在左侧安装电缆管理臂时的情况。安装电缆管理臂时，最好让它悬挂与电源相反的一侧，以方便接触电源。要在右侧安装电缆管理臂，请遵循指示信息并在对侧上安装硬件。将锁钉放下 (1) 到滑轨后部上的水平插槽中。然后将棒的另一端朝机架 (2) 的方向旋转。

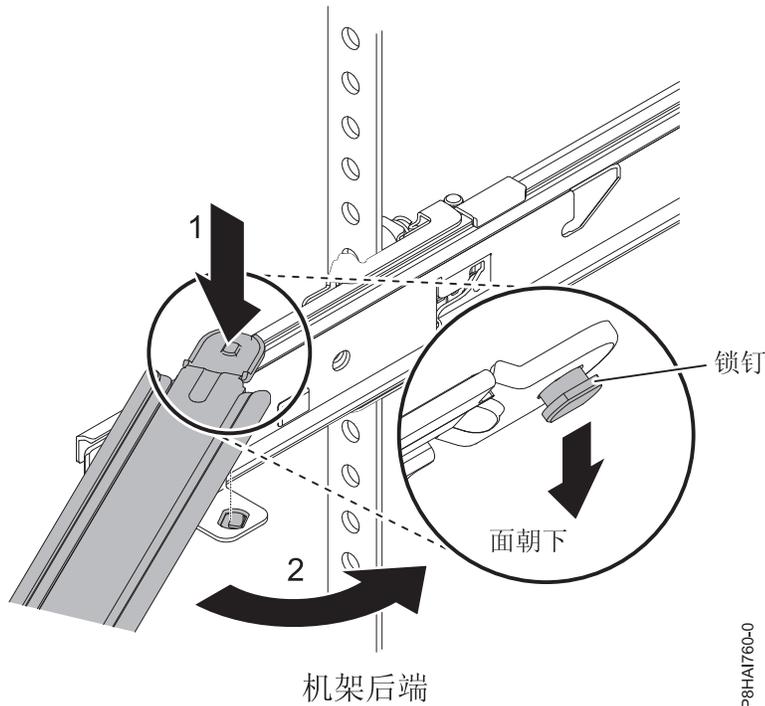


图 59. 支持臂连接

注：电缆管理支持棒必须位于滑轨卡扣上方才能正常发挥作用。

9. 在支持臂未连接端上安装电缆管理固定支架（具有大写字母 O）。确保支持臂已安全地安装。

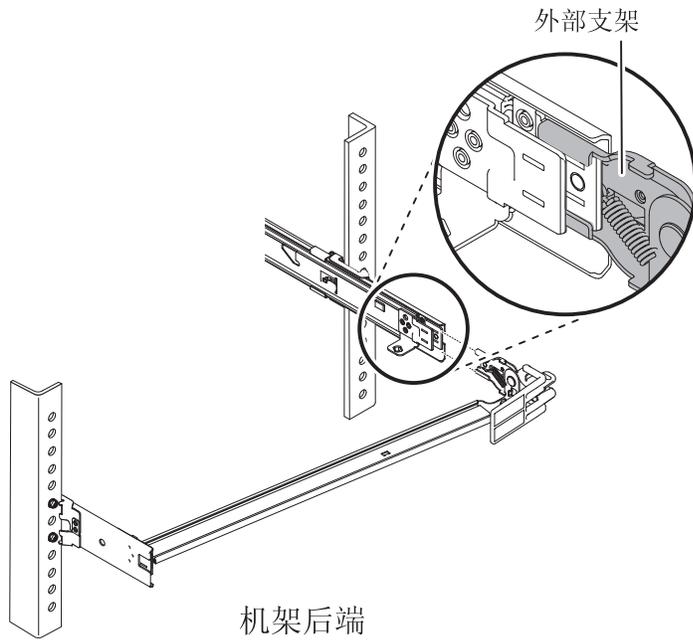


图 60. 将固定架连接到滑轨

P8HA1761-0

注：电缆管理臂锁钉上标有大写字母 **O**，标识外部锁钉。

10. 将电缆管理臂放置和支持臂上。将电缆管理臂卡扣滑入滑轨的内部和外部插槽。推动卡扣直至其咬合到位。

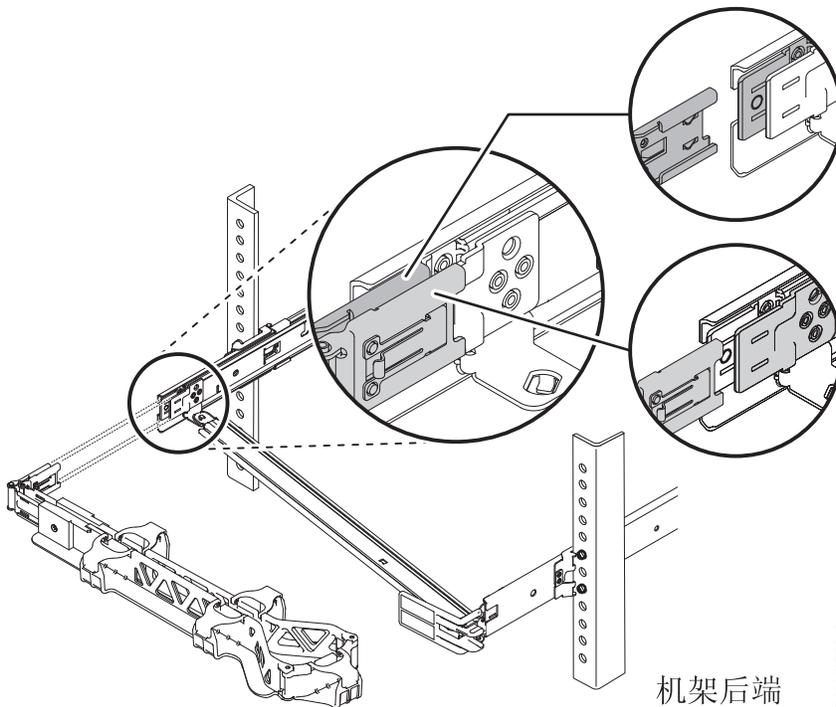
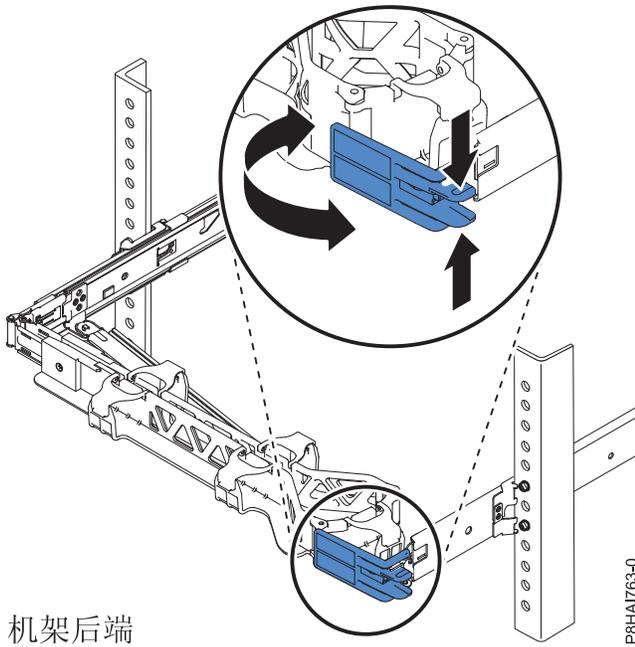


图 61. 电缆管理臂连接

P8HA1762-0

11. 要使得电缆管理支持臂上的电缆管理臂旋紧和旋松更容易，可以将卡扣推动到电缆管理支持臂上方来打开固定架，将卡扣推动到电缆管理支持臂下方来关闭固定架。

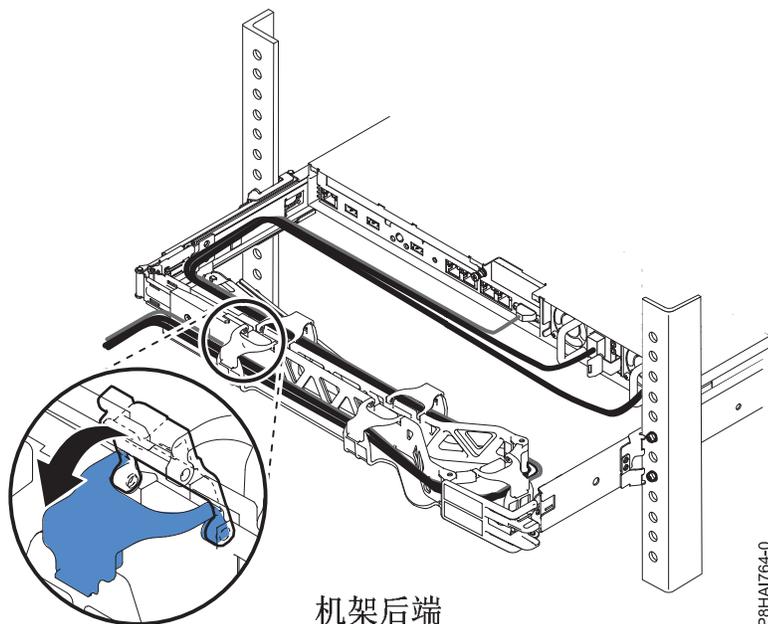


机架后端

图 62. 电缆管理支持固定

12. 将电源线和其他电缆连接至服务器（需要时，包括键盘、监视器和鼠标电缆）的后端。将电缆与电源线路由在电缆管理臂上，并使用电缆扎带或钩环固定器将它们固定。

注：电缆皮带的位置可能与其他系统稍有不同。使用系统后端提供的电缆皮带固定电缆，防止它们下垂。



机架后端

图 63. 连接电源线和电缆

13. 必须使用电缆系带扎紧电缆，以使电缆管理臂可进行适当移动。

注：请确保电缆不会下垂到 U 空间的下方，这样它们不会缠到下方的系统。允许所有电缆中存在松弛情况，以避免当电缆管理臂移动时这些电缆中出现拉紧状态。

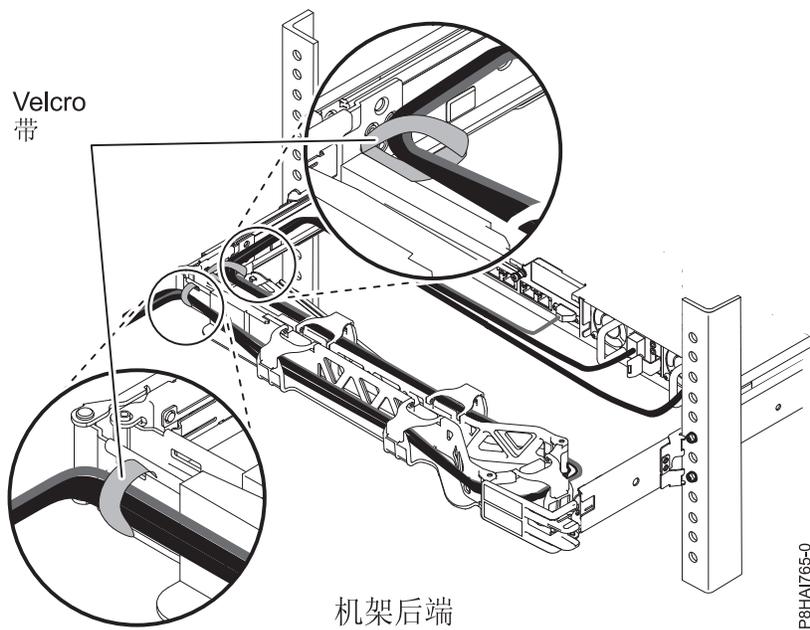


图 64. 钩环固定器

14. 如果要装运安装了系统的机架，或者您处于易振动的区域，请在滑轨的后部插入 M5 螺钉。使用电缆扎带将电缆管理臂的活动端固定到机架（如果需要）。

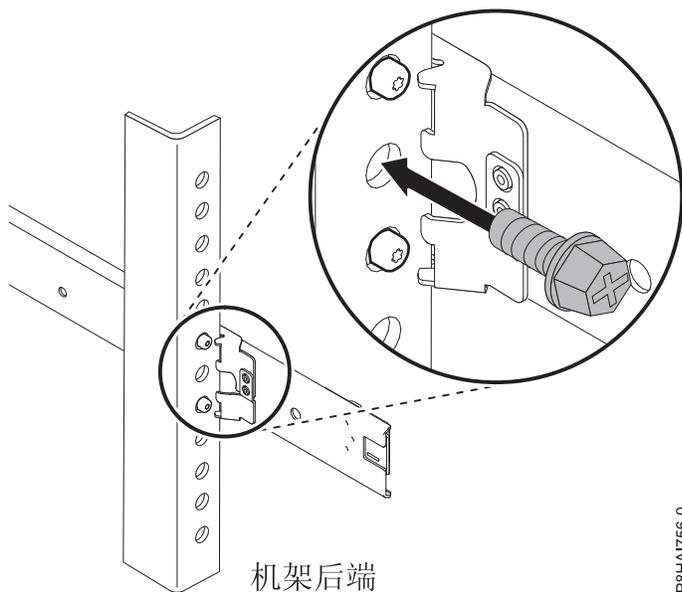


图 65. 固定好服务器以进行装运

将 7063-CR1 安装到机架中

了解如何将 7063-CR1 硬件管理控制台 (HMC) 安装到机架中。

有关安装机架安装式 7063-CR1 系统的先决条件

使用此信息来了解安装系统所需满足的先决条件。

安装服务器之前，可能需要阅读下列文档：

- 此文档的最新版本以在线方式维护，请参阅将 7063-CR1 安装到机架中 (http://www.ibm.com/support/knowledgecenter/POWER8/p8hai/p8hai_install7063_kickoff.htm)。
- 要规划您的服务器安装，请参阅规划系统 (http://www.ibm.com/support/knowledgecenter/POWER8/p8had/p8had_8xx_kickoff.htm)。

开始安装之前，确保您具有下列各项：

- Phillips 十字螺丝刀
- 一字头螺丝刀
- 开箱器
- 静电释放 (ESD) 腕带
- 空间为两个电子工业协会 (EIA) 单位 (2U) 的机架

注：如果您未安装机架，请进行安装。有关指示信息，请参阅机架和机架功能 (http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/p8hbf_8xx_kickoff.htm)。

清点系统的清单

使用此信息来清点系统的清单。

1. 验证是否已收到订购的所有箱子。
2. 根据需要，打开服务器组件的包装。
3. 在安装每个服务器组件之前，通过完成下列步骤来清点部件清单：
 - a. 找到服务器的清单列表。
 - b. 确保已收到订购的所有部件。

注：订单信息随产品一起提供。您还可以从销售代表或 IBM 业务合作伙伴处获取订单信息。

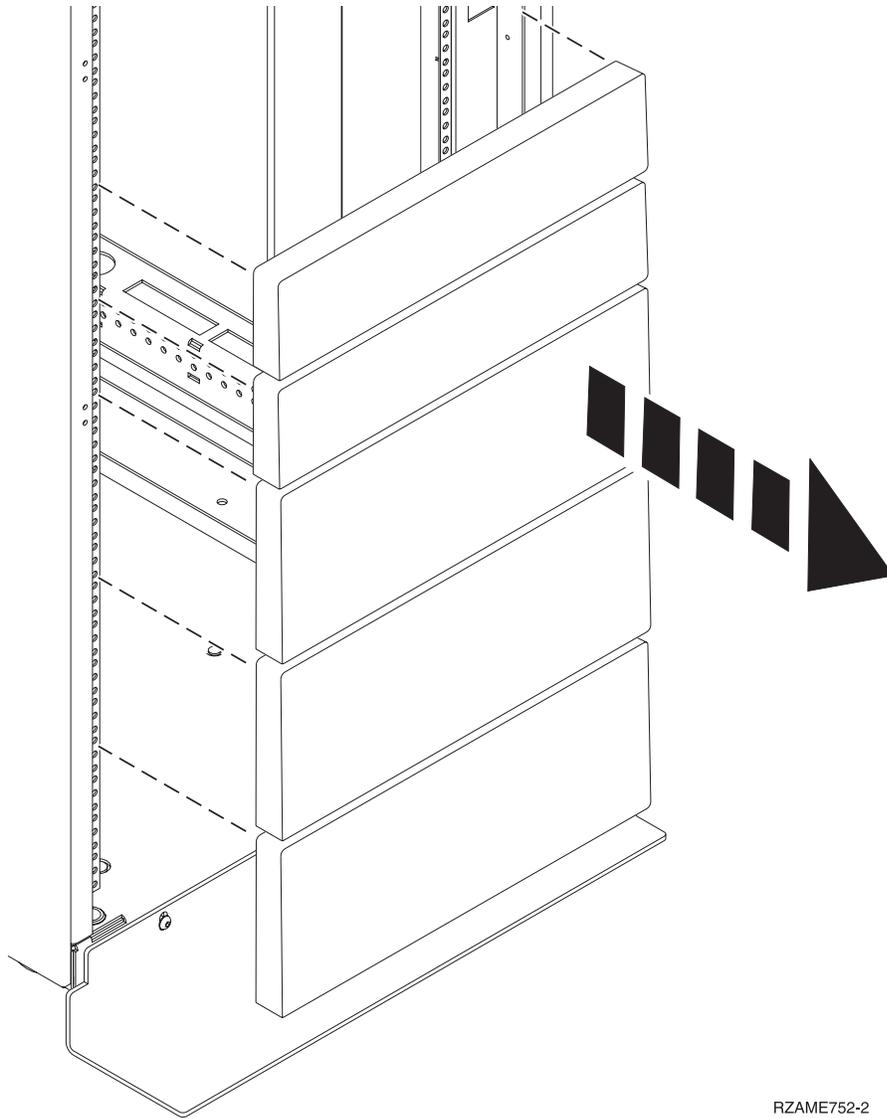
如果发现部件不正确、缺失或损坏，请联系以下任意资源：

- 您的 IBM 经销商。
- IBM Rochester 制造厂的自动信息热线 1-800-300-8751（仅限美国）。
- 全球联系人通讯录 Web 站点 <http://www.ibm.com/planetwide>。选择您所在的位置，以查看相应的服务和支持联系人信息。

确定并标记 7063-CR1 系统在机架中的位置

您可能需要确定系统部件在机架中的安装位置。

1. 阅读机架安全声明 (<http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/racksafety.htm>)。
2. 确定在机架中放置系统部件的位置。计划在机架中安装系统部件时，请考虑以下信息：
 - 将较大和较重的部件安排到机架下部。
 - 首先计划将部件安装到机架下部。
 - 将电子工业协会 (EIA) 位置记录在您的计划中。
3. 必要时，卸下填充板，以便可以检修到计划放置部件的机架箱内部，如 第 43 页的图 66。



RZAME752-2

图 66. 卸下填充板

4. 确定将系统放置在机架中。记录 EIA 位置。
5. 面向机架正面，从右侧使用胶带、记号笔或铅笔来标记每个 EIA 单位的底部孔。
6. 对位于机架左边的相应孔重复步骤 5。
7. 移至机架后端。
8. 在右边，找到与机架前端标记的底部 EIA 单位对应的 EIA 单位。
9. 标记底部 EIA 单位。
10. 标记机架左边的相应孔。

使用固定导轨将 HMC 安装到机架中

如果要使用固定导轨将 7063-CR1 HMC 安装到机架中，请完成下列任务。

将固定导轨连接到系统机箱和机架：

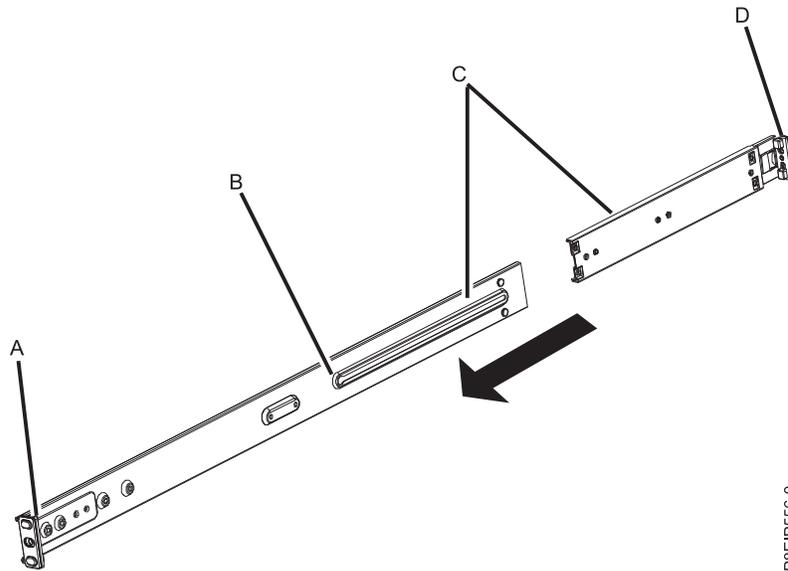
必须将导轨安装到机箱和机架。使用以下过程来执行此任务。

警告： 要避免导轨发生故障和对您自身以及部件可能造成的危险，请确保机架具有正确的导轨和配件。如果机架具有方形支承法兰孔或螺纹支承法兰孔，请确保导轨和配件与机架上使用的支承法兰孔匹配。请勿使用垫圈或垫片来安装不匹配的硬件。如果机架不具有正确的导轨和配件，请与 IBM 经销商联系。

注： 系统需要 1 EIA 机架单位 (1U) 的空间。

确保您具有安装导轨所必需的部件。下列部件随导轨套件一起提供：

- 滑轨螺钉，用来连接每个滑轨的两个部分
 - 滑轨机架螺钉，用来将滑轨固定到机架
 - 导轨
 - 10 - 32 个 0.635 厘米 (0.25 英寸) 螺钉，用来将导轨连接到系统机箱
1. 从包装中取出导轨各部分并将其放置在工作台面上。
 2. 连接每个机架滑轨的两个部分。要连接机架滑轨的两个部分，请执行下列任务：
 - a. 识别机架左滑轨的两个部分。将短的部分与长的部分对齐 (C)。确保机架导轨锁钉指向相同方向 (A) 和 (D)。



P88EIP556-0

- b. 机架滑轨的较短部分有一个金属锁钉。将该锁钉插入机架滑轨的较长部分的孔中 (B)。将机架导轨的较短部分滑入机架导轨的较长部分。
- c. 对齐机架滑轨两个部分中的孔。使用十字螺丝刀将两个导轨螺钉松散拧入机架滑轨的孔中，从而连接这两个部分。

注： 请勿拧紧机架滑轨螺钉。

- d. 对右滑轨重复这些步骤。
3. 将机箱导轨连接到系统机箱。要将机箱导轨连接到系统机箱，请执行下列任务：
 - a. 在系统左侧，将系统机箱左侧的金属卡扣与机箱左滑轨上的方孔对齐。将机箱滑轨向机架正面滑动，直到机箱滑轨锁定到位。
 - b. 通过拧入导轨套件中提供的两个螺钉，将系统机箱滑轨连接到系统机箱。

- c. 在系统右侧对机箱滑轨重复此过程。
4. 将机架滑轨安装到机架。
 - a. 移到机架正面。
 - b. 选择机架左滑轨，并找到您先前标记的 EIA 单位。每个滑轨还标有 **Back**，以表示机架背面。确保您握住的是机架滑轨的前端。
 - c. 将导轨从机架正面伸长到机架背面，并将机架滑轨锁钉与机架凸缘中您先前标记的孔对齐。
 - d. 将机架导轨锁钉推入背面的机架凸缘，直到背面的机架导轨撞锁锁定到位。
 - e. 将机架导轨的前端拉向机架导轨凸缘的前端。将滑轨锁钉与导轨凸缘中的孔对齐，并将其拉出，直到导轨撞锁锁定到位。
 - f. 使用螺丝刀拧紧您在步骤 2 中安装的导轨螺钉。
 - g. 对右滑轨重复步骤 4a 至 4f。
5. 将导轨固定送到机架中。
 - a. 移到机架背面。
 - b. 将每个垫圈套到随导轨套件一起提供的每个较长螺钉上。
 - c. 将螺钉和垫圈拧入机架背面两侧每个导轨的中间孔。

将系统安装到机架并连接和布置电源线：

将系统到安装机架中的导轨之后，请连接并布置电源线。

注：此系统需要两个人员来将其安装到机架中。

1. 从系统机箱顶部撕除塑料保护膜。
2. 移到机架正面。
3. 安排两个人员来抬起系统，并将系统机箱两侧的机箱导轨与机架滑轨对齐。
4. 让一个人员承受系统的重量，而让另一个人员将系统轻轻推送到机架中，直到每个滑轨都锁定到位。
5. 将系统向机架背面推送，直到系统。
6. 通过将螺钉拧入系统机箱两侧的孔中，将系统固定到机架。
7. 将电源线插入电源。

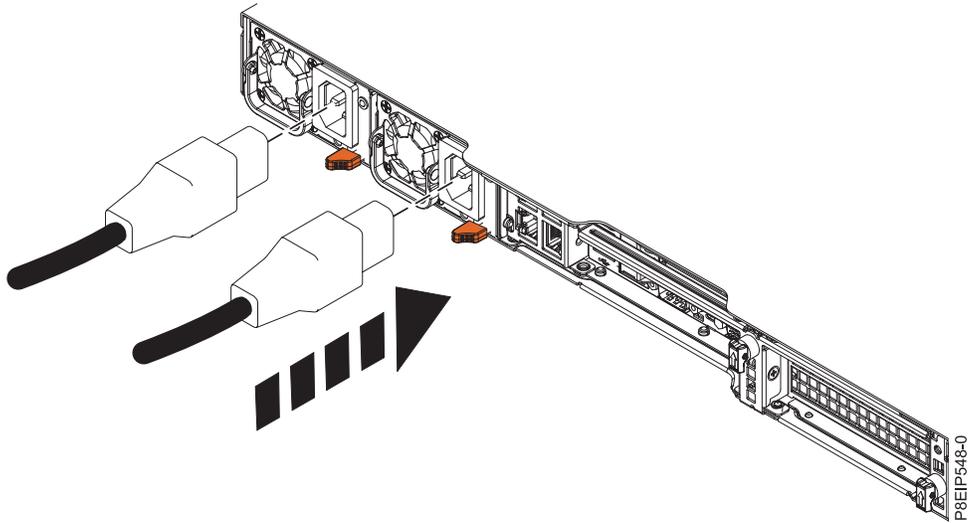


图 67. 将电源线插入电源

8. 将所有电缆都连接到服务器背面。

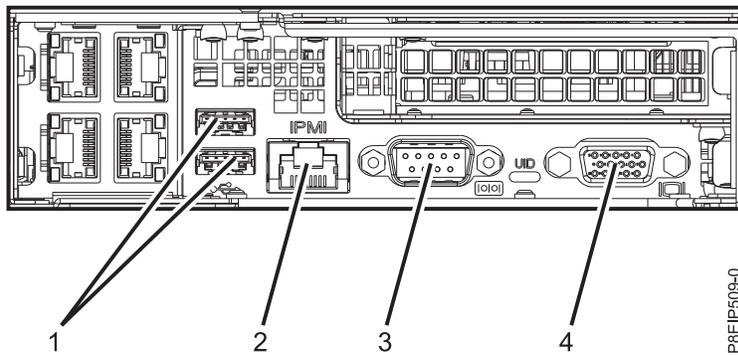


图 68. 背面端口

表 9. 输入和输出端口

标识	描述
1	USB 2.0, 用于键盘和鼠标
2	以太网智能平台管理界面 (IPMI)
3	串行 IPMI
4	用于监视器的视频图形阵列 (VGA)。仅支持 1024 x 768 (60 赫兹) VGA 设置。仅支持长度不超过 3 米的电缆。基于文本的功能仅在此时受支持。

9. 将系统电源线和任何其他已连接设备的电源线插入交流 (AC) 电源。
10. 继续执行第 113 页的『使用 HMC 增强型+ 界面配置 HMC』。

使用滑轨将 HMC 安装到机架中

如果要使用滑轨将 HMC 安装到机架中，请完成下列任务。

将滑轨连接至系统和机架：

将滑轨连接至系统，然后连接至机架。

警告： 要避免导轨发生故障和对您自身以及部件可能造成的危险，请确保机架具有正确的导轨和配件。如果机架具有方形支承法兰孔或螺纹支承法兰孔，请确保导轨和配件与机架上使用的支承法兰孔匹配。请勿使用垫圈或垫片来安装不匹配的硬件。如果机架不具有正确的导轨和配件，请与 IBM 经销商联系。

滑轨在收到时已完全组合在一起。要将滑轨安装到机架，必须将滑轨拆卸成四个部分。

1. 卸下两侧下部的直接访问存储设备 (DASD) 底板螺钉，以便您以后可以维护底板，而不必将系统从机架中卸下。

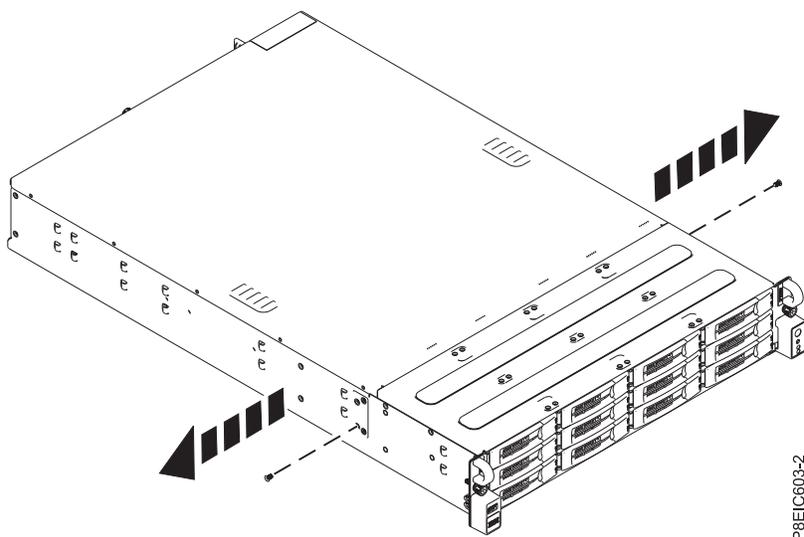
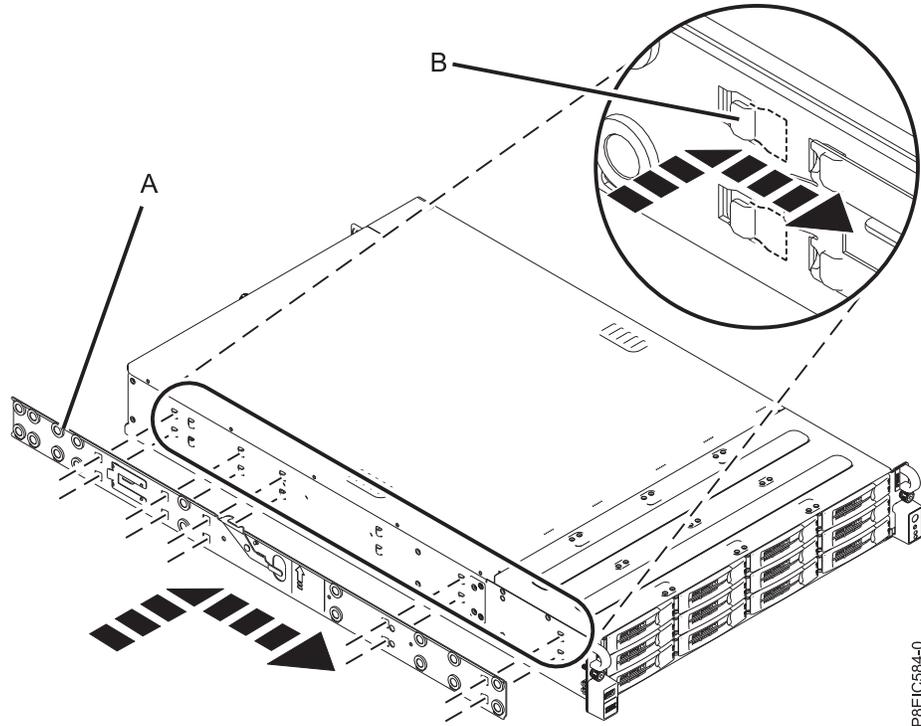


图 69. 卸下 DASD 底板螺钉

2. 将系统机箱滑轨连接到系统机箱的两侧。在系统机箱的背面，将系统机箱上的卡扣 (B) 与滑轨上的插槽 (A) 对齐。将机箱滑轨向前推送，以便撞锁锁定到位。

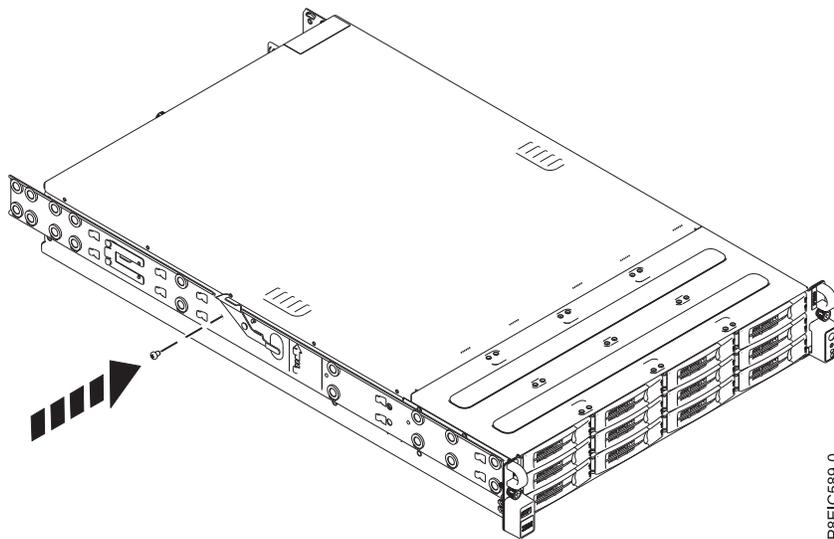
注： 系统导轨标有 **L**（用于表示系统左导轨）和 **R**（用于表示系统右导轨），左和右相对于系统正面而言。



P8E1C584-0

图 70. 在系统左侧将机箱滑轨连接到机箱

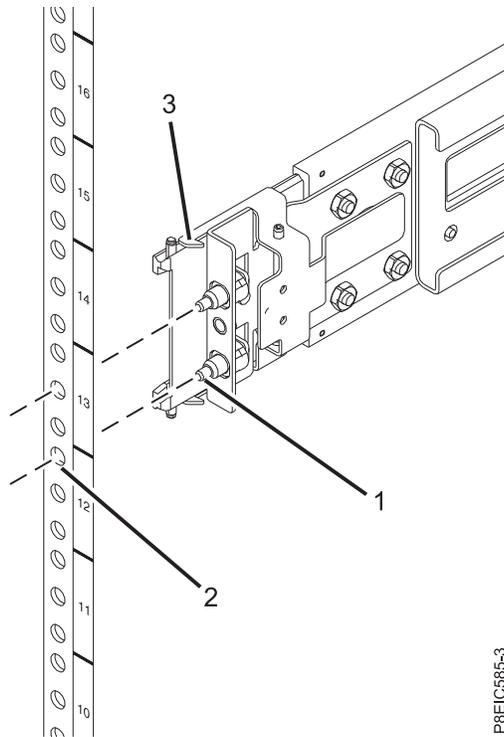
3. 在系统机箱的每个滑轨上安装紧固螺钉，以进一步将滑轨连接到系统机箱。



P8E1C589-0

图 71. 在系统左侧将机箱导轨紧固螺钉连接到机箱

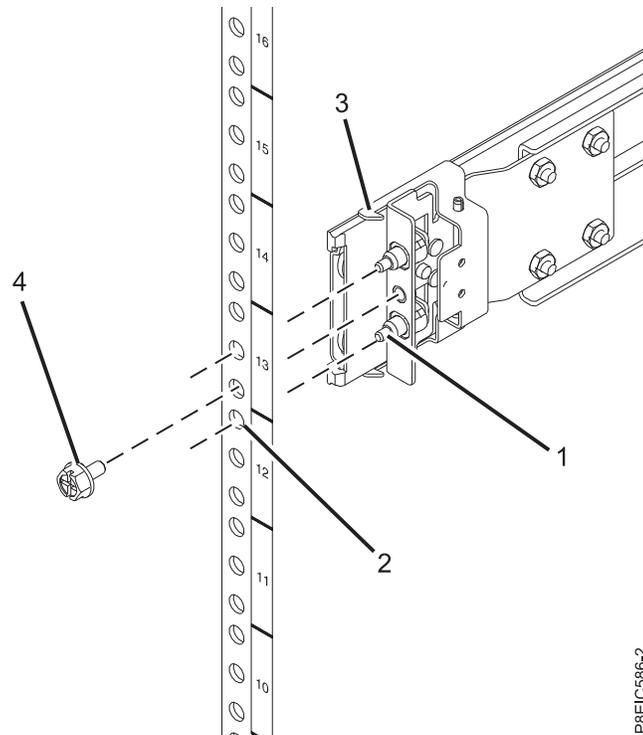
4. 接下来，将机架滑轨安装到机架。从前端看时，每个机架滑轨都标有 **R**（右）或 **L**（左）。选择右滑轨，将其带到机架正面，并找到所选 EIA 单位。
5. 从机架正面，将滑轨前端的锁钉 **(1)** 插入机架正面您先前标记的孔 **(2)** 中。将导轨向前拉，以便导轨弹簧夹 **(3)** 套到导轨凸缘并锁定到位。



P8E1C585-3

图 72. 从机架正面安装滑轨

6. 对左导轨重复步骤 3 和 4。
7. 移到机架背面。将滑轨朝您的方向拉，以将两个锁钉 **(1)** 插入机架孔 **(2)** 中。拉出导轨，直到导轨弹簧夹 **(3)** 锁定到位。安装螺钉 **(4)**，以将滑轨固定到机架。



P8EIC586-2

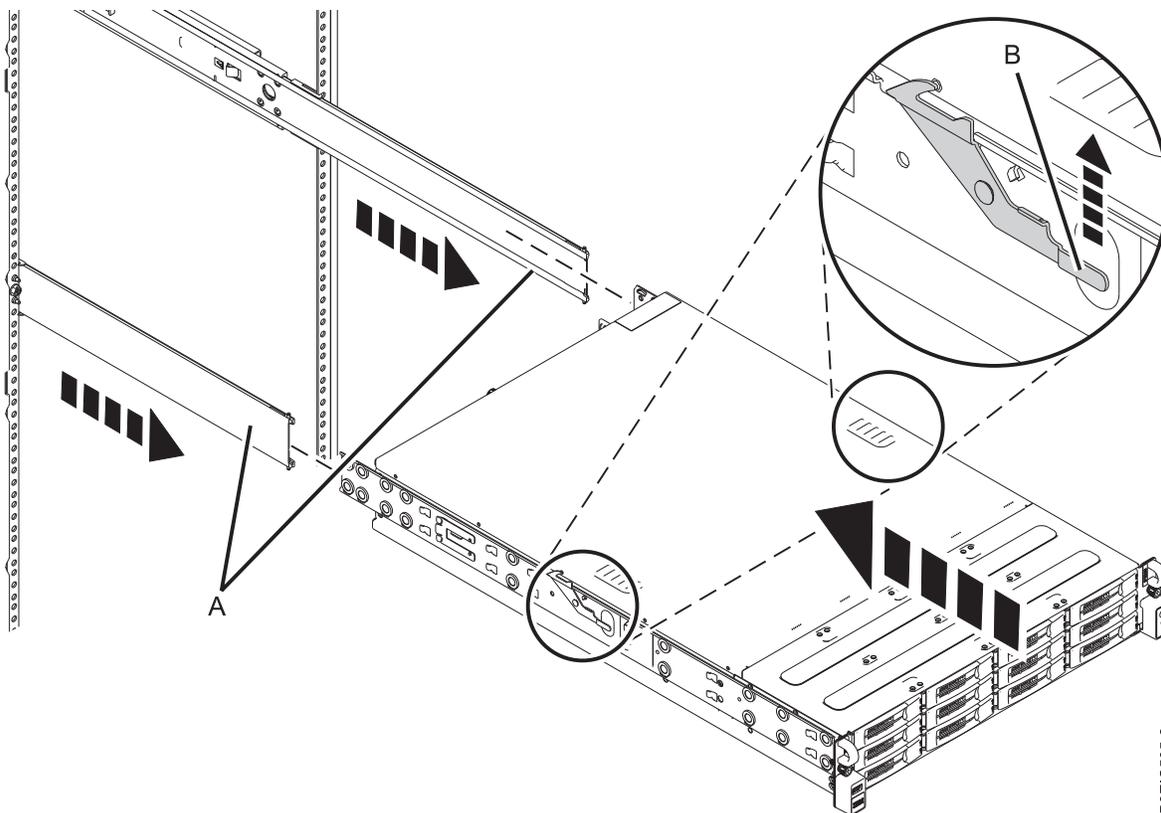
图 73. 在机架背面安装滑轨

将系统安装到机架并连接和布置电源线：

将系统安装到机架中的导轨之后，请连接并布置电源线。

注：此系统需要两个人员来将其安装到机架中。

1. 将滑轨完全伸长，直到导轨咔嗒一声锁定到服务位置 **(A)**。
2. 安排两个人员来抬起系统，并将机箱导轨的下部滚轮锁钉与两侧的机架滑轨中的槽对齐。



P8EIC595-2

图 74. 将机箱导轨的下部滚轮锁钉与机架滑轨中的槽对齐

3. 同时抬起机架两侧用绿色箭头标记的撞锁 (B)。
4. 将系统推送到机架中。
5. 拧紧系统两侧的翼形螺钉，以将系统固定到机架。

用电缆连接机架安装式 7063-CR1 HMC

了解如何在物理上安装机架安装式硬件管理控制台 (HMC)。

1. 确保将 HMC 置于正确位置。
2. 将 HMC 安装到机架。有关更多信息，请参阅第 41 页的『将 7063-CR1 安装到机架中』。将 HMC 安装到机架之后，继续执行下一个步骤。
3. 将电源线插入 HMC。
4. 连接键盘、监视器和鼠标。
5. 将以太网（或交叉）电缆从 HMC 连接至受管服务器。

注：要了解有关 HMC 网络连接的更多信息，请参阅第 71 页的『HMC 网络连接』。

6. 如果已安装受管系统，那么可在安装过程中通过同时观察 HMC 和受管系统以太网端口的绿色状态灯来验证以太网电缆连接是否处于活动状态。
7. 将以太网智能平台管理界面 (IPMI) 端口连接至网络。

注：在 HMC 上访问基板管理控制器 (BMC) 时，需要此连接。执行服务任务以及维护 HMC 固件时，需要访问 BMC。有关更多信息，请参阅第 71 页的『HMC 网络连接的类型』。

8. 将 HMC 上的以太网端口连接至受管服务器上标有 **HMC1** 的以太网端口：
9. 如果要将第二个 HMC 连接至受管服务器，那么连接至受管服务器上标有 **HMC2** 的以太网端口。

10. 将监视器、HMC 和 HMC 外置调制解调器的电源线插入电源插座。

注：如果要将此 HMC 连接至新的受管系统，请勿现在将该受管系统连接至电源。

接下来需要安装和配置 HMC 软件。继续执行『配置 7063-CR1 HMC』。

配置 7063-CR1 HMC

了解如何安装和配置硬件管理控制台 (HMC)。

可以从 Fix Central 的 Web 站点下载所需 HMC 版本。使用可移动介质（例如 DVD 或 USB）根据 HMC 软件包（ISO 映像）创建可引导 ISO 文件。

注：显示了下列安装以作为示例。

使用 USB 闪存驱动器安装 HMC

对于 Linux 系统，要使用 USB 闪存驱动器安装 HMC，请完成下列步骤：

1. 从 Fix Central 的 Web 站点下载所需 HMC 版本。
2. 运行以下命令：`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`（其中 `sdx` 是 USB 驱动器的名称）。

注：USB 驱动器必须至少为 4 GB。

3. 插入 USB 驱动器，然后打开系统的电源。

从控制台查看器使用远程介质安装 HMC

要从控制台查看器使用远程介质安装 HMC，请完成下列步骤：

1. 登录到 BMC Web 界面 (<http://<bmc-ip>>)。
2. 选择远程控制。
3. 选择控制台重定向。
4. 单击启动控制台。
5. 在 Java™ iKVM 查看器中，选择虚拟介质 > 虚拟存储器。
6. 在逻辑驱动器类型之下，选择 ISO 文件。
7. 单击打开映像并找到系统上的 ISO 文件。
8. 按插件以安装 ISO 文件。
9. 打开系统的电源。

从 BMC Web 界面使用远程介质安装 HMC

要从 BMC Web 界面使用远程介质安装 HMC，请完成下列步骤：

1. 登录到 BMC Web 界面 (<http://<bmc-ip>>)。
2. 选择虚拟介质。
3. 选择 CD-ROM 映像。
4. 填写以下信息：

共享主机

服务器消息块 (SMB) 主机的 IP。如果要使用主机名，请确保正确配置 BMC 上的域名系统 (DNS)。

映像路径

系统的 SMB 路径。例如: /<share name>/<rest of path>/<name of iso>.iso

用户 (可选)

用来登录到 SMB 主机的用户名。

密码 (可选)

用户的密码。

5. 单击**保存**。
6. 单击**安装**。
7. 设备 1 现在显示以下消息：**未安装 ISO 文件**。

注：如果未显示此消息，请重新检查信息并重复步骤 5 至 7。

8. 打开系统的电源。

注：服务器消息块 V3 (SMBv3) 不受支持。

接下来需要配置 HMC 软件。有关指示信息，请参阅第 113 页的『使用 HMC 增强型+ 界面配置 HMC』。

相关概念:

第 136 页的『配置 BMC 连接』

可以配置或查看管理控制台的 BMC 网络设置。

安装 HMC 虚拟设备

了解如何安装 硬件管理控制台 (HMC) 虚拟设备。

可以将 HMC 虚拟设备安装在现有 x86 或 POWER® 虚拟化基础结构中。HMC 虚拟设备支持下列 x86 虚拟化管理程序：

- 基于内核的虚拟机 (KVM)
- Xen
- VMware

运行 HMC 虚拟设备 的最低需求：

- 8 GB 内存
- 4 个处理器
- 1 个网络接口 (最多允许 4 个)
- 160 GB 磁盘空间 (建议：700 GB 以获得足够的“性能和容量监视”(PCM) 数据)

注意：

1. 托管 HMC 虚拟设备 的系统上的处理器必须是支持 Intel VT-x 或 AMD-V 硬件虚拟化的处理器。
2. 您接收的 HMC 虚拟设备 DVD 不可引导。您必须首先安装媒体，然后复制媒体中的 .tgz 文件。用于安装 DVD 的方法可能会视您使用的操作系统而不同。
3. 下列示例中所使用的命令语法可能会视您使用的操作系统而不同。

相关信息:

HMC V8 网络安装映像和安装指示信息

在 x86 上安装 HMC 虚拟设备

了解如何在 x86 环境中安装硬件管理控制台 (HMC) 虚拟设备。

使用 *KVM* 管理程序安装 *HMC* 虚拟设备：

了解如何使用基于内核的虚拟机 (KVM) 管理程序来安装 硬件管理控制台 (HMC) 虚拟设备。

要在 KVM 上安装 HMC 虚拟设备，请完成以下步骤：

注：以下步骤使用命令行界面且需要 root 用户权限。命令语法可能视操作系统而不同。

1. 验证是否已在具有 Red Hat Enterprise Linux (RHEL) V6.7 或更高版本的系统上安装虚拟化包。
2. 将 <KVM vHMC installation filename>.tar.gz 文件下载到主机系统。
3. 运行以下命令：mkdir -p /var/lib/libvirt/images/vHMC。
4. 运行以下命令：cd /var/lib/libvirt/images/vHMC。
5. 要解压缩虚拟盘映像，请运行以下命令：tar -zxvf <KVM vHMC installation filename>.tgz

注：在此命令中，指定 HMC 虚拟设备 .tar 文件的完整路径。

6. **domain.xml** 文件在 <KVM vHMC installation filename>.tar.gz 文件中提供。请完成以下步骤：
 - a. 编辑 **domain.xml** 文件并验证磁盘路径是否正确。此文件包含字符串 **DISK_PATH**。
 - b. 确保在磁盘设备的总线值中使用了 **virtio**。
 - c. 可以选择让 VM 具有不同的名称。**domain.xml** 文件中的缺省名称是 **vHMC**。
 - d. 验证是否已在 **domain.xml** 文件中设置介质访问控制 (MAC) 地址。此文件包含字符串 **MAC_ADDRESS**。

注：如果要系统自动生成 MAC 地址，请移除此行。

- e. 验证网桥与以太网设备是否匹配。缺省 **domain.xml** 文件指定了一个以太网。
7. 要定义 VM，请运行以下命令：virsh define <domain>.xml。
 8. 要启动 VM，请运行以下命令：virsh start vHMC。
 9. 要确定控制台的虚拟网络计算 (VNC) 显示编号，请运行以下命令：virsh vncdisplay vHMC。
 10. 要通过 VNC 查看器连接到控制台，请运行以下命令：vncviewer HOSTNAME:ID (其中 ID 是显示编号，例如 0)。

注：如果需要远程访问，必须删除或配置防火墙以允许访问端口 5900。

使用 *Xen* 虚拟机管理器安装 *HMC* 虚拟设备：

了解如何使用 Xen 虚拟机管理器安装 硬件管理控制台 (HMC) 虚拟设备。

HMC 虚拟设备 支持 Xen V4.2 或更高版本。

要使用 Xen 虚拟机管理器安装 HMC 虚拟设备，请完成下列步骤：

注：下列步骤使用命令行界面，并且需要具备 root 用户权限才能执行这些步骤。命令语法可能视操作系统而不同。

1. 验证是否已在具有 Red Hat Enterprise Linux (RHEL) V6.4 或更高版本的系统上安装虚拟化包。
2. 将 <XEN vHMC installation filename>.tar.gz 文件下载到主机系统。
3. 运行以下命令：mkdir -p /var/lib/libvirt/images/vHMC。

4. 运行以下命令：`cd /var/lib/libvirt/images/vHMC。`
5. 要解压缩虚拟磁盘映像，请运行以下命令：`tar -zxvf <XEN vHMC installation filename>.tgz`

注：在此命令中，指定 HMC 虚拟设备 .tar 文件的完整路径。

6. 在 `<XEN vHMC installation filename>.tar.gz` 文件中提供了 **vhmc.cfg** 文件。在文件编辑器中打开 **vhmc.cfg** 文件并编辑下列值：

- a. 更改虚拟 HMC 的名称（可选）：编辑 **vhmc.cfg** 文件，并验证磁盘路径是否正确。此文件包含字符串 **DISK_PATH**。

- b. 将 **DISK_PATH** 替换为 `disk1.img` 的路径：

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

- c. 替换以太网适配器，并添加 MAC 地址（可选）：

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

可选 MAC 地址：

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

注：重新引导虚拟 HMC 时，Xen 虚拟机管理器会自动重新生成 MAC 地址。添加可选 MAC 地址可以解决此问题。

- d. 替换 **FLOPPYPATH**（如果您正在使用 Activation Engine）：

```
device_model_args = [ "-fda", "FLOPPYPATH" ]
```

7. 要创建并启动 VM，请运行以下命令：`xl create vHMC.cfg。`
8. 要检查是否已将 VM 添加至所定义的虚拟机列表中，请运行以下命令：`xl list。`
9. 要访问 VM 本地控制台，请运行以下命令：`vncviewer localhost 0。`

使用 VMware ESXi 安装 HMC 虚拟设备：

了解如何使用 VMware ESXi 来安装 硬件管理控制台 (HMC) 虚拟设备。

可以在 vSphere 客户机上，使用图形用户界面在 VMware ESXi 上安装 HMC 虚拟设备，以便部署"开放式虚拟化格式"(OVF) 模板。

注：可以在 VMware ESXi V5.5 或更高版本上安装 HMC 虚拟设备。

要使用 vSphere 客户机在 VMware ESXi 上安装 HMC 虚拟设备，请完成以下步骤：

注：命令语法可能视操作系统而不同。

1. 获取 Tar 归档文件：`<VMware vHMC installation file name>.tgz。`
2. 使用 `tar` 命令从 Tar 归档文件解压缩 OVA 文件。
3. 启动 vSphere 客户机并登录 ESXi 主机。
4. 从文件菜单中，选择部署 **OVF** 模板。
5. 单击浏览并选择 OVA 文件。
6. 单击下一步。
7. 部署完成之后，单击关闭并选择 HMC 虚拟设备 图标以打开 HMC 虚拟设备。

在 PowerVM（逻辑分区）上安装 HMC 虚拟设备

了解如何在 PowerVM® 环境中安装硬件管理控制台 (HMC) 虚拟设备。

注：使用 HMC ISO 映像文件在分区中安装 HMC 虚拟设备时，您对 Web 用户界面将不具有本地图形控制台访问权。

要在 PowerVM 上安装 HMC 虚拟设备，请完成下列步骤：

1. 遵循用于在 PowerVM 上安装 ISO 映像的常规过程。有关更多信息，请参阅如何配置 VIOS 介质存储库/虚拟介质库。
2. 完成安装并启动系统之后，必须从语言选择对话框中选择语言。
3. 接受许可协议。

注：运行任何命令之前，请确保命令控制器已可以接受命令。例如，运行 `lshmc -V` 命令，直到它成功。

4. 以 `hscroot` 身份登录，然后使用 `chhmc` 命令来配置网络。

以下示例显示了一系列 `chhmc` 命令，这些命令可以用来配置网络以及在 HMC 上启用 `ssh` 和远程 Web 访问权。

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

- **hmc ip address** 是 HMC 的 IP 地址。
- **hmc network mask** 是 HMC 的网络掩码。
- **hmc hostname** 是 HMC 的主机名。
- **hmc domain name** 是 HMC 的域名。
- **gateway ip** 是网络上网关的 IP 地址。
- **name server** 是网络的名称服务器地址。
- **domain search** 是您希望 HMC 搜索的域的名称。
- 要允许在所有 IP 地址处进行访问，请使用 `-a 0.0.0.0 -nm 0` 代替 `ip address`。

5. 重新启动系统。

将激活引擎用于 HMC 虚拟设备

了解如何将激活引擎用于 硬件管理控制台 (HMC) 虚拟设备。

激活引擎是一个框架，可允许在系统启动期间配置虚拟机中的各种组件。激活引擎只能与预先捕获的磁盘映像配合使用。例如，如果使用 HMC 恢复 ISO 文件创建了 HMC 虚拟设备，那么激活引擎不可用。要使用激活引擎，需要设置 XML 配置概要文件以允许 HMC 虚拟设备在首次启动时处于管理就绪状态。有关配置 XML 配置概要文件的更多信息，请参阅第 57 页的『设置激活引擎的配置概要文件』。可以使用配置文件来配置以下选项：

- 设置缺省键盘 (US)
- 缺省语言环境 (US)
- 许可协议和机器代码协议
- 禁用设置向导
- 禁用回拨向导
- 最多配置四个网络接口卡
- 配置每个接口的防火墙设置

要设置激活引擎，请完成以下步骤：

1. 使用文本编辑器或使用在 **<vHMC install file>.tgz** 包中提供的样本文件，创建名为 **vHMC-Conf.xml** 的 XML 文件。

2. 创建软盘映像。在运行 Linux 操作系统的系统上，可使用 `dd` 命令执行此任务：

```
dd if=/dev/zero of=/Floppy/Path/Floppy.img count=1440 bs=1k
```

3. 使用 `mkfs.ext2` 命令设置文件的格式：

```
/sbin/mkfs.ext2 /Floppy/Path/Floppy.img
```

4. 将 **vHMC-Conf.xml** 文件复制到软盘映像：

```
mkdir /Path/to/Tempfolder/Temp
mount -o loop,rw /Floppy/Path/Floppy.img /Path/to/Tempfolder/Temp
cp /Path/to/vHMC-Conf.xml /Path/to/Tempfolder/Temp
umount /Path/to/Tempfolder/Temp
```

5. 对于基于内核的虚拟机 (KVM) 管理程序，将软盘位置添加至 **domain.xml** 文件：

```
<disk type='file' device='floppy'>
  <driver name='qemu' type='raw' cache='default' />
  <source file='Path/to/Floppy' />
  <target dev='fda' bus='fdc' />
  <address type='drive' controller='0' bus='0' target='0' unit='0' />
</disk>
```

6. 要定义 VM，请运行以下命令：`virsh define PATH_TO_DOMAIN_XML`。

7. 要启动 VM，请运行以下命令：`virsh start NAME_OF_VM` (`NAME_OF_VM` 在 `Domain.xml` 文件中描述)。

设置激活引擎的配置概要文件：

了解如何使用 XML 标记来设置激活引擎配置文件。

配置文件的 XML 标记

在激活引擎配置文件中使用了 XML 标记来为各种属性设置特定值。可以在激活引擎配置文件中手动设置这些值。请使用下列各节来查看每个标记及其允许值的描述：

- 『HMC 标记』
- 第 58 页的 『以太网标记』
- 第 59 页的 『防火墙标记』
- 第 61 页的 『NTPServers 标记』

注：“动态主机配置概要文件”守护程序 (DHCPD) 服务器设置不是由激活引擎提供的。

请使用下列各节来查看配置文件的示例配置：

- 第 61 页的 『不含 NTPServers 的激活引擎 XML 配置文件示例』
- 第 62 页的 『含 NTPServers 的激活引擎 XML 配置文件示例』

HMC 标记

HMC 标记存放 HMC 设置配置的值。下面的示例显示了可用的 HMC 标记：

HMC 许可协议标记：

```
标记: <AcceptLicense></AcceptLicense>
可接受的值:
Yes -> 将接受 HMC 许可协议
No -> 将提示用户接受 HMC 许可协议
```

HMC 语言环境标记:

标记: <Locale></Locale>
可接受的值:
en_US.UTF-8

HMC 设置向导标记:

标记: <SetupWizard></SetupWizard>
可接受的值:
Yes -> 将显示 HMC 设置向导
No -> 将禁用 HMC 设置向导

HMC 设置回拨向导标记:

标记: <SetupCallHomeWizard></SetupCallHomeWizard>
可接受的值:
Yes -> 将显示 HMC 回拨向导
No -> 将禁用 HMC 回拨向导

HMC 设置键盘标记:

标记: <SetupKeyboard></SetupKeyboard>
可接受的值:
Yes -> 将提示用户进行键盘配置:wq
No -> 将接受缺省键盘设置 (U.S.)

以太网标记

以太网标记存放以太网适配器配置的值。激活引擎最多可配置四个以太网适配器。下面的示例显示了可用的以太网标记:

以太网启用标记:

标记: <Enable></Enable>
可接受的值:
Yes -> 配置此适配器
No -> 不配置此适配器

以太网 MACAddr 标记:

标记: <MACAddr></MACAddr>
可接受的值:
XX:XX:XX:XX:XX:XX -> 其中 X 是 0-F 值
XX-XX-XX-XX-XX-XX -> 其中 X 是 0-F 值

以太网 IPVersion 标记:

标记: <IPVersion></IPVersion>
可接受的值:
IPV4 -> 使用 IPV4 配置
IPV6 -> 使用 IPV6 配置
MIX -> 同时使用 IPV4 和 IPV6 配置

以太网 IPV4 网络类型标记:

标记: <IPv4NetworkType></IPv4NetworkType>
可接受的值:
Static -> 使用静态配置来配置适配器
Dhcp -> 使用 DHCP 配置来配置适配器

以太网 IPV4 地址标记:

标记: <IPv4Address></IPv4Address>
可接受的值:

任何有效的 IPV4 地址值

以太网 IPV4 网路掩码标记:

标记: <IPv4Netmask></IPv4Netmask>
可接受的值:
任何有效的 IPV4 网路掩码值

以太网 IPV4 网关标记:

标记: <IPv4Gateway></IPv4Gateway>
可接受的值:
任何有效的 IPV4 地址值

以太网 IPV6 网络类型标记:

标记: <IPv6NetworkType></IPv6NetworkType>
可接受的值:
Static -> 使用静态配置来配置适配器
Dhcp -> 使用 DHCP 配置来配置适配器

以太网 IPV6 地址标记:

标记: <IPv6Address></IPv6Address>
可接受的值:
任何有效的 IPV6 地址值

以太网 IPV6 网关标记:

标记: <IPv6Gateway></IPv6Gateway>
可接受的值:
任何有效的 IPV6 地址值

以太网主机名标记:

标记: <Hostname></Hostname>
可接受的值:
有效的字符串

以太网域标记:

标记: <Domain></Domain>
可接受的值:
任何有效的域值
例如, austin.ibm.com

以太网 DNS 服务器标记:

标记: <DNSServers></DNSServers>
可接受的值:
使用 3 组有效的 IPV4 或 IPV6 地址, 用逗号分隔
可接受空的 DNS 服务器值。
示例 1 IPv4: 9.3.2.1 IPv6: 2001:4860:4860::8888
示例 2 IPv4: 9.3.2.1,9.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844
示例 3 IPv4: 9.3.2.1,9.5.4.1,9.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844,
::ffff:903:201

防火墙标记

防火墙标记存放对应以太网适配器的代表性防火墙值。下面的示例显示了可用的 HMC 标记:

注: 所有标记都需要已启用或已禁用值。

防火墙 PEGASUS 标记:

标记: <PEGASUS></PEGASUS>
可接受的值:
Enabled -> 将允许 PEGASUS 端口处于打开状态
Disabled -> 将禁用 PEGASUS 端口

防火墙 RPD 标记:

标记: <RPD></RPD>
可接受的值:
Enabled -> 将允许 RMC 端口处于打开状态
Disabled -> 将禁用 RMC 端口

防火墙 FCS 标记:

标记: <FCS></FCS>
可接受的值:
Enabled -> 将允许 FCS 端口处于打开状态
Disabled -> 将禁用 FCS 端口

防火墙 I5250 标记:

标记: <I5250></I5250>
可接受的值:
Enabled -> 将允许 5250 端口处于打开状态
Disabled -> 将禁用 5250 端口

防火墙 PING 标记:

标记: <PING></PING>
可接受的值:
Enabled -> 将允许 PING 端口处于打开状态
Disabled -> 将禁用 PING 端口

防火墙 L2TP 标记:

标记: <L2TP></L2TP>
可接受的值:
Enabled -> 将允许 L2TP 端口处于打开状态
Disabled -> 将禁用 L2TP 端口

防火墙 SLP 标记:

标记: <SLP></SLP>
可接受的值:
Enabled -> 将允许 SLP 端口处于打开状态
Disabled -> 将禁用 SLP 端口

防火墙 RSCT 标记:

标记: <RSCT></RSCT>
可接受的值:
Enabled -> 将允许 RSCT 端口处于打开状态
Disabled -> 将禁用 RSCT 端口

防火墙 SECUREREMOTEACCESS 标记:

标记: <SECUREREMOTEACCESS></SECUREREMOTEACCESS>
可接受的值:
Enabled -> 将允许"安全远程访问"端口处于打开状态
Disabled -> 将禁用"安全远程访问"端口

防火墙 SSH 标记:

标记: <SSH></SSH>
可接受的值:

Enabled -> 将允许 SSH 端口处于打开状态
Disabled -> 将禁用 SSH 端口

防火墙 VTTY 标记:

标记: <VTTY></VTTY>
可接受的值:
Enabled -> 将允许 VTTY 端口处于打开状态
Disabled -> 将禁用 VTTY 端口

防火墙 NTP 标记:

标记: <NTP></NTP>
可接受的值:
Enabled -> 将允许 NTP 端口处于打开状态
Disabled -> 将禁用 NTP 端口

防火墙 SNMPTraps 标记:

标记: <SNMPTraps></SNMPTraps>
可接受的值:
Enabled -> 将允许"SNMP 陷阱"端口处于打开状态
Disabled -> 将禁用"SNMP 陷阱"端口

防火墙 SNMPAgents 标记:

标记: <SNMPAgents></SNMPAgents>
可接受的值:
Enabled -> 将允许"SNMP 代理"端口处于打开状态
Disabled -> 将禁用"SNMP 代理"端口

NTPServers 标记

如果您要在 HMC 虚拟设备 中配置多达五个 NTP 服务器,那么 NTPServers 标记是必需的。可以使用 <ntpparam ntpserver="server" ntpversion="1-4"/> 标记来添加 NTP 服务器。服务器参数接受 IPv4 或 IPv6 值或域名。下面的示例显示了可用的 NTPServers 标记:

NTPServers 标记:

标记: <NTPServers></NTPServers>
接受 <ntpparam ntpserver="server" ntpversion="1-4"/>

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

示例 2 <NTPServers>
<ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
<ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
<ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>

ntpparam 标记

标记: <ntpparam ntpserver="" ntpverion="" />
属性值:

ntpserver: 将接受 IPv4/IPv6 值和有效的 nostname
ntpversion: 将接受 1-4 数字值

不含 NTPServers 的激活引擎 XML 配置文件示例

下面的示例显示了不含 NTPServers 的激活引擎 XML 配置文件示例:

```

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

```

含 NTPServers 的激活引擎 XML 配置文件示例

下面的示例显示了含 NTPServers 的激活引擎 XML 配置文件示例：

```

<vHMC-Configuration>
  <LicenseAgreement>
  </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
<Ethernet>
  <Enable>No</Enable>
  <MACAddr></MACAddr>
  <IPVersion></IPVersion>
  <IPv4NetworkType></IPv4NetworkType>
  <IPv4Address></IPv4Address>
  <IPv4Netmask></IPv4Netmask>
  <IPv4Gateway></IPv4Gateway>
  <IPv6NetworkType></IPv6NetworkType>
  <IPv6Address></IPv6Address>
  <IPv6Gateway></IPv6Gateway>
  <Hostname></Hostname>
  <Domain></Domain>
  <DNSServers></DNSServers>

```

```

<Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <VTTY>Disabled</VTTY>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>
  <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
<NTPServers>
  <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
  <ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
  <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>
</vHMC-Configuration>

```

安装监视器和键盘

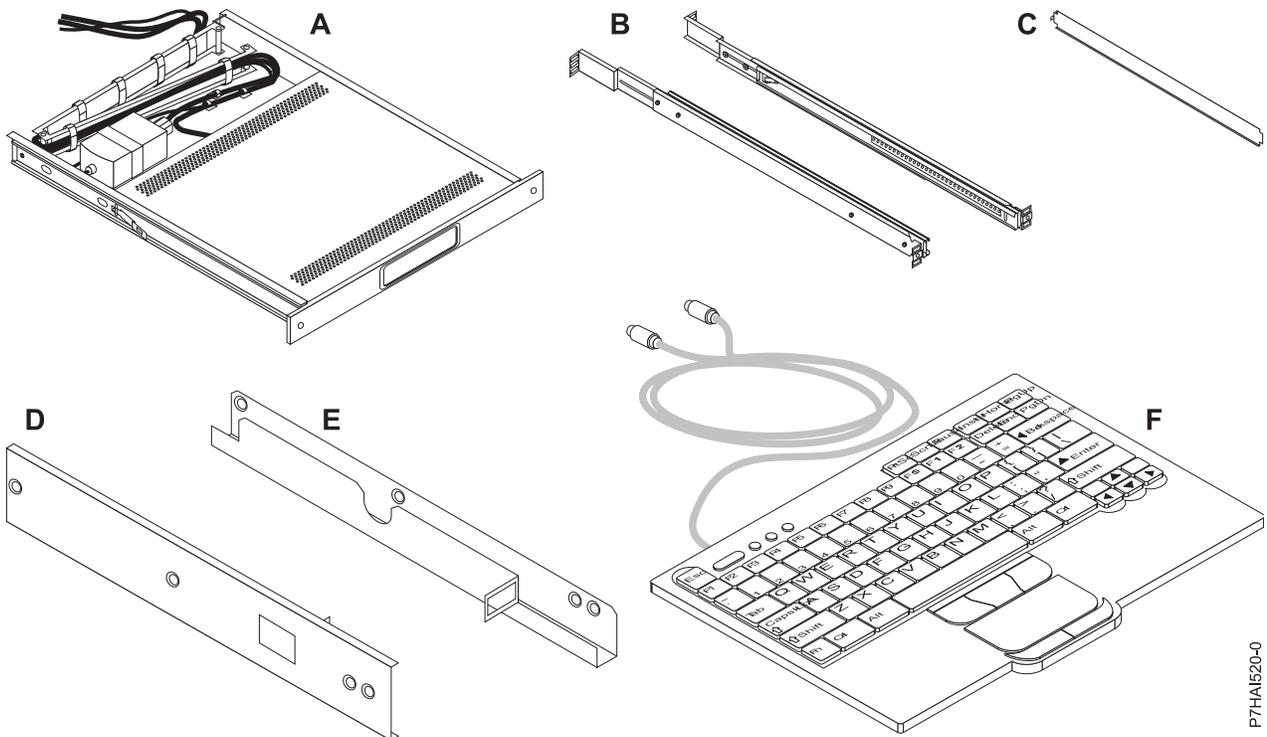
了解如何将随 7042-CR6 HMC 一起提供的监视器和键盘安装到机架中。这是一个客户任务。

如果 HMC 用来管理基于 POWER8 处理器的系统，那么该 HMC 必须为 CR3 或更高级别的机架安装式 HMC 模型。IBM eserver 7316-TF3 是一种 17 英寸平板机架安装式监视器和键盘托盘。适用于各种语言的特殊键盘安装在键盘托盘前部。监视器和键盘托盘占用机架机柜中 1 个电子工业协会 (EIA) 单位的空间。您可以将控制台开关安装在托盘后，以将多个服务器连接至平板监视器和键盘。

要将 7042-CR6 HMC 安装到机架中，请完成以下步骤：

警告： 将导轨安装到机架是一个复杂过程。要正确安装导轨，必须按以下顺序执行每个任务。

1. 清点部件清单。有关指示信息，请参阅清点部件清单。
2. 找到机架安装硬件工具箱和随系统部件一起提供的系统导轨组合件。



P7HA620-0

图 75. 安装工具箱部件

表 10. 安装工具包部件内容

安装工 具包	部件内容
A	一个具有内置平板监视器的键盘托盘
B	外部导轨 (2)
C	导轨对齐定位器 (1)
D	右侧控制台开关装配支架 (1)
E	左侧控制台开关装配支架 (1)
F	具有内置定位设备的键盘 (1)
G	其他硬件工具包: 12 个四角多用途螺母、12 个对开螺母、10 个十字螺钉、4 个 (8-32) 螺钉和 2 个翼形螺钉。
H	1.8 米 (即 6 英尺) 电源线 (1)
I	2.4 米 (即 8 英尺) 国际电工技术委员会 (IEC) 连接器电源线 (1)
J	键盘延长线 (1)
K	鼠标延长线 (1)
L	包含 Windows 键盘和鼠标驱动程序的 CD (不适用于 Eserver pSeries 系统或者任何基于 AIX®、Linux 或 OS/400 的系统)
<p>要点: 使用下列工具来安装平板机架安装式监视器和键盘:</p> <ul style="list-style-type: none"> • 剪刀 • Phillips 十字螺丝刀 • 一字头螺丝刀 	

清点部件清单

您可能需要清点部件清单。

如果您尚未清点部件清单，请清点之后再继续安装。

1. 找到附件箱中的工具清单。
2. 确保您已收到订购的所有部件。

如果有不正确、遗漏或损坏的部件，请联系 IBM 经销商或 IBM 销售与支持。

在不使用机架安装模板的情况下标记位置

您可以在不使用模板的情况下标记位置。

本系统不包含机架安装模板。这些系统的高度为 1 个 EIA 单位。

要确定安装位置，请完成下列步骤：

1. 确定将系统放置在机架中。记录 EIA 位置。

注：机架上的一个 EIA 单位由三个孔组成。

2. 面向机架正面并从右边开始将一块提供的不干胶贴到 EIA 单位的顶部孔的旁边。

注：不干胶用于帮助标识机架上的位置。如果用完了不干胶，请使用其他标记工具来帮助标识孔位置，例如，胶带、记号笔或铅笔。如果您要安装滑轨，请在每个 EIA 单位的下部孔和中间孔上作标记或贴上不干胶。

3. 将另一块不干胶贴到该 EIA 单位上面的下部孔。

注：如果您要数孔，请从第一块不干胶标识的孔开始并向上数两个孔。将第二块不干胶贴到第三个孔旁边。

4. 对位于机架左边的相应孔重复步骤第 8 页的 1。
5. 移至机架后端。
6. 在右边，找到与机架前端标记的底部 EIA 单位对应的 EIA 单位。
7. 将一块不干胶贴到底部 EIA 单位上。
8. 将一块不干胶贴到该 EIA 单位的顶部孔上。
9. 标记机架左边的相应孔。

将监视器和键盘安装到机架中

了解如何将随 7042-CR6 HMC 一起提供的监视器和键盘安装到机架中。

IBM 7316-TF3 17 英寸平板机架式安装的监视器和键盘占用机架机柜中 1.75 英寸 (1 EIA) 的机架安装空间。可使用随此工具箱一起提供的机架将可选控制台开关安装在与监视器控制台工具箱相同的机架安装空间中。

要将 7042-CR6 HMC 的监视器和键盘安装到机架中，请完成以下步骤：

警告： 卸下机架门和边面板以便可以轻松进行安装。

完成以下步骤以将监视器和键盘安装到机架中：

1. 在机架中为监视器和键盘托盘选择一个位置。有关更多信息，请参阅标记位置。
2. 将 4 个四角多用途螺母（在方孔机架凸缘上）或 4 个对开螺母（在圆孔机架凸缘上）安装在机架前端和后端的相同 EIA 位置。

注：如果您计划安装可选控制台开关，请将四角多用途螺母或对开螺母安装在中央靠后的位置，如下图所示。

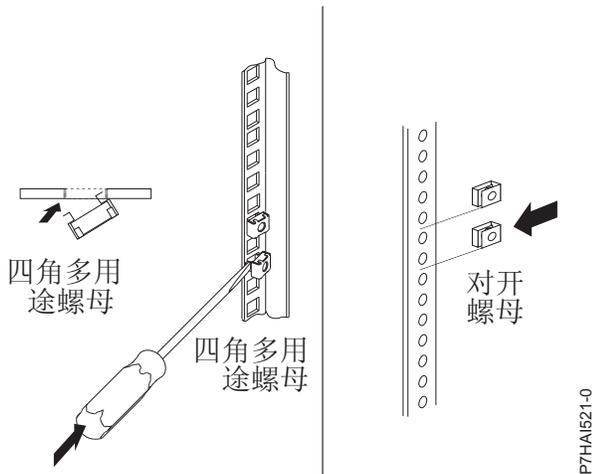


图 76. 安装四角多用途螺母

3. 拧松位于每个外滑轨的两个导轨对齐螺钉。将导轨延长为向外调整的最大值。
4. 调整外滑轨支架以适合机架机柜的深度。然后，使用其他硬件工具箱中的 4 个螺钉连接滑轨支架的前端，以适合机架机柜的深度。螺钉应该是可手指旋紧的，以允许调整导轨。

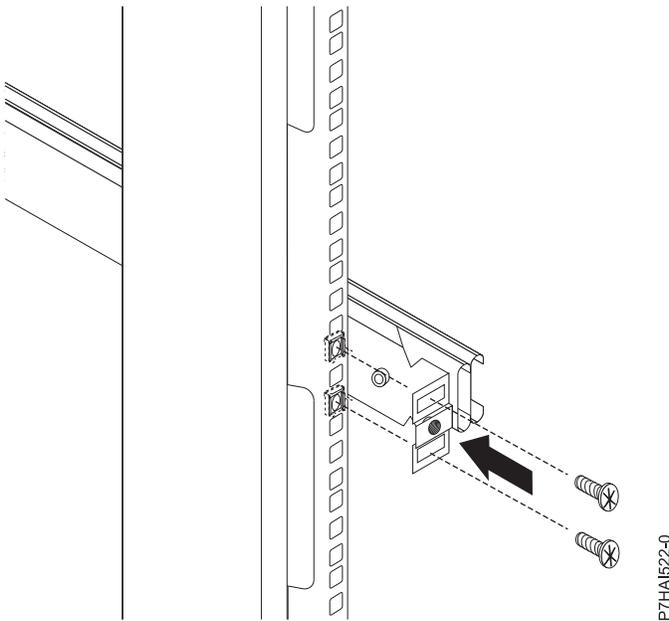


图 77. 调整滑轨支架

注：请确保滑轨支架超出机架机柜安装凸缘范围。不要将螺钉安装在滑轨支架前端或后端的中间孔。这些孔将用于稍后在此过程中分别连接翼形螺钉或可选控制台开关安装支架。

5. 使用其他硬件工具箱中的 4 个螺钉并用手指将其从滑轨支架后端旋紧到机架机柜中。请确保滑轨支架超出机架机柜安装凸缘范围。
6. 拧紧您在步骤 5 中拧松的每个外导轨上的两个导轨对齐螺钉。
7. 将导轨对齐定位器插入到滑轨中间孔。请确保导轨对齐定位器回绕导轨。拧紧前部 4 个螺钉，然后卸下定位器。

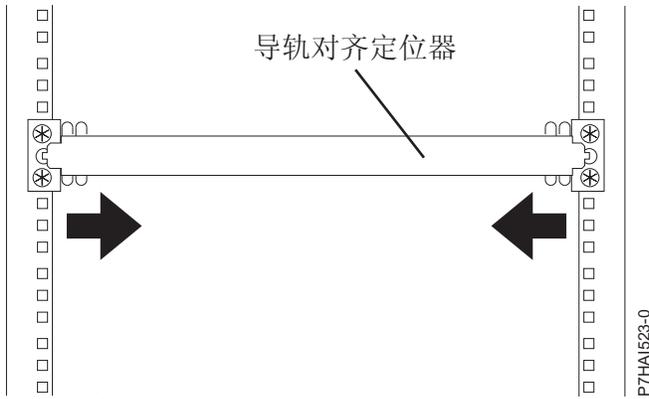


图 78. 插入导轨对齐定位器

8. 扩大安装在机架中的导轨的内部，然后将滚珠轴承的组合件向前滑至导轨前部。
9. 将平板监视器和键盘托盘滑至导轨中滚珠轴承的组合件。

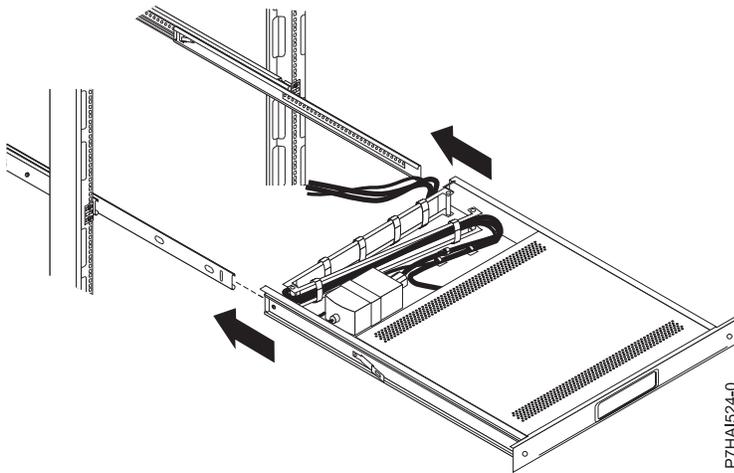


图 79. 滑动监视器和键盘

10. 按释放插销并将平板监视器和键盘托盘完全推进机架。最初可能会遇到一些阻力，因为滚珠轴承的组合件将在内导轨与外导轨之间对齐。将托盘拉出一半，然后将其推回以使托盘在导轨中完全到位。执行此操作几次以确保托盘在导轨中平滑地移动。

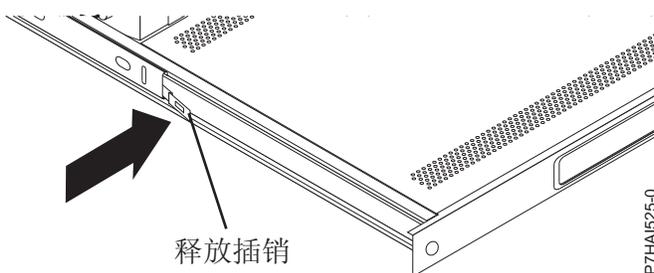


图 80. 使用释放插销

注：

视频线已连接到平板监视器。当您安装托盘中时，请确保未挤压或剪切视频线。

11. 将托盘推进机架并拧紧滑轨支架后端的 4 个螺钉。

12. 将键盘置于平稳的表面上，并卸下位于新键盘底部每一端的粘性橡胶垫。不要保留键盘上的橡胶垫，因为橡胶垫可能延伸到托盘下的空间。

注：

不要延伸键盘支脚。如果在关闭监视器的情况下延伸支脚，平板监视器屏幕可能被损坏。

13. 将托盘从机架一直拉到其在导轨上完全延伸。
14. 抬起平板监视器的前部，然后将监视器升至完全直立位置。

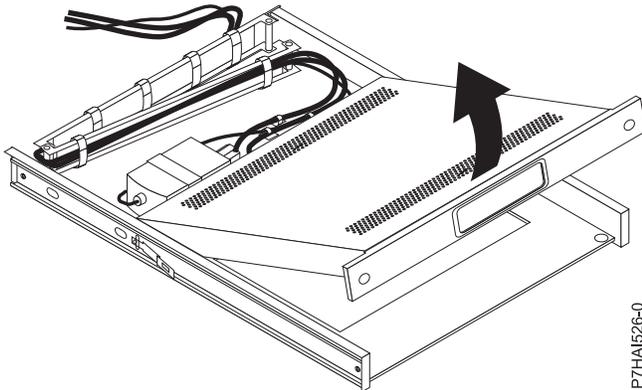


图 81. 将监视器升至完全直立位置

15. 将键盘插入到托盘中。然后，沿着托盘底部的线夹检修键盘和鼠标线，向上沿着托盘右侧的开口，向前沿着电缆管理臂。沿着开口拉出电缆的完整长度。
16. 将键盘线和鼠标线放在监视器后的托盘上。请确保在将托盘推进其位置时电缆不会阻塞机架中的设备。在以下步骤中，您将沿着电缆管理臂检修电缆。
17. 将监视器放低到较低位置，然后将托盘一直推进机架。使用翼形螺钉将托盘前部固定到机架中。
18. 从机架后端，卸下用于将电缆管理臂固定到托盘的运输带。
19. 沿着电缆管理臂检修键盘和鼠标线。使用现有电缆扎带固定电缆。
20. 卸下离左滑轨的机架后端最近的导轨对齐螺钉。使用螺钉将电缆管理臂连接到导轨。

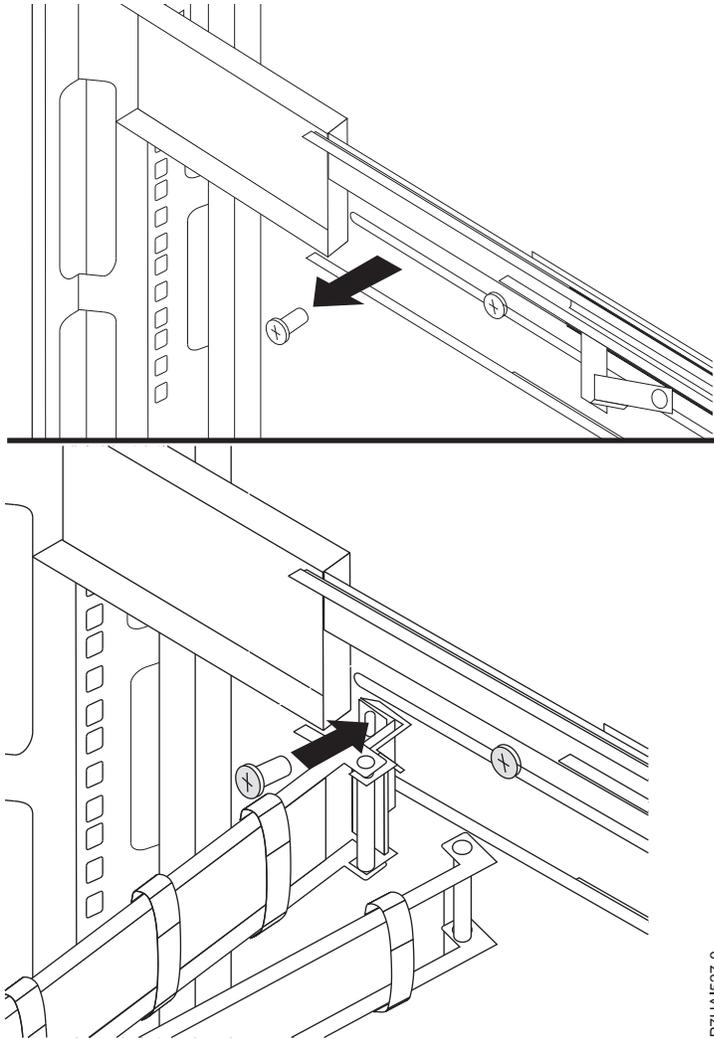


图 82. 连接电缆管理臂

21. 将视频连接器、键盘连接器和鼠标连接器连接到服务器或机架机柜中的可选控制台开关。如果要安装可选控制台开关，请参阅安装可选控制台开关并完成所述步骤。如果不安装，请遵循步骤 21 中的过程完成安装监视器和键盘托盘。
22. 将电源线连接到电缆管理臂上的短跳线。
23. 将所有电缆和信号连接器连接到相应的设备或接口。
24. 确保所有电源开关都已关闭。将电源线连接到接地电源插座或配电装置 (PDU)。

注：请在将交流电源线连接到直流适配器插座之前，确保本地电源的电压在 100 到 240V 交流之间。

25. 从机架机柜前部展开托盘。检修机架机柜内的电缆，并将它们与电缆扎带固定在一起。

安装控制台开关（可选）

了解如何安装可选控制台开关。

可使用控制台开关将多个服务器连接到单个监视器和键盘。控制台开关选项单独提供，但开关的定制安装支架与安装工具箱一起提供。

通过将控制台开关安装在监视器和键盘托盘后面，监视器和键盘托盘会占用机架中的相同空间。要将控制台开关安装在托盘后面，请使用随安装工具箱一起提供的支架。

完成以下步骤以将控制台开关安装在托盘后面：

1. 使用 2 个 8-32 螺钉将左右两侧的支架分别连接到控制台开关的左侧和右侧。

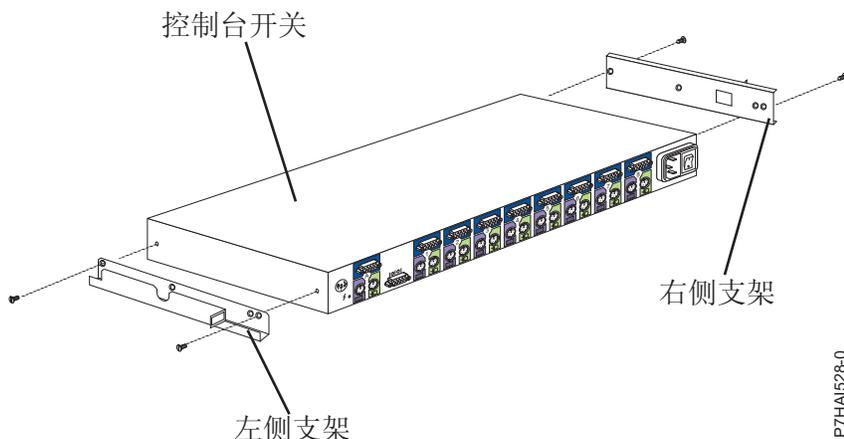


图 83. 安装控制台开关

注：左侧支架具有一个用于检修电源线、视频线、键盘线和鼠标线的通道。请确保将两个支架连接到控制台开关，以便左侧支架上的通道正面朝上。

2. 通过使用其他硬件工具箱中提供的 4 个（每一端各 2 个）十字螺钉，将控制台开关安装在平板监视器和键盘托盘后面。
3. 沿着控制台开关左侧支架上的通道来检修电源线、视频线、键盘线和鼠标线。然后，将视频连接器、键盘连接器和鼠标连接器连接到控制台开关。

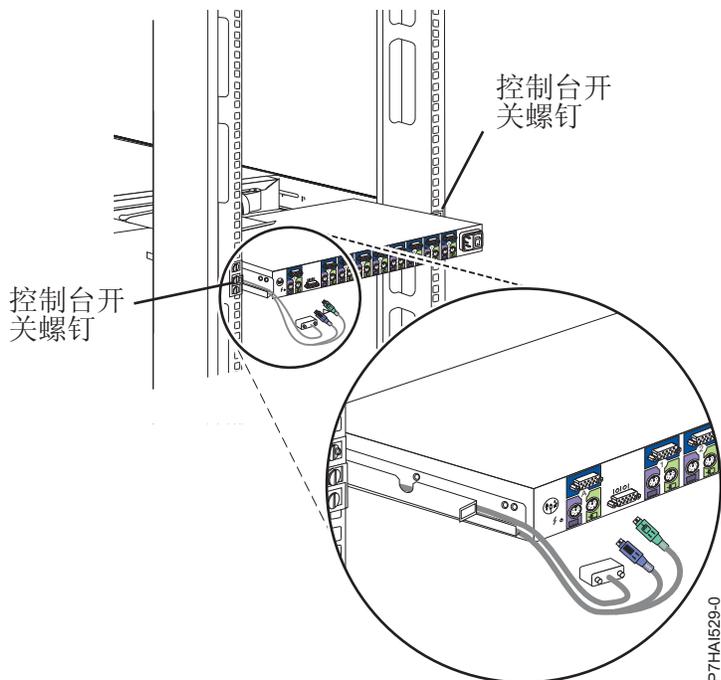


图 84. 路由电缆

4. 连接电源线、路由电缆和电缆扎带。有关指示信息，请参阅将电源线连接到电缆管理臂上的短跳线。

使用 HMC Classic 或 HMC Enhanced 界面配置 HMC

了解如何使用 HMC Classic 或 HMC Enhanced 界面设置网络连接、配置 HMC、执行配置后步骤以及升级和更新 HMC。

注意：

1. HMC Classic 界面在硬件管理控制台 (HMC) V8.7.0 或更高版本中不再可用。以前通过 HMC Classic 界面提供的功能现在通过 HMC 增强型+ 界面提供。
2. HMC Enhanced GUI 在 HMC V8.1.0.1 或 8.2.0 上可用，登录 HMC 时选择 HMC Enhanced 选项即可。从 HMC V8.3.0 开始，HMC Enhanced 界面的过程和功能现在是 HMC 增强型+ 界面的一部分。
3. 依据要应用于 HMC 配置的定制级别，可以有多种方式来设置 HMC 以满足您的需要。指导式安装向导是 HMC 上的一种工具，旨在方便设置 HMC。您可以通过向导选择一个快速路径以便迅速创建建议的 HMC 环境，也可以选择充分浏览向导所指引的可用设置。没有向导的帮助时，还可通过使用 HMC 菜单配置 HMC 来执行配置步骤。

在 HMC 上选择网络设置

了解可在 HMC 上使用的网络设置。

HMC 网络连接

您可以使用不同类型的网络连接将 HMC 连接至受管系统。有关如何配置 HMC 以连接至网络的更多信息，请参阅第 87 页的『配置 HMC』。有关在网络上使用 HMC 的更多信息，请参阅以下内容：

HMC 网络连接的类型：

了解如何通过网络来使用 HMC 远程管理和服务功能。

HMC 支持以下类型的逻辑通信：

HMC 至受管系统

用于执行大多数硬件管理功能，其中 HMC 会通过受管系统的服务处理器发出控制功能请求。HMC 与服务处理器之间的连接有时又称为服务网络。管理受管系统时需要此连接。

HMC 至逻辑分区

用来从逻辑分区中正在运行的操作系统收集与平台相关的信息（硬件错误事件和硬件清单），并用来使某些平台活动（动态 LPAR 和并发维修）与这些操作系统协调一致。如果要使用服务和错误通知功能，那么必须创建此连接。

HMC 至 BMC

注：基板管理控制器 (BMC) 连接仅适用于 HMC 型号 7063-CR1。

用来使用服务和维护任务。BMC 连接用来在系统上装入和维护 HMC 固件。在 HMC 上访问 BMC 时，需要此连接。

HMC 至远程用户

允许远程用户访问 HMC 功能。远程用户可以通过以下方式访问 HMC：

- 使用 Web 浏览器以远程方式访问所有 HMC GUI 功能。
- 使用安全套接字 Shell (SSH) 以远程方式访问 HMC 命令行功能。

HMC 至服务和支持

用于将数据（如硬件错误报告、清单数据和微码更新）传送到服务供应商以及从服务供应商传送这些数据。您可以使用此通信路径来调用自动服务。

根据型号，HMC 最多可支持 4 个不同物理以太网接口。独立版本的 HMC 仅支持三个 HMC 接口（使用一个集成以太网适配器和最多两个插件适配器）。通过以下方式使用其中每个接口：

- 可将一个或多个网络接口专门用于 HMC 至受管系统通信，这意味着该网络上只有 HMC 和受管系统的服务处理器。尽管连接至服务处理器的网络接口使用了安全套接字层 (SSL) 协议进行加密，并用密码加以保护，但具有单独的专用网络可以为这些接口提供更高级别的安全性。
- 开放式网络接口通常用于 HMC 和受管系统上的逻辑分区之间的网络连接，以支持 HMC 至逻辑分区的通信。还可使用此开放式网络接口来远程管理 HMC。
- 可选择使用第三个接口来连接逻辑分区并远程管理 HMC。此接口还可用作与不同逻辑分区组的单独 HMC 连接。例如，您可能想获得一个管理 LAN，该 LAN 独立于正在运行所有普通业务交易的 LAN。远程管理员可以使用此方法访问 HMC 和其他受管单元。有时，逻辑分区位于不同的网络安全域，可能在防火墙后面，因此您可能要建立与两个域的每一个域的不同 HMC 网络连接。

HMC 的 Web 浏览器需求

硬件管理控制台 (HMC) V8.7.0 受 Google Chrome V57、Microsoft Internet Explorer (IE) V11.0、Mozilla Firefox V45 和 V52 长期支持版 (ESR) 以及 Safari V10.1 支持。

如果您的浏览器配置为使用因特网代理，那么异常列表中应该包括一个本地 IP 地址。有关异常列表的更多信息，请咨询您的网络管理员。如果您仍需要使用代理来获取 HMC，请启用"Internet 选项"窗口中"高级"选项卡下面的"通过代理连接使用 HTTP 1.1"。

在远程连接到 HMC 时需要启用会话 cookie 以便使 ASMI 运行。ASM 代理代码保存会话信息并使用。遵循启用会话 cookie 的步骤。

在 Internet Explorer 中启用会话 cookie。

1. 选择"工具"，然后单击"Internet 选项"
2. 选择"隐私"，然后单击"高级"
3. 确保选中了"总是允许会话 cookie"。如果未选中，请选中"替代自动 cookie 处理"和"总是允许会话 cookie"。
4. 在"第一方 cookie"和"第三方 cookie"下面选择"提示"
5. 单击"确定"。

在 Firefox 中启用会话 cookie。

1. 选择"工具"，然后单击"选项"
2. 单击"cookie"
3. 选择"允许站点设置 cookie"。
4. 选择"异常"，然后添加 HMC。
5. 单击"确定"。

HMC 环境中的专用网络和开放式网络：

HMC 可配置为使用开放式网络和专用网络。专用网络允许使用所选范围的不可路由 IP 地址。公用网络或"开放式"网络描述 HMC 与任何逻辑分区以及 HMC 与常规网络上的其他系统之间的连接。

专用网络

HMC 专用网络上的设备只有 HMC 本身以及该 HMC 连接至的每个受管系统。该 HMC 连接至每个受管系统的 FSP（弹性服务处理器）。

在大多数系统上，FSP 提供标签为 **HMC1** 和 **HMC2** 的两个以太网端口。这允许您连接至两个 HMC。

一些系统具有双 FSP 选项。在此情况中，第二个 FSP 充当“冗余”备份。具有两个 FSP 的系统的基本设置要求与只有一个 FSP 的系统的基本设置要求大致相同。HMC 必须连接至每个 FSP，所以有多个 FSP 或多个受管系统时需要其他网络硬件（如 LAN 交换机或集线器）。

注：受管系统上的每个 FSP 端口只能连接至一个 HMC。

公用网络

开放式网络可连接用于连接因特网的防火墙或路由器。连接至因特网允许 HMC 在发生需要报告的任何硬件错误时进行“回拨”。

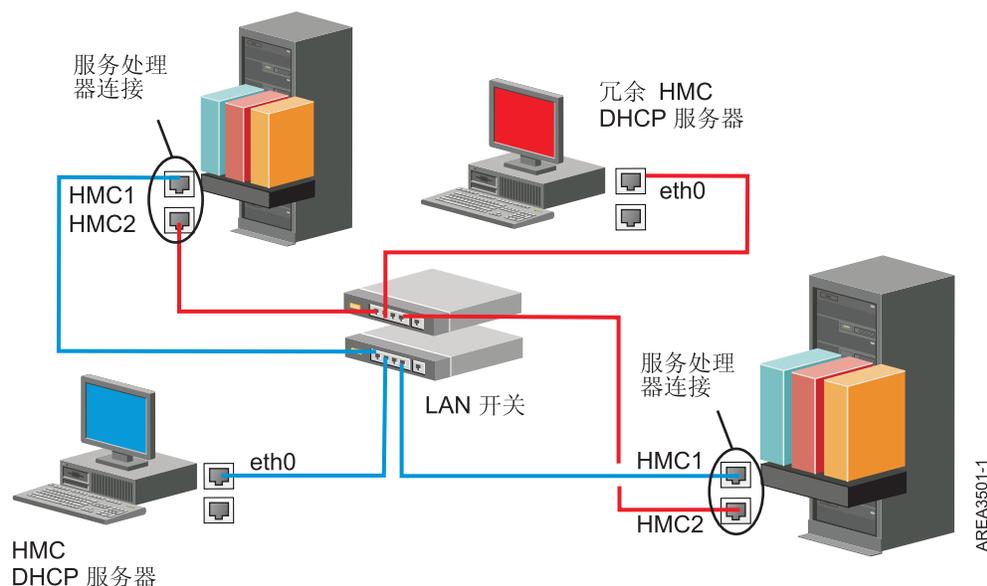
HMC 本身在它的每个网络接口上提供自己的防火墙。运行 HMC 指导式安装向导时会自动配置基本防火墙，但您应在初始 HMC 安装和配置后定制防火墙设置。

将 HMC 用作 DHCP 服务器：

可将 HMC 用作动态主机配置协议 (DHCP) 服务器。

注：如果要使用 IPv6，那么必须手动完成发现过程。对于 IPv6，不存在自动发现。

有关如何将 HMC 配置为 DHCP 服务器的更多信息，请参阅第 93 页的『将 HMC 配置为 DHCP 服务器』。

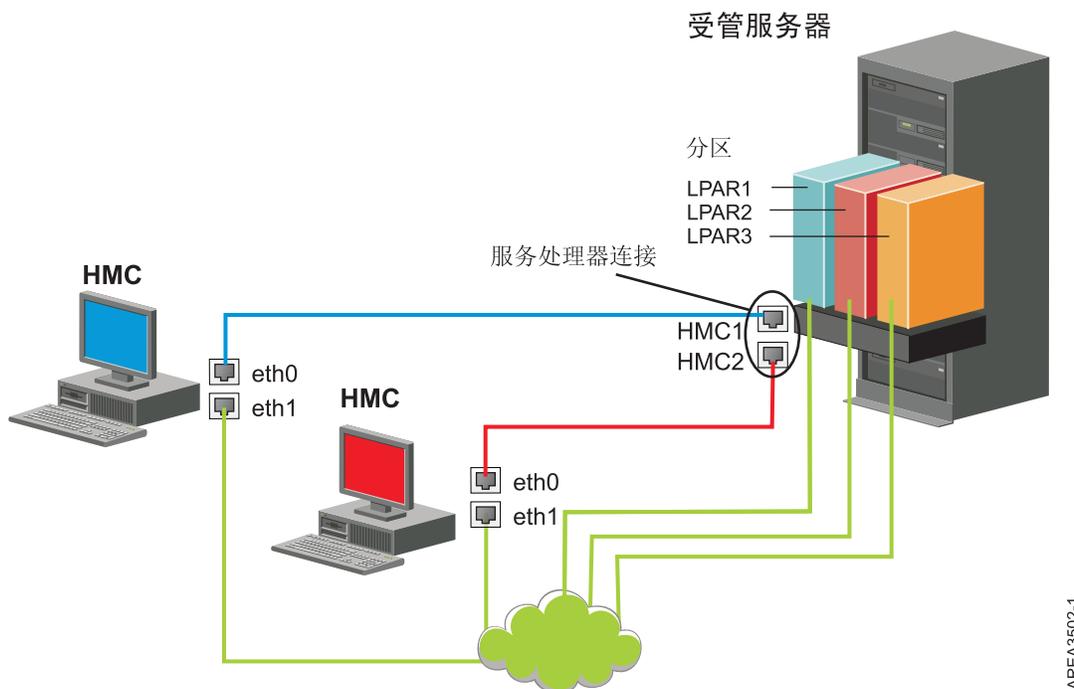


此图显示具有两个受管系统的冗余 HMC 环境。第一个 HMC 连接至每个 FSP 的第一个端口，冗余 HMC 连接至每个 HMC 的第二个端口。每个 HMC 被配置为 DHCP 服务器（使用不同范围的 IP 地址）。连接位于单独的专用网络上。确保未将任何 FSP 端口连接至多个 HMC 也同样重要。

连接至 HMC 的每个受管系统的 FSP 端口需要一个唯一的 IP 地址。要确保每个 FSP 具有一个唯一的 IP 地址，请使用 HMC 的内置 DHCP 服务器功能。当 FSP 检测到活动网络链接时，它会发出一个广播请求来定位某个 DHCP 服务器。如果 HMC 的配置正确，那么它会通过分配所选地址范围中的一个地址来响应该请求。

当存在多个 FSP 时，对于 HMC 至 FSP 专用网络，您必须拥有自己的 LAN 交换机或集线器。或者，此专用段可以作为多个端口存在于较大受管交换机上的专用虚拟 LAN (VLAN) 中。如果有多个专用 VLAN，那么必须确保它们被隔离开并且没有任何交叉流量。

如果有多个 HMC，那么还必须将同一开放式网络上的每个 HMC 连接至逻辑分区。



此图显示了连接至专用网络上单个受管服务器和公用网络上的三个逻辑分区两个 HMC。您可以将一个额外的以太网适配器用于 HMC，以便具有三个网络接口。可以将第三个网络用作管理网络，也可以将它连接至 CSM（集群系统管理器）管理服务器。

有关如何将 HMC 配置为 DHCP 服务器的更多信息，请参阅第 93 页的『将 HMC 配置为 DHCP 服务器』。

决定要用于回拨服务器的连接方法：

了解有关使用回拨服务器时可使用的连接选项的更多信息。

通过使用基于 LAN 的因特网连接或基于调制解调器的拨号连接，可将 HMC 配置为将硬件服务相关信息发送至 IBM。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

配置基于 LAN 的因特网连接时，有两个通信选项。第一个选项是使用标准安全套接字层 (SSL)。可启用 SSL 通信以通过代理服务器连接至因特网。SSL 连接符合公司安全准则的可能性更高。第二个选项是使用 VPN 连接。

注：如果开放式网络接口连接仅使用因特网协议 V6 (IPv6)，那么不能使用因特网协议 VPN 来连接至支持系统。有关所使用协议的更多信息，请参阅第 76 页的『选择因特网协议』。

使用因特网连接的优点可能包括以下几点：

- 传输速度更快

- 降低客户开销（例如，专用模拟电话线路的成本）
- 可靠性更高

不管所选连接方法如何，下列安全性特征都会生效：

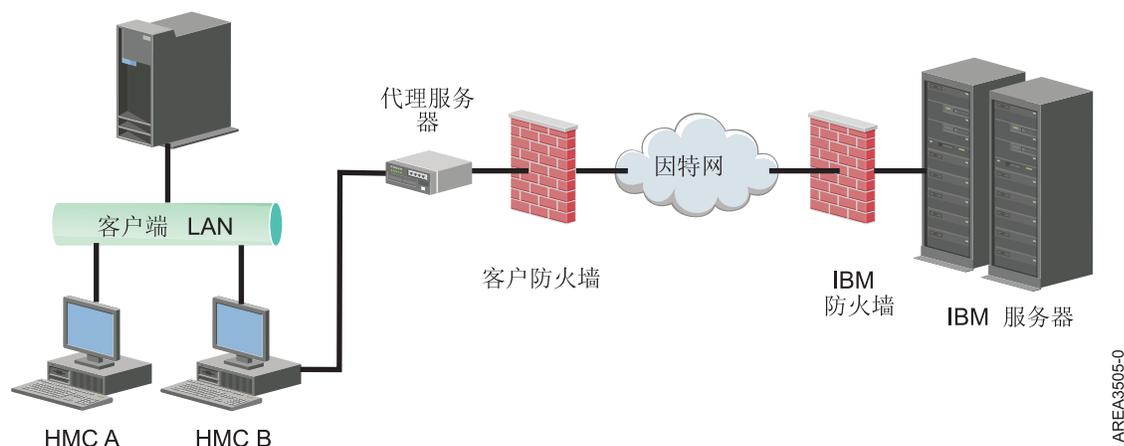
- 总是将远程支持设施请求从 HMC 发送至 IBM。决不会从 IBM 服务支持系统发出入站连接。
- HMC 与 IBM 服务支持系统之间传输的所有数据都是使用高级加密进行加密的。根据所选连接方法，会使用 SSL 或 IPSec 封装安全性有效负载 (ESP) 来进行加密。
- 初始化加密连接时，HMC 会将目标认证为 IBM 服务支持系统的目标。

发送至 IBM 服务支持系统的信息仅包含硬件问题和配置的相关信息。应用程序或客户数据不会传送至 IBM。

将间接因特网连接与代理服务器配合使用。

如果安装要求 HMC 放在专用网络上，那么您可使用 SSL 代理间接连接至因特网，SSL 代理会将请求转发至因特网。使用 SSL 代理的其他潜在优点之一是代理可能支持日志记录和审计设施。

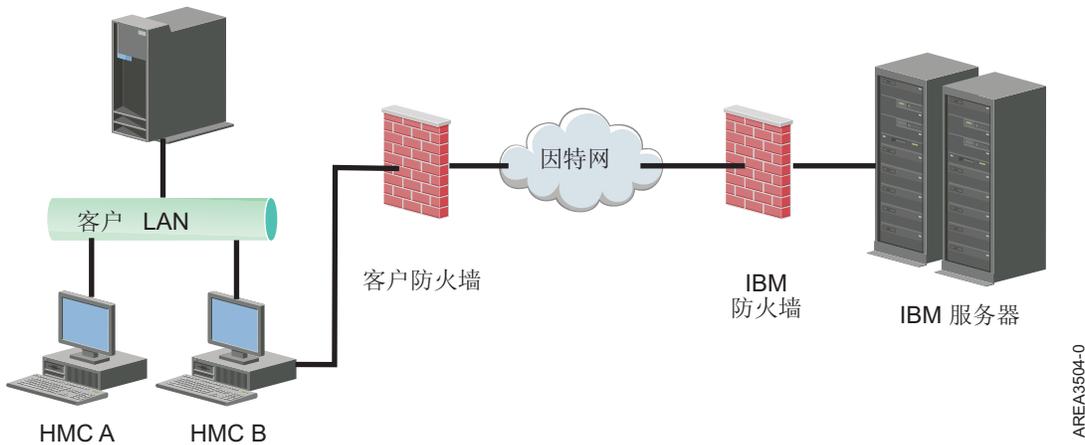
要转发 SSL 套接字，代理服务器必须支持基本代理服务器头功能（如 RFC 2616 中所述）和 CONNECT 方法。可选择配置基本代理认证 (RFC 2617) 以便在尝试通过代理服务器转发套接字之前让 HMC 进行认证。



要使 HMC 成功通信，客户机的代理服务器必须允许连接至端口 443。可配置代理服务器以将具体 IP 地址限制为 HMC 可连接的 IP 地址。请参阅第 77 页的『因特网 SSL 地址列表』以获取 IP 地址列表。

使用直接因特网 SSL 连接

如果 HMC 可连接至因特网，并且可设置外部防火墙以允许所建立的 TCP 包将出站数据传递至第 77 页的『因特网 SSL 地址列表』中所述的目标，那么您可使用直接因特网连接。



简化的连接：

了解 HMC 在使用简化的连接时所用的 IP 地址。

有新的回拨服务器环境可用，它提供了面向当前回拨基础结构的前端代理。此环境减少了 IBM 服务器的数目、支持 IPv6 连接并通过支持 NIST 800-131A 提供增强的安全性，从而简化了所需的信息技术。在防火墙上需要打开的 IBM IP 地址更少。所有回拨因特网流量都流经回拨代理。

注：简化的连接在 HMC V8.3.0 或更高版本上可用。

HMC 在配置为使用简化的连接时，会使用以下 IPv4 地址来与 IBM 服务和支持联系：

- 129.42.56.189
- 129.42.60.189
- 129.42.54.189

HMC 在配置为使用简化的连接时，会使用以下 IPv6 地址来与 IBM 服务和支持联系：

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

使用因特网 SSL 以连接至远程支持：

所有通信是通过 HMC 发出的 TCP 套接字处理的，并且这些通信会使用高级 SSL 来加密传送的数据。将发布目标 TCP/IP 地址（请参阅第 77 页的『因特网 SSL 地址列表』）以便将外部防火墙配置为允许这些连接。

注：标准 HTTPS 端口 443 将用于所有通信。

可启用 HMC 以直接连接至因特网，或通过客户提供的代理服务器间接连接至因特网。哪个方法最适用于您的安装版本取决于企业的安全性和联网要求。HMC（直接连接或通过 SSL 代理连接）在配置为使用因特网 SSL 连接时会使用下列地址。

选择因特网协议：

确定 HMC 连接至服务供应商时使用的 IP 地址版本。

大多数用户使用因特网协议 V4 (IPv4) 来连接至服务供应商。用于访问因特网的 IPv4 地址的显示格式为 4 个 IPv4 地址字节，字节之前用句点分隔（如 9.60.12.123）。还可使用因特网协议 V6 (IPv6) 来连接至服务供应

商。网络管理员通常使用 IPv6 以确保地址空间唯一。如果您不确定安装版本所使用的因特网协议，请与网络管理员联系。有关使用每个版本的更多信息，请参阅第 94 页的『设置 IPv4 地址』和第 94 页的『设置 IPv6 地址』。

因特网 **SSL** 地址列表：

了解 HMC 在使用因特网 SSL 连接时所用的地址。

HMC 在配置为使用因特网 SSL 连接时，会使用以下 IPv4 地址来与 IBM 服务和支持联系。

以下 IPv4 地址用于所有位置：

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

以下 IPv4 地址用于美国：

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

以下 IPv4 地址用于美国以外的所有位置：

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

注：将防火墙配置为允许 HMC 连接至这些服务器时，只需要特定于地理区域的 IP 地址。

HMC 在配置为使用因特网 SSL 连接时，会使用以下 IPv6 地址来与 IBM 服务和支持联系：

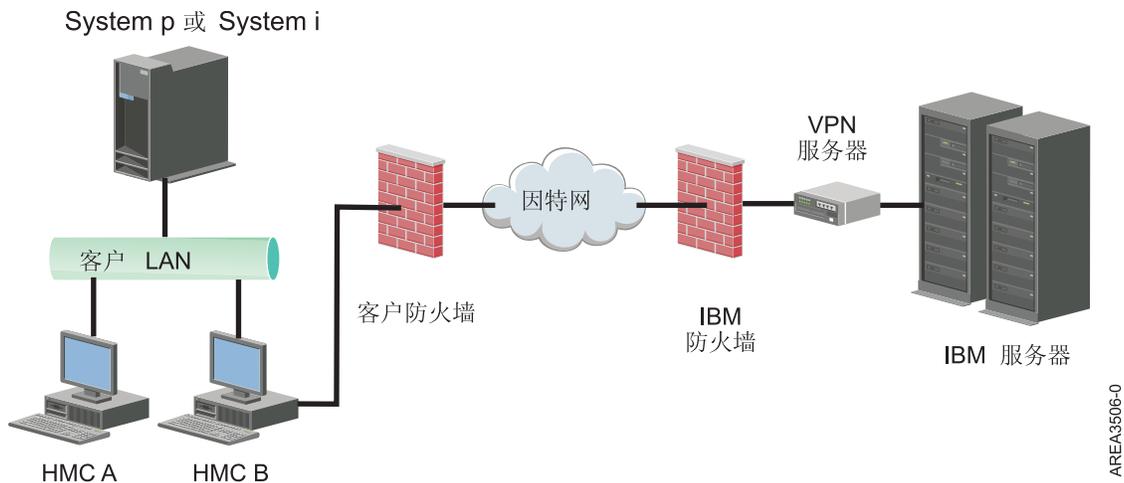
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

使用虚拟专用网连接至远程支持：

当连接至远程支持时，虚拟专用网 (VPN) 提供安全性。

注：此连接类型仅在 HMC V8.2.0 或更低版本上可用。

通过以加密和其他安全性方法来替代传统专用网络的物理上独立的网络线路，VPN 通过公用线路为用户提供了单独网线的私密性。除了能够用于出站连接之外，VPN 连接还可根据需要配置为支持远程服务请求。



因特网连接由系统管理员提供。防火墙还可以将具体 IP 地址限制为 HMC 可连接的 IP 地址。如果需要配置防火墙以限制 IP 地址，请参阅『VPN 服务器地址列表』以获取可使用的地址的列表。

有关如何使用基于 LAN 的 VPN 连接至因特网的更多信息，请参阅第 90 页的『配置 HMC 网络类型』。

VPN 服务器地址列表：

列示 HMC 配置为使用因特网 VPN 连接时使用的服务器。

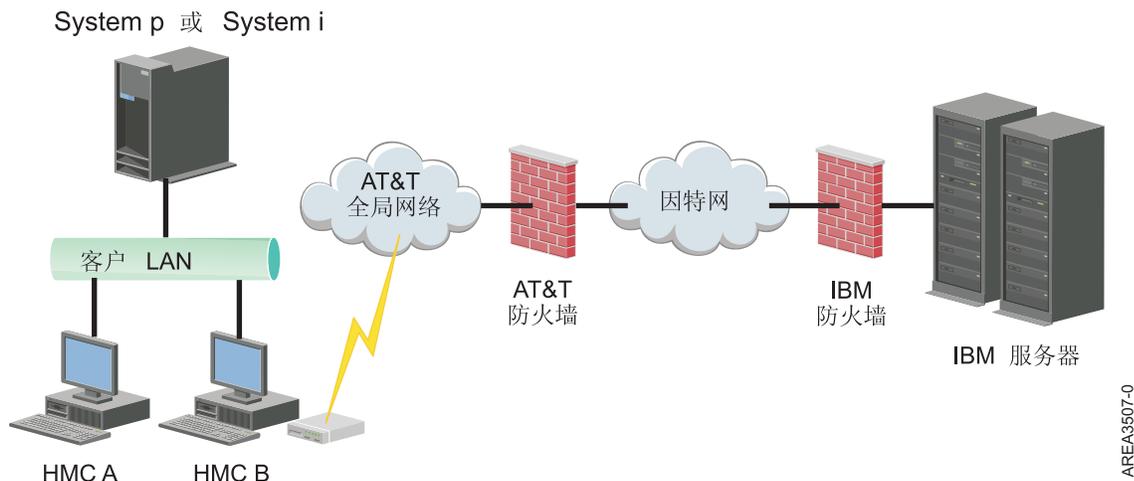
HMC 配置为使用因特网 VPN 连接时使用下列服务器。使用网络地址转换 (NAT) 防火墙时，所有连接在端口 500 和端口 4500 上使用 ESP 和 UPD。

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

使用电话和调制解调器连接至远程支持：

如果要使用调制解调器连接至远程支持，必须提供专用模拟线路来连接至 HMC 调制解调器。HMC 使用调制解调器来拨通全局网络并连接至 IBM 服务和支持。

注：此连接类型仅在 HMC V8.2.0 或更低版本上可用。



有关使用电话和调制解调器连接至远程支持的更多信息，请参阅第 90 页的『配置 HMC 网络类型』。

使用多个回拨服务器：

本主题描述决定使用多个回拨服务器时需要了解的事项。

为避免单点故障，请将 HMC 配置为使用多个回拨服务器。第一个可用的回拨服务器尝试处理每个服务事件。如果此回拨服务器的连接或传输失败，那么会使用其他可用回拨服务器重试服务请求，直到某个服务器操作成功或已尝试所有服务器。

由问题分析标识为给定受管系统的主分析控制台的已连接 HMC 将报告该问题。此主控制台还会将问题报告复制至所有辅助 HMC。此辅助 HMC 在网络上必须可被主 HMC 识别。出现以下情况时，辅助 HMC 被主 HMC 识别为另一回拨服务器：

- 主 HMC 配置为使用“发现的”回拨服务器，并且回拨服务器与主 HMC 在同一子网上或管理同一系统
- 回拨服务器已手动添加至可用于出站连接的回拨服务器控制台列表

准备 HMC 配置

使用本节来收集开始配置步骤之前需要知道的必需配置设置。

要配置 HMC，必须了解相关概念、制定决策和准备信息。

本节描述将 HMC 连接至下列各项时所需的信息：

- 受管系统中的服务处理器
- 这些受管系统上的逻辑分区
- 远程工作站
- IBM 服务，用于实现“回拨”功能

注：提供了其他连接和安全性信息。有关更多信息，请参阅 **ESA for HMC Connectivity Security for IBM POWER6®, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000®** 白皮书，可从以下网址取得：IBM Electronic Service Agent™ (<http://www-01.ibm.com/support/esa/security.htm>)。

要准备 HMC 配置，请完成以下步骤：

1. 获取要安装的 HMC 代码版本的最新级别并进行安装。
2. 确定 HMC 相对于它要管理的服务器的物理位置。如果 HMC 与其受管系统相距超过 25 英尺，那么必须允许从受管系统的位置使用 Web 浏览器访问 HMC，以便服务人员能够访问 HMC。
3. 标识 HMC 将管理的服务器。
4. 确定是使用专用网络还是开放式网络来管理服务器。如果决定使用专用网络，请使用 DHCP，除非您在使用集群系统管理 (CSM) 配置。CSM 不支持 IPv6。要访问 CSM，必须有两个网络。有关 CSM 的更多信息，请参阅随该功能部件提供的文档。有关专用网络和开放式网络的更多信息，请参阅第 72 页的『HMC 环境中的专用网络和开放式网络』。
5. 如果您使用开放式网络来管理 FSP，那么必须通过"高级系统管理界面"菜单来手动设置 FSP 的地址。建议使用不可路由的专用网络。
6. 如果有两个 HMC，请指定主 HMC 和辅助 HMC。主 HMC 在物理位置上应该更接近机器，并且应该是配置为回拨的 HMC。
7. 确定将 HMC 连接至远程工作站、逻辑分区和网络设备时所需的网络设置。
8. 定义 HMC 如何"回拨"。回拨选项包括通过仅出站安全套接字层 (SSL) 因特网连接、调制解调器或虚拟专用网 (VPN) 连接。
9. 确定您将创建的 HMC 用户及其密码以及将给予他们的角色。必须对 hscroot 和 hscpe 用户指定密码。
10. 描述配置回拨时所需的以下公司联系人信息：
 - 公司名称
 - 管理员联系人
 - 电子邮件地址
 - 电话号码
 - 传真号码
 - HMC 物理位置的街道地址
11. 如果计划通过回拨将信息发送至 IBM 服务时使用电子邮件来通知操作员或系统管理员，请标识简单电子邮件传输协议 (SMTP) 服务器和您要使用的电子邮件地址。
12. 必须定义以下密码：
 - 用于向 FSP 认证 HMC 的访问密码
 - 用于管理用户的 ASMI 密码
 - 用于一般用户的 ASMI 密码

第一次从 HMC 连接至新服务器时创建密码。如果 HMC 是冗余或辅助 HMC，请获取 HMC 用户密码并准备在第一次连接至受管服务器的 FSP 时输入此密码。

完成这些准备步骤后，请填写『HMC 的安装前配置工作表』。

HMC 的安装前配置工作表

使用此工作表来准备安装所需的安装信息。

网络设置

LAN 接口：选择可用的适配器（如 eth0 和 eth1），此 HMC 将使用这些适配器连接至受管系统、逻辑分区、服务和支持以及远程用户。有关更多信息，请参阅第 71 页的『HMC 网络连接』。从 HMC 发出的连接可以是在专用网络或开放式网络上进行的。

以太网适配器速度和双工

输入期望的以太网适配器速度和双工方式。如果您不确定哪种速度和双工能使您的硬件性能达到最佳，那么自动检测选项会确定最佳选项。“缺省值 = 自动检测介质速度”会指定以太网适配器双工方式下的速度。除非您要求指定固定介质速度，否则请选择“自动检测”。与 FSP（交换机/HMC）连接的任何设备都必须设置为“自动（速度）/自动（双工）”方式，因为这是缺省的 FSP 设置，不能更改。

表 11. 以太网适配器速度和双工

	eth0	eth1	eth2	eth3
选择速度和双工方式				
介质速度（自动检测，10/100/1000 全/半双工）				

有关专用网络和开放式网络的更多信息，请参阅第 72 页的『HMC 环境中的专用网络和开放式网络』。

表 12. 专用网络和开放式网络

	eth0	eth1	eth2	eth3
对每个适配器指定专用或开放式网络				

动态主机配置协议 (DHCP) 提供动态客户机的自动配置方法。可将此 HMC 指定为 DHCP 服务器。如果这是专用网络中的第一个或唯一的 HMC，那么将此 HMC 启用为 DHCP 服务器。执行此操作时，HMC 会自动配置和查找网络上的受管系统。

对于指定为专用网络的以太网适配器，请填写下表：

表 13. 专用网络

	eth0	eth1
是否要将此 HMC 指定为 DHCP 服务器？（是/否）		
如果答案为“是”，请记录要使用的 IP 地址范围		

如果您使用的是 7063-CR1 HMC，那么必须将以太网 IPMI 端口连接至网络，才能在 HMC 上访问基板管理控制器 (BMC)。有关更多信息，请参阅第 136 页的『配置 BMC 连接』。针对您的 BMC 连接填写下表。

表 14. BMC 连接

	IPMI
是否要通过 DHCP 方式配置此连接？（是/否）	
如果答案为“否”，请列出下面的已指定静态地址：	
IP 地址：	
子网掩码：	
网关：	

对于指定为开放式网络的以太网适配器，请填写下列各表。有关不同因特网协议版本的更多信息，请参阅第 76 页的『选择因特网协议』。

使用 IPv6

如果要使用 IPv6，请告诉网络管理员并决定获取 IP 地址的方式。然后，完成下列各表：

表 15. 使用 IPv6

	eth0	eth1	eth2	eth3
是否正使用以静态方式指定的 IP 地址？如果答案为"是"，请将该地址记录在此处。				

表 16. 使用 IPv6

	eth0	eth1	eth2	eth3
是否正从 DHCP 服务器获取 IP 地址？ (是/否)				

表 17. 使用 IPv6

	eth0	eth1	eth2	eth3
是否正从 IPv6 路由器获取 IP 地址？				

有关设置 IPv6 地址的更多信息，请参阅第 94 页的『设置 IPv6 地址』。有关仅使用 IPv6 地址的更多信息，请参阅第 94 页的『仅使用 IPv6 地址』。

使用 IPv4

对于指定为使用 IPv4 的开放式网络的以太网适配器，请填写下列各表。

表 18. 使用 IPv4

	eth0	eth1	eth2	eth3
是否要自动获取 IP 地址？（是/否）				
如果答案为"否"，请列出下面的指定地址：				
TCP/IP 接口地址：				
TCP/IP 接口网络掩码：				
防火墙设置：				
是否要配置 HMC 防火墙设置？（是/否）				
如果是，请列出应该允许通过防火墙的应用程序和 IP 地址：				

TCP/IP 信息

每个节点（支持元素 (SE) 和“硬件管理控制台 (HMC)”）都需要唯一 TCP/IP 地址。缺省情况下，指定的网络掩码用于为本地专用 LAN 生成唯一地址。如果节点将连接至带有受管 TCP/IP 地址的较大网络，那么可指定要使用的 TCP/IP 地址。系统会生成缺省值。

防火墙设置

HMC 防火墙设置会创建安全性壁垒，该壁垒允许或拒绝访问 HMC 上的特定网络应用程序。可分别对每个物理网络接口指定这些控制设置，这允许您控制每个网络上可访问的 HMC 网络应用程序。

如果已至少将一个适配器配置为开放式网络适配器，那么必须提供其他信息以允许 HMC 访问 LAN：

表 19. 本地主机信息

本地主机信息	
HMC 主机名：	
域名：	
HMC 的描述：	
网关信息	
网关地址：(nnn.nnn.nnn.nnn)	
网关设备：	
DNS 启用	
是否要使用 DNS？（是/否）	
如果答案为“是”，请指定下面的 DNS 服务器搜索顺序：	
1.	
2.	
域后缀搜索顺序：	
1.	
2.	

本地主机信息

要向网络标识硬件管理控制台 (HMC)，请输入 HMC 的主机名和域名。除非您在网络上仅使用简短主机名，否则输入标准主机名称。域名示例：name.yourcompany.com

网关信息

要定义缺省网关，请填写要用于发送 IP 包的 TCP/IP 地址。如果目标站与源站不在同一子网上，网关地址会告诉每台计算机或网络设备何时发送数据。

DNS 启用

可使用域名系统 (DNS) 来提供用于查找基于 IP 的计算机的标准命名约定。通过定义 DNS 服务器，可使用主机名来标识服务器和硬件管理控制台 (HMC) 而不是 IP 地址。

DNS 服务器搜索顺序

输入为映射主机名和 IP 地址而搜索的 DNS 服务器的 IP 地址。此搜索顺序仅在启用 DNS 时可用。

域后缀搜索顺序

输入正在使用的域后缀。HMC 使用要追加到 DNS 搜索的非限定名称结尾的域后缀。将按后缀的列出顺序来搜索后缀。此搜索顺序仅在启用 DNS 时可用。

电子邮件通知

如果希望系统上发生硬件问题事件时通过电子邮件得到通知，请列出电子邮件联系人信息。

表 20. 电子邮件通知

域	
电子邮件地址:	
SMTP 服务器:	
端口:	
要通知的错误:	
仅回拨问题事件	
所有问题事件	

SMTP 服务器

输入要向其通知系统事件的服务器的简单电子邮件传输协议 (SMTP) 地址。SMTP 服务器名称的示例是 relay.us.ibm.com。

SMTP 是用于发送电子邮件的协议。使用 SMTP 时，客户机会发送消息并使用 SMTP 协议与 SMTP 服务器通信。

如果不知道或不确定服务器的 SMTP 地址，请与网络管理员联系。

端口 输入要向其通知系统事件的服务器的端口号或使用缺省端口。

要通知的电子邮件地址

输入发生系统事件时要通知的已配置电子邮件地址。

- 选择仅回拨问题事件以便仅在发生创建回拨功能的事件时接收通知。
- 选择所有问题事件以便在发生任何事件时接收通知。

服务联系人信息

表 21. 服务联系人信息

服务联系人信息	
公司名称	
管理员姓名	
电子邮件地址	
电话号码	
备用电话号码	
传真号码	
备用传真号码	
街道地址	
街道地址 2	
城市或地区	
州	
邮编	

表 21. 服务联系人信息 (续)

服务联系人信息	
国家或地区	
HMC 的位置 (如果与上述管理员地址相同, 请指定"相同") :	
街道地址	
街道地址 2	
城市或地区	
州	
邮编	
国家或地区	

服务授权和连接

选择要用于联系服务供应商的连接的类型。有关这些方法的描述 (包括安全性特征和配置要求), 请参阅第 74 页的『决定要用于回拨服务器的连接方法』。

表 22. 连接类型

连接类型	
	通过因特网连接的安全套接字层 (SSL)
	通过本地 HMC 进行拨号
	通过因特网连接的虚拟专用网 (VPN)

通过因特网连接的安全套接字层 (SSL):

如果 HMC 已连接至因特网, 那么可使用它来呼叫服务供应商。可通过使用借助现有因特网连接的加密安全套接字层 (SSL) 直接连接至服务供应商。如果要使用借助 SSL 代理的间接连接来配置使用加密 SSL, 请选择使用 **SSL 代理**。

表 23. 通过因特网连接的安全套接字层 (SSL)

通过因特网连接的安全套接字层 (SSL)	
是否使用 SSL 代理? (是/否)	
如果答案为"是", 请列出下面的信息:	
地址:	
端口:	
是否使用 SSL 代理进行认证?	
如果答案为"是", 请列出下面的信息:	
用户:	
密码:	

使用的因特网连接协议

有关不同因特网协议的更多信息, 请参阅第 76 页的『选择因特网协议』。

___ IPv4

IPv6

IPv4 和 IPv6

通过本地 HMC 进行拨号

输入用于配置本地调制解调器的拨号信息。指定要用于呼叫服务供应商的电话号码。进行连接时，应按列示顺序拨打电话号码。

表 24. 通过本地 HMC 进行拨号

域	
拨号前缀:	
音调:	
脉冲:	
是否等待拨号音?	
是否启用扬声器?	

虚拟专用网 (VPN)

如果 HMC 已连接至因特网，那么可使用它来呼叫服务供应商。可通过使用现有因特网连接的虚拟专用网 (VPN) 直接连接至服务供应商。

注：如果选择通过因特网连接的虚拟专用网 (VPN)，那么不会引导您选择任何其他选项。

回拨服务器

确定要配置为回拨服务器以连接至服务和支持的 HMC。有关使用多个回拨服务器的更多信息，请参阅第 79 页的『使用多个回拨服务器』。

此 HMC

另一 HMC

如果已选择另一 HMC，那么在此处列出已配置为回拨服务器的其他 HMC：

表 25. 已配置为回拨服务器的其他 HMC

已配置为回拨服务器的 HMC 主机名或 IP 地址的列表	

其他支持优点

My Systems 和 Premium Search

表 26. 其他支持优点

域	
列出您的 IBM 标识	
列出您的 IBM 标识	

为了在 Electronic Services Web 站点的“My Systems”和“Premium Search”部分中访问有价值的定制支持信息，客户必须向此系统注册其 IBM 标识。如果还没有 IBM 标识，可在 www.ibm.com/account/profile 注册 IBM ID。

注：IBM 提供个性化 Web 功能，而这些功能使用 IBM Electronic Service Agent 应用程序收集到的信息。要使用这些功能，必须先在 IBM 注册 Web 站点（网址为 <http://www.ibm.com/account/profile>）上进行注册。

要授权用户使用 Electronic Service Agent 信息来个性化 Web 功能，请输入您在 IBM 注册 Web 站点上注册的 IBM 标识。要查看可供向系统注册 IBM 标识的客户使用的有价值支持信息，请访问 <http://www.ibm.com/support/electronic>。

配置 HMC

了解如何配置网络连接、安全性、服务应用程序和一些用户首选项。

依据要应用于 HMC 配置的定制级别，可以有多种方式来设置 HMC 以满足您的需要。指导式安装向导是 HMC 上的一种工具，旨在方便设置 HMC。您可以通过向导选择一个快速路径以便迅速创建建议的 HMC 环境，也可以选择充分浏览向导所指引的可用设置。没有向导的帮助时，还可通过使用 HMC 菜单配置 HMC 来执行配置步骤。

开始之前，应该收集成功完成步骤所需的配置信息。有关所需信息的列表，请参阅第 79 页的『准备 HMC 配置』。完成准备时，应确保完成了第 80 页的『HMC 的安装前配置工作表』，然后返回至本节。

通过指导式安装向导使用快速路径来配置 HMC

在大多数情况下，可以使用许多缺省设置来设置 HMC，以便高效率地操作。使用此快速路径核对表来准备 HMC 以获取服务。完成这些步骤之后，HMC 将被配置为（直接连接的）专用网络中的“动态主机配置协议”(DHCP) 服务器。

启动 HMC 并完成指导式安装向导中的步骤：

登录 HMC 界面并使用指导式安装向导来配置 HMC。

注：如果这是新安装，请确保受管系统未连接至电源。对于机架安装式 HMC，这意味着在插入主电源之前，此 HMC 是插入配电总线 (PDB) 的唯一设备。如果这是连接至同一受管系统中的第二个 HMC，那么可以将该受管系统连接至电源。

1. 按下电源按钮以开启 HMC。
2. 等待 HMC 在 30 秒后自动选择缺省语言和语言环境首选项。
3. 接受硬件管理控制台许可协议。如果拒绝硬件管理控制台许可协议，那么将无法完成 HMC 配置。
4. 单击登录并启动硬件管理控制台 **Web** 应用程序。
5. 登录 HMC：

注：如果系统管理员 (**hmcadmin**) 更改了密码，请在此处输入该密码。

- 标识：hscroot
- 密码：abc123

指导式安装向导将打开。

6. 在指导式安装条目窗口中单击**确定**。

注：如果启动HMC时未显示指导式安装向导，请在 HMC 欢迎页面的导航区域中单击**指导式安装向导**。

7. 通过使用您完成的安装前配置工作表来完成指导式安装向导中的步骤。单击是继续，并完成"连接和回拨服务器"向导中的步骤。
8. 在"摘要"窗口中，单击**完成**。
9. 如果未将以太网交叉电缆连接至受管系统，请立即连接。
10. 在 HMC 导航区域中，单击**服务管理**。
11. 在内容区域中，单击**向用户授权**。"向用户授权"窗口将打开。
12. 在字段中输入 IBM 标识并单击**确定**。

复查您的配置：

在"状态"窗口中，监视您选择的不同配置设置的进度。对于某些任务，此窗口可能在几分钟内显示为"暂挂"状态。单击**查看日志**，查看每个任务的相关状态消息。在任何时候单击**关闭**以关闭指导式安装向导。正在运行的任务将继续运行。现在您的 HMC 已完成配置。

使用 HMC 菜单配置 HMC

本节提供 HMC 配置任务的完整列表，这些任务将引导您完成配置 HMC 的过程。如果您不喜欢使用指导式安装向导，那么选择此选项。

必须重新启动 HMC 才能使配置设置生效，所以您可能要打印此核对表并在配置 HMC 时使用。

此信息包含本 PDF 中未包括的任务的参考资料。通过引用 HMC 欢迎页面上的**其他资源**部分，可以访问其他支持资料。

先决条件

使用 HMC 菜单开始配置 HMC 之前，应完成第 79 页的『准备 HMC 配置』中描述的配置准备活动。

表 27. 手动 HMC 配置任务以及在何处查找相关信息

任务	在何处查找相关信息
1. 启动 HMC。	第 89 页的『启动 HMC』
2. 设置日期和时间。	
3. 更改预定义密码。	
4. 创建其他用户并在完成此步骤时返回至此核对表。	
5. 配置网络连接。	第 90 页的『配置 HMC 网络类型』
6. 如果使用开放式网络和固定 IP 地址，请设置标识信息。	
7. 如果使用开放式网络和固定的 IP 地址，请将路由条目配置为缺省网关。	第 96 页的『将路由条目配置为缺省网关』
8. 如果使用开放式网络和固定 IP 地址，请配置域名服务。	第 96 页的『配置域名服务』
9. 如果使用固定 IP 地址并启用了 DNS，请配置域后缀。	第 96 页的『配置域后缀』
10. 配置服务器以连接至 IBM 服务和支持，并在完成此步骤时返回至此核对表。	第 98 页的『配置 HMC 以便它可与服务和支持联系』
11. 配置回拨事件管理器	第 102 页的『配置回拨事件管理器』
12. 将受管系统连接到电源。	
13. 设置受管系统的密码以及每个 ASMI 密码（通用密码和管理员密码）	第 103 页的『为受管系统设置密码』
14. 访问 ASMI 以在受管系统上设置日期和时间。	
15. 启动受管系统并在完成此步骤时返回至此核对表。	

表 27. 手动 HMC 配置任务以及在何处查找相关信息 (续)

任务	在何处查找相关信息
16. 确保受管系统上具有一个逻辑分区。	
17. 可选：添加另一受管系统并在完成此步骤时返回至此核对表。	
18. 可选：如果要使用 HMC 安装新服务器，请配置逻辑分区并安装操作系统。	
19. 如果此时未在安装新服务器，请执行可选配置后任务以进一步定制配置。	第 104 页的『配置后步骤』

启动 HMC:

您可以登录到 HMC 并选择希望在界面中显示的语言。第一次使用缺省用户标识 hscroot 和密码 abc123 登录 HMC。

要启动 HMC，请执行以下过程：

1. 按下电源按钮以开启 HMC。
2. 如果首选语言为英语，请继续执行步骤 4。

如果首选语言不是英语，那么当系统提示您更改语言环境时，请输入数字 **2**。

注：如果您不执行操作，那么此提示在 30 秒后消失。

3. 在“语言环境选择”窗口的列表中，选择要显示的语言环境，然后单击**确定**。语言环境标识 HMC 界面使用的语言。
4. 单击**登录并启动硬件管理控制台 Web 应用程序**。
5. 使用以下缺省用户标识和密码登录 HMC：

标识：hscroot

密码：abc123

注：在 HMC V8.1.0.1 上，您可以从以下登录选项中选择：

登录：最近一次登录、HMC Classic 或 HMC Enhanced

选择要在登录 HMC 时使用的软件界面。HMC Classic 界面可访问 HMC 的所有传统功能，而 HMC Enhanced 界面提供重新设计的以及新的虚拟化任务和功能。

最近一次登录

显示您从先前登录会话中选择的图形用户界面 (GUI)。

HMC Enhanced

向新手显示具有增强的 PowerVM 功能的增强 GUI。

HMC Classic

显示不具备增强的 PowerVM 功能的标准 GUI。

注：当 HMC 作为 DHCP 服务器工作时，HMC 将在其首次连接到服务处理器时使用缺省密码。

6. 按 Enter 键。

更改日期和时间：

以电池供电的时钟为 HMC 显示日期和时间。如果更换了电池或将系统移动到其他时区，那么您可能需要重新设置控制台日期和时间。了解如何更改 HMC 的日期和时间。

如果更改了日期和时间信息，那么此更改不会影响 HMC 管理的系统和逻辑分区。

要更改 HMC 的日期和时间，请执行以下操作：

1. 确保您是以下某个角色的成员：
 - 超级管理员
 - 服务代表
 - 操作员
 - 查看者
2. 在导航区域中，单击 **HMC 管理**。
3. 在"内容"窗格中，单击**更改日期和时间**。
4. 如果您在时钟字段中选择 **UTC**，那么时间设置将根据所选时区的夏令时自动进行调整。输入日期、时间和时区，然后单击**确定**。

配置 HMC 网络类型：

配置 HMC 以便它可与受管系统、逻辑分区、远程用户以及服务和支持通信。

配置 HMC 设置以使用开放式网络来连接至受管系统：

配置 HMC 以便它能够使用开放式网络来连接和管理受管系统。

要配置 HMC 网络设置以便它能够使用开放式网络来连接受管系统，请执行以下操作：

表 28. 配置 HMC 设置以使用开放式网络来连接至受管系统

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。 eth0 是首选值。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 通过执行下列任务来配置以太网适配器：	
a. 设置介质速度。	第 93 页的『设置介质速度』
b. 选择开放式网络类型。	第 93 页的『选择专用网络或开放式网络』
c. 设置静态地址。	第 94 页的『设置 IPv4 地址』
d. 设置防火墙。	第 95 页的『更改 HMC 防火墙设置』
e. 配置缺省网关。	第 96 页的『将路由条目配置为缺省网关』
f. 配置 DNS。	第 96 页的『配置域名服务』
4. 配置其他适配器（如果有的话）。	
5. 测试受管服务器与 HMC 之间的连接。	第 104 页的『测试 HMC 与受管系统之间的连接』

配置 HMC 设置以使用专用网络来连接至受管系统：

配置 HMC 以便它能够使用专用网络来连接和管理受管系统。

要配置 HMC 网络设置以便它能够使用专用网络来连接至受管系统，请执行以下操作：

表 29. 配置 HMC 设置以使用专用网络来连接至受管系统

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 将 HMC 配置为 DHCP 服务器。	第 93 页的『将 HMC 配置为 DHCP 服务器』
4. 测试受管服务器与 HMC 之间的连接。	第 104 页的『测试 HMC 与受管系统之间的连接』

配置 HMC 设置以使用开放式网络来连接至逻辑分区：

要配置 HMC 网络设置以便它能够使用开放式网络来连接至逻辑分区，请执行以下操作：

表 30. 配置 HMC 设置以使用开放式网络来连接至逻辑分区

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 通过执行下列任务来配置以太网适配器：	
a. 设置介质速度。	第 93 页的『设置介质速度』
b. 选择开放式网络类型。	第 93 页的『选择专用网络或开放式网络』
c. 设置静态地址。	第 94 页的『设置 IPv4 地址』
d. 设置防火墙。	第 95 页的『更改 HMC 防火墙设置』
e. 配置缺省网关。	第 96 页的『将路由条目配置为缺省网关』
f. 配置 DNS。	第 96 页的『配置域名服务』
4. 配置其他适配器（如果有的话）。	
5. 测试受管服务器与 HMC 之间的连接。	第 104 页的『测试 HMC 与受管系统之间的连接』

配置 HMC 设置以使用开放式网络来连接至远程用户：

要配置 HMC 网络设置以便它能够使用开放式网络来连接至远程用户，请执行以下操作：

表 31. 配置 HMC 设置以使用开放式网络来连接至远程用户

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 通过执行下列任务来配置以太网适配器：	
a. 设置介质速度。	第 93 页的『设置介质速度』
b. 选择开放式网络类型。	第 93 页的『选择专用网络或开放式网络』
c. 设置静态地址。	第 94 页的『设置 IPv4 地址』
d. 设置防火墙。	第 95 页的『更改 HMC 防火墙设置』
e. 配置缺省网关。	第 96 页的『将路由条目配置为缺省网关』
f. 配置 DNS。	第 96 页的『配置域名服务』
g. 配置后缀。	第 96 页的『配置域后缀』
4. 配置其他适配器（如果有的话）。	

配置 HMC 回拨服务器设置：

要配置 HMC 回拨服务器设置以便能够报告问题，请执行以下操作：

表 32. 配置 HMC 回拨服务器设置

任务	在何处查找相关信息
1. 确保您具有所有必需的客户信息	第 80 页的『HMC 的安装前配置工作表』
2. 配置此 HMC 以报告错误或选择现有回拨服务器来报告错误	第 98 页的『配置本地控制台以向服务和支持报告错误』 第 101 页的『对此 HMC 选择用于连接至服务和支持的现有回拨服务器』
3. 验证回拨配置是否在工作	第 101 页的『验证与服务和支持的连接是否在工作』
4. 授权用户查看收集的系統数据	第 101 页的『授权用户查看收集的系統数据』
5. 安排系統数据的传输	第 102 页的『传输服务信息』

标识已定义为 `eth0` 的以太网端口：

必须使用 HMC 上定义为 `eth0` 的以太网端口进行与受管服务器的以太网连接。

如果未在 HMC 上的 PCI 槽中安装任何其他以太网适配器，并且计划将 HMC 用作受管系统的 DHCP 服务器，那么主集成以太网端口在 HMC 上始终定义为 `eth0` 或 `eth1`。

如果在 PCI 槽中安装了其他以太网适配器，那么定义为 `eth0` 的端口取决于安装的以太网适配器的位置和类型。

注：这些是一般规则，可能并不适用于所有配置。

下表根据 HMC 类型描述以太网布置的规则。

表 33. HMC 类型和以太网布置的相关规则

HMC 类型	以太网布置规则
机架安装式 HMC，带有两个集成以太网端口	HMC 仅支持一个额外的以太网适配器。 <ul style="list-style-type: none"> 如果已安装一个额外的以太网适配器，那么该端口定义为 <code>eth0</code>。在这种情况下，主集成以太网端口定义为 <code>eth1</code>，辅助集成以太网端口定义为 <code>eth2</code>。 如果以太网适配器是双端口以太网适配器，那么标签为 Act/Link A 的端口通常为 <code>eth0</code>。标签为 Act/link B 的端口将为 <code>eth1</code>。在此情况下，主集成以太网端口定义为 <code>eth2</code>，而辅助集成以太网端口定义为 <code>eth3</code>。 如果未安装任何适配器，那么主集成以太网端口定义为 <code>eth0</code>。
独立模型，带有单个集成以太网端口	定义取决于已安装的以太网适配器的类型： <ul style="list-style-type: none"> 如果只安装了一个以太网适配器，那么该适配器被定义为 <code>eth0</code>。 如果以太网适配器是双端口以太网适配器，那么标签为 Act/link A 的端口通常为 <code>eth0</code>。标签为 Act/link B 的端口将为 <code>eth1</code>。在此情况下，主集成以太网端口被定义为 <code>eth2</code>。 如果未安装任何适配器，那么该集成以太网端口被定义为 <code>eth0</code>。 如果安装了多个以太网适配器，请参阅第 93 页的『确定以太网适配器的接口名称』。

确定以太网适配器的接口名称：

如果将 HMC 配置为 DHCP 服务器，那么该服务器只能在 HMC 标识为 eth0 和 eth1 的网络接口卡 (NIC) 连接上运行。您可能需要确定要将以太网电缆插入其中的 NIC 连接器。了解有关确定 HMC 标识为 eth0 和 eth1 的 NIC 连接器的更多信息。

要确定 HMC 指定给以太网适配器的名称，请执行下列操作：

1. 打开受限 shell 程序终端。选择 **HMC 管理** > **打开受限 shell 程序终端**。
2. 在命令行上输入以下命令：`tail -f /var/log/messages`。消息日志会在发生新事件时滚动。
3. 插入以太网电缆。如果已插入电缆，那么拔出电缆，等 5 秒钟，然后再次插入电缆。受限 shell 程序会在您插入电缆时滚动以显示消息。以下示例条目显示此以太网端口被标识为 eth0：Aug 28 12:41:20 termite kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100。
4. 对所有其他以太网端口重复此过程，并记录结果。
5. 输入 Ctrl+C 以停止 **tail** 命令。

设置介质速度：

了解如何指定包括速度的介质速度和以太网适配器的双工方式。

HMC 适配器是指的缺省值为**自动检测**。如果此适配器连接至 LAN 交换机，那么您必须匹配交换机端口设置。要设置介质速度和双工，请完成以下步骤：

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 在"局域网信息"部分，选择**自动检测**或适当的介质速度和双工组合。
6. 单击**确定**。

选择专用网络或开放式网络：

专用服务网络由 HMC 和受管系统组成。专用服务网络仅限于控制台及其管理的系统，且独立于公司网络之外。开放式网络由专用服务网络和公司网络组成。除控制台和受管系统之外，开放式网络可能包含网络端点，且可能包括多个子网和网络设备。

要选择专用网络或公用网络，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击 **LAN 适配器**选项卡。
6. 在局域网信息页中，选择**专用**或**开放式**。
7. 单击**确定**。

将 HMC 配置为 DHCP 服务器：

动态主机配置协议 (DHCP) 提供动态客户机的自动配置方法。

要将 HMC 配置 DHCP 服务器，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 在"工作"区域中，单击**更改网络设置**。"定制网络设置"窗口将打开。
3. 选择要使用的 LAN 适配器并单击**详细信息**。
4. 选择**专用**，然后选择网络类型。
5. 在"DHCP 服务器"部分中，选择**启用 DHCP 服务器**以将 HMC 作为 DHCP 服务器启用。

注：只能在专用网络上将 HMC 配置为 DHCP 服务器。如果您使用开放式网络，那么您将不会有选择**启用 DHCP**选项。

6. 输入 DHCP 服务器的地址范围。
7. 单击**确定**。

如果您已将 HMC 配置为专用网络上的 DHCP 服务器，那么必须验证是否已正确配置 HMC DHCP 专用网络。有关将 HMC 连接到专用网络的信息，请参阅第 93 页的『选择专用网络或开放式网络』。

有关更多信息，请参阅第 73 页的『将 HMC 用作 DHCP 服务器』。

设置 IPv4 地址：

了解如何在 HMC 上设置 IPv4 地址。

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击**基本设置**选项卡。
6. 选择 IPv4 地址。
7. 如果选择指定 IP 地址，请输入 TCP/IP 接口地址和 TCP/IP 接口网络掩码。
8. 单击**确定**。

设置 IPv6 地址：

了解如何在 HMC 上设置 IPv6 地址。

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击 **IPv6 设置**选项卡。
6. 选择 Autoconfig 选项或添加静态 IP 地址。
7. 如果添加了 IP 地址，请输入 IPv6 地址和前缀长度，然后单击**确定**。
8. 单击**确定**。

仅使用 IPv6 地址：

了解如何配置 HMC 以便它仅使用 IPv6 地址。

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**更改网络设置**。

3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 选择**无 IPv4 地址**。
6. 单击 **IPv6 设置**选项卡。
7. 选择使用 **DHCPv6** 来配置 IP 设置或添加静态 IP 地址。然后，单击**确定**。

单击"确定"后，必须重新引导 HMC 才能使这些更改生效。

更改 HMC 防火墙设置：

在开放式网络中，防火墙通常用于控制对公司网络的外部访问。HMC 在每个以太网适配器上都有防火墙。要以远程方式控制 HMC 或以远程方式访问其他 HMC，请修改连接至开放式网络的 HMC 上的以太网适配器防火墙设置。

要配置防火墙，请执行以下步骤：

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击**防火墙**选项卡。
6. 使用以下方法中的一种，您可以允许任何使用特定应用程序的 IP 地址通过防火墙，或指定一个或多个 IP 地址：
 - 允许使用特定应用程序的 IP 地址通过防火墙：
 - a. 在顶部框中，突出显示此应用程序。
 - b. 单击**允许进入**。此应用程序显示在底部框中表示已被选中。
 - 指定允许通过防火墙的 IP 地址：
 - a. 在顶部框中，选中某个应用程序。
 - b. 单击**允许 IP 地址进入**。
 - c. 在"允许的主机"窗口中，输入 IP 地址和网络掩码。
 - d. 单击**添加**，然后单击**确定**。
7. 单击**确定**。

启用远程受限 *shell* 程序访问：

可在配置防火墙时启用远程受限 *shell* 程序访问。

要启用远程受限 *shell* 程序访问，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**远程命令执行**。
3. 选择使用 **ssh** 设施启用远程命令执行，然后单击**确定**。

现在就启用了远程受限 *shell* 程序访问。

启用远程 *web* 访问：

可启用对 HMC 的远程 Web 访问。

要启用远程 Web 访问，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**远程操作**。
3. 选择**启用**，然后单击**确定**。

现在就启用了远程 Web 访问。

将路由条目配置为缺省网关：

了解如何将路由条目配置为缺省网关。此任务对使用开放式网络的用户可用。

要将路由条目配置为缺省网关，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 在"工作"区域中，单击**更改网络设置**。"定制网络设置"窗口将打开。
3. 单击**路由选项卡**。
4. 在"缺省网关信息"部分中，输入要设置为缺省网关的路由条目的网关地址和网关设备。
5. 单击**确定**。

配置域名服务：

如果计划设置开放式网络，请配置域名服务。

如果计划设置开放式网络，请配置域名服务。"域名系统"(DNS) 是用来管理主机名及其相关"因特网协议"(IP) 地址的分布式数据库系统。配置域名服务包括启用 DNS 和指定域后缀搜索顺序。

1. 在导航区域中，单击 **HMC 管理**。
2. 在"工作"区域中，单击**更改网络设置**。"更改网络设置"窗口将打开。
3. 单击**名称服务选项卡**。
4. 选择**启用 DNS**，以启用 DNS。
5. 指定 DNS 服务器和域后缀搜索顺序，然后单击**添加**。
6. 单击**确定**。

配置域后缀：

域后缀列表用于解析从列表中第一个条目开始的 IP 地址。

域后缀是追加到主机名的字符串，用于帮助解析其 IP 地址。例如，主机名 myname 可能无法解析。但是，如果字符串 myloc.mycompany.com 是域后缀表中的元素，那么还将尝试解析 myname.mloc.mycompany.com。

要配置域后缀项，请执行以下步骤：

1. 在导航区域中，单击 **HMC 管理**。
2. 在"工作"区域中，单击**更改网络设置**。"定制网络设置"窗口将打开。
3. 单击**名称服务选项卡**。
4. 输入用作域后缀项的字符串。
5. 单击**添加**以将其添加到列表中。

配置 HMC 以便它使用 LDAP 远程认证:

可配置 HMC 以便它使用 LDAP (轻量级目录访问协议) 远程认证。

用户登录 HMC 时, 会首先针对本地密码文件执行认证。如果找不到本地密码文件, 那么 HMC 会与远程 LDAP 服务器联系以进行认证。必须配置 HMC 以便它使用 LDAP 远程认证。

注: 配置 HMC 以便它使用 LDAP 认证之前, 必须确保 HMC 与 LDAP 服务器之间存在有效网络连接。有关配置 HMC 网络连接的更多信息, 请参阅第 90 页的『配置 HMC 网络类型』。

要配置 HMC 以便它使用 LDAP 认证, 请完成以下步骤:

1. 在导航区域中, 单击 **HMC 管理**。
2. 在内容区域中, 单击配置 **LDAP**。将打开 **LDAP 服务器定义**窗口。
3. 选择启用 **LDAP**。
4. 定义要用于认证的 LDAP 服务器 (例如 Microsoft Active Directory、Tivoli® 和 Open LDAP)。
5. 定义用来标识已认证的用户的 LDAP 属性。缺省值为 **uid**, 但您可使用您自己的属性。对于 Microsoft Active Directory, 请将 **sAMAccountName** 用作该属性。
6. 对 LDAP 服务器定义专有名称树 (又称为搜索条件)。
7. 单击**确定**。
8. 如果某用户要使用 LDAP 认证, 那么该用户必须配置其概要文件, 使得概要文件使用 LDAP 远程认证而不是本地认证。

配置 HMC 以便它使用密钥分发中心服务器进行 Kerberos 远程认证:

配置 HMC 以便它使用密钥分发中心 (KDC) 服务器进行 Kerberos 远程认证。

用户登录 HMC 时, 会首先针对本地密码文件执行认证。如果找不到本地密码文件, 那么 HMC 会与远程 Kerberos 服务器联系以进行认证。必须配置 HMC 以便它使用 Kerberos 远程认证。

注: 配置 HMC 以便它使用 KDC 服务器进行 Kerberos 远程认证之前, 必须确保 HMC 与 KDC 服务器之间存在有效网络连接。有关配置 HMC 网络连接的更多信息, 请参阅第 90 页的『配置 HMC 网络类型』。

要配置 HMC 以便它使用 KDC 服务器进行 Kerberos 远程认证, 请执行以下操作:

1. 在 HMC 上启用网络时间协议 (NTP) 服务, 并设置 HMC 和 KDC 服务器以使时间与同一 NTP 服务器同步。要在 HMC 上启用 NTP 服务, 请执行以下操作:
 - a. 在导航区域中, 选择 **HMC 管理**。
 - b. 在内容区域中, 选择**更改日期和时间**。
 - c. 选择 **NTP 配置**选项卡。
 - d. 选择在此 **HMC** 上启用 **NTP 服务**。
 - e. 单击**确定**。
2. 配置每个远程 HMC 用户的概要文件以便 HMC 使用 Kerberos 远程认证而不是本地认证。
3. 可选: 可将服务密钥文件导入到此 HMC 中。服务密钥文件包含向 KDC 服务器标识 HMC 的主机主体。服务密钥文件又称为 *keytab*。要将服务密钥文件导入到此 HMC 中, 请执行以下操作:
 - a. 在导航区域中, 选择 **HMC 管理**。
 - b. 在内容区域中, 选择配置 **KDC**。"密钥分发中心配置"窗口将打开。
 - c. 选择操作 > **导入服务密钥**。"导入服务密钥"窗口将打开。

- d. 输入服务密钥文件的位置。
 - e. 单击**确定**。
4. 向此 HMC 添加新的 KDC 服务器。要向此 HMC 添加新的 KDC 服务器，请执行以下操作：
 - a. 在导航区域中，选择 **HMC 管理**。
 - b. 在内容区域中，选择**配置 KDC**。"密钥分发中心配置"窗口将打开。
 - c. 选择**操作 > 添加 KDC 服务器**。"导入服务密钥"窗口将打开。
 - d. 输入域和 KDC 服务器的主机名或 IP 地址。
 - e. 单击**确定**。

配置 HMC 以便它可与服务和支持联系：

配置 HMC 以便它可在发生时通知您。

使用回拨设置向导来配置 HMC 以便它可连接至服务和支持：

使用回拨向导来配置 HMC 以便它成为回拨服务器。

此过程描述如何将 HMC 配置为使用直接基于 (LAN) 和间接 (SSL) 连接来连接至因特网的回拨服务器。

在开始此任务之前，请确保符合下列条件：

- 网络管理员已验证允许连接。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 如果您通过代理服务器配置因特网支持，那么还必须了解以下信息：
 - 代理服务器的 IP 地址和端口
 - 代理认证信息
- 使用了指定为 **eth1** (被指定为开放式网络) 的适配器。有关更多信息，请参阅第 71 页的『在 HMC 上选择网络设置』。
- 以太网电缆已在物理上将 HMC 连接至 LAN。

要使用回拨向导来配置 HMC 以便它成为回拨服务器，请执行以下操作：

1. 在导航区域中，选择**服务管理**。
2. 在内容区域中，选择**回拨设置向导**。"连接和回拨服务器"向导将打开。遵循向导中的指示信息来配置回拨。

配置本地控制台以向服务和支持报告错误：

配置此 HMC，以便它可以使用 LAN 连接来回拨错误。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

将 HMC 配置为使用基于 LAN 的因特网和 SSL 与服务和支持联系：

描述如何将 HMC 配置为使用直接基于 (LAN) 和间接 (SSL) 连接来连接至因特网的回拨服务器。

在开始此任务之前，请确保符合下列条件：

- 网络管理员已验证允许连接。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 已配置客户联系人信息。通过进至 HMC 界面并单击**服务管理 > 管理客户信息**来验证此项。
- 如果您通过代理服务器配置因特网支持，那么还必须了解以下信息：
 - 代理服务器的 IP 地址和端口

- 代理认证信息
- 您至少需要配置一个开放式网络接口。有关更多信息，请参阅第 72 页的『HMC 环境中的专用网络和开放式网络』。
- 以太网电缆已在物理上将 HMC 连接至 LAN。

要将 HMC 配置为使用直接基于 (LAN) 和间接 (SSL) 连接来连接至因特网的回拨服务器，请执行以下操作：

1. 在导航区域中，单击**服务管理**。
2. 在"连接"部分中，单击**管理出站连接**。"回拨服务器控制台"窗口将打开。
3. 单击**配置**。
4. 在"出站连接设置"窗口中，选择将本地系统启用为回拨服务器。
5. 接受协议。
6. 在"出站连接设置"窗口中，选择因特网页面。
7. 选择允许使用现有因特网连接来获取服务框。
8. 如果要使用 SSL 代理，请选择使用 **SSL 代理框**。
9. 如果要使用 SSL 代理，请填写代理的地址和端口。从网络管理员处获取此信息。
10. 如果选择了使用 **SSL 代理**并且该代理需要用户标识和密码认证，请选择向 **SSL 代理认证框**。输入用户标识和密码。从网络管理员处获取用户标识和密码。
11. 选择连接因特网时要使用的协议。
12. 在因特网页面上，单击**测试**。
13. 在"测试因特网"窗口中，单击**开始**。
14. 验证测试是否成功完成。
15. 在"测试因特网"窗口中，单击**取消**。
16. 在"出站连接设置"窗口中，选择**确定**。

使用电话和调制解调器连接至服务和支持：

描述如何将 HMC 配置为使用调制解调器访问 IBM 支持的回拨服务器。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

在开始此任务之前，请确保符合下列条件：

- 已有可用的专用模拟电话线路。
- 已有配置调制解调器所需的信息。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 已配置客户联系人信息。您可通过进至 HMC 界面并单击**服务管理 > 管理客户信息**来验证此项。
- 确保下列信息可用：
 - 模拟线路的类型，即音调或脉冲。大多数线路为音调，但某些仍在使用的线路是较旧循环或脉冲类型。
 - 拿起电话时线路是否发出拨号音。大多数线路会发出拨号音，但某些仍在使用的线路则不会。
 - 是否需要拨号前缀字符串。拨号前缀字符串是访问外线时所需加拨的若干数字。

要将 HMC 配置为使用调制解调器访问 IBM 支持的回拨服务器，请执行以下操作：

1. 在导航区域中，单击**服务管理**。
2. 在"连接"部分中，单击**管理出站连接**。
3. 单击**配置**
4. 在"出站连接设置"窗口中，选择将本地系统启用为回拨服务器。

5. 接受协议。
6. 在"出站连接设置"窗口中，单击本地调制解调器选项卡。
7. 在"本地调制解调器"页面上，选中允许使用本地调制解调器拨号以获取服务复选框。
8. 在"本地调制解调器"页面上，选中调制解调器配置复选框。
9. 在"定制调制解调器设置"窗口中，单击拨号类型（音调或脉冲）。如果接收方挂断时线路发出拨号音，那么请选中等待拨号音复选框。填写拨打外线时所需的任何拨号前缀字符串。
10. 单击**确定**。
11. 在"本地调制解调器"页面上，单击**添加**。
12. 从列表中选择号码。
13. 如果这是本地号码，那么从电话号码字段中除去区号。
14. 在"添加电话号码"面板中，单击**添加**。
15. 在"定制调制解调器设置"面板中，单击**测试**。
16. 在"测试电话号码"面板中，单击**开始**。
17. 验证测试是否成功完成。
18. 在"测试电话号码"窗口中，单击**取消**。
19. 最多可配置 5 个电话号码。至少配置 2 个电话号码（主电话号码和备用电话号码）。将按电话号码的配置顺序来尝试这些电话号码。要将其他号码添加至可拨列表，请重复此过程中的步骤。
20. 在"出站连接设置"窗口中，选择**确定**。

使用基于 LAN 的 VPN 连接至服务和支持：

配置使用 VPN 的回拨服务器。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

在开始此任务之前，请确保符合下列条件：

- 网络管理员已验证允许连接。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 使用了指定为 **eth1**（被指定为开放式网络）的适配器。有关更多信息，请参阅第 71 页的『在 HMC 上选择网络设置』。
- 以太网电缆已在物理上将 HMC 连接至 LAN。
- 已配置客户联系人信息。通过在 HMC 界面上单击**服务管理 > 管理客户信息**来验证此情况。

要配置使用 VPN 的回拨服务器，请执行以下操作：

1. 在导航区域中，单击**服务管理**。
2. 在"连接"部分中，单击**管理出站连接**。
3. 单击**配置**
4. 在"出站连接设置"窗口中，选择将本地系统启用为回拨服务器。
5. 接受协议。
6. 在"出站连接设置"窗口中，选择因特网 **VPN** 选项卡。
7. 在"因特网 VPN"页面上，选择**允许使用 VPN 和现有因特网连接来获取服务**。
8. 在"因特网 VPN"页面上，单击**测试复选框**。
9. 在"测试因特网 VPN"窗口中，单击**开始**。
10. 验证测试是否成功完成。

11. 在"测试因特网 VPN"窗口中, 单击**取消**。
12. 在"出站连接设置"窗口中, 选择**确定**。

对此 HMC 选择用于连接至服务和支持的现有回拨服务器:

选择此 HMC 已识别或发现的现有 HMC 回拨服务器来报告错误。

已发现的 HMC 是启用为回拨服务器的 HMC 以及与此 HMC 位于同一子网或管理同一受管系统的 HMC。

要选择已发现的 HMC 以在此 HMC 报告错误时进行回拨, 请执行以下操作:

1. 在导航区域中, 单击**服务管理**。
2. 在内容区域中, 单击**管理出站连接**。"回拨服务器控制台"窗口将打开。
3. 单击**使用发现的回拨服务器控制台**。该 HMC 将显示配置为回拨的 HMC 的 IP 地址或主机名。
4. 单击**确定**。

还可手动添加不同子网上的现有 HMC 回拨服务器。选择配置为回拨的 HMC 的 IP 地址或主机名, 单击**添加**。然后, 单击**确定**。

验证与服务和支持的连接是否在工作:

测试问题报告以确保与服务和支持的连接是否在工作。

要验证回拨配置是否在工作, 请执行以下操作:

1. 在导航区域中, 单击**服务管理**。
2. 在"工作"区域中, 单击**创建事件**。
3. 选择**测试自动问题报告**并输入注释。
4. 单击**请求服务**。等几分钟以便发送请求。
5. 在"服务管理"窗口中, 选择**管理事件**。
6. 选择**所有未解决问题**。
7. 验证是否存在指定给未解决问题编号的 PMH 事件和编号。
8. 选择该事件并选择**关闭**。
9. 在"关闭"窗口中, 输入您的姓名和简短注释。

授权用户查看收集的系统数据:

必须对用户授权, 用户才能查看您系统的相关数据。

在您授权用户查看收集的系统数据之前, 您必须获取 IBM 标识。有关获取 IBM 标识的更多信息, 请参阅第 80 页的『HMC 的安装前配置工作表』。

要授权用户查看收集的系统数据, 请执行以下操作:

1. 在导航区域中, 选择**服务管理**。
2. 在内容区域中, 选择**向用户授权**。
3. 输入 IBM 标识。
4. 单击**确定**。

传输服务信息：

请传输服务信息，以便可以将其用于问题确定。

IBM 提供个性化 Web 功能，这些功能使用 IBM Electronic Service Agent 收集的信息。要使用这些功能，必须先在 IBM 注册 Web 站点（网址为 <http://www.ibm.com/account/profile>）上进行注册。要授权用户使用 Electronic Service Agent 信息来个性化 Web 功能，请参阅第 101 页的『授权用户查看收集的系統数据』。有关向系统注册 IBM 标识的优点的更多信息，请参阅 <http://www.ibm.com/support/electronic>。

注：应在安装并配置 HMC 以供使用后立即传送服务供应商信息。

要传输服务信息，请完成下列步骤：

1. 在导航区域中，单击**服务管理**。
2. 在内容区域中，单击**传送服务信息**。
3. 单击下列其中一个选项卡：
 - **传输**。使用此页面来安排何时将服务数据传输到服务提供者（按天和一天中的时间来指定频率），以及您想要如何传输服务信息和性能管理信息。
 - **FTP**。使用此页面来配置 FTP 服务器的文件传输协议 (FTP) 信息，使用防火墙或者不使用防火墙，以卸载服务信息。此服务信息是扩展错误数据，由有关在 HMC 或受管系统的硬件管理控制台 (HMC) 上产生的问题的数据组成。
 - **将服务数据传输到 IBM**。使用此页面可以发送存储在 HMC 上的信息，此信息可用于问题确定。数据可能是跟踪、日志或转储，数据的目标可能是 IBM 服务支持系统、软盘、USB 闪存驱动器或者 DVD-RAM。在您可以将信息发送至 IBM 服务支持系统之前，必须启用 Phone Server 和远程服务。
4. 完成“传输服务信息”窗口中的任务，然后单击**确定**。

配置回拨事件管理器：

了解如何配置“回拨事件管理器”任务。您可以通过此任务监视和核准从 HMC 传输到 IBM 的任何数据。

已通过使用 HMC 命令行界面设置“回拨事件管理器”方式（启用或禁用）。启用“回拨事件管理器”任务将阻止 HMC 在事件发生时自动对其进行回拨。要阻止事件在未进行核准的情况下回拨，所有在此环境中运行的 HMC 都必须已启用“回拨事件管理器”。

要启用或禁用“回拨事件管理器”任务，请运行以下命令：

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

注：启用“回拨事件管理器”任务将阻止回拨事件，直到它们获得回拨任务批准为止。如果您禁用“回拨事件管理器”任务，那么系统不会自动启用回拨功能。此设置会阻止数据的任何非计划回拨到 IBM。从下列命令选项中选择以设置必需的配置：

- 要启用“回拨事件管理器”任务：**chhmc -c emch -s enable**
- 要禁用“回拨事件管理器”任务并重新启用自动回拨：**chhmc -c emch -s disable --callhome enable**
- 要禁用“回拨事件管理器”任务且不重新启用自动回拨：**chhmc -c emch -s disable --callhome disable**

确保 HMC 可与部署在此环境中的其他 HMC 进行通信。回拨事件管理器在注册 HMC 时具有测试连接功能。

您可以使用回拨事件管理器来注册 HMC。注册 HMC 之后，事件管理器将查询已注册的 HMC 以获取等待回拨到 IBM 的任何事件。事件管理器显示正发送回 IBM 的数据并对这些事件进行核准。核准后，事件管理器会向已注册的 HMC 发出通知，其可继续执行回拨操作。

"回拨事件管理器"任务可从任一 HMC 运行，也可从多个 HMC 运行。要使用"回拨事件管理器"任务注册管理控制台，请完成以下步骤：

1. 在导航区域中，选择**服务管理**。
2. 在内容区域中，选择**回拨事件管理器**。
3. 从**回拨事件管理器**窗口中，单击**管理控制台**。
4. 从**管理已注册的控制台**窗口，单击**添加控制台**以输入信息，以使用"回拨事件管理器"任务注册管理控制台。
5. 单击**确定**以落实对已注册的管理控制台列表进行的更改。

注：回拨事件管理器可与禁用的事件管理器方式配合使用。您仍可以在事件管理器中注册 HMC 并查看事件，但事件管理器不会在回拨事件时进行控制。

为受管系统设置密码：

必须同时为服务器和高级系统管理 (ADM) 设置密码。了解有关如何使用 HMC 界面设置这些密码的更多信息。

如果接收到认证暂挂消息，那么 HMC 会提示您为受管系统设置密码。

如果未接收到"认证暂挂"消息，那么完成以下步骤来为受管系统设置密码。

更新服务器密码：

要更新服务器密码，请执行以下操作：

1. 在导航区域中，选择**受管系统**。
2. 在"任务"区域中，单击**操作**。
3. 单击**更改密码**。"更新密码"窗口将打开。
4. 输入所需信息并单击**确定**。

更新高级系统管理 (ASM) 通用密码：

注：通用用户标识的缺省密码为 `general`，管理员标识的缺省密码为 `admin`。

要更新 ASM 通用密码，请执行以下操作：

1. 在 HMC 的导航区域中，选择**受管系统**。
2. 在"任务"区域中，单击**操作**。
3. 单击**高级系统管理 (ASM)**。"启动 ASM 界面"窗口将打开。
4. 选择"服务处理器 IP 地址"并单击**确定**。ASM 界面将打开。
5. 在"欢迎使用 ASMI"窗格中，请指定您的用户标识和密码，然后单击**登录**。
6. 在导航区域中，展开**登录概要文件**。
7. 选择**更改密码**。
8. 指定所需的信息并单击**继续**。

复位高级系统管理 (ASM) 管理员密码：

要重新设置管理员密码，请与授权服务供应商联系。

测试 HMC 与受管系统之间的连接：

此选项使您能够验证是否已正确连接至网络。

要测试网络连接，您必须为以下某个角色的成员：

- 超级管理员
- 服务代表

要测试 HMC 与受管系统之间的连接，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 单击**测试网络连接**。
3. 在 Ping 选项卡中，输入您想要连接的任何系统的主机名或 IP 地址。要测试开放式网络，请输入网关。单击 **Ping**。

如果尚未创建任何逻辑分区，那么您将无法对地址执行 ping 操作。可使用 HMC 在服务器上创建逻辑分区。有关更多信息，请参阅逻辑分区。

要了解如何在网络中使用 HMC，请参阅 第 71 页的『HMC 网络连接』。

有关配置 HMC 以连接至网络的更多信息，请参阅第 88 页的『使用 HMC 菜单配置 HMC』。

配置后步骤

安装并配置 HMC 后，根据需要备份 HMC 数据。

备份重要的 HMC 数据

可将重要控制台信息备份至 USB 闪存设备或 DVD，也可通过 FTP 或网络进行备份。

您可以使用 HMC 来备份所有重要数据，如以下数据：

- 用户首选项文件
- 用户信息
- HMC 平台配置文件
- HMC 日志文件
- 通过安装纠正服务的 HMC 更新

备份功能会将存储在 HMC 硬盘上的 HMC 数据保存至以下设备：

- DVD 介质
- USB 闪存设备
- 安装至 HMC 文件系统（如 NFS）的远程系统
- 远程站点（通过 FTP）

请在对 HMC 或与逻辑分区相关联的信息进行更改之后备份 HMC。

注：必须将介质格式化，然后才能将数据保存到可移动介质。要格式化介质，请单击 **HMC 管理 > 格式化介质**并遵循步骤。

要备份 HMC，您必须为以下某个角色的成员：

- 超级管理员
- 操作员
- 服务代表

要备份 HMC 的重要数据，请执行以下操作：

1. 在导航区域中，单击 **HMC 管理**。
2. 选择**备份 HMC 数据**。
3. 选择归档选项。您可以备份到本地系统上的介质和已安装的远程系统或将备份数据发送到远程站点。
4. 遵循窗口上的指示信息来备份数据。

将整个 HMC 硬盘驱动器备份到远程系统

可以使用 HMC 来将 HMC 的整个硬盘驱动器备份到远程系统。

远程系统必须已配置网络文件系统 (NFS) 或安全 Shell (ssh)，并且此网络必须可从 HMC 访问。要完成此任务，您必须关闭 HMC 并对它进行重新引导。仅使用 HMC 来执行这些任务。

要将 HMC 硬盘驱动器备份到远程系统，您必须为以下某个角色的成员：

- 超级管理员
- 操作员
- 服务代表

要将 HMC 硬盘驱动器备份到远程系统，请执行以下操作：

1. 记录 HMC 上每个网络适配器的接口号 (eth0、eth1 等)、MAC 地址和 IP 地址。为此，单击 **HMC 管理 > 更改网络设置 > LAN 适配器**。
2. 关闭 HMC 并关闭它的电源。
3. 打开 HMC 控制台的电源，并将 HMC 恢复介质插入 DVD 驱动器中。如果您要从已配置的网络引导服务器启动 HMC 界面，那么确保网络接口是启动顺序中的一个设备。要查看启动设备列表，当 HMC 打开电源时按 F12，并选择您要从中引导的网络接口。
4. 选择备份选项并单击下一步。
5. 选择要用于与远程服务器通信的网络接口。如果您要通过连接网络引导服务器来启动 HMC，并且此服务器也是您要将数据备份至的远程服务器，那么选择缺省设置。然后单击下一步并进入步骤 7。如果未选择缺省设置，那么继续执行下一步。

注：接口编号 (eth0 和 eth1) 可能与步骤 1 中记录的编号不匹配。列示的 MAC 地址可用于标识期望的接口。有关更多信息，请参阅第 92 页的『标识已定义为 eth0 的以太网端口』。

6. 如果不选择缺省设置，那么必须选择要与所选接口配合使用的网络协议。可以选择从网络中的 DHCP 服务器获取 IP 地址或将静态 IP 地址分配给所选网络接口。作出选择并单击下一步。
7. 如果您未选择缺省设置，那么输入远程服务器的 IP 地址或主机名。将使用 gzip 压缩实用程序和 tar 命令创建备份文件。在远程主机上的文件字段中指定扩展名为 .tgz 的文件。如果已选择缺省网络设置，那么必须使用网络引导配置中的目录设置。此信息显示在远程主机上的文件字段中。在完成所有必需的信息之后，单击下一步。
8. 选择您要用于将数据从 HMC 传送到远程服务器的方法。如果选择加密数据，那么远程主机必须让安全 Shell (SSH) 服务器处于运行状态。如果选择传送数据而不进行加密，那么远程主机必须运行网络文件服务器 (NFS)，且必须导出您要将数据备份至的目录以获取写访问权。作出选择并单击下一步。
9. 如果您选择使用加密方式来传送数据，那么必须输入远程服务器的用户标识和密码。

10. 验证您所输入的信息正确并单击**完成**。如果备份完成，那么会显示 HMC 界面。

如果在打开 HMC 的电源时通过按 F1 修改了启动顺序，那么必须重新引导 HMC 并再次更改设置。更改启动顺序时，确保在启动顺序中硬盘列示在网络接口前面。

更新，升级和迁移 HMC 机器代码

HMC 的更新和升级会定期发布，以添加新功能和改进现有功能。了解有关更新、升级和迁移 HMC 机器代码之间的差别的更多信息。同时了解如何执行 HMC 机器代码更新、升级或迁移。

完成每个任务时，HMC 会重新引导但分区不会。

更新 HMC 代码

对现有 HMC 级别应用维护

不要求您执行**保存升级数据**任务

升级 HMC 代码

将 HMC 软件替换为同一程序的新发行版或修订级别

要求您从恢复介质进行引导

迁移 HMC 代码

将 HMC 数据从一个 HMC 版本移至另一个 HMC 版本

迁移是一种升级。

确定 HMC 机器代码版本和发行版

了解如何查看 HMC 机器代码版本和发行版

HMC 上的机器代码级别将确定可用功能部件，包括要升级至新发行版的并发服务器固件维护和增强功能。

要查看 HMC 机器代码版本和发行版，请执行以下操作：

1. 在导航区域中，单击**更新**。
2. 在"工作"区域中，查看并记录出现在"HMC 代码级别"标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。

对连接至因特网的 HMC 获取并应用机器代码更新

了解如何对连接至因特网的 HMC 获取机器代码更新。

要获取 HMC 的机器代码更新，请执行步骤 1 到 5。

步骤 1. 确保已连接至因特网：

要将更新从服务和支持系统或 Web 站点下载至 HMC 或服务器，必须具有下列其中一项：

- 带有或不带 SSL 代理的 SSL 连接
- 因特网 VPN

为确保已连接至因特网，请执行以下操作：

1. 在导航区域中，单击**服务管理**。
2. 选择**管理出站连接**。
3. 选择对应为 HMC 选择的出站连接类型（因特网 VPN 或 SSL 连接）的选项卡。

注：如果与服务和支持的连接不存在，请先设置服务连接，然后继续此过程。有关如何设置与服务和支持的连接的指示信息，请参阅“设置服务器以连接至 IBM 服务和支持”。

4. 单击测试。
5. 验证测试是否成功完成。如果测试未成功，请诊断连接并更正问题，然后继续此过程。或者，可获取 DVD 上的更新。
6. 继续执行『步骤 2. 查看现有 HMC 机器代码级别』。

步骤 2. 查看现有 HMC 机器代码级别：

要查看现有 HMC 机器代码级别，请执行以下操作：

1. 在导航区域中，单击更新。
2. 在“工作”区域中，查看并记录出现在“HMC 代码级别”标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
3. 继续执行『步骤 3. 查看可用的 HMC 机器代码级别』。

步骤 3. 查看可用的 HMC 机器代码级别：

要查看可用 HMC 机器代码级别，请执行以下操作：

1. 在连接至因特网的计算机或服务器上，访问 <http://www.ibm.com/eserver/support/fixes>。
2. 从产品系列列表中选择适当的系列。
3. 在产品或修订类型列表中选择硬件管理控制台。
4. 单击继续。将显示硬件管理控制台站点。
5. 下滚至 HMC 版本级别以查看可用 HMC 级别。

注：如果愿意，可与服务和支持联系。

6. 继续执行『步骤 4. 应用 HMC 机器代码更新』。

步骤 4. 应用 HMC 机器代码更新：

要应用 HMC 机器代码更新，请执行以下操作：

1. 在安装 HMC 机器代码的更新之前，请备份 HMC 上的关键控制台信息。有关指示信息，请参阅第 104 页的『备份重要的 HMC 数据』。然后继续执行下一步。
2. 在导航区域中，单击更新。
3. 单击更新 HMC。“安装纠正服务向导”将打开。
4. 遵循向导中的指示信息来安装更新。
5. 关闭 HMC，然后重新启动 HMC 以使更新生效。
6. 单击登录并启动硬件管理控制台 Web 应用程序。
7. 登录 HMC 界面。

步骤 5. 验证 HMC 机器代码更新是否安装成功：

要验证 HMC 机器代码更新是否安装成功，请执行以下操作：

1. 在导航区域中，单击更新。
2. 在“工作”区域中，HMC 版本、发行版、维护级别、构建级别和基本版本会显示在“HMC 代码级别”标题下。
3. 验证版本和发行版是否与安装的更新相匹配。
4. 如果显示的代码级别与安装的级别不同，请执行以下步骤：
 - a. 选择 HMC 上的网络连接。
 - b. 使用另一存储库重试固件更新。

- c. 如果问题仍然存在，请与您的上一级支持机构联系。

使用 DVD 或 FTP 服务器获取并应用 HMC 的机器代码更新

了解如何使用 DVD 或 FTP 服务器获取 HMC 的机器代码更新。

要获取 HMC 机器代码更新，请执行步骤 1 到 5。

步骤 1. 查看现有 HMC 机器代码级别：

要查看现有 HMC 机器代码级别，请执行以下操作：

1. 在导航区域中，单击**更新**。
2. 在"工作"区域中，查看并记录出现在"HMC 代码级别"标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
3. 继续执行『步骤 2. 查看可用的 HMC 机器代码级别』。

步骤 2. 查看可用的 HMC 机器代码级别：

要查看可用 HMC 机器代码级别，请执行以下操作：

1. 在连接至因特网的计算机或服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 下滚至 HMC 版本级别以查看可用 HMC 级别。

注：如果愿意，可与 IBM 服务和支持联系。

3. 继续执行『步骤 3. 获取 HMC 机器代码更新』。

步骤 3. 获取 HMC 机器代码更新：

要获取 HMC 机器代码更新，请执行以下操作：

可通过 Fix Central 的 Web 站点订购 HMC 机器代码更新、与服务和支持联系或将 HMC 机器代码升级下载至 FTP 服务器。

通过 Fix Central 的 Web 站点订购 HMC 机器代码更新

1. 在连接至因特网的计算机或服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 在"受支持的 HMC 产品"中，选择最新 HMC 级别。
3. 下滚至"文件名/包"区域并查找要订购的更新。
4. 在"订购"列中，选择**执行**。
5. 单击**继续**以使用您的 IBM 标识登录。
6. 遵循屏幕上的提示来提交订单。

将 HMC 机器代码更新下载至可移动介质

1. 在连接至因特网的计算机或服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 在"受支持的 HMC 产品"中，选择最新 HMC 级别。
3. 下滚至"文件名/包"区域并查找要下载的更新。
4. 单击要下载的更新。
5. 接受许可协议，并将更新保存至可移动介质。

完成时继续执行第 109 页的『步骤 4. 应用 HMC 机器代码更新』。

步骤 4. 应用 HMC 机器代码更新:

要应用 HMC 机器代码更新, 请执行以下操作:

1. 在安装 HMC 机器代码的更新之前, 请备份 HMC 数据。有关更多信息, 请参阅第 104 页的『备份重要的 HMC 数据』。
2. 如果在 DVD-RAM 上获取或创建了更新, 请将该 DVD-RAM 插入到 HMC 上的 DVD 驱动器中。如果在 USB 存储设备上获取或创建了更新, 请插入该存储设备。
3. 在导航区域中, 单击**更新**。
4. 单击**更新 HMC**。"安装 HMC 纠正服务向导"将打开。
5. 遵循向导中的指示信息来安装更新。
6. 关闭 HMC, 然后重新启动并登录回 HMC 以使更新生效。
7. 继续执行『步骤 5. 验证 HMC 机器代码更新是否安装成功』。

步骤 5. 验证 HMC 机器代码更新是否安装成功:

要验证 HMC 机器代码更新是否安装成功, 请执行以下操作:

1. 在导航区域中, 单击**更新**。在"工作"区域中, HMC 版本、发行版、维护级别、构建级别和基本版本会显示在"HMC 代码级别"标题下。
2. 验证版本和发行版是否与安装的更新相匹配。
3. 如果显示的代码级别与安装的级别不同, 请执行以下步骤:
 - a. 重试机器代码更新。如果为此过程创建了 DVD, 请使用新介质。
 - b. 如果问题仍然存在, 请与您的上一级支持机构联系。

升级 HMC 软件

了解如何在保留 HMC 配置数据的同时将 HMC 上的软件从一个发行版升级至下一个发行版。

要升级 HMC 上的机器代码, 请执行步骤 1 到 9。

步骤 1. 获取升级:

您可以通过 Fix Central 的 Web 站点订购 HMC 机器代码升级。

要通过 Fix Central 的 Web 站点获取升级, 请执行以下操作:

1. 在连接至因特网的计算机或服务器上, 访问硬件管理控制台 Web 站点 (网址为 <http://www-933.ibm.com/support/fixcentral/>)。
2. 单击**继续**。将显示硬件管理控制台站点。
3. 浏览至要升级至的 HMC 版本。
4. 找到下载和订购部分。

注: 如果您无权访问因特网, 请与 IBM 服务和支持联系以订购 DVD 上的升级。

5. 遵循屏幕上的提示来提交订单。
6. 升级后继续执行『步骤 2. 查看现有 HMC 机器代码级别』。

步骤 2. 查看现有 HMC 机器代码级别:

要确定 HMC 上的机器代码的现有级别, 请执行以下步骤:

1. 在导航区域中, 单击**更新**。
2. 在"工作"区域中, 查看并记录出现在"HMC 代码级别"标题下的信息, 包括 HMC 版本、发行版、维护级别、构建级别和基本版本。

3. 继续执行『步骤 3. 备份受管系统的概要文件数据』。

步骤 3. 备份受管系统的概要文件数据：

要备份受管系统的概要文件数据，请执行以下操作：

1. 在导航区域中，选择**系统管理**。
2. 选择**服务器**。
3. 选择服务器并确保状态为正在运行或备用。
4. 在"任务"中选择**配置 > 管理分区数据 > 备份**。
5. 输入备份文件名称并记录此信息。
6. 单击**确定**。
7. 对每个受管系统重复这些步骤。
8. 继续执行『步骤 4. 备份 HMC 数据』。

步骤 4. 备份 HMC 数据：

在安装新版本的 HMC 软件之前备份 HMC 数据，以便可在升级软件期间发生问题时恢复先前级别。成功升级至新版本的 HMC 软件后，不要使用此关键控制台数据。

注：要备份至可移动介质，需要让该介质可用。

要备份 HMC 数据，请执行以下操作：

1. 如果计划备份至介质，请执行以下步骤来格式化介质：
 - a. 将介质插入到驱动器中。
 - b. 在导航区域中，选择**服务管理**
 - c. 选择**格式化介质**。
 - d. 选择介质类型。
 - e. 选择格式类型。
 - f. 单击**确定**。
2. 在导航区域中，选择**HMC 管理**。
3. 选择**备份 HMC 数据**。 "备份 HMC 数据"窗口将打开。
4. 选择归档选项。 可备份至本地系统上的介质和已安装到 HMC 文件系统（例如，NFS）的远程系统，或使用文件传输协议 (FTP) 将备份发送至远程站点。
 - 要备份至本地系统，请选择**备份至本地系统上的介质**并遵循指示信息。
 - 要备份至已安装的远程系统，请选择**备份至已安装的远程系统**并遵循指示信息。
 - 要备份至远程 FTP 站点，请选择**将备份关键数据发送至远程站点**并遵循指示信息。
5. 继续执行『步骤 5. 记录当前 HMC 配置信息』。

步骤 5. 记录当前 HMC 配置信息：

在升级至新版本的 HMC 软件之前，应记录 HMC 配置信息以预防出现问题。

要记录当前 HMC 配置，请执行以下操作：

1. 要查看针对受管系统或其逻辑分区安排的操作，请打开**系统管理**。如果要记录对 HMC 本身安排的操作，请选择**HMC 管理**并跳至步骤 3。
2. 选择要对其记录 HMC 配置信息的受管系统和所有分区。
3. 在任务列表中，选择**安排操作**。 将显示对所选目标安排的所有操作。

4. 选择**排序 > 按对象**。
5. 选择每个对象并记录以下详细信息：
 - 对象名
 - 安排日期
 - 操作时间（以 24 小时制显示）
 - 重复（如果为"是"，请执行以下步骤）：
 - a. 选择**查看 > 安排详细信息**。
 - b. 记录时间间隔信息。
 - c. 关闭安排的操作窗口。
 - d. 对每个安排操作重复此过程。
6. 关闭"定制安排的操作"窗口。
7. 继续执行『步骤 6. 记录远程命令状态』。

步骤 6. 记录远程命令状态：

要记录远程命令状态，请执行以下操作：

1. 在导航区域中，选择 **HMC 管理**。
2. 在任务列表中，单击**远程命令执行**。
3. 记录是否选择了使用 **ssh** 设施启用远程命令执行复选框。
4. 单击**取消**。
5. 继续执行『步骤 7. 保存升级数据』。

步骤 7. 保存升级数据：

可将当前 HMC 配置保存在 HMC 上的指定磁盘分区中或保存至本地介质。正好在将 HMC 软件升级至新发行版之前保存升级数据。此操作允许您在升级之后恢复 HMC 配置设置。

注：仅允许保存一个级别的备份数据。每次保存升级数据时，先前级别会被覆盖。

要保存升级数据，请执行以下操作：

1. 在导航区域中，选择 **HMC 管理**。
2. 在"操作"下的内容区域中，选择**保存升级数据**。"保存升级数据向导"将打开
3. 选择要在其上保存升级数据的介质。如果选择保存到可移动介质，现在请插入介质。单击**下一步**。
4. 单击**完成**。
5. 等待任务完成。 如果"保存升级数据"任务失败，请在继续之前与您的上一级支持机构联系。

注：如果"保存升级数据"任务失败，请不要继续执行升级进程。

6. 单击**确定**。
7. 继续执行『步骤 8. 升级 HMC 软件』。

步骤 8. 升级 HMC 软件：

要升级 HMC 软件，请使用 DVD 驱动器中的可移动介质重新启动系统。

1. 将 HMC 产品安装介质插入到 DVD 驱动器中。
2. 在"导航"栏中，选择 **HMC 管理**。
3. 在内容区域中，选择**关闭或重新启动 HMC**。
4. 确保选择了**重新启动 HMC**。

5. 单击**确定**。 HMC 将重新启动，而系统信息会在窗口上滚动显示。
6. 选择**升级**并单击**下一步**。
7. 从以下选项中进行选择：
 - 如果在上一任务中保存了升级数据，请继续执行下一步。
 - 如果先前未在此过程中保存升级数据，那么在继续之前，现在必须先保存升级数据。
8. 选择**从介质升级**并单击**下一步**。
9. 确认设置并单击**完成**。
10. 遵循提示执行操作。

注：

- 如果屏幕转为空白，请按空格键以查看信息。
 - 第一张 DVD 的安装时间大约为 20 分钟。
11. 在登录提示下使用您的用户标识和密码登录。 HMC 代码安装已完成。
 12. 继续执行『步骤 9. 验证 HMC 机器代码升级是否安装成功』。

步骤 9. 验证 HMC 机器代码升级是否安装成功：

要验证 HMC 升级是否安装成功，请执行以下操作：

1. 在导航区域中，单击**更新**。在"工作"区域中，HMC 版本、发行版、维护级别、构建级别和基本版本会显示在"HMC 代码级别"标题下。
2. 验证版本和发行版是否与安装的更新相匹配。
3. 如果显示的代码级别与安装的级别不同，请使用新 DVD 重试升级任务。如果问题仍然存在，请与您的上一级支持机构联系。

使用网络升级图像从远程位置升级 HMC

了解如何使用网络升级图像从远程位置升级 HMC 上的软件。

了解如何使用网络升级图像从远程位置升级 HMC 上的软件。使用以下过程升级 V6R1.2 或更高级别的 HMC (包括所有 HMC V7 级别)。

1. 从连接到因特网的计算机或服务器，访问硬件管理控制台 Web 站点 (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)
2. 下载相应的 HMC V7 网络图像并将其保存在 FTP 服务器上。 不能将这些文件直接下载到 HMC 上。 必须将图像文件下载到接受 FTP 请求的服务器上。
3. 确保下载下列文件：
 - img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. 将升级数据保存在 HMC 上。执行以下命令行以保存升级数据：
 - 要将数据同时保存在 DVD 和 HDD 上，请执行以下命令：

```
mount /media/cdrom
```

```
saveupgdata -r diskdvd
```

- 要将数据保存在 HDD 上，请执行以下命令：

```
saveupgdata -r disk
```

5. 将升级文件复制到 HMC 上的可引导磁盘分区。运行 `getupgfiles` 命令以复制文件。

示例：`getupgfiles -h <ftp server> -u <user id> -d <remote directory>`

其中，

- `ftp server` 是您将 HMC 网络图像下载到的 FTP 服务器的主机名或 IP 地址。
 - `user id` 是 FTP 服务器上的有效用户标识。如果您未使用 `--passwd` 参数指定密码，那么将提示您输入密码。
 - `remote directory` 是保存 HMC 网络图像的 FTP 服务器上的目录。
6. 重新引导 HMC 以升级复制到可引导磁盘分区的代码。运行 `chhmc -c altdiskboot -s enable --mode upgrade` 以重新引导 HMC。
 7. 重新引导 HMC，然后启动升级。运行 `hmcshutdown -r -t now` 命令以启动升级。

使用 HMC 增强型+ 界面配置 HMC

了解如何使用 HMC 增强型+ 界面设置网络连接、配置 HMC、执行配置后步骤以及升级和更新 HMC。

注：HMC Enhanced + 技术预览 (Pre-GA) 界面（它是 HMC V8.20 随附的选项）与 HMC V8.30 随附的 HMC 增强型+ 界面具有相同的过程和功能。文档中仅引用了 HMC 增强型+，但是该内容也适用于 HMC Enhanced + 技术预览 (Pre-GA) 界面。

在 HMC 上选择网络设置

了解可在 HMC 上使用的网络设置。

HMC 网络连接

您可以使用不同类型的网络连接将 HMC 连接至受管系统。有关如何配置 HMC 以连接到网络的更多信息，请参阅第 87 页的『配置 HMC』。有关在网络上使用 HMC 的更多信息，请参阅以下内容：

HMC 网络连接的类型：

了解如何通过网络来使用 HMC 远程管理和服务功能。

HMC 支持以下类型的逻辑通信：

HMC 至受管系统

用于执行大多数硬件管理功能，其中 HMC 会通过受管系统的服务处理器发出控制功能请求。HMC 与服务处理器之间的连接有时又称为服务网络。管理受管系统时需要此连接。

HMC 至逻辑分区

用来从逻辑分区中正在运行的操作系统收集与平台相关的信息（硬件错误事件和硬件清单），并用来使某些平台活动（动态 LPAR 和并发维修）与这些操作系统协调一致。如果要使用服务和错误通知功能，那么必须创建此连接。

HMC 至 BMC

注：基板管理控制器 (BMC) 连接仅适用于 HMC 型号 7063-CR1。

用来使用服务和维护任务。BMC 连接用来在系统上装入和维护 HMC 固件。在 HMC 上访问 BMC 时，需要此连接。

HMC 至远程用户

允许远程用户访问 HMC 功能。远程用户可以通过以下方式访问 HMC：

- 使用 Web 浏览器以远程方式访问所有 HMC GUI 功能。
- 使用安全套接字 Shell (SSH) 以远程方式访问 HMC 命令行功能。

HMC 至服务和支持

用于将数据（如硬件错误报告、清单数据和微码更新）传送到服务供应商以及从服务供应商传送这些数据。您可以使用此通信路径来调用自动服务。

根据型号，HMC 最多可支持 4 个不同物理以太网接口。独立版本的 HMC 仅支持三个 HMC 接口（使用一个集成以太网适配器和最多两个插件适配器）。通过以下方式使用其中每个接口：

- 可将一个或多个网络接口专门用于 HMC 至受管系统通信，这意味着该网络上只有 HMC 和受管系统的服务处理器。尽管连接至服务处理器的网络接口使用了安全套接字层 (SSL) 协议进行加密，并用密码加以保护，但具有单独的专用网络可以为这些接口提供更高级别的安全性。
- 开放式网络接口通常用于 HMC 和受管系统上的逻辑分区之间的网络连接，以支持 HMC 至逻辑分区的通信。还可使用此开放式网络接口来远程管理 HMC。
- 可选择使用第三个接口来连接逻辑分区并远程管理 HMC。此接口还可用作与不同逻辑分区组的单独 HMC 连接。例如，您可能想获得一个管理 LAN，该 LAN 独立于正在运行所有普通业务交易的 LAN。远程管理员可以使用此方法访问 HMC 和其他受管单元。有时，逻辑分区位于不同的网络安全域，可能在防火墙后面，因此您可能要建立与两个域的每一个域的不同 HMC 网络连接。

HMC 的 Web 浏览器需求

硬件管理控制台 (HMC) V8.7.0 受 Google Chrome V57、Microsoft Internet Explorer (IE) V11.0、Mozilla Firefox V45 和 V52 长期支持版 (ESR) 以及 Safari V10.1 支持。

如果您的浏览器配置为使用因特网代理，那么异常列表中应该包括一个本地 IP 地址。有关异常列表的更多信息，请咨询您的网络管理员。如果您仍需要使用代理来获取 HMC，请启用"Internet 选项"窗口中"高级"选项卡下面的"通过代理连接使用 HTTP 1.1"。

在远程连接到 HMC 时需要启用会话 cookie 以便使 ASMI 运行。ASM 代理代码保存会话信息并使用。遵循启用会话 cookie 的步骤。

在 Internet Explorer 中启用会话 cookie。

1. 选择"工具"，然后单击"Internet 选项"
2. 选择"隐私"，然后单击"高级"
3. 确保选中了"总是允许会话 cookie"。如果未选中，请选中"替代自动 cookie 处理"和"总是允许会话 cookie"。
4. 在"第一方 cookie"和"第三方 cookie"下面选择"提示"
5. 单击"确定"。

在 Firefox 中启用会话 cookie。

1. 选择"工具"，然后单击"选项"
2. 单击"cookie"
3. 选择"允许站点设置 cookie"。
4. 选择"异常"，然后添加 HMC。
5. 单击"确定"。

HMC 环境中的专用网络和开放式网络:

HMC 可配置为使用开放式网络和专用网络。专用网络允许使用所选范围的不可路由 IP 地址。公用网络或"开放式"网络描述 HMC 与任何逻辑分区以及 HMC 与常规网络上的其他系统之间的连接。

专用网络

HMC 专用网络上的设备只有 HMC 本身以及该 HMC 连接至的每个受管系统。该 HMC 连接至每个受管系统的 FSP (弹性服务处理器)。

在大多数系统上, FSP 提供标签为 **HMC1** 和 **HMC2** 的两个以太网端口。这允许您连接至两个 HMC。

一些系统具有双 FSP 选项。在此情况中, 第二个 FSP 充当"冗余"备份。具有两个 FSP 的系统的基本设置要求与只有一个 FSP 的系统的基本设置要求大致相同。HMC 必须连接至每个 FSP, 所以有多个 FSP 或多个受管系统时需要其他网络硬件 (如 LAN 交换机或集线器)。

注: 受管系统上的每个 FSP 端口只能连接至一个 HMC。

公用网络

开放式网络可连接用于连接因特网的防火墙或路由器。连接至因特网允许 HMC 在发生需要报告的任何硬件错误时进行"回拨"。

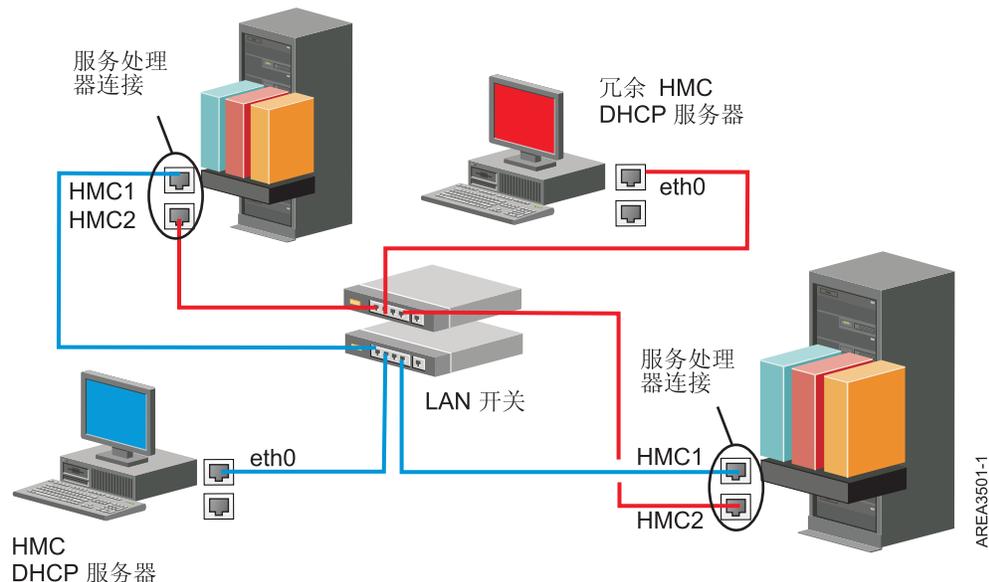
HMC 本身在它的每个网络接口上提供自己的防火墙。运行 HMC 指导式安装向导时会自动配置基本防火墙, 但您应在初始 HMC 安装和配置后定制防火墙设置。

将 HMC 用作 DHCP 服务器:

可将 HMC 用作动态主机配置协议 (DHCP) 服务器。

注: 如果要使用 IPv6, 那么必须手动完成发现过程。对于 IPv6, 不存在自动发现。

有关如何将 HMC 配置为 DHCP 服务器的更多信息, 请参阅第 93 页的『将 HMC 配置为 DHCP 服务器』。

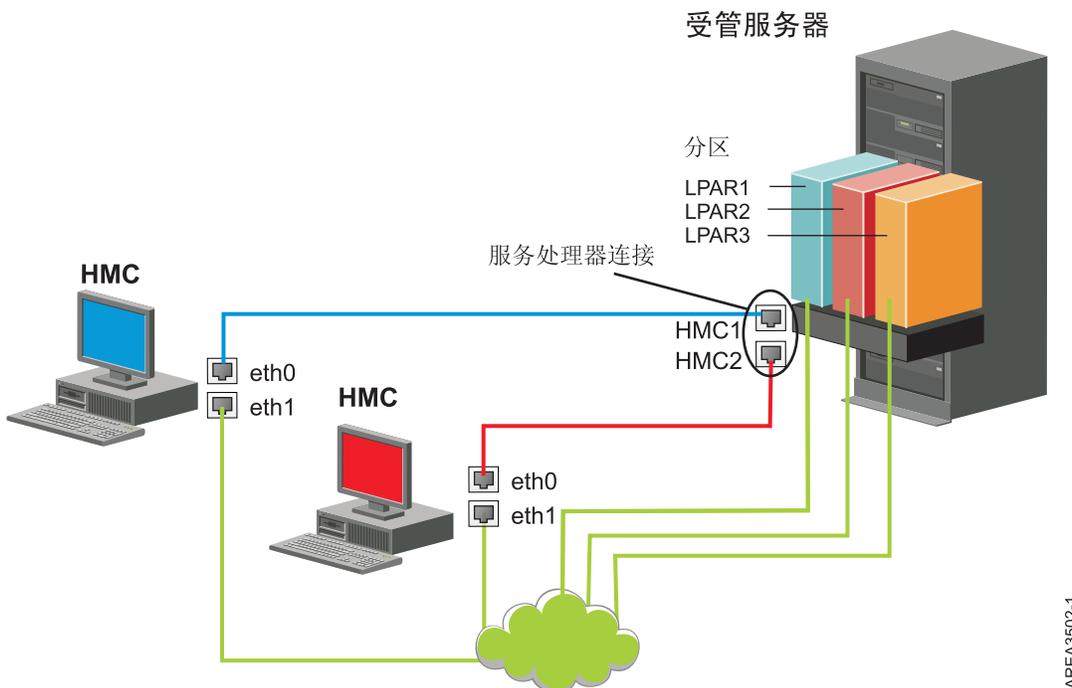


此图显示具有两个受管系统的冗余 HMC 环境。第一个 HMC 连接至每个 FSP 的第一个端口，冗余 HMC 连接至每个 HMC 的第二个端口。每个 HMC 被配置为 DHCP 服务器（使用不同范围的 IP 地址）。连接位于单独的专用网络上。确保未将任何 FSP 端口连接至多个 HMC 也同样重要。

连接至 HMC 的每个受管系统的 FSP 端口需要一个唯一的 IP 地址。要确保每个 FSP 具有一个唯一的 IP 地址，请使用 HMC 的内置 DHCP 服务器功能。当 FSP 检测到活动网络连接时，它会发出一个广播请求来定位某个 DHCP 服务器。如果 HMC 的配置正确，那么它会通过分配所选地址范围中的一个地址来响应该请求。

当存在多个 FSP 时，对于 HMC 至 FSP 专用网络，您必须拥有自己的 LAN 交换机或集线器。或者，此专用段可以作为多个端口存在于较大受管交换机上的专用虚拟 LAN (VLAN) 中。如果有多个专用 VLAN，那么必须确保它们被隔离开并且没有任何交叉流量。

如果有多个 HMC，那么还必须将同一开放式网络上的每个 HMC 连接至逻辑分区。



此图显示了连接至专用网络上单个受管服务器和公用网络上的三个逻辑分区的两个 HMC。您可以将一个额外的以太网适配器用于 HMC，以便具有三个网络接口。可以将第三个网络用作管理网络，也可以将它连接至 CSM（集群系统管理器）管理服务器。

有关如何将 HMC 配置为 DHCP 服务器的更多信息，请参阅第 93 页的『将 HMC 配置为 DHCP 服务器』。

决定要用于回拨服务器的连接方法：

了解有关使用回拨服务器时可使用的连接选项的更多信息。

通过使用基于 LAN 的因特网连接或基于调制解调器的拨号连接，可将 HMC 配置为将硬件服务相关信息发送至 IBM。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

配置基于 LAN 的因特网连接时，有两个通信选项。第一个选项是使用标准安全套接字层 (SSL)。可启用 SSL 通信以通过代理服务器连接至因特网。SSL 连接符合公司安全准则的可能性更高。第二个选项是使用 VPN 连接。

注：如果开放式网络接口连接仅使用因特网协议 V6 (IPv6)，那么不能使用因特网协议 VPN 来连接至支持系统。有关所使用协议的更多信息，请参阅第 76 页的『选择因特网协议』。

使用因特网连接的优点可能包括以下几点：

- 传输速度更快
- 降低客户开销（例如，专用模拟电话线路的成本）
- 可靠性更高

不管所选连接方法如何，下列安全性特征都会生效：

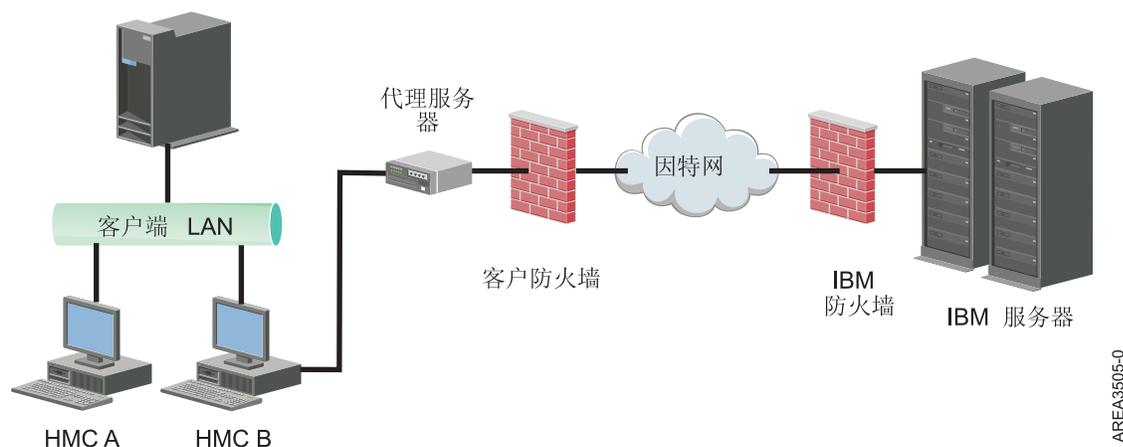
- 总是将远程支持设施请求从 HMC 发送至 IBM。决不会从 IBM 服务支持系统发出入站连接。
- HMC 与 IBM 服务支持系统之间传输的所有数据都是使用高级加密进行加密的。根据所选连接方法，会使用 SSL 或 IPSec 封装安全性有效负载 (ESP) 来进行加密。
- 初始化加密连接时，HMC 会将目标认证为 IBM 服务支持系统的目标。

发送至 IBM 服务支持系统的信息仅包含硬件问题和配置的相关信息。应用程序或客户数据不会传送至 IBM。

将间接因特网连接与代理服务器配合使用。

如果安装要求 HMC 放在专用网络上，那么您可使用 SSL 代理间接连接至因特网，SSL 代理会将请求转发至因特网。使用 SSL 代理的其他潜在优点之一是代理可能支持日志记录和审计设施。

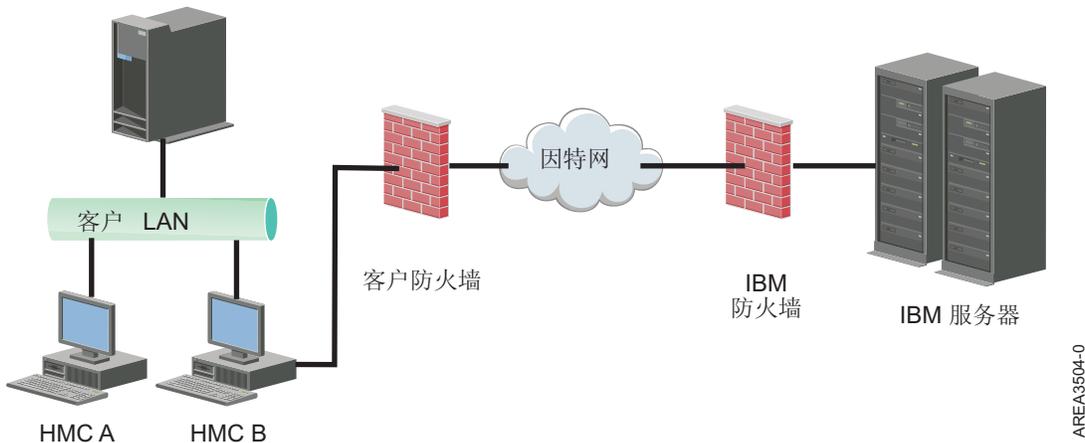
要转发 SSL 套接字，代理服务器必须支持基本代理服务器头功能（如 RFC 2616 中所述）和 CONNECT 方法。可选择配置基本代理认证 (RFC 2617) 以便在尝试通过代理服务器转发套接字之前让 HMC 进行认证。



要使 HMC 成功通信，客户机的代理服务器必须允许连接至端口 443。可配置代理服务器以将具体 IP 地址限制为 HMC 可连接的 IP 地址。请参阅第 77 页的『因特网 SSL 地址列表』以获取 IP 地址列表。

使用直接因特网 SSL 连接

如果 HMC 可连接至因特网，并且可设置外部防火墙以允许所建立的 TCP 包将出站数据传递至第 77 页的『因特网 SSL 地址列表』中所述的目标，那么您可使用直接因特网连接。



使用因特网 **SSL** 以连接至远程支持：

所有通信是通过 HMC 发出的 TCP 套接字处理的，并且这些通信会使用高级 SSL 来加密传送的数据。将发布目标 TCP/IP 地址（请参阅第 77 页的『因特网 SSL 地址列表』）以便将外部防火墙配置为允许这些连接。

注：标准 HTTPS 端口 443 将用于所有通信。

可启用 HMC 以直接连接至因特网，或通过客户提供的代理服务器间接连接至因特网。哪个方法最适用于您的安装版本取决于企业的安全性和联网要求。HMC（直接连接或通过 SSL 代理连接）在配置为使用因特网 SSL 连接时会使用下列地址。

选择因特网协议：

确定 HMC 连接至服务供应商时使用的 IP 地址版本。

大多数用户使用因特网协议 V4 (IPv4) 来连接至服务供应商。用于访问因特网的 IPv4 地址的显示格式为 4 个 IPv4 地址字节，字节之前用句点分隔（如 9.60.12.123）。还可使用因特网协议 V6 (IPv6) 来连接至服务供应商。网络管理员通常使用 IPv6 以确保地址空间唯一。如果您不确定安装版本所使用的因特网协议，请与网络管理员联系。有关使用每个版本的更多信息，请参阅第 94 页的『设置 IPv4 地址』和第 94 页的『设置 IPv6 地址』。

因特网 **SSL** 地址列表：

了解 HMC 在使用因特网 SSL 连接时所用的地址。

HMC 在配置为使用因特网 SSL 连接时，会使用以下 IPv4 地址来与 IBM 服务和支持联系。

以下 IPv4 地址用于所有位置：

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

以下 IPv4 地址用于美国：

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

以下 IPv4 地址用于美国以外的所有位置：

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

注：将防火墙配置为允许 HMC 连接至这些服务器时，只需要特定于地理区域的 IP 地址。

HMC 在配置为使用因特网 SSL 连接时，会使用以下 IPv6 地址来与 IBM 服务和支持联系：

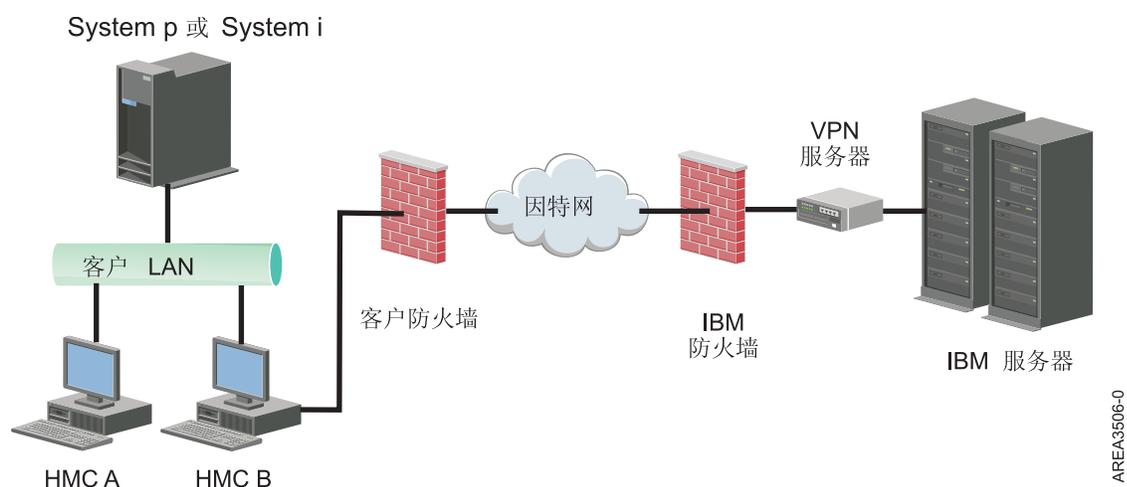
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

使用虚拟专用网连接至远程支持：

当连接至远程支持时，虚拟专用网 (VPN) 提供安全性。

注：此连接类型仅在 HMC V8.2.0 或更低版本上可用。

通过以加密和其他安全性方法来替代传统专用网络的物理上独立的网络线路，VPN 通过公用线路为用户提供了单独网线的私密性。除了能够用于出站连接之外，VPN 连接还可根据需要配置为支持远程服务请求。



因特网连接由系统管理员提供。防火墙还可以将具体 IP 地址限制为 HMC 可连接的 IP 地址。如果需要配置防火墙以限制 IP 地址，请参阅第 78 页的『VPN 服务器地址列表』以获取可使用的地址的列表。

有关如何使用基于 LAN 的 VPN 连接至因特网的更多信息，请参阅第 90 页的『配置 HMC 网络类型』。

VPN 服务器地址列表：

列示 HMC 配置为使用因特网 VPN 连接时使用的服务器。

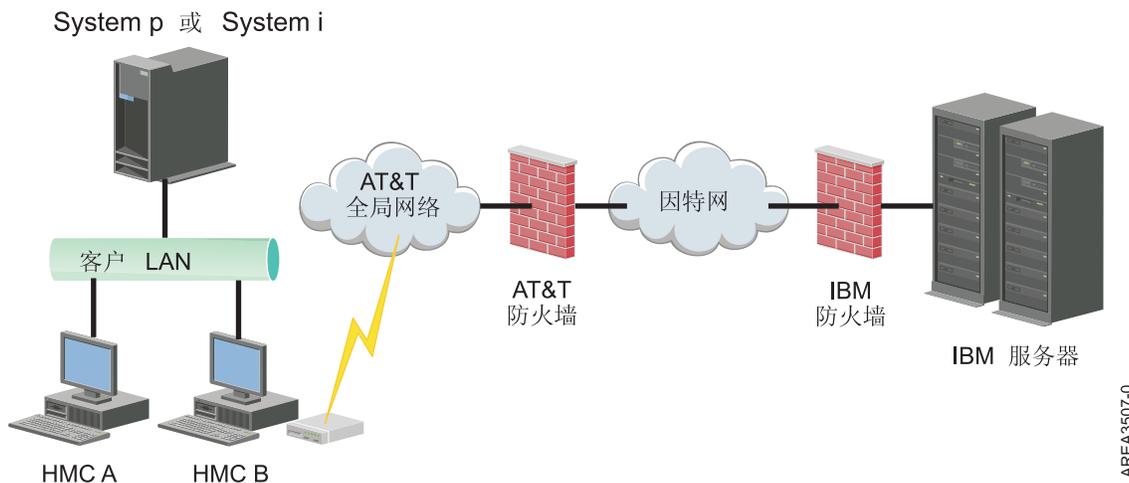
HMC 配置为使用因特网 VPN 连接时使用下列服务器。使用网络地址转换 (NAT) 防火墙时，所有连接在端口 500 和端口 4500 上使用 ESP 和 UDP。

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

使用电话和调制解调器连接至远程支持：

如果要使用调制解调器连接至远程支持，必须提供专用模拟线路来连接至 HMC 调制解调器。HMC 使用调制解调器来拨通全局网络并连接至 IBM 服务和支持。

注：此连接类型仅在 HMC V8.2.0 或更低版本上可用。



有关使用电话和调制解调器连接至远程支持的更多信息，请参阅第 90 页的『配置 HMC 网络类型』。

使用多个回拨服务器：

本主题描述决定使用多个回拨服务器时需要了解的事项。

为避免单点故障，请将 HMC 配置为使用多个回拨服务器。第一个可用的回拨服务器尝试处理每个服务事件。如果此回拨服务器的连接或传输失败，那么会使用其他可用回拨服务器重试服务请求，直到某个服务器操作成功或已尝试所有服务器。

由问题分析标识为给定受管系统的主分析控制台的已连接 HMC 将报告该问题。此主控制台还会将问题报告复制至所有辅助 HMC。此辅助 HMC 在网络上必须可被主 HMC 识别。出现以下情况时，辅助 HMC 被主 HMC 识别为另一回拨服务器：

- 主 HMC 配置为使用“发现的”回拨服务器，并且回拨服务器与主 HMC 在同一子网上或管理同一系统
- 回拨服务器已手动添加至可用于出站连接的回拨服务器控制台列表

准备 HMC 配置

使用本节来收集开始配置步骤之前需要知道的必需配置设置。

要配置 HMC，必须了解相关概念、制定决策和准备信息。

本节描述将 HMC 连接至下列各项时所需的信息：

- 受管系统中的服务处理器
- 这些受管系统上的逻辑分区
- 远程工作站
- IBM 服务，用于实现“回拨”功能

注：提供了其他连接和安全性信息。有关更多信息，请参阅 **ESA for HMC Connectivity Security for IBM POWER6, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000** 白皮书，可从以下网址取得：IBM Electronic Service Agent (<http://www-01.ibm.com/support/esa/security.htm>)。

要准备 HMC 配置，请完成以下步骤：

1. 获取要安装的 HMC 代码版本的最新级别并进行安装。
2. 确定 HMC 相对于它要管理的服务器的物理位置。如果 HMC 与其受管系统相距超过 25 英尺，那么必须允许从受管系统的位置使用 Web 浏览器访问 HMC，以便服务人员能够访问 HMC。
3. 标识 HMC 将管理的服务器。
4. 确定是使用专用网络还是开放式网络来管理服务器。如果决定使用专用网络，请使用 DHCP，除非您在使用集群系统管理 (CSM) 配置。CSM 不支持 IPv6。要访问 CSM，必须有两个网络。有关 CSM 的更多信息，请参阅随该功能部件提供的文档。有关专用网络和开放式网络的更多信息，请参阅第 72 页的『HMC 环境中的专用网络和开放式网络』。
5. 如果您使用开放式网络来管理 FSP，那么必须通过“高级系统管理界面”菜单来手动设置 FSP 的地址。建议使用不可路由的专用网络。
6. 如果有两个 HMC，请指定主 HMC 和辅助 HMC。主 HMC 在物理位置上应该更接近机器，并且应该是配置为回拨的 HMC。
7. 确定将 HMC 连接至远程工作站、逻辑分区和网络设备时所需的网络设置。
8. 定义 HMC 如何“回拨”。回拨选项包括通过仅出站安全套接字层 (SSL) 因特网连接、调制解调器或虚拟专用网 (VPN) 连接。
9. 确定您将创建的 HMC 用户及其密码以及将给予他们的角色。必须对 hscroot 和 hscpe 用户指定密码。
10. 描述配置回拨时所需的以下公司联系人信息：
 - 公司名称
 - 管理员联系人
 - 电子邮件地址
 - 电话号码
 - 传真号码
 - HMC 物理位置的街道地址
11. 如果计划通过回拨将信息发送至 IBM 服务时使用电子邮件来通知操作员或系统管理员，请标识简单电子邮件传输协议 (SMTP) 服务器和您要使用的电子邮件地址。
12. 必须定义以下密码：
 - 用于向 FSP 认证 HMC 的访问密码

- 用于管理用户的 ASMI 密码
- 用于一般用户的 ASMI 密码

第一次从 HMC 连接至新服务器时创建密码。如果 HMC 是冗余或辅助 HMC，请获取 HMC 用户密码并准备在第一次连接至受管服务器的 FSP 时输入此密码。

完成这些准备步骤后，请填写第 80 页的『HMC 的安装前配置工作表』。

HMC 的安装前配置工作表

使用此工作表来准备安装所需的安装信息。

网络设置

LAN 接口：选择可用的适配器（如 eth0 和 eth1），此 HMC 将使用这些适配器连接至受管系统、逻辑分区、服务和支持以及远程用户。有关更多信息，请参阅第 71 页的『HMC 网络连接』。从 HMC 发出的连接可以是在专用网络或开放式网络上进行的。

以太网适配器速度和双工

输入期望的以太网适配器速度和双工方式。如果您不确定哪种速度和双工能使您的硬件性能达到最佳，那么自动检测选项会确定最佳选项。"缺省值 = 自动检测介质速度"会指定以太网适配器双工方式下的速度。除非您要求指定固定介质速度，否则请选择"自动检测"。与 FSP（交换机/HMC）连接的任何设备都必须设置为"自动（速度）/自动（双工）"方式，因为这是缺省的 FSP 设置，不能更改。

表 34. 以太网适配器速度和双工

	eth0	eth1	eth2	eth3
选择速度和双工方式				
介质速度（自动检测，10/100/1000 全/半双工）				

有关专用网络和开放式网络的更多信息，请参阅第 72 页的『HMC 环境中的专用网络和开放式网络』。

表 35. 专用网络和开放式网络

	eth0	eth1	eth2	eth3
对每个适配器指定专用或开放式网络				

动态主机配置协议 (DHCP) 提供动态客户机的自动配置方法。可将此 HMC 指定为 DHCP 服务器。如果这是专用网络中的第一个或唯一的 HMC，那么将此 HMC 启用为 DHCP 服务器。执行此操作时，HMC 会自动配置和查找网络上的受管系统。

对于指定为专用网络的以太网适配器，请填写下表：

表 36. 专用网络

	eth0	eth1
是否要将此 HMC 指定为 DHCP 服务器？（是/否）		
如果答案为"是"，请记录要使用的 IP 地址范围		

如果您使用的是 7063-CR1 HMC，那么必须将以太网 **IPMI** 端口连接至网络，才能在 HMC 上访问基板管理控制器 (BMC)。有关更多信息，请参阅第 136 页的『配置 BMC 连接』。针对您的 BMC 连接填写下表。

表 37. BMC 连接

	IPMI
是否要通过 DHCP 方式配置此连接？（是/否）	
如果答案为"否"，请列出下面的已指定静态地址：	
IP 地址：	
子网掩码：	
网关：	

对于指定为开放式网络的以太网适配器，请填写下列各表。有关不同因特网协议版本的更多信息，请参阅第 76 页的『选择因特网协议』。

使用 IPv6

如果要使用 IPv6，请告诉网络管理员并决定获取 IP 地址的方式。然后，完成下列各表：

表 38. 使用 IPv6

	eth0	eth1	eth2	eth3
是否正使用以静态方式指定的 IP 地址？如果答案为"是"，请将该地址记录在此处。				

表 39. 使用 IPv6

	eth0	eth1	eth2	eth3
是否正从 DHCP 服务器获取 IP 地址？（是/否）				

表 40. 使用 IPv6

	eth0	eth1	eth2	eth3
是否正从 IPv6 路由器获取 IP 地址？				

有关设置 IPv6 地址的更多信息，请参阅第 94 页的『设置 IPv6 地址』。有关仅使用 IPv6 地址的更多信息，请参阅第 94 页的『仅使用 IPv6 地址』。

使用 IPv4

对于指定为使用 IPv4 的开放式网络的以太网适配器，请填写下列各表。

表 41. 使用 IPv4

	eth0	eth1	eth2	eth3
是否要自动获取 IP 地址？（是/否）				
如果答案为"否"，请列出下面的指定地址：				
TCP/IP 接口地址：				

表 41. 使用 IPv4 (续)

	eth0	eth1	eth2	eth3
TCP/IP 接口网络掩码:				
防火墙设置:				
是否要配置 HMC 防火墙设置? (是/否)				
如果为是, 请列出应该允许通过防火墙的应用程序和 IP 地址:				

TCP/IP 信息

每个节点 (支持元素 (SE) 和"硬件管理控制台 (HMC)") 都需要唯一 TCP/IP 地址。缺省情况下, 指定的网络掩码用于为本地专用 LAN 生成唯一地址。如果节点将连接至带有受管 TCP/IP 地址的较大网络, 那么可指定要使用的 TCP/IP 地址。系统会生成缺省值。

防火墙设置

HMC 防火墙设置会创建安全性壁垒, 该壁垒允许或拒绝访问 HMC 上的特定网络应用程序。可分别对每个物理网络接口指定这些控制设置, 这允许您控制每个网络上可访问的 HMC 网络应用程序。

如果已至少将一个适配器配置为开放式网络适配器, 那么必须提供其他信息以允许 HMC 访问 LAN:

表 42. 本地主机信息

本地主机信息	
HMC 主机名:	
域名:	
HMC 的描述:	
网关信息	
网关地址: (nnn.nnn.nnn.nnn)	
网关设备:	
DNS 启用	
是否要使用 DNS? (是/否)	
如果答案为"是", 请指定下面的 DNS 服务器搜索顺序:	
1.	
2.	
域后缀搜索顺序:	
1.	
2.	

本地主机信息

要向网络标识硬件管理控制台 (HMC)，请输入 HMC 的主机名和域名。除非您在网络上仅使用简短主机名，否则输入标准主机名称。域名示例：name.yourcompany.com

网关信息

要定义缺省网关，请填写要用于发送 IP 包的 TCP/IP 地址。如果目标站与源站不在同一子网上，网关地址会告诉每台计算机或网络设备何时发送数据。

DNS 启用

可使用域名系统 (DNS) 来提供用于查找基于 IP 的计算机的标准命名约定。通过定义 DNS 服务器，可使用主机名来标识服务器和硬件管理控制台 (HMC) 而不是 IP 地址。

DNS 服务器搜索顺序

输入为映射主机名和 IP 地址而搜索的 DNS 服务器的 IP 地址。此搜索顺序仅在启用 DNS 时可用。

域后缀搜索顺序

输入正在使用的域后缀。HMC 使用要追加到 DNS 搜索的非限定名称结尾的域后缀。将按后缀的列出顺序来搜索后缀。此搜索顺序仅在启用 DNS 时可用。

电子邮件通知

如果希望系统上发生硬件问题事件时通过电子邮件得到通知，请列出电子邮件联系人信息。

表 43. 电子邮件通知

域	
电子邮件地址：	
SMTP 服务器：	
端口：	
要通知的错误：	
仅回拨问题事件	
所有问题事件	

SMTP 服务器

输入要向其通知系统事件的服务器的简单电子邮件传输协议 (SMTP) 地址。SMTP 服务器名称的示例是 relay.us.ibm.com。

SMTP 是用于发送电子邮件的协议。使用 SMTP 时，客户机会发送消息并使用 SMTP 协议与 SMTP 服务器通信。

如果不知道或不确定服务器的 SMTP 地址，请与网络管理员联系。

端口 输入要向其通知系统事件的服务器的端口号或使用缺省端口。

要通知的电子邮件地址

输入发生系统事件时要通知的已配置电子邮件地址。

- 选择仅回拨问题事件以便仅在发生创建回拨功能的事件时接收通知。
- 选择所有问题事件以便在发生任何事件时接收通知。

服务联系人信息

表 44. 服务联系人信息

服务联系人信息	
公司名称	
管理员姓名	
电子邮件地址	
电话号码	
备用电话号码	
传真号码	
备用传真号码	
街道地址	
街道地址 2	
城市或地区	
州	
邮编	
国家或地区	
HMC 的位置（如果与上述管理员地址相同，请指定"相同")：	
街道地址	
街道地址 2	
城市或地区	
州	
邮编	
国家或地区	

服务授权和连接

选择要用于联系服务供应商的连接的类型。有关这些方法的描述（包括安全性特征和配置要求），请参阅第 74 页的『决定要用于回拨服务器的连接方法』。

表 45. 连接类型

连接类型	
	通过因特网连接的安全套接字层 (SSL)
	通过本地 HMC 进行拨号
	通过因特网连接的虚拟专用网 (VPN)

通过因特网连接的安全套接字层 (SSL)：

如果 HMC 已连接至因特网，那么可使用它来呼叫服务供应商。可通过使用借助现有因特网连接的加密安全套接字层 (SSL) 直接连接至服务供应商。如果要使用借助 SSL 代理的间接连接来配置使用加密 SSL，请选择使用 **SSL 代理**。

表 46. 通过因特网连接的安全套接字层 (SSL)

通过因特网连接的安全套接字层 (SSL)	
是否使用 SSL 代理? (是/否)	
如果答案为"是", 请列出下面的信息:	
地址:	
端口:	
是否使用 SSL 代理进行认证?	
如果答案为"是", 请列出下面的信息:	
用户:	
密码:	

使用的因特网连接协议

有关不同因特网协议的更多信息, 请参阅第 76 页的『选择因特网协议』。

- IPv4
- IPv6
- IPv4 和 IPv6

通过本地 HMC 进行拨号

输入用于配置本地调制解调器的拨号信息。指定要用于呼叫服务供应商的电话号码。进行连接时, 应按列示顺序拨打电话号码。

表 47. 通过本地 HMC 进行拨号

域	
拨号前缀:	
音调:	
脉冲:	
是否等待拨号音?	
是否启用扬声器?	

虚拟专用网 (VPN)

如果 HMC 已连接至因特网, 那么可使用它来呼叫服务供应商。可通过使用现有因特网连接的虚拟专用网 (VPN) 直接连接至服务供应商。

注: 如果选择通过因特网连接的虚拟专用网 (VPN), 那么不会引导您选择任何其他选项。

回拨服务器

确定要配置为回拨服务器以连接至服务和支持的 HMC。有关使用多个回拨服务器的更多信息, 请参阅第 79 页的『使用多个回拨服务器』。

- 此 HMC
- 另一 HMC

如果已选择另一 HMC, 那么在此处列出已配置为回拨服务器的其他 HMC:

表 48. 已配置为回拨服务器的其他 HMC

已配置为回拨服务器的 HMC 主机名或 IP 地址的列表	

其他支持优点

My Systems 和 Premium Search

表 49. 其他支持优点

域	
列出您的 IBM 标识	
列出您的 IBM 标识	

为了在 Electronic Services Web 站点的“My Systems”和“Premium Search”部分中访问有价值的定制支持信息，客户必须向此系统注册其 IBM 标识。如果还没有 IBM 标识，可在 www.ibm.com/account/profile 注册 IBM ID。

注：IBM 提供个性化 Web 功能，而这些功能使用 IBM Electronic Service Agent 应用程序收集到的信息。要使用这些功能，必须先在 IBM 注册 Web 站点（网址为 <http://www.ibm.com/account/profile>）上进行注册。

要授权用户使用 Electronic Service Agent 信息来个性化 Web 功能，请输入您在 IBM 注册 Web 站点上注册的 IBM 标识。要查看可供向系统注册 IBM 标识的客户使用的有价值支持信息，请访问 <http://www.ibm.com/support/electronic>。

配置 HMC

了解如何配置网络连接、安全性、服务应用程序和一些用户首选项。

依据要应用于 HMC 配置的定制级别，可以有多种方式来设置 HMC 以满足您的需要。指导式安装向导是 HMC 上的一种工具，旨在方便设置 HMC。您可以通过向导选择一个快速路径以便迅速创建建议的 HMC 环境，也可以选择充分浏览向导所指引的可用设置。没有向导的帮助时，还可通过使用 HMC 菜单配置 HMC 来执行配置步骤。

开始之前，应该收集成功完成步骤所需的配置信息。有关所需信息的列表，请参阅第 79 页的『准备 HMC 配置』。完成准备时，应确保完成了第 80 页的『HMC 的安装前配置工作表』，然后返回至本节。

通过指导式安装向导使用快速路径来配置 HMC

在大多数情况下，可以使用许多缺省设置来设置 HMC，以便高效率地操作。使用此快速路径核对表来准备 HMC 以获取服务。完成这些步骤之后，HMC 将被配置为（直接连接的）专用网络中的“动态主机配置协议”(DHCP) 服务器。

启动 **HMC** 并完成指导式安装向导中的步骤：

登录 HMC 界面并使用指导式安装向导来配置 HMC。

注：如果这是新安装，请确保受管系统未连接至电源。对于机架安装式 HMC，这意味着在插入主电源之前，此 HMC 是插入配电总线 (PDB) 的唯一设备。如果这是连接至同一受管系统中的第二个 HMC，那么可以将该受管系统连接至电源。

1. 按下电源按钮以开启 HMC。
2. 等待 HMC 在 30 秒后自动选择缺省语言和语言环境首选项。
3. 接受硬件管理控制台许可协议。如果拒绝硬件管理控制台许可协议，那么将无法完成 HMC 配置。
4. 单击登录并启动硬件管理控制台 **Web** 应用程序。
5. 登录 HMC：

注：如果系统管理员 (**hmcadmin**) 更改了密码，请在此处输入该密码。

- 标识：hscroot
- 密码：abc123

指导式安装向导将打开。

6. 在指导式安装条目窗口中单击**确定**。

注：如果启动HMC时未显示指导式安装向导，请在 HMC 欢迎页面的导航区域中单击**指导式安装向导**。

7. 通过使用您完成的安装前配置工作表来完成指导式安装向导中的步骤。单击是继续，并完成"连接和回拨服务器"向导中的步骤。
8. 在"摘要"窗口中，单击**完成**。
9. 如果未将以太网交叉电缆连接至受管系统，请立即连接。
10. 在 HMC 导航区域中，单击**服务管理**。
11. 在内容区域中，单击**向用户授权**。"向用户授权"窗口将打开。
12. 在字段中输入 IBM 标识并单击**确定**。

复查您的配置：

在"状态"窗口中，监视您选择的不同配置设置的进度。对于某些任务，此窗口可能在几分钟内显示为"暂挂"状态。单击**查看日志**，查看每个任务的相关状态消息。在任何时候单击**关闭**以关闭指导式安装向导。正在运行的任务将继续运行。现在您的 HMC 已完成配置。

使用 HMC 菜单配置 HMC

本节提供 HMC 配置任务的完整列表，这些任务将引导您完成配置 HMC 的过程。如果您不喜欢使用指导式安装向导，那么选择此选项。

必须重新启动 HMC 才能使配置设置生效，所以您可能要打印此核对表并在配置 HMC 时使用。

此信息包含本 PDF 中未包括的任务的参考资料。通过引用 HMC 欢迎页面上的**其他资源**部分，可以访问其他支持资料。

先决条件

使用 HMC 菜单开始配置 HMC 之前，应完成第 79 页的『准备 HMC 配置』中描述的配置准备活动。

表 50. 手动 HMC 配置任务以及在何处查找相关信息

任务	在何处查找相关信息
1. 启动 HMC。	第 89 页的『启动 HMC』
2. 设置日期和时间。	

表 50. 手动 HMC 配置任务以及在何处查找相关信息 (续)

任务	在何处查找相关信息
3. 更改预定义密码。	
4. 创建其他用户并在完成此步骤时返回至此核对表。	
5. 配置网络连接。	第 90 页的『配置 HMC 网络类型』
6. 如果使用开放式网络和固定 IP 地址, 请设置标识信息。	
7. 如果使用开放式网络和固定的 IP 地址, 请将路由条目配置为缺省网关。	第 96 页的『将路由条目配置为缺省网关』
8. 如果使用开放式网络和固定 IP 地址, 请配置域名服务。	第 96 页的『配置域名服务』
9. 如果使用固定 IP 地址并启用了 DNS, 请配置域后缀。	第 96 页的『配置域后缀』
10. 配置服务器以连接至 IBM 服务和支持, 并在完成此步骤时返回至此核对表。	第 98 页的『配置 HMC 以便它可与服务和支持联系』
11. 配置回拨事件管理器	第 102 页的『配置回拨事件管理器』
12. 将受管系统连接到电源。	
13. 设置受管系统的密码以及每个 ASMI 密码 (通用密码和管理员密码)	第 103 页的『为受管系统设置密码』
14. 访问 ASMI 以在受管系统上设置日期和时间。	
15. 启动受管系统并在完成此步骤时返回至此核对表。	
16. 确保受管系统上具有一个逻辑分区。	
17. 可选: 添加另一受管系统并在完成此步骤时返回至此核对表。	
18. 可选: 如果要使用 HMC 安装新服务器, 请配置逻辑分区并安装操作系统。	
19. 如果此时未在安装新服务器, 请执行可选配置后任务以进一步定制配置。	第 104 页的『配置后步骤』

启动 HMC:

您可以登录到硬件管理控制台 (HMC) 并选择希望在界面中显示的语言。第一次使用缺省用户标识 hscroot 和密码 abc123 登录 HMC。

要启动 HMC, 请完成下列步骤:

1. 按下电源按钮以开启 HMC。
2. 如果首选语言为英语, 请继续执行步骤 4。

如果首选语言不是英语, 那么当系统提示您更改语言环境时, 请输入数字 **2**。

注: 如果您不执行操作, 那么此提示在 30 秒后消失。

3. 在"语言环境选择"窗口的列表中, 选择要显示的语言环境, 然后单击**确定**。语言环境标识 HMC 界面使用的语言。
4. 使用以下缺省用户标识和密码登录 HMC:
 - 用户名: hscroot
 - 密码: abc123

在登录页面上，可以查看系统、分区和 Virtual I/O Server 的状态。还可以查看"提醒 LED"和可维护事件的数目。通过从登录页面单击各种社交媒体链接和 IBM developerWorks® 链接，可以了解有关 HMC 和可用功能的更多信息。

注：在 HMC V8.6.0.1 上，您可以从下列登录选项中进行选择：

登录：HMC Classic 或 HMC 增强型+

选择 HMC 增强型+ 界面以继续。HMC Classic 界面允许访问 HMC 的所有传统功能，而 HMC 增强型+ 界面提供了系统、分区和 Virtual I/O Server 的图形视图以及简化的导航。

HMC Classic

显示不具备增强的 PowerVM 功能的标准 GUI。

HMC 增强型+

显示完全重新设计的 HMC 管理界面的新视图，该界面通过系统、分区和 Virtual I/O Server 的图形视图以及简化的导航提供一个直观的界面工作环境。

注：当 HMC 作为 DHCP 服务器工作时，HMC 将在其首次连接到服务处理器时使用缺省密码。

5. 单击登录。

更改日期和时间：

以电池供电的时钟为 HMC 显示日期和时间。如果更换了电池或将系统移动到其他时区，那么您可能需要重新设置控制台日期和时间。了解如何更改 HMC 的日期和时间。

如果更改了日期和时间信息，那么此更改不会影响 HMC 管理的系统和逻辑分区。

要更改 HMC 的日期和时间，请完成以下步骤：

1. 确保您是以下某个角色的成员：

- 超级管理员
- 服务代表
- 操作员
- 查看者



2. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台设置。

3. 在"内容"窗格中，单击**更改日期和时间**。

4. 如果您在**时钟**字段中选择 **UTC**，那么时间设置将根据所选时区的夏令时自动进行调整。输入日期、时间和时区，然后单击**确定**。

配置 HMC 网络类型：

配置 HMC 以便它可与受管系统、逻辑分区、远程用户以及服务和支持通信。

配置 HMC 设置以使用开放式网络来连接至受管系统：

配置 HMC 以便它能够使用开放式网络来连接和管理受管系统。

要配置 HMC 网络设置以便它能够使用开放式网络来连接受管系统，请执行以下操作：

表 51. 配置 HMC 设置以使用开放式网络来连接至受管系统

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。 eth0 是首选值。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 通过执行下列任务来配置以太网适配器：	
a. 设置介质速度。	第 93 页的『设置介质速度』
b. 选择开放式网络类型。	第 93 页的『选择专用网络或开放式网络』
c. 设置静态地址。	第 94 页的『设置 IPv4 地址』
d. 设置防火墙。	第 95 页的『更改 HMC 防火墙设置』
e. 配置缺省网关。	第 96 页的『将路由条目配置为缺省网关』
f. 配置 DNS。	第 96 页的『配置域名服务』
4. 配置其他适配器（如果有的话）。	
5. 测试受管服务器与 HMC 之间的连接。	第 104 页的『测试 HMC 与受管系统之间的连接』

配置 HMC 设置以使用专用网络来连接至受管系统：

配置 HMC 以便它能够使用专用网络来连接和管理受管系统。

要配置 HMC 网络设置以便它能够使用专用网络来连接至受管系统，请执行以下操作：

表 52. 配置 HMC 设置以使用专用网络来连接至受管系统

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 将 HMC 配置为 DHCP 服务器。	第 93 页的『将 HMC 配置为 DHCP 服务器』
4. 测试受管服务器与 HMC 之间的连接。	第 104 页的『测试 HMC 与受管系统之间的连接』

配置 HMC 设置以使用开放式网络来连接至逻辑分区：

要配置 HMC 网络设置以便它能够使用开放式网络来连接至逻辑分区，请执行以下操作：

表 53. 配置 HMC 设置以使用开放式网络来连接至逻辑分区

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 通过执行下列任务来配置以太网适配器：	
a. 设置介质速度。	第 93 页的『设置介质速度』
b. 选择开放式网络类型。	第 93 页的『选择专用网络或开放式网络』
c. 设置静态地址。	第 94 页的『设置 IPv4 地址』
d. 设置防火墙。	第 95 页的『更改 HMC 防火墙设置』
e. 配置缺省网关。	第 96 页的『将路由条目配置为缺省网关』
f. 配置 DNS。	第 96 页的『配置域名服务』
4. 配置其他适配器（如果有的话）。	
5. 测试受管服务器与 HMC 之间的连接。	第 104 页的『测试 HMC 与受管系统之间的连接』

配置 HMC 设置以使用开放式网络来连接至远程用户：

要配置 HMC 网络设置以便它能够使用开放式网络来连接至远程用户，请执行以下操作：

表 54. 配置 HMC 设置以使用开放式网络来连接至远程用户

任务	在何处查找相关信息
1. 决定要用于受管系统的接口。	第 80 页的『HMC 的安装前配置工作表』
2. 标识 HMC 的以太网端口。	第 92 页的『标识已定义为 eth0 的以太网端口』
3. 通过执行下列任务来配置以太网适配器：	
a. 设置介质速度。	第 93 页的『设置介质速度』
b. 选择开放式网络类型。	第 93 页的『选择专用网络或开放式网络』
c. 设置静态地址。	第 94 页的『设置 IPv4 地址』
d. 设置防火墙。	第 95 页的『更改 HMC 防火墙设置』
e. 配置缺省网关。	第 96 页的『将路由条目配置为缺省网关』
f. 配置 DNS。	第 96 页的『配置域名服务』
g. 配置后缀。	第 96 页的『配置域后缀』
4. 配置其他适配器（如果有的话）。	

配置 HMC 回拨服务器设置：

要配置 HMC 回拨服务器设置以便能够报告问题，请执行以下操作：

表 55. 配置 HMC 回拨服务器设置

任务	在何处查找相关信息
1. 确保您具有所有必需的客户信息	第 80 页的『HMC 的安装前配置工作表』
2. 配置此 HMC 以报告错误或选择现有回拨服务器来报告错误	第 98 页的『配置本地控制台以向服务和支持报告错误』 第 101 页的『对此 HMC 选择用于连接至服务和支持的现有回拨服务器』
3. 验证回拨配置是否在工作	第 101 页的『验证与服务和支持的连接是否在工作』
4. 授权用户查看收集的系统数据	第 101 页的『授权用户查看收集的系统数据』
5. 安排系统数据的传输	第 102 页的『传输服务信息』

标识已定义为 *eth0* 的以太网端口：

必须使用 HMC 上定义为 *eth0* 的以太网端口进行与受管服务器的以太网连接。

如果未在 HMC 上的 PCI 槽中安装任何其他以太网适配器，并且计划将 HMC 用作受管系统的 DHCP 服务器，那么主集成以太网端口在 HCM 上始终定义为 *eth0* 或 *eth1*。

如果在 PCI 槽中安装了其他以太网适配器，那么定义为 *eth0* 的端口取决于安装的以太网适配器的位置和类型。

注：这些是一般规则，可能并不适用于所有配置。

下表根据 HMC 类型描述以太网布置的规则。

表 56. HMC 类型和以太网布置的相关规则

HMC 类型	以太网布置规则
机架安装式 HMC，带有两个集成以太网端口	<p>HMC 仅支持一个额外的以太网适配器。</p> <ul style="list-style-type: none"> 如果已安装一个额外的以太网适配器，那么该端口定义为 eth0。在这种情况下，主集成以太网端口定义为 eth1，辅助集成以太网端口定义为 eth2。 如果以太网适配器是双端口以太网适配器，那么标签为 Act/Link A 的端口通常为 eth0。标签为 Act/link B 的端口将为 eth1。在此情况下，主集成以太网端口定义为 eth2，而辅助集成以太网端口定义为 eth3。 如果未安装任何适配器，那么主集成以太网端口定义为 eth0。
独立模型，带有单个集成以太网端口	<p>定义取决于已安装的以太网适配器的类型：</p> <ul style="list-style-type: none"> 如果只安装了一个以太网适配器，那么该适配器被定义为 eth0。 如果以太网适配器是双端口以太网适配器，那么标签为 Act/link A 的端口通常为 eth0。标签为 Act/link B 的端口将为 eth1。在此情况下，主集成以太网端口被定义为 eth2。 如果未安装任何适配器，那么该集成以太网端口被定义为 eth0。 如果安装了多个以太网适配器，请参阅第 93 页的『确定以太网适配器的接口名称』。

确定以太网适配器的接口名称：

如果将 HMC 配置为 DHCP 服务器，那么该服务器只能在 HMC 标识为 eth0 和 eth1 的网络接口卡 (NIC) 连接器上运行。您可能还需要确定要将以太网电缆插入其中的 NIC 连接器。了解有关确定 HMC 标识为 eth0 和 eth1 的 NIC 连接器的更多信息。

要确定 HMC 指定给以太网适配器的名称，请执行下列操作：

1. 打开受限 shell 程序终端。选择 **HMC 管理 > 打开受限 shell 程序终端**。
2. 在命令行上输入以下命令：`tail -f /var/log/messages`。消息日志会在发生新事件时滚动。
3. 插入以太网电缆。如果已插入电缆，那么拔出电缆，等 5 秒钟，然后再次插入电缆。受限 shell 程序会在您插入电缆时滚动以显示消息。以下示例条目显示此以太网端口被标识为 eth0：`Aug 28 12:41:20 terminate kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100。`
4. 对所有其他以太网端口重复此过程，并记录结果。
5. 输入 `Ctrl+C` 以停止 `tail` 命令。

设置介质速度：

了解如何指定包括速度的介质速度和以太网适配器的双工方式。

HMC 适配器是指的缺省值为**自动检测**。如果此适配器连接至 LAN 交换机，那么您必须匹配交换机端口设置。要设置介质速度和双工，请完成以下步骤：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台设置。
2. 在内容窗格中，单击**更改网络设置**。
3. 单击 **LAN 适配器** 选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 在"局域网信息"部分，选择**自动检测**或适当的介质速度和双工组合。
6. 单击**确定**。

选择专用网络或开放式网络：

专用服务网络由 HMC 和受管系统组成。专用服务网络仅限于控制台及其管理的系统，且独立于公司网络之外。开放式网络由专用服务网络和公司网络组成。除控制台和受管系统之外，开放式网络可能包含网络端点，且可能包括多个子网和网络设备。

要选择专用网络或公用网络，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台设置。
2. 在内容窗格中，单击**更改网络设置**。
3. 单击 **LAN 适配器** 选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击 **LAN 适配器** 选项卡。
6. 在局域网信息页中，选择**专用**或**开放式**。
7. 单击**确定**。

将 HMC 配置为 DHCP 服务器：

动态主机配置协议 (DHCP) 提供动态客户机的自动配置方法。

要将 HMC 配置 DHCP 服务器，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台设置。
2. 在内容窗格中，单击**更改网络设置**。"定制网络设置"窗口将打开。
3. 选择要使用的 LAN 适配器并单击**详细信息**。
4. 选择**专用**，然后选择网络类型。
5. 在"DHCP 服务器"部分中，选择启用 **DHCP 服务器**以将 HMC 作为 DHCP 服务器启用。

注：只能在专用网络上将 HMC 配置为 DHCP 服务器。如果您使用开放式网络，那么您将不会有选择启用 **DHCP** 选项。

6. 输入 DHCP 服务器的地址范围。
7. 单击**确定**。

如果您已将 HMC 配置为专用网络上的 DHCP 服务器，那么必须验证是否已正确配置 HMC DHCP 专用网络。有关将 HMC 连接到专用网络的信息，请参阅第 93 页的『选择专用网络或开放式网络』。

有关更多信息，请参阅第 73 页的『将 HMC 用作 DHCP 服务器』。

配置 BMC 连接：

可以配置或查看管理控制台的 BMC 网络设置。

注：此任务仅适用于 7063-CR1。在 HMC 上访问基板管理控制器 (BMC) 时，需要此连接。

要配置 BMC 连接，请完成下列步骤：



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台设置。
2. 在内容窗格中，单击**更改 BMC/IPMI 网络设置**。
3. 选择连接方式 (**DHCP** 或**静态**)。

如果选择**静态**方式，请填写下列地址：

- **IP 地址**
 - **子网掩码**
 - **网关**
4. 单击**确定**。

还可以使用 Petitboot 引导装入程序界面来配置 BMC 网络连接。有关更多信息，请参阅配置固件 IP 地址。

设置 IPv4 地址：

了解如何在 HMC 上设置 IPv4 地址。



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台设置。
2. 在内容窗格中，单击**更改网络设置**。
3. 单击 **LAN 适配器** 选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击**基本设置** 选项卡。
6. 选择 IPv4 地址。
7. 如果选择指定 IP 地址，请输入 TCP/IP 接口地址和 TCP/IP 接口网络掩码。
8. 单击**确定**。

设置 IPv6 地址：

了解如何在 HMC 上设置 IPv6 地址。



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台设置。

2. 在内容窗格中，单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击 **IPv6 设置**选项卡。
6. 选择 **Autoconfig** 选项或添加静态 IP 地址。
7. 如果添加了 IP 地址，请输入 IPv6 地址和前缀长度，然后单击**确定**。
8. 单击**确定**。

仅使用 IPv6 地址：

了解如何配置 HMC 以便它仅使用 IPv6 地址。



1. 在导航区域中，单击 **HMC 管理**图标，然后选择**控制台设置**。
2. 在内容窗格中，单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 选择**无 IPv4 地址**。
6. 单击 **IPv6 设置**选项卡。
7. 选择使用 **DHCPv6** 来配置 IP 设置或添加静态 IP 地址。然后，单击**确定**。

单击"确定"后，必须重新引导 HMC 才能使这些更改生效。

更改 HMC 防火墙设置：

在开放式网络中，防火墙通常用于控制对公司网络的外部访问。HMC 在每个以太网适配器上都有防火墙。要以远程方式控制 HMC 或以远程方式访问其他 HMC，请修改连接至开放式网络的 HMC 上的以太网适配器防火墙设置。

要配置防火墙，请执行以下步骤：



1. 在导航区域中，单击 **HMC 管理**图标，然后选择**控制台设置**。
2. 在内容窗格中，单击**更改网络设置**。
3. 单击 **LAN 适配器**选项卡。
4. 选择要使用的 LAN 适配器并单击**详细信息**。
5. 单击**防火墙**选项卡。
6. 使用以下方法中的一种，您可以允许任何使用特定应用程序的 IP 地址通过防火墙，或指定一个或多个 IP 地址：
 - 允许使用特定应用程序的 IP 地址通过防火墙：
 - a. 在顶部框中，突出显示此应用程序。
 - b. 单击**允许进入**。此应用程序显示在底部框中表示已被选中。
 - 指定允许通过防火墙的 IP 地址：
 - a. 在顶部框中，选中某个应用程序。

- b. 单击**允许 IP 地址进入**。
- c. 在"允许的主机"窗口中, 输入 IP 地址和网络掩码。
- d. 单击**添加**, 然后单击**确定**。

7. 单击**确定**。

启用远程受限 *shell* 程序访问:

可在配置防火墙时启用远程受限 *shell* 程序访问。

要启用远程受限 *shell* 程序访问, 请执行以下操作:

1. 在导航区域中, 单击 **HMC 管理**。
2. 单击**远程命令执行**。
3. 选择使用 **ssh** 设施启用远程命令执行, 然后单击**确定**。

现在就启用了远程受限 *shell* 程序访问。

启用远程 *web* 访问:

可启用对 HMC 的远程 Web 访问。

要启用远程 Web 访问, 请执行以下操作:

1. 在导航区域中, 单击 **HMC 管理**。
2. 单击**远程操作**。
3. 选择**启用**, 然后单击**确定**。

现在就启用了远程 Web 访问。

将路由条目配置为缺省网关:

了解如何将路由条目配置为缺省网关。此任务对使用开放式网络的用户可用。

要将路由条目配置为缺省网关, 请执行以下操作:



1. 在导航区域中, 单击 **HMC 管理**图标  , 然后选择**控制台设置**。
2. 在内容窗格中, 单击**更改网络设置**。"定制网络设置"窗口将打开。
3. 单击**路由**选项卡。
4. 在"缺省网关信息"部分中, 输入要设置为缺省网关的路由条目的网关地址和网关设备。
5. 单击**确定**。

配置域名服务:

如果计划设置开放式网络, 请配置域名服务。

如果计划设置开放式网络, 请配置域名服务。"域名系统"(DNS) 是用来管理主机名及其相关"因特网协议"(IP) 地址的分布式数据库系统。配置域名服务包括启用 DNS 和指定域后缀搜索顺序。



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台设置。
2. 在内容窗格中，单击**更改网络设置**。"更改网络设置"窗口将打开。
3. 单击**名称服务**选项卡。
4. 选择**启用 DNS**，以启用 DNS。
5. 指定 DNS 服务器和域后缀搜索顺序，然后单击**添加**。
6. 单击**确定**。

配置域后缀：

域后缀列表用于解析从列表中第一个条目开始的 IP 地址。

域后缀是追加到主机名的字符串，用于帮助解析其 IP 地址。例如，主机名 myname 可能无法解析。但是，如果字符串 myloc.mycompany.com 是域后缀表中的元素，那么还将尝试解析 myname.mloc.mycompany.com。

要配置域后缀项，请执行以下步骤：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台设置。
2. 在内容窗格中，单击**更改网络设置**。"定制网络设置"窗口将打开。
3. 单击**名称服务**选项卡。
4. 输入用作域后缀项的字符串。
5. 单击**添加**以将其添加到列表中。

配置 **HMC** 以便它使用 **LDAP** 远程认证：

可配置硬件管理控制台 (HMC) 以便它使用 LDAP (轻量级目录访问协议) 远程认证。

用户登录 HMC 时，会首先针对本地密码文件执行认证。如果找不到本地密码文件，那么 HMC 会与远程 LDAP 服务器联系以进行认证。必须配置 HMC 以便它使用 LDAP 远程认证。

注：配置 HMC 以便它使用 LDAP 认证之前，必须确保 HMC 与 LDAP 服务器之间存在有效网络连接。有关配置 HMC 网络连接的更多信息，请参阅第 90 页的『配置 HMC 网络类型』。

要配置 HMC 以使它使用 LDAP 认证，请完成以下步骤：



1. 在导航区域中，单击**用户和安全性**图标 ，然后选择**系统和控制台安全性**。
2. 在内容窗格中，单击**管理 LDAP**。"LDAP 服务器定义"窗口将打开。
3. 选择**启用 LDAP**。
4. 定义要用于认证的 LDAP 服务器。
5. 定义用于标识要认证的用户 LDAP 属性。缺省值为 **uid**，但您可使用您自己的属性。
6. 对 LDAP 服务器定义专有名称树（又称为搜索条件）。
7. 单击**确定**。

8. 如果某用户要使用 LDAP 认证，那么该用户必须配置其概要文件，使得概要文件使用 LDAP 远程认证而不是本地认证。

配置 HMC 以便它使用密钥分发中心服务器进行 **Kerberos** 远程认证：

配置 HMC 以便它使用密钥分发中心 (KDC) 服务器进行 Kerberos 远程认证。

用户登录 HMC 时，会首先针对本地密码文件执行认证。如果找不到本地密码文件，那么 HMC 会与远程 Kerberos 服务器联系以进行认证。必须配置 HMC 以便它使用 Kerberos 远程认证。

注：配置 HMC 以便它使用 KDC 服务器进行 Kerberos 远程认证之前，必须确保 HMC 与 KDC 服务器之间存在有效网络连接。有关配置 HMC 网络连接的更多信息，请参阅第 90 页的『配置 HMC 网络类型』。

要配置 HMC 以便它使用 KDC 服务器进行 Kerberos 远程认证，请执行以下操作：

1. 在 HMC 上启用网络时间协议 (NTP) 服务，并设置 HMC 和 KDC 服务器以使时间与同一 NTP 服务器同步。要在 HMC 上启用 NTP 服务，请执行以下操作：



- a. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台设置。
 - b. 在内容窗格中，选择更改日期和时间。
 - c. 选择 **NTP** 配置选项卡。
 - d. 选择在此 **HMC** 上启用 **NTP** 服务。
 - e. 单击确定。
2. 配置每个远程 HMC 用户的概要文件以便 HMC 使用 Kerberos 远程认证而不是本地认证。
 3. 可选：可将服务密钥文件导入到此 HMC 中。服务密钥文件包含向 KDC 服务器标识 HMC 的主机主体。服务密钥文件又称为 *keytab*。要将服务密钥文件导入到此 HMC 中，请执行以下操作：



- a. 在导航区域中，单击 **用户和安全性** 图标，然后选择系统和控制台安全性。
 - b. 在内容窗格中，单击管理 **KDC**。
 - c. 选择操作 > 导入服务密钥。"导入服务密钥"窗口将打开。
 - d. 输入服务密钥文件的位置。
 - e. 单击确定。
4. 向此 HMC 添加新的 KDC 服务器。要向此 HMC 添加新的 KDC 服务器，请执行以下操作：



- a. 在导航区域中，单击 **用户和安全性** 图标，然后选择系统和控制台安全性。
- b. 在内容窗格中，单击管理 **KDC**。
- c. 选择操作 > 添加 **KDC** 服务器。"导入服务密钥"窗口将打开。
- d. 输入域和 KDC 服务器的主机名或 IP 地址。
- e. 单击确定。

配置本地控制台以向服务和支持报告错误：

配置此 HMC，以便它可以使用 LAN 连接来回拨错误。

使用回拨设置向导来配置 HMC 以便它可连接至服务和支持：

使用回拨向导来配置 HMC 以便它成为回拨服务器。

此过程描述如何将 HMC 配置为使用直接基于 (LAN) 和间接 (SSL) 连接来连接至因特网的回拨服务器。

在开始此任务之前，请确保符合下列条件：

- 网络管理员已验证允许连接。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 如果您通过代理服务器配置因特网支持，那么还必须了解以下信息：
 - 代理服务器的 IP 地址和端口
 - 代理认证信息
- 使用了指定为 **eth1**（被指定为开放式网络）的适配器。有关更多信息，请参阅第 71 页的『在 HMC 上选择网络设置』。
- 以太网电缆已在物理上将 HMC 连接至 LAN。

要使用回拨向导来配置 HMC 以便它成为回拨服务器，请执行以下操作：



1. 在导航区域中，单击**可维护性**图标，然后选择**服务管理**。
2. 在内容窗格中，单击**回拨设置向导**。“连接和回拨服务器”向导将打开。遵循向导中的指示信息来配置回拨。

配置本地控制台以向服务和支持报告错误：

配置此 HMC，以便它可以使用 LAN 连接来回拨错误。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

将 HMC 配置为使用基于 LAN 的因特网和 SSL 与服务和支持联系：

描述如何将 HMC 配置为使用直接基于 (LAN) 和间接 (SSL) 连接来连接至因特网的回拨服务器。

在开始此任务之前，请确保符合下列条件：

- 网络管理员已验证允许连接。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 已配置客户联系人信息。通过进至 HMC 界面并单击**可维护性 > 服务管理 > 管理客户信息**来验证此项。
- 如果您通过代理服务器配置因特网支持，那么还必须了解以下信息：
 - 代理服务器的 IP 地址和端口
 - 代理认证信息
- 您至少需要配置一个开放式网络接口。有关更多信息，请参阅第 72 页的『HMC 环境中的专用网络和开放式网络』。
- 以太网电缆已在物理上将 HMC 连接至 LAN。

要将 HMC 配置为使用直接基于 (LAN) 和间接 (SSL) 连接来连接至因特网的回拨服务器，请执行以下操作：



1. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
2. 在"连接"部分中，单击管理出站连接。"回拨服务器控制台"窗口将打开。
3. 单击配置。
4. 在"出站连接设置"窗口中，选择将本地系统启用为回拨服务器。
5. 接受协议。
6. 在"出站连接设置"窗口中，选择因特网页面。
7. 选择允许使用现有因特网连接来获取服务框。
8. 如果要使用 SSL 代理，请选择使用 **SSL** 代理框。
9. 如果要使用 SSL 代理，请填写代理的地址和端口。从网络管理员处获取此信息。
10. 如果选择了使用 **SSL** 代理并且该代理需要用户标识和密码认证，请选择向 **SSL** 代理认证框。输入用户标识和密码。从网络管理员处获取用户标识和密码。
11. 选择连接因特网时要使用的协议。
12. 在因特网页面上，单击测试。
13. 在"测试因特网"窗口中，单击开始。
14. 验证测试是否成功完成。
15. 在"测试因特网"窗口中，单击取消。
16. 在"出站连接设置"窗口中，选择确定。

使用电话和调制解调器连接至服务和支持：

描述如何将 HMC 配置为使用调制解调器访问 IBM 支持的回拨服务器。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

在开始此任务之前，请确保符合下列条件：

- 已有可用的专用模拟电话线路。
- 已有配置调制解调器所需的信息。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 已配置客户联系人信息。您可通过进至 HMC 界面并单击可维护性 > 服务管理 > 管理客户信息来验证此项。
- 确保下列信息可用：
 - 模拟线路的类型，即音调或脉冲。大多数线路为音调，但某些仍在使用的线路是较旧循环或脉冲类型。
 - 拿起电话时线路是否发出拨号音。大多数线路会发出拨号音，但某些仍在使用的线路则不会。
 - 是否需要拨号前缀字符串。拨号前缀字符串是访问外线时所需加拨的若干数字。

要将 HMC 配置为使用调制解调器访问 IBM 支持的回拨服务器，请执行以下操作：



1. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
2. 在"连接"部分中，单击管理出站连接。
3. 单击配置。
4. 在"出站连接设置"窗口中，选择将本地系统启用为回拨服务器。

5. 接受协议。
6. 在"出站连接设置"窗口中，单击本地调制解调器选项卡。
7. 在"本地调制解调器"页面上，选中允许使用本地调制解调器拨号以获取服务复选框。
8. 在"本地调制解调器"页面上，选中调制解调器配置复选框。
9. 在"定制调制解调器设置"窗口中，单击拨号类型（音调或脉冲）。如果接收方挂断时线路发出拨号音，那么请选中等待拨号音复选框。填写拨打外线时所需的任何拨号前缀字符串。
10. 单击确定。
11. 在"本地调制解调器"页面上，单击添加。
12. 从列表中选择号码。
13. 如果这是本地号码，那么从电话号码字段中除去区号。
14. 在"添加电话号码"面板中，单击添加。
15. 在"定制调制解调器设置"面板中，单击测试。
16. 在"测试电话号码"面板中，单击开始。
17. 验证测试是否成功完成。
18. 在"测试电话号码"窗口中，单击取消。
19. 最多可配置 5 个电话号码。至少配置 2 个电话号码（主电话号码和备用电话号码）。将按电话号码的配置顺序来尝试这些电话号码。要将其他号码添加至可拨列表，请重复此过程中的步骤。
20. 在"出站连接设置"窗口中，选择确定。

使用基于 LAN 的 VPN 连接至服务和支持：

配置使用 VPN 的回拨服务器。

注：因特网虚拟专用网 (VPN) 和拨号连接类型仅在 HMC V8.2.0 或更低版本上可用。

在开始此任务之前，请确保符合下列条件：

- 网络管理员已验证允许连接。有关更多信息，请参阅第 79 页的『准备 HMC 配置』。
- 使用了指定为 **eth1**（被指定为开放式网络）的适配器。有关更多信息，请参阅第 71 页的『在 HMC 上选择网络设置』。
- 以太网电缆已在物理上将 HMC 连接至 LAN。
- 已配置客户联系人信息。通过在 HMC 界面上单击可维护性 > 服务管理 > 管理客户信息来验证此情况。

要配置使用 VPN 的回拨服务器，请执行以下操作：



1. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
2. 在"连接"部分中，单击管理出站连接。
3. 单击配置。
4. 在"出站连接设置"窗口中，选择将本地系统启用为回拨服务器。
5. 接受协议。
6. 在"出站连接设置"窗口中，选择因特网 VPN 选项卡。
7. 在"因特网 VPN"页面上，单击允许使用 VPN 和现有因特网连接来获取服务。
8. 在"因特网 VPN"页面上，选择测试复选框。

9. 在"测试因特网 VPN"窗口中，单击**开始**。
10. 验证测试是否成功完成。
11. 在"测试因特网 VPN"窗口中，单击**取消**。
12. 在"出站连接设置"窗口中，选择**确定**。

对此 HMC 选择用于连接至服务和支持的现有回拨服务器：

选择此 HMC 已识别或发现的现有 HMC 回拨服务器来报告错误。

已发现的 HMC 是启用为回拨服务器的 HMC 以及与此 HMC 位于同一子网或管理同一受管系统的 HMC。

要选择已发现的 HMC 以在此 HMC 报告错误时进行回拨，请执行以下操作：



1. 在导航区域中，单击**可维护性图标**，然后选择**服务管理**。
2. 在内容窗格中，单击**管理出站连接**。"回拨服务器控制台"窗口将打开。
3. 单击**使用发现的回拨服务器控制台**。该 HMC 将显示配置为回拨的 HMC 的 IP 地址或主机名。
4. 单击**确定**。

还可手动添加不同子网上的现有 HMC 回拨服务器。选择配置为回拨的 HMC 的 IP 地址或主机名，单击**添加**。然后，单击**确定**。

验证与服务和支持的连接是否在工作：

测试问题报告以确保与服务和支持的连接是否在工作。

要验证回拨配置是否在工作，请执行以下操作：



1. 在导航区域中，单击**可维护性图标**，然后选择**服务管理**。
2. 在内容窗格中，单击**创建事件**。
3. 选择**测试自动问题报告**并输入注释。
4. 单击**请求服务**。等几分钟以便发送请求。
5. 在"服务管理"窗口中，选择**管理事件**。
6. 选择**所有未解决问题**。
7. 验证是否存在指定给未解决问题编号的 PMH 事件和编号。
8. 选择该事件并单击**关闭**。
9. 在"关闭"窗口中，输入您的姓名和简短注释。

授权用户查看收集的系統数据：

必须对用户授权，用户才能查看您系统的相关数据。

在您授权用户查看收集的系統数据之前，您必须获取 IBM 标识。有关获取 IBM 标识的更多信息，请参阅第 80 页的『HMC 的安装前配置工作表』。

要授权用户查看收集的系統数据，请执行以下操作：



1. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
2. 在内容窗格中，选择向用户授权。
3. 输入 IBM 标识。
4. 单击确定。

传送服务信息：

可即时将信息传送给服务供应商，也可安排定期发送信息。

IBM 提供个性化 Web 功能，这些功能使用 IBM Electronic Service Agent 收集的信息。要使用这些功能，必须先在 IBM 注册 Web 站点（网址为 <http://www.ibm.com/account/profile>）上进行注册。要授权用户使用 Electronic Service Agent 信息来个性化 Web 功能，请参阅第 101 页的『授权用户查看收集的系統数据』。有关向系统注册 IBM 标识的优点的更多信息，请参阅 <http://www.ibm.com/support/electronic>。

注：应在安装并配置 HMC 以供使用后立即传送服务供应商信息。

要传送服务信息，请执行以下操作：



1. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
2. 在内容窗格中，单击传送服务信息。
3. 完成“传送服务信息”窗口中的任务，然后单击确定。

安排服务信息：

安排何时传输服务信息以用于问题确定。

注：您应该在安装和配置硬件管理控制台 (HMC) 以供使用之后立即传输服务提供者信息。

要安排服务信息，请完成下列步骤：



1. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
2. 在内容窗格中，单击安排服务信息。
3. 在内容窗格中，单击安排和发送数据选项卡以安排服务信息。

注：您还可以单击下列选项卡以选择要发送的数据和配置 FTP 连接：

- **安排和发送数据：**立即将信息传输到服务提供者，或者安排传输。
 - **发送问题报告：**选择您想要的的数据以及数据的目标。
 - **配置 FTP 连接：**提供配置数据以允许使用 FTP 来卸载服务信息。
4. 选择您想要启用常规传输或者立即发送的服务信息的类型。
 - **可运行测试（脉动信号）信息 -- 始终启用：**发送“问题事件日志”文件。
 - **硬件服务信息 (VPD)：**为所有连接至此 HMC 的受管系统发送重要产品数据 (VPD)。
 - **软件服务信息：**为所有正在分区上运行的软件发送 VPD。

- **性能管理信息**：收集和发送性能管理信息。
 - **更新访问密钥信息**：验证并更新访问密钥信息。
5. 选择安排重复传输的时间间隔（天）和时间。要立即传输信息，请单击**立即发送**。
 6. 单击**确定**。

使用联机帮助以获取有关安排服务信息的其他信息。

配置回拨事件管理器：

了解如何配置"回拨事件管理器"任务。您可以通过此任务监视和核准从 HMC 传输到 IBM 的任何数据。

已通过使用 HMC 命令行界面设置"回拨事件管理器"方式（启用或禁用）。启用"回拨事件管理器"任务将阻止 HMC 在事件发生时自动对其进行回拨。要阻止事件在未进行核准的情况下回拨，所有在此环境中运行的 HMC 都必须已启用"回拨事件管理器"。

要启用或禁用"回拨事件管理器"任务，请运行以下命令：

```

chhmc -c emch

-s {enable | disable}

[--callhome {enable | disable}]

[--help]

```

注：启用"回拨事件管理器"任务将阻止回拨事件，直到它们获得回拨任务批准为止。如果您禁用"回拨事件管理器"任务，那么系统不会自动启用回拨功能。此设置会阻止数据的任何非计划回拨到 IBM。从下列命令选项中选择以设置必需的配置：

- 要启用"回拨事件管理器"任务：**chhmc -c emch -s enable**
- 要禁用"回拨事件管理器"任务并重新启用自动回拨：**chhmc -c emch -s disable --callhome enable**
- 要禁用"回拨事件管理器"任务且不重新启用自动回拨：**chhmc -c emch -s disable --callhome disable**

确保 HMC 可与部署在此环境中的其他 HMC 进行通信。回拨事件管理器在注册 HMC 时具有测试连接功能。

您可以使用回拨事件管理器来注册 HMC。注册 HMC 之后，事件管理器将查询已注册的 HMC 以获取等待回拨到 IBM 的任何事件。事件管理器显示正发送回 IBM 的数据并对这些事件进行核准。核准后，事件管理器会向已注册的 HMC 发出通知，其可继续执行回拨操作。

"回拨事件管理器"任务可从任一 HMC 运行，也可从多个 HMC 运行。要使用"回拨事件管理器"任务注册管理控制台，请完成以下步骤：



1. 在导航区域中，单击**可维护性图标** ，然后选择**回拨事件管理器**。
2. 从**回拨事件管理器**窗格中，单击**管理控制台**。
3. 从**管理已注册的控制台**窗口，单击**添加控制台**以输入信息，以使用"回拨事件管理器"任务注册管理控制台。
4. 单击**确定**以落实对已注册的管理控制台列表进行的更改。

注：回拨事件管理器可与禁用的事件管理器方式配合使用。您仍可以在事件管理器中注册 HMC 并查看事件，但事件管理器不会在回拨事件时进行控制。

为受管系统设置密码：

必须同时为服务器和高级系统管理 (ADM) 设置密码。了解有关如何使用 HMC 界面设置这些密码的更多信息。

如果接收到认证暂挂消息，那么 HMC 会提示您为受管系统设置密码。

如果未接收到"认证暂挂"消息，那么完成以下步骤来为受管系统设置密码。

更新服务器密码：

要更新服务器密码，请执行以下操作：



1. 在导航区域中，选择受管系统并单击**用户和安全性**图标 ，然后选择**用户和角色**。
2. 单击**更改密码**。"更新密码"窗口将打开。
3. 输入所需信息并单击**确定**。

更新高级系统管理 (ASM) 通用密码：

注：通用用户标识的缺省密码为 `general`，管理员标识的缺省密码为 `admin`。

要更新 ASM 通用密码，请执行以下操作：

1. 在 HMC 的导航区域中，选择受管系统。
2. 在"任务"区域中，单击**操作**。
3. 单击**高级系统管理 (ASM)**。"启动 ASM 界面"窗口将打开。
4. 选择"服务处理器 IP 地址"并单击**确定**。ASM 界面将打开。
5. 在"欢迎使用 ASMI"窗格中，请指定您的用户标识和密码，然后单击**登录**。
6. 在导航区域中，展开**登录概要文件**。
7. 选择**更改密码**。
8. 指定所需的信息并单击**继续**。

复位高级系统管理 (ASM) 管理员密码：

要重新设置管理员密码，请与授权服务供应商联系。

测试 HMC 与受管系统之间的连接：

此选项使您能够验证是否已正确连接至网络。

要测试网络连接，您必须为以下某个角色的成员：

- 超级管理员
- 服务代表

要测试 HMC 与受管系统之间的连接，请执行以下操作：



1. 在导航区域中，单击**HMC 管理**图标 ，然后选择**控制台设置**。

2. 在内容窗格中，单击**测试网络连接**。
3. 在 Ping 选项卡中，输入您想要连接的任何系统的主机名或 IP 地址。要测试开放式网络，请输入网关。单击 **Ping**。

如果尚未创建任何逻辑分区，那么您将无法对地址执行 ping 操作。可使用 HMC 在服务器上创建逻辑分区。有关更多信息，请参阅逻辑分区。

要了解如何在网络中使用 HMC，请参阅第 71 页的『HMC 网络连接』。

有关配置 HMC 以连接至网络的更多信息，请参阅第 88 页的『使用 HMC 菜单配置 HMC』。

配置后步骤

安装并配置 HMC 后，根据需要备份 HMC 数据。

备份重要的 HMC 数据

可将重要控制台信息备份至 USB 闪存设备或 DVD，也可通过 FTP 或网络进行备份。

您可以使用 HMC 来备份所有重要数据，如以下数据：

- 用户首选项文件
- 用户信息
- HMC 平台配置文件
- HMC 日志文件
- 通过安装纠正服务的 HMC 更新

备份功能会将存储在 HMC 硬盘上的 HMC 数据保存至以下设备：

- DVD 介质
- USB 闪存设备
- 安装至 HMC 文件系统（如 NFS）的远程系统
- 远程站点（通过 FTP）

请在对 HMC 或与逻辑分区相关联的信息进行更改之后备份 HMC。

注：必须将介质格式化，然后才能将数据保存到可移动介质。要格式化介质，请单击 **HMC 管理 > 控制台管理 > 格式化介质**并遵循步骤。

要备份 HMC，您必须为以下某个角色的成员：

- 超级管理员
- 操作员
- 服务代表

要备份 HMC 的重要数据，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理**图标 ，然后选择**控制台管理**。
2. 在内容窗格中，单击**备份管理控制台数据**。
3. 选择归档选项。您可以备份到本地系统上的介质和已安装的远程系统或将备份数据发送到远程站点。

4. 遵循窗口上的指示信息来备份数据。

将整个 HMC 硬盘驱动器备份到远程系统

可以使用 HMC 来将 HMC 的整个硬盘驱动器备份到远程系统。

远程系统必须已配置网络文件系统 (NFS) 或安全 Shell (ssh)，并且此网络必须可从 HMC 访问。要完成此任务，您必须关闭 HMC 并对它进行重新引导。仅使用 HMC 来执行这些任务。

要将 HMC 硬盘驱动器备份到远程系统，您必须为以下某个角色的成员：

- 超级管理员
- 操作员
- 服务代表

要将 HMC 硬盘驱动器备份到远程系统，请执行以下操作：

1. 记录 HMC 上每个网络适配器的接口号 (eth0、eth1 等)、MAC 地址和 IP 地址。为此，单击 **HMC 管理 > 控制台设置 > 更改网络设置 > LAN 适配器**。
2. 关闭 HMC 并关闭它的电源。
3. 打开 HMC 控制台的电源，并将 HMC 恢复介质插入 DVD 驱动器中。如果您要从已配置的网络引导服务器启动 HMC 界面，那么确保网络接口是启动顺序中的一个设备。要查看启动设备列表，当 HMC 打开电源时按 F12，并选择您要从中引导的网络接口。
4. 选择备份选项并单击下一步。
5. 选择要用于与远程服务器通信的网络接口。如果您要通过连接网络引导服务器来启动 HMC，并且此服务器也是您要将数据备份至的远程服务器，那么选择缺省设置。然后单击下一步并进入步骤 7。如果未选择缺省设置，那么继续执行下一步。

注：接口编号 (eth0 和 eth1) 可能与步骤 1 中记录的编号不匹配。列示的 MAC 地址可用于标识期望的接口。有关更多信息，请参阅第 92 页的『标识已定义为 eth0 的以太网端口』。

6. 如果不选择缺省设置，那么必须选择要与所选接口配合使用的网络协议。可以选择从网络中的 DHCP 服务器获取 IP 地址或将静态 IP 地址分配给所选网络接口。作出选择并单击下一步。
7. 如果您未选择缺省设置，那么输入远程服务器的 IP 地址或主机名。将使用 gzip 压缩实用程序和 tar 命令创建备份文件。在远程主机上的文件字段中指定扩展名为 .tgz 的文件。如果已选择缺省网络设置，那么必须使用网络引导配置中的目录设置。此信息显示在远程主机上的文件字段中。在完成所有必需的信息之后，单击下一步。
8. 选择您要用于将数据从 HMC 传送到远程服务器的方法。如果选择加密数据，那么远程主机必须让安全 Shell (SSH) 服务器处于运行状态。如果选择传送数据而不进行加密，那么远程主机必须运行网络文件服务器 (NFS)，且必须导出您要将数据备份至的目录以获取写访问权。作出选择并单击下一步。
9. 如果您选择使用加密方式来传送数据，那么必须输入远程服务器的用户标识和密码。
10. 验证您所输入的信息正确并单击完成。如果备份完成，那么会显示 HMC 界面。

如果在打开 HMC 的电源时通过按 F1 修改了启动顺序，那么必须重新引导 HMC 并再次更改设置。更改启动顺序时，确保在启动顺序中硬盘列示在网络接口前面。

更新，升级和迁移 HMC 机器代码

HMC 的更新和升级会定期发布，以添加新功能和改进现有功能。了解有关更新、升级和迁移 HMC 机器代码之间的差别的更多信息。同时了解如何执行 HMC 机器代码更新、升级或迁移。

完成每个任务时，HMC 会重新引导但分区不会。

更新 HMC 代码

对现有 HMC 级别应用维护

不要求您执行保存升级数据任务

升级 HMC 代码

将 HMC 软件替换为同一程序的新发行版或修订级别

要求您从恢复介质进行引导

迁移 HMC 代码

将 HMC 数据从一个 HMC 版本移至另一个 HMC 版本

迁移是一种升级。

确定 HMC 机器代码版本和发行版

了解如何查看 HMC 机器代码版本和发行版

HMC 上的机器代码级别将确定可用功能部件，包括要升级至新发行版的并发服务器固件维护和增强功能。

要查看 HMC 机器代码版本和发行版，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择 **控制台管理**。
2. 在内容窗格中，单击 **更新硬件管理控制台**。
3. 在新的窗口中，查看并记录出现在“当前 HMC 驱动程序信息”标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。

对连接至因特网的 HMC 获取并应用机器代码更新

了解如何对连接至因特网的 HMC 获取机器代码更新。

要获取 HMC 的机器代码更新，请执行步骤 1 到 5。

步骤 1. 确保已连接至因特网：

要将更新从服务和支持系统或 Web 站点下载至 HMC 或服务器，必须具有下列其中一项：

- 带有或不带 SSL 代理的 SSL 连接
- 因特网 VPN

为确保已连接至因特网，请执行以下操作：



1. 在导航区域中，单击 **可维护性** 图标，然后选择 **服务管理**。
2. 在内容窗格中，单击 **管理出站连接**。
3. 选择对应为 HMC 选择的出站连接类型（因特网 VPN 或 SSL 连接）的选项卡。

注：如果与服务和支持的连接不存在，请先设置服务连接，然后继续此过程。有关如何设置与服务和支持的连接的指示信息，请参阅“设置服务器以连接至 IBM 服务和支持”。

4. 单击 **测试**。
5. 验证测试是否成功完成。如果测试未成功，请诊断连接并更正问题，然后继续此过程。或者，可获取 DVD 上的更新。

6. 继续执行『步骤 2. 查看现有 HMC 机器代码级别』。

步骤 2. 查看现有 HMC 机器代码级别：

要查看现有 HMC 机器代码级别，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台管理。
2. 在内容窗格中，单击更新硬件管理控制台。
3. 在新的窗口中，查看并记录出现在"当前 HMC 驱动程序信息"标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
4. 继续执行『步骤 3. 查看可用的 HMC 机器代码级别』。

步骤 3. 查看可用的 HMC 机器代码级别：

要查看可用 HMC 机器代码级别，请执行以下操作：

1. 在连接至因特网的计算机或服务器上，访问 <http://www.ibm.com/eserver/support/fixes>。
2. 从产品系列列表中选择适当的系列。
3. 在产品或修订类型列表中选择硬件管理控制台。
4. 单击继续。将显示硬件管理控制台站点。
5. 下滚至 HMC 版本级别以查看可用 HMC 级别。

注：如果愿意，可与服务和支持联系。

6. 继续执行『步骤 4. 应用 HMC 机器代码更新』。

步骤 4. 应用 HMC 机器代码更新：

要应用 HMC 机器代码更新，请执行以下操作：

1. 在安装 HMC 机器代码的更新之前，请备份 HMC 上的关键控制台信息。有关指示信息，请参阅第 104 页的『备份重要的 HMC 数据』。然后继续执行下一步。



2. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台管理。
3. 在内容窗格中，单击更新硬件管理控制台。"安装纠正服务向导"将打开。
4. 遵循向导中的指示信息来安装更新。
5. 关闭 HMC，然后重新启动 HMC 以使更新生效。
6. 单击登录并启动硬件管理控制台 Web 应用程序。
7. 登录 HMC 界面。

步骤 5. 验证 HMC 机器代码更新是否安装成功：

要验证 HMC 机器代码更新是否安装成功，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台管理。
2. 在内容窗格中，单击更新硬件管理控制台。
3. 在新的窗口中，查看并记录出现在"当前 HMC 驱动程序信息"标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。

4. 验证版本和发行版是否与安装的更新相匹配。
5. 如果显示的代码级别与安装的级别不同，请执行以下步骤：
 - a. 选择 HMC 上的网络连接。
 - b. 使用另一存储库重试固件更新。
 - c. 如果问题仍然存在，请与您的上一级支持机构联系。

使用 DVD 或 FTP 服务器获取并应用 HMC 的机器代码更新

了解如何使用 DVD 或 FTP 服务器获取 HMC 的机器代码更新。

要获取 HMC 机器代码更新，请执行步骤 1 到 5。

步骤 1. 查看现有 HMC 机器代码级别：

要查看现有 HMC 机器代码级别，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台管理。
2. 在内容窗格中，单击更新硬件管理控制台。
3. 在新的窗口中，查看并记录出现在“当前 HMC 驱动程序信息”标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
4. 继续执行『步骤 2. 查看可用的 HMC 机器代码级别』。

步骤 2. 查看可用的 HMC 机器代码级别：

要查看可用 HMC 机器代码级别，请执行以下操作：

1. 在连接至因特网的计算机或服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 下滚至 HMC 版本级别以查看可用 HMC 级别。

注：如果愿意，可与 IBM 服务和支持联系。

3. 继续执行『步骤 3. 获取 HMC 机器代码更新』。

步骤 3. 获取 HMC 机器代码更新：

要获取 HMC 机器代码更新，请执行以下操作：

可通过 Fix Central 的 Web 站点订购 HMC 机器代码更新、与服务和支持联系或将 HMC 机器代码升级下载至 FTP 服务器。

通过 Fix Central 的 Web 站点订购 HMC 机器代码更新

1. 在连接至因特网的计算机或服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 在“受支持的 HMC 产品”中，选择最新 HMC 级别。
3. 下滚至“文件名/包”区域并查找要订购的更新。
4. 在“订购”列中，选择执行。
5. 单击继续以使用您的 IBM 标识登录。
6. 遵循屏幕上的提示来提交订单。

将 HMC 机器代码更新下载至可移动介质

1. 在连接至因特网的计算机或服务服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 在"受支持的 HMC 产品"中，选择最新 HMC 级别。
3. 下滚至"文件名/包"区域并查找要下载的更新。
4. 单击要下载的更新。
5. 接受许可协议，并将更新保存至可移动介质。

完成时继续执行『步骤 4. 应用 HMC 机器代码更新』。

步骤 4. 应用 HMC 机器代码更新：

要应用 HMC 机器代码更新，请执行以下操作：

1. 在安装 HMC 机器代码的更新之前，请备份 HMC 数据。有关更多信息，请参阅第 104 页的『备份重要的 HMC 数据』。
2. 如果在 DVD-RAM 上获取或创建了更新，请将该 DVD-RAM 插入到 HMC 上的 DVD 驱动器中。如果在 USB 存储设备上获取或创建了更新，请插入该存储设备。
3. 在安装 HMC 机器代码的更新之前，请备份 HMC 上的关键控制台信息。有关指示信息，请参阅第 104 页的『备份重要的 HMC 数据』。然后继续执行下一步。



4. 在导航区域中，单击 **HMC 管理** 图标，然后选择 **控制台管理**。
5. 在内容窗格中，单击 **更新硬件管理控制台**。"安装纠正服务向导"将打开。
6. 遵循向导中的指示信息来安装更新。
7. 关闭 HMC，然后重新启动并登录回 HMC 以使更新生效。
8. 继续执行『步骤 5. 验证 HMC 机器代码更新是否安装成功』。

步骤 5. 验证 HMC 机器代码更新是否安装成功：

要验证 HMC 机器代码更新是否安装成功，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择 **控制台管理**。
2. 在内容窗格中，单击 **更新硬件管理控制台**。
3. 在新的窗口中，查看并记录出现在"当前 HMC 驱动程序信息"标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
4. 验证版本和发行版是否与安装的更新相匹配。
5. 如果显示的代码级别与安装的级别不同，请执行以下步骤：
 - a. 重试机器代码更新。如果为此过程创建了 DVD，请使用新介质。
 - b. 如果问题仍然存在，请与您的上一级支持机构联系。

升级 HMC 软件

了解如何在保留 HMC 配置数据的同时将 HMC 上的软件从一个发行版升级至下一个发行版。

要升级 HMC 上的机器代码，请执行步骤 1 到 9。

步骤 1. 获取升级：

您可以通过 Fix Central 的 Web 站点订购 HMC 机器代码升级。

要通过 Fix Central 的 Web 站点获取升级，请执行以下操作：

1. 在连接至因特网的计算机或服务器上，访问硬件管理控制台 Web 站点（网址为 <http://www-933.ibm.com/support/fixcentral/>）。
2. 单击**继续**。将显示硬件管理控制台站点。
3. 浏览至要升级至的 HMC 版本。
4. 找到下载和订购部分。

注：如果您无权访问因特网，请与 IBM 服务和支持联系以订购 DVD 上的升级。

5. 遵循屏幕上的提示来提交订单。
6. 升级后继续执行『步骤 2. 查看现有 HMC 机器代码级别』。

步骤 2. 查看现有 HMC 机器代码级别：

要确定 HMC 上的机器代码的现有级别，请执行以下步骤：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择**控制台管理**。在导航区域中，单击**更新**。
2. 在内容窗格中，单击**更新硬件管理控制台**。
3. 在新的窗口中，查看并记录出现在“当前 HMC 驱动程序信息”标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
4. 继续执行『步骤 3. 备份受管系统的概要文件数据』。

步骤 3. 备份受管系统的概要文件数据：

要备份受管系统的概要文件数据，请执行以下操作：

1. 在导航区域中，选择**系统管理**。
2. 选择**服务器**。
3. 选择服务器并确保状态为正在运行或备用。
4. 在“任务”中选择**配置 > 管理分区数据 > 备份**。
5. 输入备份文件名称并记录此信息。
6. 单击**确定**。
7. 对每个受管系统重复这些步骤。
8. 继续执行『步骤 4. 备份 HMC 数据』。

步骤 4. 备份 HMC 数据：

在安装新版本的 HMC 软件之前备份 HMC 数据，以便可在升级软件期间发生问题时恢复先前级别。成功升级至新版本的 HMC 软件后，不要使用此关键控制台数据。

注：要备份至可移动介质，需要让该介质可用。

要备份 HMC 数据，请执行以下操作：

1. 如果计划备份至介质，请执行以下步骤来格式化介质：
 - a. 将介质插入到驱动器中。



- b. 在导航区域中，单击可维护性图标 ，然后选择服务管理。
- c. 在内容窗格中，单击格式化介质。
- d. 选择介质类型。
- e. 选择格式类型。
- f. 单击确定。



2. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择控制台管理。
3. 在内容窗格中，单击备份管理控制台数据。"备份管理控制台数据"窗口将打开。
4. 选择归档选项。可备份至本地系统上的介质和已安装到 HMC 文件系统（例如，NFS）的远程系统，或使用文件传输协议 (FTP) 将备份发送至远程站点。
 - 要备份至本地系统，请选择备份至本地系统上的介质并遵循指示信息。
 - 要备份至已安装的远程系统，请选择备份至已安装的远程系统并遵循指示信息。
 - 要备份至远程 FTP 站点，请选择将备份关键数据发送至远程站点并遵循指示信息。
5. 继续执行『步骤 5. 记录当前 HMC 配置信息』。

步骤 5. 记录当前 HMC 配置信息：

在升级至新版本的 HMC 软件之前，应记录 HMC 配置信息以预防出现问题。

要记录当前 HMC 配置，请执行以下操作：

1. 要查看针对受管系统或其逻辑分区安排的操作，请打开 **HMC 管理 > 控制台管理**。如果要记录对 HMC 本身安排的操作，请选择 **HMC 管理 > 控制台管理**，然后选择并跳至步骤 3。
2. 选择要对其记录 HMC 配置信息的受管系统和所有分区。
3. 在任务列表中，选择安排操作。将显示对所选目标安排的所有操作。
4. 选择排序 > 按对象。
5. 选择每个对象并记录以下详细信息：
 - 对象名
 - 安排日期
 - 操作时间（以 24 小时制显示）
 - 重复（如果为"是"，请执行以下步骤）：
 - a. 选择查看 > 安排详细信息。
 - b. 记录时间间隔信息。
 - c. 关闭安排的操作窗口。
 - d. 对每个安排操作重复此过程。
6. 关闭"定制安排的操作"窗口。
7. 继续执行『步骤 6. 记录远程命令状态』。

步骤 6. 记录远程命令状态：

要记录远程命令状态，请执行以下操作：

1. 在导航区域中，选择 **HMC 管理**。

2. 在任务列表中，单击**远程命令执行**。
3. 记录是否选择了使用 **ssh** 设施启用远程命令执行复选框。
4. 单击**取消**。
5. 继续执行『步骤 7. 保存升级数据』。

步骤 7. 保存升级数据：

可将当前 HMC 配置保存在 HMC 上的指定磁盘分区中或保存至本地介质。正好在将 HMC 软件升级至新发行版之前保存升级数据。此操作允许您在升级之后恢复 HMC 配置设置。

注：仅允许保存一个级别的备份数据。每次保存升级数据时，先前级别会被覆盖。

要保存升级数据，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择**控制台管理**。
2. 在内容窗格中，单击**保存升级数据**。“保存升级数据向导”将打开
3. 选择要在其上保存升级数据的介质。如果选择保存到可移动介质，现在请插入介质。单击**下一步**。
4. 单击**完成**。
5. 等待任务完成。如果“保存升级数据”任务失败，请在继续之前与您的上一级支持机构联系。

注：如果“保存升级数据”任务失败，请不要继续执行升级进程。

6. 单击**确定**。
7. 继续执行『步骤 8. 升级 HMC 软件』。

步骤 8. 升级 HMC 软件：

要升级 HMC 软件，请使用 DVD 驱动器中的可移动介质重新启动系统。

1. 将 HMC 产品安装介质插入到 DVD 驱动器中。



2. 在导航区域中，单击 **HMC 管理** 图标 ，然后选择**控制台管理**。
3. 在内容窗格中，选择**关闭或重新启动管理控制台**。
4. 确保选择了**重新启动 HMC**。
5. 单击**确定**。HMC 将重新启动，而系统信息会在窗口上滚动显示。
6. 选择**升级**并单击**下一步**。
7. 从以下选项中进行选择：
 - 如果在上一任务中保存了升级数据，请继续执行下一步。
 - 如果先前未在此过程中保存升级数据，那么在继续之前，现在必须先保存升级数据。
8. 选择**从介质升级**并单击**下一步**。
9. 确认设置并单击**完成**。
10. 遵循提示执行操作。

注：

- 如果屏幕转为空白，请按空格键以查看信息。
- 第一张 DVD 的安装时间大约为 20 分钟。

11. 在登录提示下使用您的用户标识和密码登录。 HMC 代码安装已完成。
12. 继续执行『步骤 9. 验证 HMC 机器代码升级是否安装成功』。

步骤 9. 验证 HMC 机器代码升级是否安装成功：

要验证 HMC 升级是否安装成功，请执行以下操作：



1. 在导航区域中，单击 **HMC 管理** 图标，然后选择控制台管理。
2. 在内容窗格中，单击更新硬件管理控制台。
3. 在新的窗口中，查看并记录出现在“当前 HMC 驱动程序信息”标题下的信息，包括 HMC 版本、发行版、维护级别、构建级别和基本版本。
4. 验证版本和发行版是否与安装的更新相匹配。
5. 如果显示的代码级别与安装的级别不同，请使用新 DVD 重试升级任务。如果问题仍然存在，请与您的上一级支持机构联系。

使用网络升级图像从远程位置升级 HMC

了解如何使用网络升级图像从远程位置升级 HMC 上的软件。

了解如何使用网络升级图像从远程位置升级 HMC 上的软件。使用以下过程升级 V6R1.2 或更高级别的 HMC（包括所有 HMC V7 级别）。

1. 从连接到因特网的计算机或服务器，访问硬件管理控制台 Web 站点 (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)
2. 下载相应的 HMC V7 网络图像并将其保存在 FTP 服务器上。不能将这些文件直接下载到 HMC 上。必须将图像文件下载到接受 FTP 请求的服务器上。
3. 确保下载下列文件：
 - img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. 将升级数据保存在 HMC 上。执行以下命令行以保存升级数据：
 - 要将数据同时保存在 DVD 和 HDD 上，请执行以下命令：

```
mount /media/cdrom
```

```
saveupgdata -r diskdvd
```

- 要将数据保存在 HDD 上，请执行以下命令：

```
saveupgdata -r disk
```

5. 将升级文件复制到 HMC 上的可引导磁盘分区。运行 **getupgfiles** 命令以复制文件。

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

其中，

- **ftp server** 是您将 HMC 网络图像下载到的 FTP 服务器的主机名或 IP 地址。

- **user id** 是 FTP 服务器上的有效用户标识。如果您未使用 `--passwd` 参数指定密码，那么将提示您输入密码。
 - **remote directory** 是保存 HMC 网络图像的 FTP 服务器上的目录。
6. 重新引导 HMC 以升级复制到可引导磁盘分区的代码。运行 `chmc -c altdiskboot -s enable --mode upgrade` 以重新引导 HMC。
 7. 重新引导 HMC，然后启动升级。运行 `hmcshutdown -r -t now` 命令以启动升级。

HMC 端口位置

您可以通过使用位置代码查找部件位置。使用 HMC 端口位置图将位置代码映射至服务器上的 HMC 端口位置。

型号 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置

使用以下图和表来映射 8247-21L、8247-22L、8284-21A 或 8284-22A 上的 HMC 端口。

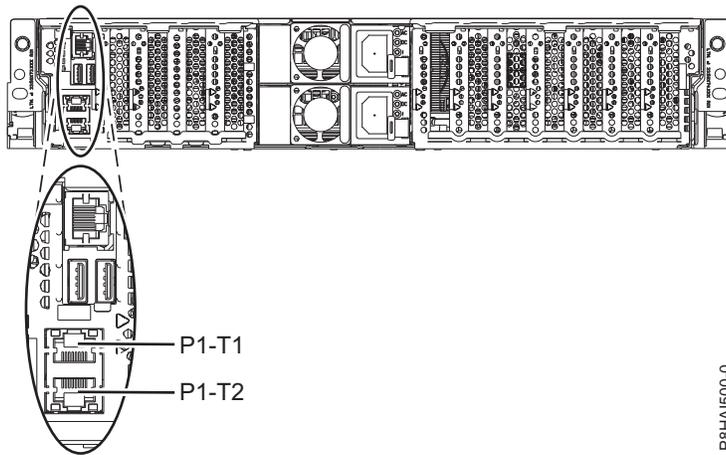


图 85. 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置

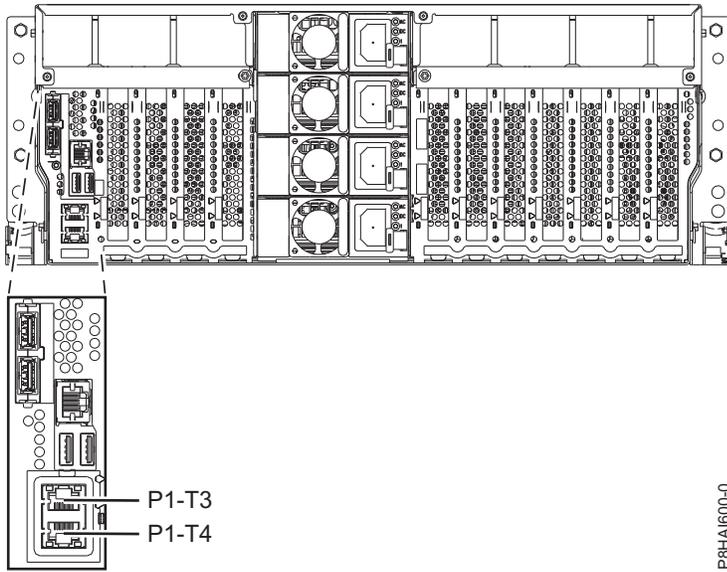
表 57. 8247-21L、8247-22L、8284-21A 或 8284-22A HMC 端口位置

端口	物理位置码	标识 LED
HMC 端口 1	Un-P1-T1	否
HMC 端口 2	Un-P1-T2	否

有关 8247-21L、8247-22L、8284-21A 或 8284-22A 上的 HMC 端口位置的更多信息，请参阅 8247-21L、8247-22L 或 8284-22A 的部件位置和位置码。

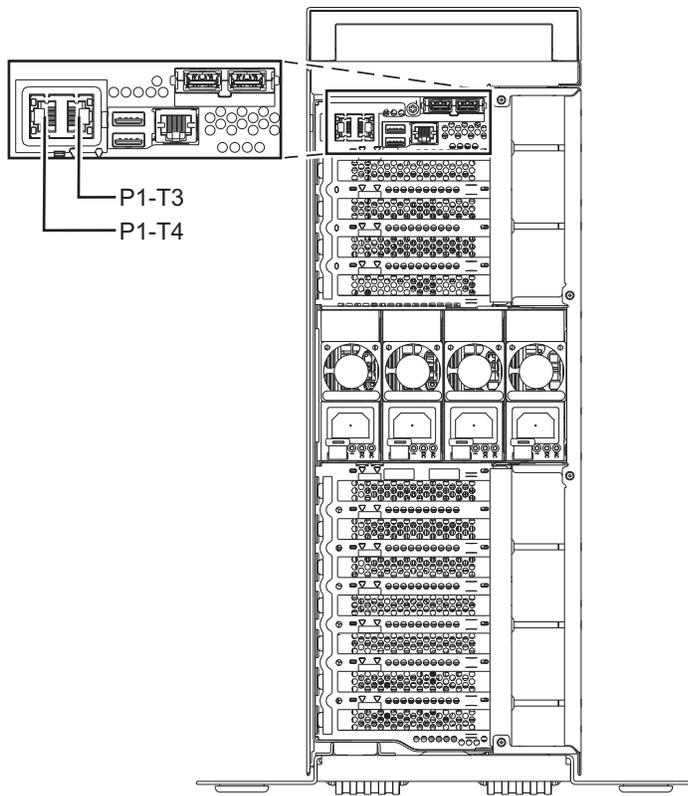
型号 8247-42L、8286-41A 或 8286-42A HMC 端口位置

使用以下图和表来映射 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口。



P8HA1600-0

图 86. 机架视图 - 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口位置



P8HA1700-0

图 87. 关于 8286-41A 上 HMC 端口位置的塔式机柜视图

表 58. 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口位置

端口	物理位置码	标识 LED
HMC 端口 1	Un-P1-T3	否
HMC 端口 2	Un-P1-T4	否

表 58. 8247-42L、8286-41A 或 8286-42A 上的 HMC 端口位置 (续)

端口	物理位置码	标识 LED
有关 8247-42L、8286-41A 或 8286-42A 上 HMC 端口位置的更多信息，请参阅 8247-42L、8286-41A 或 8286-42A 的部件位置和位置码。		

型号 9080-MHE、9080-MME、9119-MHE 和 9119-MME HMC 端口位置

使用以下图和表来映射 9080-MHE、9080-MME、9119-MHE 和 9119-MME 上的 HMC 端口。

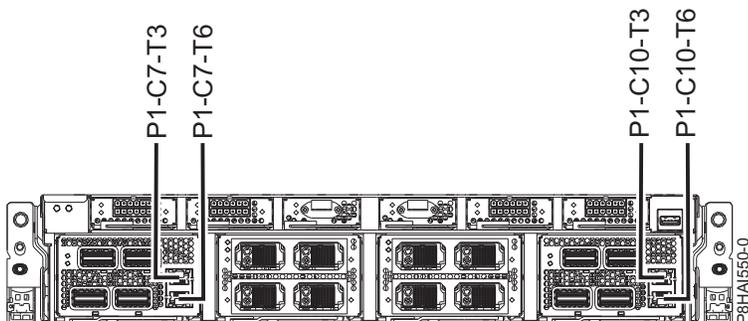


图 88. 9080-MHE、9080-MME、9119-MHE 和 9119-MME HMC 端口位置

表 59. 9080-MHE、9080-MME、9119-MHE 和 9119-MME HMC 端口位置

端口	物理位置码	标识 LED
服务处理器卡 1 - HMC 端口 1	Un-P1-C7-T3	否
服务处理器卡 1 - HMC 端口 2	Un-P1-C7-T6	否
服务处理器卡 2 - HMC 端口 1	Un-P1-C10-T3	否
服务处理器卡 2 - HMC 端口 2	Un-P1-C10-T6	否
有关 9080-MHE、9080-MME、9119-MHE 和 9119-MME 上的 HMC 端口位置的更多信息，请参阅 9080-MHE、9080-MME、9119-MHE 或 9119-MME 位置的部件位置和位置码。		

型号 8408-44E 和 8408-E8E HMC 端口位置

使用以下图和表来映射 8408-44E 和 8408-E8E 上的 HMC 端口。

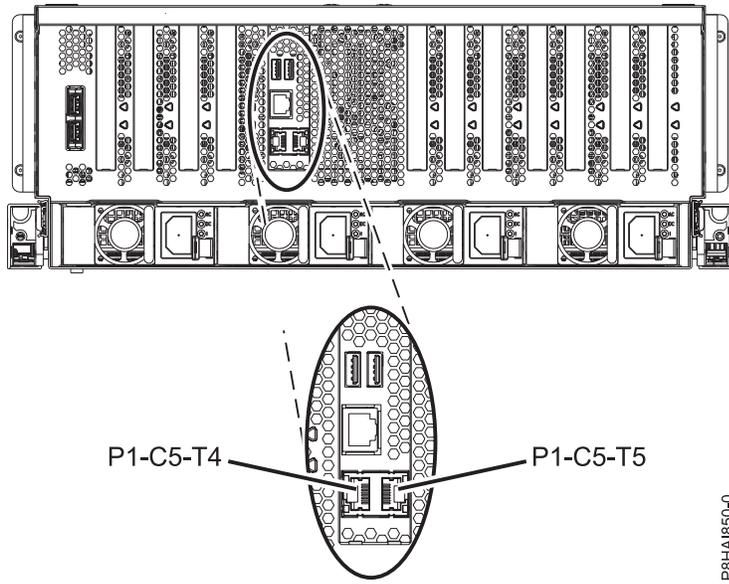


图 89. 8408-44E 和 8408-E8E HMC 端口位置

表 60. 8408-44E 和 8408-E8E HMC 端口位置

端口	物理位置码	标识 LED
HMC 端口 1	Un-P1-C5-T4	否
HMC 端口 2	Un-P1-C5-T5	否

有关 8408-44E 和 8408-E8E 上的 HMC 端口位置的更多信息，请参阅 8404-44E 和 8408-E8E 位置的部件位置和位置码。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在其他国家或地区不提供本文档中所讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。对于 IBM 产品、程序或服务的任何引用并非意在明示或默示只能使用该 IBM 产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务都可以用来代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，则由用户自行负责。

IBM 可能已拥有或正在申请与本文档中所描述主题有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄给：

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

INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供本出版物，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关非侵权、适销和适用于某特定用途的保证。某些管辖区域在某些事务中不允许免除明示或默示的保证，因此本声明可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本资料中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是本 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

所引用的性能数据和客户示例仅作参考用途。实际性能结果可能因特定的配置和操作条件而有所不同。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

显示的所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中的人物和业务企业与此相似，纯属巧合。

如果您正在查看本信息的软拷贝，图片和彩色图例可能无法显示。

在未获得 IBM 书面许可之前，不得部分或完全重新生成此处包含的图片和规格。

IBM 提供的此信息是为了与所指示的特定机器配合使用。IBM 对本出版物适用的任何其他用途不作任何陈述。

IBM 计算机系统内置了可减小未被发现的数据损坏或丢失几率的机制。但无法消除此风险。经历了意外中断、系统故障、电源波动或停电或者组件故障的用户必须验证中断或故障时或该时间附近所执行的操作以及保存或传输的数据的准确性。另外，用户必须制订一些过程来确保进行独立的数据验证，然后才在敏感操作或关键操作中信赖这些已验证的数据。用户应该定期查看 IBM 的支持 Web 站点以获取更新信息和适用于系统和相关软件的修正包。

认证声明

本产品可能在您的国家或地区未对通过任何方法到公共远程通信网络界面的连接进行验证。可能需要法律的进一步认证，才能进行所有的这些连接。如有任何疑问，请与 IBM 代表或经销商联系。

IBM Power Systems 服务器的辅助功能选项功能部件

辅助功能选项功能部件协助行动有障碍或视力不佳的用户成功使用信息技术内容。

概述

IBM Power Systems 服务器主要包含下列辅助功能选项功能部件：

- 全键盘操作
- 使用屏幕朗读器的操作

IBM Power Systems 服务器使用最新 W3C 标准 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) 以确保能够遵守 US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) 和 Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/)。如果要使用辅助功能选项功能部件，请使用您的屏幕朗读器的最新发行版以及 IBM Power Systems 服务器支持的最新版本的 Web 浏览器。

已在 IBM Knowledge Center 中为辅助功能选项启用 IBM Power Systems 服务器联机产品文档。将在 IBM Knowledge Center 帮助的"辅助功能选项"部分 (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility)中描述 IBM Knowledge Center 的辅助功能选项功能部件。

键盘导航

本产品使用标准导航键。

界面信息

IBM Power Systems 服务器用户界面不具备每秒闪烁 2 - 55 次的内容。

IBM Power Systems 服务器 Web 用户界面将使用级联样式表来恰当地呈现内容以及提供有用的体验。应用程序为弱视用户提供了一个相同方式来使用系统显示设置，其中包括高对比度模式。您可以通过使用设备或 Web 浏览器设置来控制字体大小。

IBM Power Systems 服务器 Web 用户界面包括了 WAI-ARIA 导航地标，您可以使用它在应用程序中快速导航至功能区域。

供应商软件

IBM Power Systems 服务器包含某种供应商软件，其未包括在 IBM 许可协议中。IBM 不会对这些产品的辅助功能选项功能部件作出任何表示。关于其产品的辅助功能选项信息，请联系供应商。

相关的辅助功能选项信息

除了标准 IBM 服务台和支持网站，IBM 还提供了以供聋人或听力有障碍的用户使用的 TTY 电话服务以便他们获得销售和支持服务：

TTY 服务

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

(北美地区)

有关 IBM 针对辅助功能选项的落实的更多信息，请参阅 IBM Accessibility (www.ibm.com/able)。

隐私声明注意事项

IBM 软件产品，其中包括“软件即服务”解决方案（软件产品），可使用 cookie 或者其他技术来收集产品使用情况信息，以帮助改进最终用户体验、调整与最终用户的交互或者用于其他目的。在许多情况下，软件产品不会收集任何个人可标识信息。某些软件产品可以帮助您收集个人可标识信息。如果此软件产品使用 cookie 来收集个人可标识信息，那么会在下面列出有关此产品使用 cookie 的特定信息。

根据所部署的配置，此软件产品可使用会话 cookie 来收集每个用户的用户名和 IP 地址，以进行会话管理。可以禁用这些 cookie，但同时将除去它们所启用的功能。

如果为此软件产品部署的配置使您能够作为客户通过 cookie 和其他技术从最终用户收集个人可标识信息，那么您应该自行对任何适用于该数据收集（其中包括声明和赞同的需求）的法律寻求法律咨询。

有关出于上述目的而使用各种技术（包括 cookie）的更多信息，请参阅 IBM 隐私声明（网址为 <http://www.ibm.com/privacy>）、IBM 在线隐私声明（网址为 <http://www.ibm.com/privacy/details>）中标题为“Cookie、Web Beacon 和其他技术”的部分以及“IBM 软件产品和软件即服务隐私声明”（网址为 <http://www.ibm.com/software/info/product-privacy>）。

商标

IBM、IBM 徽标和 [ibm.com](http://www.ibm.com) 是 International Business Machines Corp. 在全球范围内许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点 www.ibm.com/legal/copytrade.shtml 上“版权和商标信息”部分包含了 IBM 商标的最新列表。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft 和 Windows 是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

电子辐射声明

将监控器连接至设备时，必须使用指定的监控器电缆和随监控器提供的干扰抑制设备。

A 类声明

以下 A 类声明适用于包含 POWER8 处理器及其功能部件（除非功能部件信息中已将这些功能部件指定为电磁兼容性 (EMC) B 类）的 IBM 服务器。

联邦通信委员会 (FCC) 声明

注：This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against

harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

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

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

加拿大工业部一致性声明

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

欧盟一致性声明

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

European Community contact:

IBM Deutschland GmbH

Technical Regulations, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 800 225 5426

email: halloibm@de.ibm.com

警告：此为 A 类产品。在生活环境中，该产品可能会造成无线干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

VCCI 声明 - 日本

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

VCCI-A

以下是对上述框中 VCCI 日文版声明的总结：

根据 VCCI 委员会的标准，本产品属于 A 类产品。如果在生活环境中使用此设备，那么可能会造成无线电干扰。在这种情况下，可能需要用户采取修正措施。

日本電子和信息技术工业协会声明

此声明说明日本 JIS C 61000-3-2 产品功率合规性。

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

此声明说明适用于每相电流小于或等于 20 A 的产品的日本電子和信息技术工业协会 (JEITA) 声明。

高調波電流規格 JIS C 61000-3-2 適合品

此声明说明适用于单相电流大于 20 A 的产品 JEITA 声明。

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類：6（单相、PFC回路付）
- 換算係数：0

此声明说明适用于三相交流电中每相电流大于 20 A 的产品的 JEITA 声明。

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類：5（3相、PFC回路付）
- 換算係数：0

电磁干扰 (EMI) 声明 - 中华人民共和国

声 明

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

声明: 此为 A 类产品。在生活环境中, 该产品可能会造成无线干扰。在这种情况下, 可能需要用户对其干扰采取切实可行的措施。

电磁干扰 (EMI) 声明 - 台湾

警告使用者：

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

以下是上述 EMI 台湾版声明的摘要。

警告: 此为 A 类产品。在生活环境中, 该产品可能会造成无线干扰。在这种情况下, 可能需要用户对其干扰采取切实可行的措施。

IBM 台湾联系人信息:

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

电磁干扰 (EMI) 声明 - 韩国

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

德国一致性声明

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

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

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

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

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.

New Orchard Road

Armonk, New York 10504

Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH

Technical Relations Europe, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 (0) 800 225 5426

email: HalloIBM@de.ibm.com

Generelle Informationen:

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

电磁干扰 (EMI) 声明 - 俄罗斯

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

В 类声明

以下 В 类声明适用于功能部件安装信息中指定为电磁兼容性 (EMC) В 类的功能部件。

联邦通信委员会 (FCC) 声明

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

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

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

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

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

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

加拿大工业部一致性声明

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

欧盟一致性声明

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM

cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

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

VCCI 声明 - 日本

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

日本電子和信息技术工业协会声明

此声明说明日本 JIS C 61000-3-2 产品功率合规性。

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

此声明说明适用于每相电流小于或等于 20 A 的产品的日本电子和信息技术工业协会 (JEITA) 声明。

高調波電流規格 JIS C 61000-3-2 適合品

此声明说明适用于单相电流大于 20 A 的产品 JEITA 声明。

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類：6（单相、PFC回路付）
- 換算係数：0

此声明说明适用于三相交流电中每相电流大于 20 A 的产品的 JEITA 声明。

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類 : 5 (3相、PFC回路付)
- 換算係数 : 0

IBM 台湾联系人信息

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

德国一致性声明

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

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

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

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

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

Generelle Informationen:

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

条款和条件

只要遵守下列条款和条件，即授予对这些出版物的使用权限。

适用性：这些条款和条件是对 IBM 的 Web 站点的任何使用条款的补充。

个人使用：只要保留所有的专有权声明，您就可以为个人、非商业使用复制这些出版物。未经 IBM 明确许可，您不可以分发、显示或制作这些出版物或其中任何部分的演绎作品。

商业使用：只要保留所有的专有权声明，您就可以仅在企业内复制、分发和显示这些出版物。未经 IBM 明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

权利：在本许可权中除明示地授权以外，没有将其他许可权、许可证或权利（无论是明示的，还是默示的）授予其中包含的出版物或任何信息、数据、软件或其他知识产权。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，则 IBM 有权撤销本文授予的许可权。

您不可以下载、出口或再出口此信息，除非完全符合所有适用的法律和法规，包括所有美国出口法律和法规。

IBM 对这些出版物的内容不作任何保证。这些出版物以“按现状”的基础提供，不附有任何形式的（无论是明示的，还是默示的）保证，包括（但不限于）对非侵权性、适销性和适用于某特定用途的默示保证。



Printed in China