Power Systems

Instalación y configuración de la Hardware Management Console (HMC)

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información contenida en los apartados "Avisos de seguridad" en la página v y "Avisos" en la página 101, y en las publicaciones *IBM Systems Safety Notices*, G229-9054 e *IBM Environmental Notices and User Guide*, Z125–5823.

Esta edición hace referencia a IBM® Hardware Management Console Versión 9, Release 2, Nivel de mantenimiento 950, y a todos los releases subsiguientes hasta que se indique lo contrario en nuevas ediciones.

Contenido

Avisos de seguridad

A lo largo de toda esta guía encontrará diferentes avisos de seguridad:

- Los avisos de **PELIGRO** llaman la atención sobre situaciones que pueden ser extremadamente peligrosas o incluso letales.
- Los avisos de **PRECAUCIÓN** llaman la atención sobre situaciones que pueden resultar peligrosas debido a alguna circunstancia determinada.
- Los avisos de **Atención** indican la posibilidad de que se produzcan daños en un programa, en un dispositivo, en el sistema o en los datos.

Información de medidas de seguridad para comercio internacional

Varios países exigen que la información de medidas de seguridad contenida en las publicaciones de los productos se presente en el correspondiente idioma nacional. Si su país así lo exige, encontrará documentación de información de medidas de seguridad en el paquete de publicaciones (como en la documentación impresa, en el DVD o como parte del producto) suministrado con el producto. La documentación contiene la información de seguridad en el idioma nacional con referencias al idioma inglés de EE.UU. Antes de utilizar una publicación en inglés de EE.UU. para instalar, operar o reparar este producto, primero debe familiarizarse con la información de medidas de seguridad descrita en la documentación. También debe consultar la documentación cuando no entienda con claridad la información de seguridad expuesta en las publicaciones en inglés de EE.UU.

Puede obtener copias adicionales de la documentación de información de seguridad llamando a la línea directa de IBM al 1-800-300-8751.

Información sobre medidas de seguridad en alemán

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

Información sobre medidas de seguridad para láser

Los servidores de IBM pueden utilizar tarjetas de E/S o funciones que se basen en fibra óptica y utilicen láser o LED.

Conformidad del láser

Los servidores de IBM se pueden instalar dentro o fuera de un bastidor de equipo de tecnologías de la información.

PELIGRO: Cuando trabaje en el sistema o alrededor de él, tome las siguientes medidas de precaución:

El voltaje eléctrico y la corriente de los cables de alimentación, del teléfono y de comunicaciones son peligrosos. Para evitar un riesgo de descarga eléctrica: si IBM ha suministrado los cables de alimentación, conecte esta unidad utilizando sólo el cable proporcionado. No utilice el cable de alimentación proporcionado por IBM para ningún otro producto. No abra ningún conjunto de fuente de alimentación ni realice tareas de reparación en él. Durante una tormenta con aparato eléctrico, no conecte ni desconecte cables, ni realice tareas de instalación, mantenimiento o reconfiguración de este producto.

- 
Este producto puede estar equipado con múltiples cables de alimentación. Para evitar todo voltaje peligroso, desconecte todos los cables de alimentación. Para la alimentación CA, desconecte todos los cables de alimentación de la fuente de alimentación CA. Para bastidores con un

panel de distribución de alimentación (PDP) CC, desconecte la fuente de alimentación CC del cliente que hay en el PDP.

- Cuando suministre energía eléctrica al producto, asegúrese de que todos los cables de alimentación estén conectados correctamente. Para bastidores con alimentación CA, conecte todos los cables de alimentación o una toma de corriente eléctrico correctamente cableada y conectada a tierra. Asegúrese de que la toma de corriente eléctrica suministra el voltaje y la rotación de fases que figuran en la placa de características del sistema. Para bastidores con un panel de distribución de alimentación (PDP) CC, conecte la fuente de alimentación CC del cliente que hay en el PDP. Asegúrese de utilizar la polaridad adecuada a la hora de conectar la alimentación CC y el cableado de retorno de la alimentación CC.
- Conecte cualquier equipo que se conectará a este producto a tomas de corriente eléctrica debidamente cableadas.
- Cuando sea posible, utilice solo una mano para conectar o desconectar los cables de señal.
- No encienda nunca un equipo cuando haya indicios de fuego, agua o daño estructural.
- No encienda la máquina hasta que no se corrijan todas las posibles condiciones de peligro.
- Cuando realice una inspección de máquina: supongamos que existe un peligro de seguridad eléctrica. Realice todas las comprobaciones de continuidad, puesta a tierra y alimentación especificadas durante los procesos de instalación del subsistema para garantizar que se cumplen los requisitos de seguridad de la máquina. No intente activar la alimentación de la máquina hasta que se hayan corregido todas las posibles condiciones de riesgo. Antes de abrir el dispositivo, salvo que se indique lo contrario en los procedimientos de instalación y configuración: desconecte los cables de alimentación CA, apague los disyuntores correspondientes que hallará en el panel de distribución de alimentación (PDP) del bastidor y desconecte los sistemas de telecomunicaciones, redes y módems.
- Conecte y desconecte los cables tal como se indica en los siguientes procedimientos cuando instale, mueva o abra cubiertas en este producto o en los dispositivos conectados.

  Para desconectar: 1) Apague todo (a menos que se le indique lo contrario). 2) Para la alimentación CA, retire los cables de alimentación de las tomas de corriente eléctrica. 3) Para bastidores con un panel de distribución de alimentación (PDP) CC, apague los disyuntores que se hallan en el PDP y desconecte la alimentación de la fuente de alimentación CC del cliente. 4) Retire los cables de señal de los conectores. 5) Retire todos los cables de los dispositivos.

  Para conectar: 1) Apague todo (a menos que se le indique lo contrario). 2) Conecte todos los cables a los dispositivos. 3) Conecte los cables de señal a los conectores. 4) Para la alimentación CA, conecte los cables de alimentación a las tomas de corriente eléctrica. 5) Para bastidores con un panel de distribución de alimentación (PDP) CC, restablezca la energía de la fuente de alimentación CC del cliente y active los disyuntores que se hallan en el PDP. 6) Encienda los dispositivos.
-  Puede haber bordes, esquinas y uniones cortantes en el interior y exterior del sistema. Tenga cuidado cuando maneje el equipo para evitar cortes, arañazos y pellizcos. (D005)

(R001, parte 1 de 2):

PELIGRO: Tome las siguientes medidas de precaución cuando trabaje en el sistema en bastidor de TI o alrededor de él:

- El personal que manipula el equipo, si no sigue las medidas de seguridad, podría sufrir lesiones o causar daños en el equipo.
- Baje siempre los pies niveladores en el bastidor.
- Instale siempre las piezas de sujeción estabilizadoras en el bastidor, si las hay, a menos que deba instalar la opción contra terremotos.
- Para evitar situaciones peligrosas debido a una distribución desigual de la carga mecánica, instale siempre los dispositivos más pesados en la parte inferior del bastidor. Los servidores y dispositivos opcionales se deben instalar siempre empezando por la parte inferior del bastidor.
- Los dispositivos montados en el bastidor no se deben utilizar como repisas ni como espacios de trabajo. No coloque ningún objeto sobre los dispositivos montados en bastidor. Además, no se

apoye en los dispositivos montados en bastidor y no los utilice para estabilizar la posición de su cuerpo (por ejemplo, cuando trabaje en una escalera).

- Riesgos relacionados con la estabilidad:
  - El bastidor puede volcarse y ocasionar daños graves.
  - Antes de extender el bastidor en la posición de instalación, lea las instrucciones de montaje.
  - No coloque ninguna carga en el equipo de montaje con rieles de deslizamiento montado en la posición de instalación.
  - No deje montado el equipo de montaje con rieles de deslizamiento en la posición de instalación.
- En cada bastidor podría haber más de un cable de alimentación.
  - Para bastidores con alimentación CA, no olvide desconectar todos los cables de alimentación del bastidor cuando se le indique que desconecte la energía eléctrica mientras realiza tareas de servicio.
  - Para bastidores con un panel de distribución de alimentación (PDP) CC, apague el disyuntor que controla la alimentación en las unidades del sistema, o desconecte la fuente de alimentación CC del cliente, cuando se le indique que desconecte la alimentación mientras esté manipulando el dispositivo.
- Conecte todos los dispositivos instalados en un bastidor a los dispositivos de alimentación instalados en ese mismo bastidor. No conecte un cable de alimentación de un dispositivo instalado en un bastidor a un dispositivo de alimentación instalado en un bastidor distinto.
- Una toma de corriente eléctrica que no esté cableada correctamente podría ocasionar un voltaje peligroso en las partes metálicas del sistema o de los dispositivos que se conectan al sistema. Es responsabilidad del cliente asegurarse de que la toma de corriente eléctrica está debidamente cableada y conectada a tierra para evitar una descarga eléctrica. (R001, parte 1 de 2)

(R001, parte 2 de 2):

PRECAUCIÓN:

- No instale una unidad en un bastidor en el que las temperaturas ambientales internas vayan a superar las temperaturas ambientales recomendadas por el fabricante para todos los dispositivos montados en el bastidor.
- No instale una unidad en un bastidor en el que la circulación del aire pueda verse comprometida. Asegúrese de que no hay ningún obstáculo que bloquee o reduzca la circulación del aire en cualquier parte lateral, frontal o posterior de una unidad que sirva para que el aire circule a través de la unidad.
- Hay que prestar atención a la conexión del equipo con el circuito de suministro eléctrico, para que la sobrecarga de los circuitos no comprometa el cableado del suministro eléctrico ni la protección contra sobretensión. Para proporcionar la correcta conexión de alimentación a un bastidor, consulte las etiquetas de valores nominales situadas en el equipo del bastidor para determinar la demanda energética total del circuito eléctrico
- *(Para cajones deslizantes).* No retire ni instale cajones o dispositivos si las piezas de sujeción estabilizadoras no están sujetas al bastidor o si el bastidor no está atornillado al suelo. No abra más de un cajón a la vez. El bastidor se puede desequilibrar si se tira de más de un cajón a la vez.

- *(Para cajones fijos).* Este es un cajón fijo que no se debe mover al realizar tareas de servicio, a menos que así lo especifique el fabricante. Si se intenta sacar el cajón de manera parcial o total, se corre el riesgo de que el cajón se caiga al suelo o de que el bastidor se desestabilice. (R001, parte 2 de 2)

PRECAUCIÓN: Para mejorar la estabilidad del bastidor al cambiarlo de ubicación, conviene quitar los componentes situados en las posiciones superiores del armario del bastidor. Siempre que vaya a cambiar la ubicación de un bastidor para colocarlo en otro lugar de la sala o del edificio, siga estas directrices generales.

- Reduzca el peso del bastidor quitando dispositivos, empezando por la parte superior del armario del bastidor. Siempre que sea posible, restablezca la configuración del bastidor para que sea igual a como lo recibió. Si no conoce la configuración original, debe tomar las siguientes medidas de precaución:
  - Quite todos los dispositivos de la posición 32 U y superiores.
  - Asegúrese de que los dispositivos más pesados están instalados en la parte inferior del bastidor.
  - Asegúrese de que haya pocos o ningún nivel U vacío entre los dispositivos instalados en el bastidor por debajo del nivel 32 U, a menos que la configuración recibida lo permita específicamente.
- Si el bastidor que se propone cambiar de lugar forma parte de una suite de bastidores, desenganche el bastidor de la suite.
- Si el bastidor que se propone cambiar de lugar se ha suministrado con estabilizadores extraíbles, deberán reinstalarse antes de cambiar de lugar el bastidor.
- Inspeccione la ruta que piensa seguir para eliminar riesgos potenciales.
- Verifique que la ruta elegida puede soportar el peso del bastidor cargado. En la documentación que viene con el bastidor encontrará el peso que tiene un bastidor cargado.
- Verifique que todas las aberturas de las puertas sean como mínimo de 760 x 2083 mm (30 x 82 pulgadas).
- Asegúrese de que todos los dispositivos, repisas, cajones, puertas y cables están bien sujetos.
- Compruebe que los cuatro pies niveladores están levantados hasta la posición más alta.
- Verifique que no hay ninguna pieza de sujeción estabilizadora instalada en el bastidor durante el movimiento.
- No utilice una rampa inclinada de más de 10 grados.
- Cuando el armario del bastidor ya esté en la nueva ubicación, siga estos pasos:
  - Baje los cuatro pies niveladores.
  - Instale las piezas de sujeción estabilizadoras en el bastidor o en un entorno apto para terremotos atornille el bastidor al suelo.
  - Si ha quitado dispositivos del bastidor, vuelva a ponerlos, desde la posición más baja a la más alta.

- Si se necesita un cambio de ubicación de gran distancia, restablezca la configuración del bastidor para que sea igual a como lo recibió. Empaquete el bastidor en el material original o un material equivalente. Asimismo, baje los pies niveladores para que las ruedas giratorias no hagan contacto con el palé, y atornille el bastidor al palé.

(R002)

(L001)

PELIGRO: Existen niveles de energía, corriente o voltaje peligrosos dentro de los componentes que tienen adjunta esta etiqueta. No abra ninguna cubierta o barrera que contenga esta etiqueta. (L001)

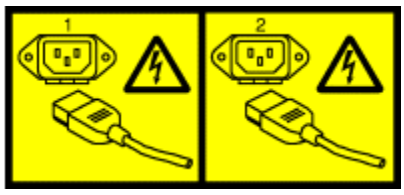
(L002)

PELIGRO: Los dispositivos montados en el bastidor no se deben utilizar como repisas ni como espacios de trabajo. No coloque ningún objeto sobre los dispositivos montados en bastidor. Además, no se apoye en los dispositivos montados en bastidor y no los utilice para estabilizar la posición de su cuerpo (por ejemplo, cuando trabaje desde una escalera). Riesgos relacionados con la estabilidad:

- El bastidor puede volcarse y ocasionar daños graves.
- Antes de extender el bastidor en la posición de instalación, lea las instrucciones de montaje.
- No coloque ninguna carga en el equipo de montaje con rieles de deslizamiento montado en la posición de instalación.
- No deje montado el equipo de montaje con rieles de deslizamiento en la posición de instalación.

(L002)

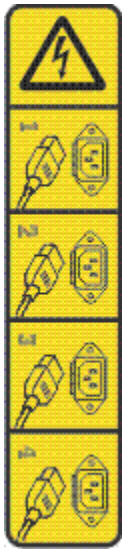
(L003)



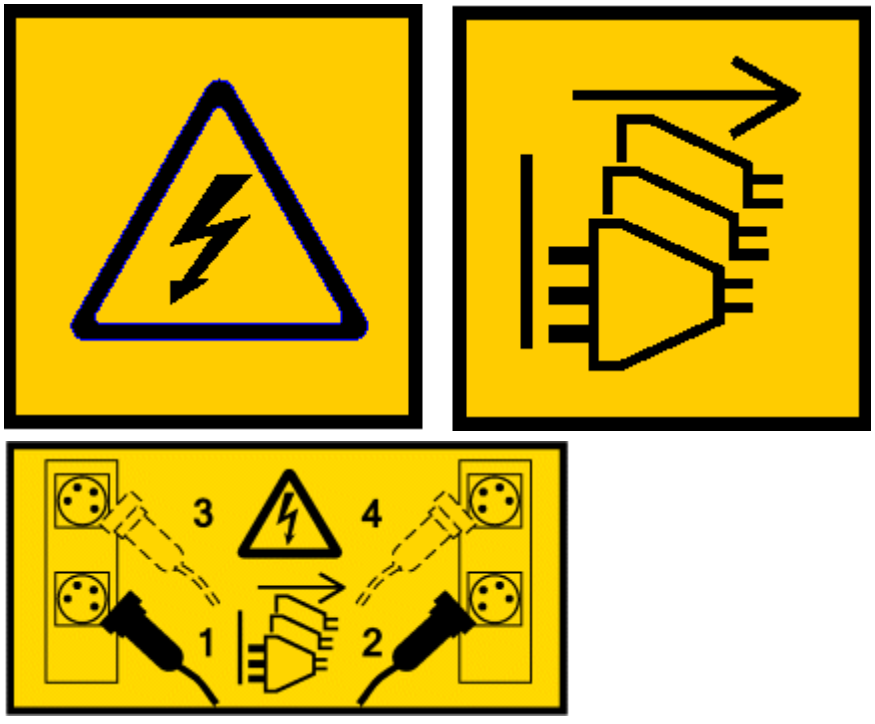
o

o

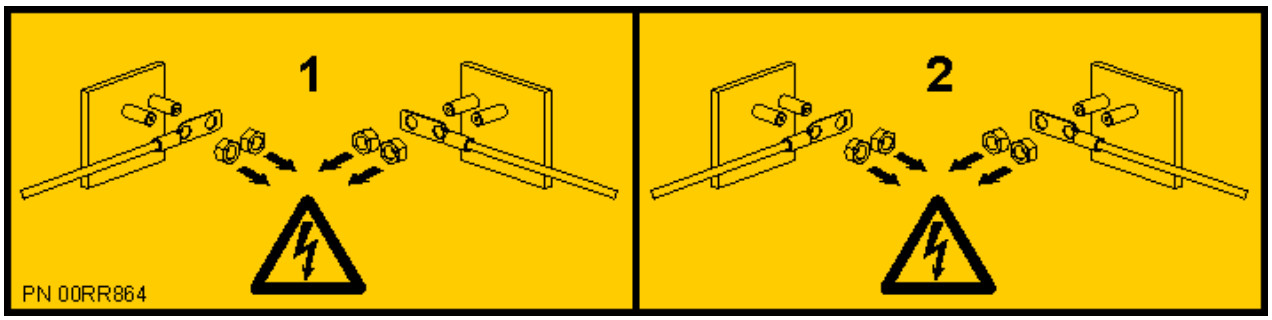
o



o



x Power Systems: Instalación y configuración de la Hardware Management Console (HMC)



PELIGRO: Varios cables de alimentación. El producto puede estar equipado con múltiples cables de alimentación CA o múltiples cables de alimentación CC. Para evitar todo voltaje peligroso, desconecte todos los cables de alimentación. (L003)

(L007)

PRECAUCIÓN: Una superficie caliente cerca. (L007)

(L008)

PRECAUCIÓN: Piezas peligrosas en movimiento cerca. (L008)

En EE.UU., todo láser tiene certificación de estar en conformidad con los requisitos de DHHS 21 CFR Subcapítulo J para productos láser de clase 1. Fuera de EE.UU., el láser tiene certificación de estar en conformidad con IEC 60825 como producto láser de clase 1. En la etiqueta de cada pieza encontrará los números de certificación de láser y la información de aprobación.

PRECAUCIÓN: Este producto puede contener uno o varios de estos dispositivos: unidad de CD-ROM, unidad de DVD-ROM, unidad de DVD-RAM o módulo láser, que son productos láser de Clase 1. Tenga en cuenta estas medidas de precaución:

- No quite las cubiertas. Si se quitan las cubiertas del producto láser, existe el riesgo de exposición a radiación láser peligrosa. Dentro del dispositivo no hay piezas que se puedan reparar.
- El uso de controles o ajustes o la realización de procedimientos distintos de los especificados aquí podría provocar una exposición a radiaciones peligrosas.

(C026)

PRECAUCIÓN: Los entornos de proceso de datos pueden contener equipo cuyas transmisiones se realizan en enlaces del sistema con módulos láser que funcionen a niveles de potencia superiores a los de Clase 1. Por este motivo, no debe mirar nunca hacia el extremo de un cable de fibra óptica ni hacia un receptáculo abierto. Aunque aplicar luz en un extremo de un cable de fibra óptica desconectado y mirar por el otro extremo para verificar su continuidad podría no dañar la vista, este procedimiento es potencialmente peligroso. Por tanto no se recomienda verificar la continuidad de los cables de fibra óptica aplicando luz en un extremo y mirando por el otro. Para

verificar la continuidad de un cable de fibra óptica, utilice una fuente de luz óptica y un medidor de intensidad. (C027)

PRECAUCIÓN: Este producto contiene un láser de Clase 1M. No hay que mirar directamente con instrumentos ópticos. (C028)

PRECAUCIÓN: Algunos productos láser contienen un diodo láser incorporado de Clase 3A o Clase 3B. Tenga en cuenta estas medidas de precaución:

- Emite radiación láser al abrirlo.
- No fije la mirada en el haz, no lo mire directamente con instrumentos ópticos y evite la exposición directa al haz. (C030)

(C030)

PRECAUCIÓN: La batería contiene litio. No debe quemar ni cargar la batería para evitar la posibilidad de una explosión.

No debe:

- Echarla ni sumergirla en agua
- Exponerla a más de 100 grados C (212 grados F)
- Repararla ni desmontarla

Solo debe cambiarla por una pieza autorizada por IBM. Para reciclar o desechar la batería, debe seguir las instrucciones de la normativa local vigente. En Estados Unidos, IBM tiene un proceso de recogida de estas baterías. Para obtener información, llame al número 1-800-426-4333. En el momento de llamar, tenga a mano el número de pieza IBM de la unidad de la batería. (C003)

PRECAUCIÓN: HERRAMIENTA DE ELEVACIÓN DEL PROVEEDOR proporcionada por IBM:

- La HERRAMIENTA DE ELEVACIÓN sólo debe utilizarla personal autorizado.
- La HERRAMIENTA DE ELEVACIÓN está destinada a ayudar, levantar, instalar y retirar unidades (carga) en elevaciones de bastidor. No es para utilizarla cargada como transporte por grandes rampas ni como sustitución de herramientas como elevadores de palés, transceptores de radio portátil, carretillas elevadoras y en las situaciones de reubicación relacionadas. Cuando esto no sea factible, deben utilizarse servicios o personas con formación especial (por ejemplo, montadores o transportistas).
- Lea y asegúrese de comprender el contenido del manual del operador de la HERRAMIENTA DE ELEVACIÓN antes de utilizarla. Si no lo lee, si no entiende lo que en él se explica, si no hace caso de las normas de seguridad y si no sigue las instrucciones puede provocar daños en la propiedad o lesiones personales. Si tiene alguna consulta, póngase en contacto con el servicio técnico del proveedor y con el personal de soporte del proveedor. El manual impreso en el idioma local debe permanecer junto con la máquina en la zona de almacenamiento protegida indicada. La última revisión del manual está disponible en el sitio web del proveedor.
- Compruebe el funcionamiento del freno del estabilizador antes de cada uso. No fuerce el movimiento o el rodamiento de la HERRAMIENTA DE ELEVACIÓN con el freno estabilizador puesto.
- No eleve, baje ni deslice la repisa de carga de la plataforma a no ser que el estabilizador (gato del pedal de freno) esté completamente metido. Mantenga puesto el freno del estabilizador siempre que la unidad no se encuentre en uso o movimiento.
- No mueva la HERRAMIENTA DE ELEVACIÓN mientras la plataforma esté levantada, excepto para cambios mínimos de posición.
- No supere la capacidad de carga aprobada. Consulte el GRÁFICO DE CAPACIDAD DE CARGA para ver las cargas máximas en el centro y en el borde de la plataforma extendida.
- Levante sólo la carga si está bien centrada en la plataforma. No coloque más de 200 libras (91 kg) en el borde de la repisa de la plataforma deslizante, teniendo en cuenta el centro de masa/gravedad (CoG) de la carga.

- No coloque de forma descentralizada las plataformas, el elevador de inclinación, la cuña de instalación de la unidad con ángulo u otra opción de accesorio. Proteja estas plataformas; las opciones de elevador de inclinación, cuña, etc. de la repisa elevadora principal o de las carretillas en las cuatro ubicaciones (4x o todo el demás montaje suministrado) sólo con hardware suministrado, antes de utilizarlas. Los objetos de carga han sido pensados para que se deslicen por plataformas lisas sin tener que ejercer ningún tipo de fuerza; por tanto, vaya con cuidado de no aplicar presión ni apoyarse en ellos. Mantenga la opción elevadora de inclinación [plataforma con ángulo ajustable] plana salvo para pequeños ajustes de ángulo en último momento, si fueran necesarios.
- No se sitúe bajo una carga que cuelgue de un lugar alto.
- No utilice la herramienta en una superficie irregular, inclinada o en pendiente (grandes rampas).
- No apile las cargas.
- No utilice la herramienta bajo la influencia de drogas o alcohol.
- No apoye la escalera de mano en la HERRAMIENTA DE ELEVACIÓN (a menos que se proporcione la dotación específica para uno de los procedimientos cualificados siguientes para trabajar en elevaciones con esta HERRAMIENTA).
- Peligro de volcado. No se apoye ni empuje la carga con la plataforma elevada.
- No utilice la herramienta como banco o plataforma de elevación del personal. Prohibido subir a personas.
- No permanezca de pie encima de ninguna parte del elevador. No es una escalera.
- No suba al mástil.
- No utilice una máquina de HERRAMIENTA DE ELEVACIÓN dañada o que no funcione correctamente.
- Peligro de ser aplastado o de quedar atrapado bajo la plataforma. Baje la carga solamente en zonas donde no haya personal ni ninguna obstrucción. Mantenga las manos y los pies alejados durante el uso.
- No utilice carretillas elevadoras. No levante nunca ni mueva la máquina de la HERRAMIENTA DE ELEVACIÓN con una elevación de horquillas, gato o carretilla de palés.
- El mástil tiene más altura que la plataforma. Tenga cuidado con la altura del techo, las bandejas de cables, los aspersores, las luces y otros objetos elevados.
- No deje desatendida la máquina de la HERRAMIENTA DE ELEVACIÓN con una carga elevada.
- Actúe con cuidado y mantenga alejadas las manos, los dedos y la ropa cuando el equipo esté en movimiento.
- Utilice sólo la fuerza de la mano para girar el cabrestante. Si el asa del cabrestante no puede girarse fácilmente con una mano, posiblemente es que hay una sobrecarga. No siga girando el cabrestante cuando llegue al límite máximo o mínimo de desplazamiento de la plataforma. Si se desenrolla demasiado, se separará el asa y se deteriorará el cable. Sujete siempre el asa cuando realice las acciones de aflojar o desenrollar. Asegúrese de que el cabrestante aguante la carga antes de soltar el asa del cabrestante.
- Un accidente ocasionado por un cabrestante podría provocar daños importantes. No sirve para mover personas. Asegúrese de haber oído un chasquido que indica que se ha levantado el equipo. Asegúrese de que el cabrestante quede bloqueado en su lugar antes de soltar el asa. Lea la página de instrucciones antes de utilizar este cabrestante. No permita nunca que el cabrestante se desenrolle solo. Un uso inadecuado puede provocar que el cable se enrolle de forma irregular en el tambor del cabrestante, puede dañar al cable y puede provocar lesiones importantes.
- Esta HERRAMIENTA debe mantenerse correctamente para que la utilice el personal de servicio de IBM. IBM inspeccionará el estado y verificará el historial de mantenimiento antes de su funcionamiento. El personal se reserva el derecho a no utilizar la HERRAMIENTA si no la considera adecuada. (C048)

Información de alimentación y cableado para NEBS (Network Equipment-Building System) GR-1089-CORE

Los comentarios siguientes se aplican a los servidores de IBM diseñados en conformidad con la especificación NEBS (Network Equipment-Building System) GR-1089-CORE:

El equipo es adecuado para instalarlo en:

- Recursos de telecomunicaciones de red
- Ubicaciones donde se aplique el NEC (Código eléctrico nacional)

Los puertos internos de este equipo son adecuados solamente para la conexión al cableado interno o protegido. Los puertos internos de este equipo *no* deben conectarse metálicamente a las interfaces que se conectan a la planta exterior o su cableado. Estas interfaces se han diseñado para su uso solo como interfaces internas al edificio (puertos de tipo 2 o de tipo 4, tal como se describe en GR-1089-CORE) y requieren el aislamiento del cableado de planta exterior al descubierto. La adición de protectores primarios no ofrece protección suficiente para conectar estas interfaces con material metálico a los cables de la OSP.

Nota: todos los cables Ethernet deben estar recubiertos y tener toma de tierra en ambos extremos.

El sistema que se alimenta con CA no requiere el uso de un dispositivo de protección contra descargas (SPD) externo.

El sistema que se alimenta con CC utiliza un diseño de retorno de CC aislado (DC-I). El terminal de retorno de la batería de CC *no* debe conectarse ni al chasis ni a la toma de tierra.

El sistema de alimentación CC es para que se instale en una red CBN (Common Bonding Network - red de acoplamiento común) tal como se describe en GR-1089-CORE.

Instalación y configuración de la Hardware Management Console

Aprenda a instalar el hardware de la Hardware Management Console (HMC), conectarlo al sistema gestionado y configurarlo para su uso. Puede realizar usted mismo esas tareas o bien ponerse en contacto con un proveedor de servicios para encargarle que las realice. El proveedor de servicios podría pedirle honorarios por este servicio.

Novedades en la instalación y configuración de la HMC

Se incluye la información sobre las novedades o los cambios significativos en el tema que trata sobre la instalación y la configuración de la HMC respecto a la actualización anterior de la colección de temas.

Abril de 2021

- Se han añadido los temas siguientes:
  - “Instalación de la HMC de IBM Power Systems (7063-CR2) en un bastidor” en la página 4
  - “Requisitos previos para instalar el sistema 7063-CR2 montado en bastidor” en la página 4
  - “Completar inventario para el sistema” en la página 5
  - “Determinación y marca de la ubicación en el bastidor para el sistema 7063-CR2 ” en la página 5
  - “Fijación de los rieles ajustables al chasis del sistema y al bastidor” en la página 7
  - “Fijación de los rieles fijos al chasis del sistema y al bastidor” en la página 9
  - “Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación” en la página 10
  - “Cableado de la HMC 7063-CR2 montada en bastidor” en la página 11
  - “Configuración de la HMC 7063-CR2” en la página 12

Noviembre de 2020

- Se han actualizado los siguientes temas:
  - “Tareas de instalación y configuración” en la página 2
  - “Protección de la HMC” en la página 88
  - “Ubicaciones de los puertos de la HMC” en la página 96

Julio de 2020

- Se han actualizado los siguientes temas:
  - “Instalación del dispositivo virtual de la HMC ” en la página 25
  - “Ubicaciones de los puertos de la HMC” en la página 96

Octubre de 2019

- Se han actualizado los siguientes temas:
  - “Instalación del dispositivo virtual de la HMC ” en la página 25
  - “Protección de la HMC” en la página 88

Febrero de 2019

- Se han añadido los temas siguientes:
  - “Protección de la HMC” en la página 88
  - “Política de contraseñas ampliada” en la página 90
  - “Cómo resolver problemas comunes al fijar la HMC” en la página 93
  - “Perfiles de seguridad: Reglamento general de protección de datos (RGPD) y Normas de Seguridad de Datos para la Industria de tarjetas de pago (PCI-DSS) ” en la página 92

Agosto de 2018

- Se han actualizado los siguientes temas:
  - “Configuración de la HMC 7063-CR1” en la página 22
  - “Ubicaciones de los puertos de la HMC” en la página 96

Diciembre de 2017

- Se ha añadido información para los servidores IBM Power Systems que contienen el procesador POWER9.

Tareas de instalación y configuración

Conozca las tareas que están asociadas con diferentes tareas de instalación y configuración de la HMC.

Conozca, en un alto nivel, las tareas que debe completar cuando instale y configure la HMC. Puede instalar y configurar la HMC de diferentes formas. Busque la situación que mejor se ajuste a la tarea que desee completar.

Notas:

- Si está gestionando servidores basados en el procesador POWER9, la HMC debe ser la versión 9.1.0 o posterior. Para obtener más información, consulte “Determinar la versión y el release del código de máquina de la HMC” en la página 77.
- La Hardware Management Console Versión 9.2.950, o posterior, no está soportada en el tipo de máquina HMC 7042. Para obtener más información sobre las versiones de HMC para la HMC 7042, consulte las notas del release de HMC disponibles en el sitio web Fix Central.

Instalar y configurar una nueva HMC con un nuevo servidor

Información adicional sobre las tareas de nivel superior que debe completar al instalar y configurar una nueva HMC con un nuevo servidor.

Tabla 1. Tareas que debe completar al instalar y configurar una nueva HMC con un nuevo servidor

Tarea	**Dónde encontrar información relacionada**
1. Reúna información y complete la hoja de trabajo de configuración de preinstalación.	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48 “Preparar la configuración de la HMC” en la página 46
2. Desempaquete el hardware.	
3. Cablee el hardware de la HMC.	“Cableado de la HMC 7063-CR1 montada en bastidor” en la página 20
4. Power en la HMC pulsando el botón de encendido.	

Tabla 1. Tareas que debe completar al instalar y configurar una nueva HMC con un nuevo servidor (continuación)	
Tarea	**Dónde encontrar información relacionada**
5. Inicie la sesión e inicie la aplicación web de la HMC.	
6. Acceda al asistente de configuración guiada o utilice los menús para configurar la HMC.	"Configurar la HMC utilizando la vía de acceso rápida a través del asistente de instalación guiada" en la página 55 "Configuración de la HMC utilizando los menús" en la página 55
7. Conecte el servidor a la HMC.	

Actualizar y ampliar el código de la HMC

Información adicional sobre las tareas de nivel superior que debe completar al actualizar y ampliar el código de la HMC.

Si dispone de una HMC y desea actualizar o ampliar su código, debe completar las siguientes tareas de nivel superior:

Tabla 2. Tareas que debe completar al actualizar o configurar código HMC	
Tarea	**Dónde encontrar información relacionada**
1. Obtenga la actualización.	"Actualización del software de la HMC" en la página 83
2. Vea el nivel de código de máquina de la HMC existente.	
3. Haga una copia de seguridad de los datos de perfil del sistema gestionado.	
4. Haga una copia de seguridad de los datos de la HMC.	
5. Anote la información de configuración actual de la HMC.	
6. Anote el estado del mandato remoto.	
7. Guarde los datos de la actualización.	
8. Amplíe el software de la HMC.	
9. Verifique que la ampliación de código de máquina de la HMC se ha instalado satisfactoriamente.	

Añadir una segunda HMC a una instalación

Información adicional sobre las tareas de nivel superior que debe completar al añadir una segunda HMC al sistema gestionado.

Si dispone de una HMC y un sistema gestionado y desea añadir una segunda HMC a esta configuración, realice los pasos siguientes:

Tabla 3. Tareas que debe completar cuando se añade una segunda HMC a una instalación existente	
Tarea	**Dónde encontrar información relacionada**
1. Asegúrese de que el hardware de la HMC dé soporte al código de la HMC versión 7.	
2. Reúna información y complete la hoja de trabajo de configuración de preinstalación.	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48
3. Desempaquete el hardware.	
4. Cablee el hardware de la HMC.	“Cableado de la HMC 7063-CR1 montada en bastidor” en la página 20
5. Power en la HMC pulsando el botón de encendido.	
6. Inicie una sesión en la HMC.	
7. Los niveles de código de la HMC deben coincidir. Cambie el código en una de las HMC para que coincida con el código de la otra HMC.	“Determinar la versión y el release del código de máquina de la HMC” en la página 77 “Actualización del software de la HMC” en la página 83
8. Acceda al Asistente de configuración guiada o utilice los menús para configurar la HMC.	“Configuración de la HMC utilizando los menús” en la página 55
9. Configure esta HMC para servicio utilizando el asistente de configuración del centro de servicio.	“Configuración de la HMC para que se pueda conectar con servicio y soporte utilizando el asistente de configuración de llamada al centro de servicio ” en la página 70
10. Conecte el servidor a la HMC.	

Instalación de la HMC

Antes de configurar el software de la HMC es necesario instalar su hardware. Hay más información sobre la configuración de una HMC de sobremesa o una HMC montada en bastidor.

Instalación de la HMC de IBM Power Systems (7063-CR2) en un bastidor

Aprenda a instalar la HMC de IBM Power Systems (7063-CR2) en un bastidor.

Puede ver la documentación de instalación en línea o puede imprimir la versión en PDF con la misma información. Para ver o imprimir la versión en PDF, consulte Instalación y configuración de la Hardware Management Console.

Requisitos previos para instalar el sistema 7063-CR2 montado en bastidor

Utilice la información para comprender los requisitos previos que son necesarios para instalar el sistema.

Acerca de esta tarea

PRECAUCIÓN: Esta es una pieza o una unidad pesada, pero su peso es menor que 18 kg (39,7 libras). Tome precauciones cuando se disponga a levantar, quitar o instalar esta pieza o esta unidad. (C008)

Se recomienda leer los siguientes documentos antes de empezar a instalar el servidor:

- La versión más reciente de este documento se mantiene en línea, consulte Instalación de 7063-CR2 en un bastidor (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm).
- Para planificar la instalación del servidor, consulte Planificación de hardware y de ubicaciones.

Procedimiento

1. Asegúrese de que tiene los siguientes elementos antes de empezar la instalación:
   - Destornillador de estrella de tamaño 2
   - Destornillador de cabeza plana
   - Destornillador T25
   - Cortador para cartón
   - Muñequera antiestática de descarga electrostática (ESD)
   - Bastidor con una unidad de espacio EIA (Electronic Industries Association) (1U).

   Notas:

   - Si no tiene un bastidor instalado, instálelo. Para obtener instrucciones, consulte Bastidores y dispositivos de bastidor (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).
   - Las calificaciones de la fuente de alimentación son 100 a 127 V CA, 9 A (x2), 200 a 240 V CA, 4,5 A (x2); 50 o 60 Hz.
2. Continúe con “Completar inventario para el sistema” en la página 5.

Completar inventario para el sistema

Utilice esta información para completar el inventario para el sistema.

Procedimiento

1. Verifique que ha recibido todas las cajas que ha solicitado.
2. Desembale los componentes de servidor según sea necesario.
3. Elabore un inventario de piezas y verifique que haya recibido todas las piezas que ha solicitado antes de instalar cada componente del servidor.

   Nota:

   La información del pedido se incluye en el producto. Puede también obtener información sobre su pedido a partir del representante de ventas o IBM Business Partner.

   Si hay componentes incorrectos o dañados, o faltan componentes, utilice cualquiera de los recursos siguientes:

   - El distribuidor de IBM.
   - Línea de información automatizada de fabricación de IBM Rochester, número 1-800-300-8751 (sólo Estados Unidos).
   - Sitio web de Directorio de contactos a nivel mundial, Directory of worldwide contacts website (http://www.ibm.com/planetwide). Seleccione la localidad para ver la información de contacto de servicio y soporte.
4. Continúe con “Determinación y marca de la ubicación en el bastidor para el sistema 7063-CR2 ” en la página 5.

Determinación y marca de la ubicación en el bastidor para el sistema 7063-CR2

Debe determinar dónde instalar la unidad del sistema en el bastidor.

Procedimiento

1. Lea los Avisos de seguridad del bastidor (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Determine el lugar donde se va a colocar la unidad del sistema en el bastidor. Cuando planifique la instalación de la unidad del sistema en un bastidor, tenga en cuenta la información siguiente:
   - Organice las unidades más grandes y más pesadas en la parte inferior del bastidor.
   - Planifique instalar primero las unidades del sistema en la parte inferior del bastidor.
   - Anote las ubicaciones EIA (Electronic Industries Alliance) en el plan.
3. Si es necesario, extraiga los paneles de relleno para permitir el acceso al interior del alojamiento del bastidor donde tenga previsto colocar la unidad, tal como se muestra en la Figura 1 en la página 6.

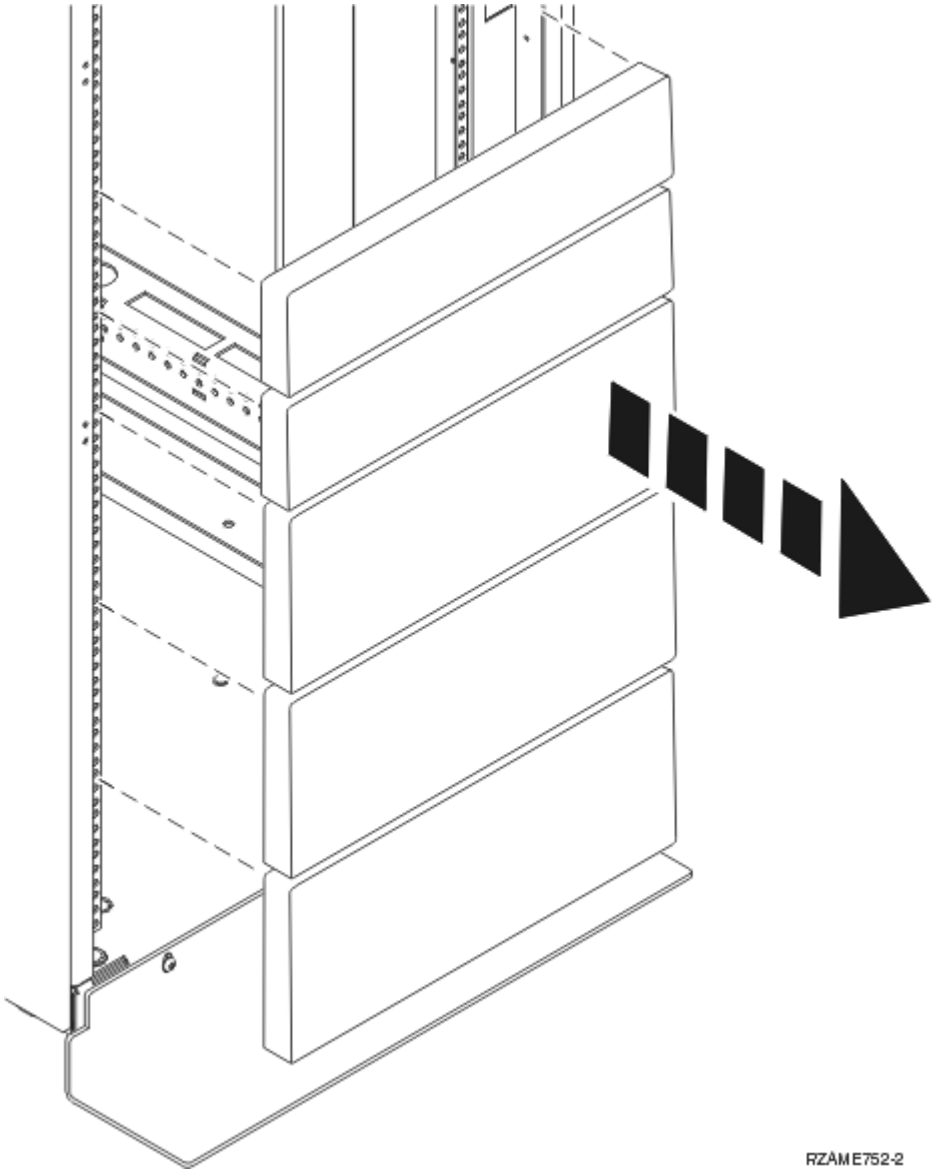


Figura 1. Extracción de los paneles de relleno

4. Determine dónde colocar el sistema en el bastidor. Tome nota de la ubicación de EIA.
5. Con la parte frontal del bastidor orientada hacia usted y comenzando por el lado derecho, utilice una cinta, un rotulador o un lápiz para marcar el agujero inferior de esta unidad EIA.
6. Repita el paso "5" en la página 6 para los agujeros correspondientes que se encuentran en la parte izquierda del bastidor.
7. Vaya a la parte posterior del bastidor.

8. En el lado derecho, localice la unidad EIA que se corresponde con la unidad EIA inferior marcada en la parte frontal del bastidor.
9. Marque la unidad EIA inferior.
10. Marque los orificios correspondientes del lado izquierdo del bastidor.
11. Continúe con "Fijación de los rieles ajustables al chasis del sistema y al bastidor" en la página 7 para instalar los rieles ajustables o continúe con "Fijación de los rieles fijos al chasis del sistema y al bastidor" en la página 9 para instalar los rieles fijos.

Fijación de los rieles ajustables al chasis del sistema y al bastidor

Debe instalar los rieles en el chasis y en el bastidor. Para realizar esta tarea, siga este procedimiento.

Acerca de esta tarea

Atención: Para evitar una anomalía del riel y posibles daños que el usuario pudiera sufrir y también la unidad, asegúrese de que cuenta con los rieles correctos y la instalación pertinente en su bastidor. Si el bastidor tiene orificios de reborde de soporte cuadrados u orificios de reborde de soporte de rosca, asegúrese de que los rieles y las piezas de ajuste coinciden con los orificios del reborde de soporte utilizados en el bastidor. No instale hardware que no coincida utilizando arandelas o espaciadores. Si no dispone de los rieles y accesorios correctos para su bastidor, póngase en contacto con su distribuidor de IBM.

Nota: Las unidades de 1 EIA en los bastidores se miden verticalmente en incrementos de 44,45 mm (1,75 pulg.). Cada incremento de 44,45 mm (1,75 pulg.) se denomina un "EIA." En algunos países, el mismo incremento puede denominarse una "U."

Nota: El sistema requiere 1 unidad de bastidor EIA (1U) de espacio.

Asegúrese de que tiene las piezas que necesita para instalar los rieles. Las piezas siguientes se incluyen con el kit de rieles:

- 4 - destornilladores Philips de 6,35 mm (0,25 pulg.)
- 2 - conjuntos de riel de bastidor y pieza deslizante
- 2 - piezas deslizantes de HMC
- 10 - clips de tuerca para orificios de montaje EIA cuadrados
- 10 - clips de tuerca para orificios de montaje EIA redondos
- 10 - tornillos de reborde hexagonal M5

Procedimiento

1. Extraiga del envoltorio las piezas del riel y póngalas sobre la superficie de trabajo.
2. Identifique el espacio 1U en el bastidor de la HMC.
3. Para acoplar las piezas deslizantes a la HMC, realice estas tareas:
   a. Identifique la pieza deslizante derecha.
   b. Alinee los orificios de la pieza deslizante derecha con las patillas de pieza deslizante situadas en el lado derecho de la HMC. Asegúrese de que todas las patillas estén alineadas con los orificios de la pieza.
   c. Empuje la pieza deslizante de la HMC hacia el lado posterior de la HMC hasta que quede completamente encajada en su posición.
   d. Fije la pieza deslizante derecha al lado derecho de la estación de trabajo HMC colocando dos tornillos Philips de 6,35 mm (0,25 pulg.) en los orificios para tornillos.
   e. Repita los pasos "3.a" en la página 7 - "3.d" en la página 7 para instalar la pieza deslizante izquierda en el lado izquierdo de la estación de trabajo HMC.
4. Sitúese en la parte frontal del bastidor.

a. En el lado izquierdo, instale tres clips de tuerca en los tres orificios del borde frontal del bastidor en la ranura 1U designada para la HMC.

   Nota: El kit de rieles incluye clips de tuerca tanto para orificios redondos como cuadrados. Asegúrese de que utiliza clips de tuerca adecuados que coincidan con los orificios del bastidor.

b. Repita el paso "4.a" en la página 8 en el lado derecho del bastidor.

5. Sitúese en la parte posterior del bastidor.

   a. En el lado izquierdo, instale dos clips de tuerca en los orificios superior e inferior del borde frontal del bastidor en la ranura 1U designada para la HMC.

      Nota: El orificio central debe quedar vacío.

   b. Repita el paso "5.a" en la página 8 en el lado derecho del bastidor.

6. Para instalar los rieles deslizantes de la HMC en el bastidor, siga estos pasos:

   a. Mida la profundidad del bastidor. La profundidad debe estar entre 558,8 mm (22 pulg.) y 863,6 mm (34 pulg.).

   b. Coloque los rieles deslizantes de la HMC sobre una superficie plana y localice los tornillos preinstalados.

      Nota: Los rieles deslizantes tienen cuatro orificios de tornillo.

   c. Afloje los tornillos preinstalados de los rieles deslizantes hasta que puedan moverse fácilmente hacia dentro y hacia fuera.

   d. En función de la profundidad del bastidor medida en el paso "6.a" en la página 8, debe ajustar los tornillos en los rieles.

      i) Si la profundidad del bastidor está entre 558,8 mm (22 pulg.) y 698,5 mm (27,5 pulg.), ponga los tornillos en los orificios primero y tercero.

      ii) Si la profundidad del bastidor está entre 698,5 mm (27,5 pulg.) y 863,6 mm (34 pulg.), ponga los tornillos en los orificios segundo y cuarto.

      Notas:

      - El primer orificio es siempre el más cercano al final del riel deslizante. Los orificios primero y cuarto están cerca entre sí.
      - Asegúrese de que los tornillos estén suficientemente flojos para poder ajustar ligeramente la longitud del riel deslizante mientras se instala en el bastidor.

7. En la parte frontal del bastidor, instale los rieles deslizantes de la HMC en el bastidor realizando los pasos siguientes:

   a. Localice el conjunto de riel deslizante izquierdo.

   b. Oriente el conjunto de riel de manera que el extremo con el orificio de tornillo más cercano (el primer orificio) entre en el bastidor primero. Asegúrese de que las cabezas de los tornillos están encaradas al interior del bastidor. La ranura abierta del conjunto de riel está más cerca de la parte frontal del bastidor.

   c. En el lado izquierdo del bastidor, acople el reborde del extremo del riel deslizante al borde frontal del bastidor utilizando dos tornillos M5, dejando el orificio central abierto. Asegúrese de que el conjunto de riel esté ligeramente flojo en la parte frontal del bastidor para permitir la inserción de la HMC.

8. En la parte posterior del bastidor, en el lado derecho, tire del extremo libre del riel deslizante hacia la parte posterior y fije el reborde del riel deslizante al bastidor utilizando dos tornillos M5, dejando el orificio del tornillo central abierto.

9. Repita el paso "7" en la página 8 y el paso "8" en la página 8 para instalar el conjunto de riel deslizante derecho en el lado derecho del bastidor.

10. En la parte frontal del bastidor, instale la estación de trabajo HMC en el bastidor realizando los pasos siguientes:

a. Manteniendo la estación de trabajo HMC nivelada, inserte las piezas deslizantes en los rieles deslizantes de la HMC que ha instalado en el paso anterior. Empuje la HMC hacia delante hasta que los rebordes de la parte frontal de la HMC estén alineados con los orificios de tornillo abiertos de la parte frontal del bastidor.

b. Fije la HMC a la izquierda del marco con un tornillo M5. Repita este paso en el lado derecho del bastidor.

11. Continúe con “Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación” en la página 10.

Fijación de los rieles fijos al chasis del sistema y al bastidor

Debe instalar los rieles en el chasis y en el bastidor. Para realizar esta tarea, siga este procedimiento.

Acerca de esta tarea

Atención: Para evitar una anomalía del riel y posibles daños que el usuario pudiera sufrir y también la unidad, asegúrese de que cuenta con los rieles correctos y la instalación pertinente en su bastidor. Si el bastidor tiene orificios de reborde de soporte cuadrados u orificios de reborde de soporte de rosca, asegúrese de que los rieles y las piezas de ajuste coinciden con los orificios del reborde de soporte utilizados en el bastidor. No instale hardware que no coincida utilizando arandelas o espaciadores. Si no dispone de los rieles y accesorios correctos para su bastidor, póngase en contacto con su distribuidor de IBM.

Nota: Las unidades de 1 EIA en los bastidores se miden verticalmente en incrementos de 44,45 mm (1,75 pulg.). Cada incremento de 44,45 mm (1,75 pulg.) se denomina un “EIA.” En algunos países, el mismo incremento puede denominarse una “U.”

Nota: El sistema requiere 1 unidad de bastidor EIA (1U) de espacio.

Asegúrese de que tiene las piezas que necesita para instalar los rieles. Las piezas siguientes se incluyen con el kit de rieles:

- 4 - destornilladores Philips de 6,35 mm (0,25 pulg.)
- 2 - rieles interiores
- 2 - rieles de soporte de HMC
- 2 - clips de tuerca para orificios de montaje EIA cuadrados
- 2 - clips de tuerca para orificios de montaje EIA redondos
- 8 - tornillos de reborde hexagonal M5

Procedimiento

1. Extraiga del envoltorio las piezas del riel y póngalas sobre la superficie de trabajo.
2. Identifique el espacio 1U en el bastidor de la HMC.
3. Para acoplar los rieles internos a la HMC, realice estas tareas:
   a. Identifique el riel interno derecho.
   b. Alinee los orificios del riel interno derecho con las patillas de riel interno situadas en el lado derecho de la HMC. Asegúrese de que todas las patillas estén alineadas con los orificios del riel interno.
   c. Empuje el riel interno de la HMC hacia el lado frontal de la HMC hasta que quede completamente encajado en su posición.
   d. Fije el riel interno derecho al lado derecho de la estación de trabajo HMC colocando dos tornillos Philips de 6,35 mm (0,25 pulg.) en los orificios para tornillos.
   e. Repita los pasos 3.a - “3.d” en la página 9 para instalar el riel interno en el lado izquierdo de la estación de trabajo HMC.

4. Sitúese en la parte frontal del bastidor. En el lado izquierdo, instale un clip de tuerca en el orificio del borde frontal del bastidor en la ranura 1U designada para la HMC.

   Nota: El kit de rieles incluye clips de tuerca tanto para orificios redondos como cuadrados. Asegúrese de que utiliza clips de tuerca adecuados que coincidan con los orificios del bastidor.
5. Sitúese en la parte posterior del bastidor. En el lado izquierdo, instale un clip de tuerca en el orificio central del borde frontal del bastidor en la ranura 1U designada para la HMC.
6. En la parte frontal del bastidor, instale los rieles de soporte de la HMC en el bastidor realizando los pasos siguientes:
   a. Alinee las patillas de los rieles de soporte por encima y por debajo del clip de tuerca que acaba de instalar en el paso anterior.
   b. En el lado derecho del bastidor, acople el reborde del extremo del riel de soporte al borde frontal del bastidor utilizando dos tornillos M5 en los orificios para tornillos superior en inferior, dejando el orificio central abierto. Asegúrese de que el conjunto de riel esté ligeramente flojo en la parte frontal del bastidor para permitir la inserción de la HMC.
7. En la parte posterior del bastidor, en el lado derecho, tire del extremo libre del riel de soporte hacia la parte posterior y fije el reborde del riel de soporte al bastidor utilizando dos tornillos M5, dejando el orificio del tornillo central abierto.
8. Repita el paso “6” en la página 10 y el paso “7” en la página 10 para instalar el conjunto de riel de soporte izquierdo en el lado izquierdo del bastidor.
9. En la parte frontal del bastidor, instale la estación de trabajo HMC en el bastidor realizando los pasos siguientes:
   a. Manteniendo la estación de trabajo HMC nivelada, inserte los rieles interiores en los rieles de soporte de la HMC que ha instalado en el paso anterior. Empuje la HMC hacia delante hasta que los rebordes de la parte frontal de la HMC estén alineados con los orificios de tornillo abiertos de la parte frontal del bastidor.
   b. Fije la HMC a la izquierda del marco con un tornillo M5. Repita este paso en el lado derecho del bastidor.

   Nota: Si las hay, extraiga las abrazaderas de envío naranjas ubicadas en la parte posterior del sistema y vuelva a colocar el tornillo.
10. Continúe con “Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación” en la página 10.

Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación

Instale el sistema en los rieles y conecte y direccione los cables de alimentación.

Acerca de esta tarea

PRECAUCIÓN: Esta es una pieza o una unidad pesada, pero su peso es menor que 18 kg (39,7 libras). Tome precauciones cuando se disponga a levantar, quitar o instalar esta pieza o esta unidad. (C008)

Procedimiento

1. Quite la capa protectora de plástico de la parte superior del chasis del sistema.
2. Conecte los cables de alimentación a las fuentes de alimentación.

   Nota: No conecte el otro extremo del cable de alimentación a la fuente de alimentación ahora.

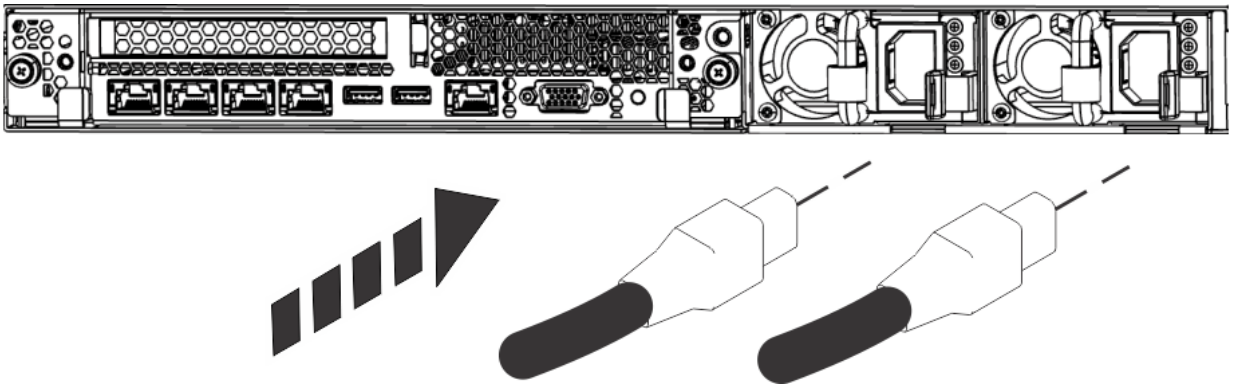


Figura 2. Conexión de los cables de alimentación a las fuentes de alimentación

3. Instale los cierres velcro para fijar los cables de alimentación.
4. Continúe con "Cableado de la HMC 7063-CR2 montada en bastidor" en la página 11.

Cableado de la HMC 7063-CR2 montada en bastidor

Información sobre cómo instalar de forma física la Hardware Management Console (HMC) montada en bastidor.

Procedimiento

1. Asegúrese de que la HMC está instalada en un bastidor y que los cables de alimentación están enchufados en las fuentes de alimentación. Para obtener más información, consulte "Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación" en la página 10. Tras instalar la HMC en un bastidor, continúe con el paso siguiente.
2. Conecte el teclado, el monitor y el ratón.

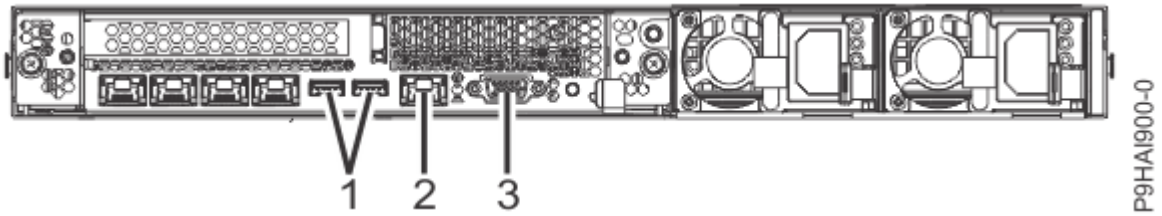


Figura 3. Puertos posteriores

Tabla 4. Puertos de entrada y salida

Identificador	**Descripción**
1	USB 2.0 utilizado para teclado y ratón
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	La Video Graphics Array (VGA) utilizada para la pantalla. Solo está soportado el valor VGA de 1024 x 768 a 60 Hz. Solo se admite un cable de hasta 3 metros.

Nota: El sistema tiene dos puertos USB frontales que puede utilizar.

3. Conecte el puerto de la Ethernet Intelligent Platform Management Interface (IPMI) a una red.

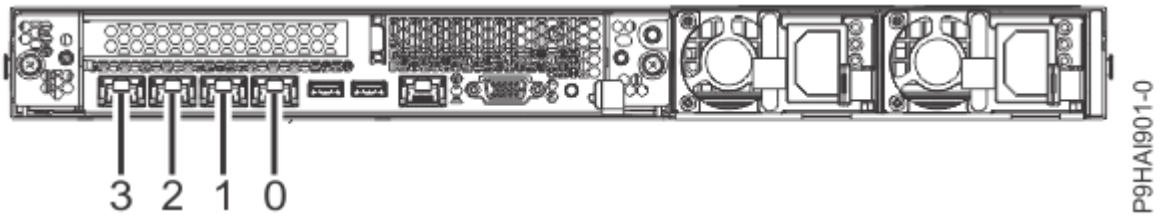


Figura 4. puertos Ethernet

Tabla 5. puertos Ethernet	
Identificador	**Descripción**
0	Shared Ethernet Intelligent Platform Management Interface (IPMI) y Conexión de red de la HMC
1, 2 y 3	Conexión de red de la HMC

Nota: Esta conexión es necesaria para acceder al controlador de gestión de placa base (BMC) en la HMC. Se tiene que acceder a la BMC para obtener las tareas de servicio y para realizar el mantenimiento del firmware de la HMC. Para obtener más información, consulte "Tipos de conexiones de red de la HMC" en la página 39.

Aviso: Es posible que este producto no esté certificado para la conexión a través de algún medio, sea cual sea, a las interfaces de las redes públicas de telecomunicaciones. Es posible que la ley requiera más certificación antes de realizar una conexión de ese estilo. Póngase en contacto con IBM para obtener más información.

4. Conecte el cable Ethernet que está destinado a la conexión con el sistema o los sistemas gestionados.

   Notas:

   - Si va a utilizar una conexión compartida para IPMI y la HMC, un solo cable en el puerto 0 de la figura 2 puede satisfacer ambos requisitos, IPMI y HMC.
   - Para saber más sobre las conexiones de la red HMC, consulte "Conexiones de red de la HMC" en la página 38.
5. Si el sistema gestionado ya está instalado, puede comprobar que la conexión del cable Ethernet está activa observando las luces de estado verdes en los puertos Ethernet de la HMC y el sistema gestionado a medida que avanza la instalación.
6. Conecte los cables de alimentación del sistema y los cables de alimentación para cualquier dispositivo conectado en la fuente de alimentación de corriente alterna (CA).
7. Verifique el estado de la alimentación utilizando los LED de fuente de alimentación como indicadores. Para obtener más información, consulte LED en el sistema 7063-CR2LED en el sistema 7063-CR2.
8. Pulse el botón de alimentación para iniciar el sistema. La luz de encendido deja de parpadear y queda fija, lo que indica que el sistema está encendido.

Resultados

A continuación, tiene que instalar y configurar el software de su HMC. Continúe con "Configuración de la HMC 7063-CR2" en la página 12.

Configuración de la HMC 7063-CR2

Información para instalar y configurar la Hardware Management Console (HMC).

Compruebe la versión de HMC que se suministra con la HMC. Para averiguar cómo ver la versión y el release del código de máquina de la HMC, consulte Comprobar la versión de la HMC que se suministra con la HMC. Puede descargar la versión más reciente de la HMC que está disponible del sitio web de Fix

Central. Utilice soportes de almacenamiento extraíbles (como, por ejemplo, un DVD o USB) para crear un archivo ISO arrancable desde el paquete de la HMC (imagen ISO).

Nota: En la tabla siguiente se describe la información de inicio de sesión predefinida (predeterminada) para las interfaces HMC y BMC.

Tabla 6.

Consola o interfaz	ID predeterminado	Contraseña predeterminada	Descripción
BMC (OpenBMC)	`root`	`0penBmc`	El ID de usuario root y la contraseña se utilizan para iniciar la sesión en la BMC por primera vez.
HMC	`hscroot`	`abc123`	El ID de usuario hscroot y su contraseña se utilizan para iniciar sesión por primera vez en la HMC. Son sensibles a las mayúsculas/minúsculas y solo los puede utilizar un miembro del rol de superadministrador.
HMC	`raíz`	`passw0rd`	El ID de usuario root y la contraseña los utiliza el proveedor de servicios para realizar procedimientos de mantenimiento. No se pueden utilizar para iniciar sesión en la HMC.

Nota: Las instalaciones siguientes se muestran como ejemplos.

Instalación de la HMC utilizando la unidad flash USB

Para instalar la HMC utilizando la unidad flash USB, lleve a cabo los pasos siguientes para sistemas Linux®:

Nota: Por ejemplo, en diferentes sistemas operativos, verá:

- Windows: Soporte de instalación flash USB (Windows)
- Mac: Soporte de instalación flash USB (macOS)

1. Descargue la versión de la HMC que desee del sitio web de Fix Central.
2. Ejecute el mandato siguiente: **`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`** (donde **sdx** es el nombre de la unidad USB).

   Nota: Puede ejecutar el mandato de Linux `lsblk` para determinar el nombre de la unidad USB cuando esté conectada.
3. Inserte la unidad USB y encienda el sistema.

   Nota: La unidad USB debe tener al menos 8 GB. Algunas unidades USB podrían ser demasiada anchas para entrar correctamente en el puerto USB de la parte posterior del sistema. Pruebe el ajuste de la unidad USB antes de continuar.
4. Cuando se visualiza el menú Petitboot, seleccione la opción **Instalar Hardware Management Console** que se encuentra en **USB**.

Instalación de la HMC utilizando medios virtuales desde la BMC

Para instalar la HMC utilizando medios virtuales desde el BMC, siga estos pasos:

1. Abra un navegador web soportado. En la barra de direcciones, especifique la dirección IP del BMC con la que desea conectarse. Por ejemplo, puede utilizar el formato `https://<IP BMC>` en la barra de direcciones del navegador web.
2. En la ventana **Inicio de sesión de OpenBMC**, especifique la dirección **Host** del BMC, así como el **Nombre de usuario** y la **Contraseña** que tiene asignados.

   Nota: El ID de usuario predeterminado es `root` y la contraseña predeterminada es `0penBmc`.

   Si está utilizando el nivel de firmware OP940.01 o posterior, la contraseña de root caduca de forma predeterminada. Debe cambiar la contraseña predeterminada antes de poder acceder al BMC. Para obtener más información sobre cómo cambiar la contraseña predeterminada caducada, consulte Establecimiento de la contraseña.

   Si ha olvidado la contraseña, puede realizar un restablecimiento de fábrica del sistema para restaurar la contraseña predeterminada. Para restablecer el sistema, consulte Realización de un restablecimiento de fábrica.
3. Pulse **Iniciar sesión**.
4. Seleccione **Control de servidor**.
5. Seleccione **Almacenamiento virtual**.
6. Haga clic en **Seleccionar archivo**.
7. Localice el ISO de soporte de recuperación de la HMC y pulse **Abrir**.
8. Pulse **Iniciar**.
9. Encienda el sistema.
10. Cuando se visualiza el menú Petitboot, seleccione la opción **Instalar Hardware Management Console** que se encuentra en **USB**.

Instalación de la HMC mediante una unidad de DVD conectada a USB externa

Para instalar la HMC mediante una unidad de DVD conectada a USB externa, siga estos pasos:

1. Descargue la versión de recuperación de la HMC que desee del sitio web de Fix Central.
2. Grabe la imagen DVD de la recuperación HMC en un soporte DVD-R DL como imagen.
3. Apague la HMC.
4. Conecte la unidad de DVD USB externa a la HMC e inserte el DVD de recuperación HMC.

   Nota: Puede que necesite conectar la unidad de DVD USB a una fuente de alimentación externa o utilice un cable USB Y para conectarse a un puerto USB adicional que proporcione energía suficiente para la unidad de DVD.
5. Encienda la HMC.

   Nota: Es posible que el monitor de pantalla no muestre señal durante el inicio. El proceso puede tomar 2 o 3 minutos antes de que el supervisor muestre cualquier estado.
6. Cuando se inicia el cargador de arranque Petitboot, vaya al arranque automático.

   Nota: Se impone un tiempo de espera de 10 segundos. Si no se toman medidas en un periodo de 10 segundos, el sistema intenta arrancar desde la unidad de disco duro.
7. Espere hasta que el dispositivo **CD/DVD** aparezca en el menú Petitboot.

   Nota: Este proceso puede tardar hasta un minuto.
8. Seleccione la opción **Instalar Hardware Management Console** que se encuentra en **CD/DVD**.

Instalación del modelo 7063-CR1 en un bastidor

Información sobre cómo instalar la Hardware Management Console (HMC) 7063-CR1 en un bastidor.

Puede ver la documentación de instalación en línea o puede imprimir la versión en PDF con la misma información. Para ver o imprimir la versión en PDF, consulte Instalación y configuración de la Hardware Management Console.

Requisitos previos para instalar el sistema 7063-CR1 montado en bastidor

Utilice la información para comprender los requisitos previos que son necesarios para instalar el sistema.

Acerca de esta tarea

PRECAUCIÓN:

o

o

El peso de esta pieza o unidad está comprendido entre 18 y 32 kg (39,7 y 70,5 libras). Hacen falta dos personas para levantar esta pieza o unidad sin peligro. (C009)

Se recomienda leer los siguientes documentos antes de empezar a instalar el servidor:

- La versión más reciente de este documento se mantiene en línea, consulte Instalación de 7063-CR1 en un bastidor (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm).
- Para planificar la instalación del servidor, consulte Planificación de hardware y de ubicaciones.

Procedimiento

Asegúrese de que tiene los siguientes elementos antes de empezar la instalación:

- Destornillador de estrella de tamaño 2
- Destornillador de cabeza plana
- Cortador para cartón
- Muñequera antiestática de descarga electrostática (ESD)
- Bastidor con una unidad de espacio EIA (Electronic Industries Association) (1U).

Nota: Si no tiene un bastidor instalado, instálelo. Para obtener instrucciones, consulte Bastidores y dispositivos de bastidor (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).

Completar inventario para el sistema

Utilice esta información para completar el inventario para el sistema.

Procedimiento

1. Verifique que ha recibido todas las cajas que ha solicitado.
2. Desembale los componentes de servidor según sea necesario.
3. Elabore un inventario de piezas y verifique que haya recibido todas las piezas que ha solicitado antes de instalar cada componente del servidor.

Nota:

La información del pedido se incluye en el producto. Puede también obtener información sobre su pedido a partir del representante de ventas o IBM Business Partner.

Si hay componentes incorrectos o dañados, o faltan componentes, utilice cualquiera de los recursos siguientes:

- El distribuidor de IBM.
- Línea de información automatizada de fabricación de IBM Rochester, número 1-800-300-8751 (sólo Estados Unidos).
- Sitio web de Directorio de contactos a nivel mundial, Directory of worldwide contacts website (http://www.ibm.com/planetwide). Seleccione la localidad para ver la información de contacto de servicio y soporte.

Determinación y marca de la ubicación en el bastidor para el sistema 7063-CR1

Es posible que tenga que determinar dónde instalar la unidad del sistema en el bastidor.

Procedimiento

1. Lea los Avisos de seguridad del bastidor (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Determine el lugar donde se va a colocar la unidad del sistema en el bastidor. Cuando planifique la instalación de la unidad del sistema en un bastidor, tenga en cuenta la información siguiente:
   - Organice las unidades más grandes y más pesadas en la parte inferior del bastidor.
   - Planifique instalar primero las unidades del sistema en la parte inferior del bastidor.
   - Anote las ubicaciones EIA (Electronic Industries Alliance) en el plan.
3. Si es necesario, extraiga los paneles de relleno para permitir el acceso al interior del alojamiento del bastidor donde tenga previsto colocar la unidad, tal como se muestra en la Figura 5 en la página 17.

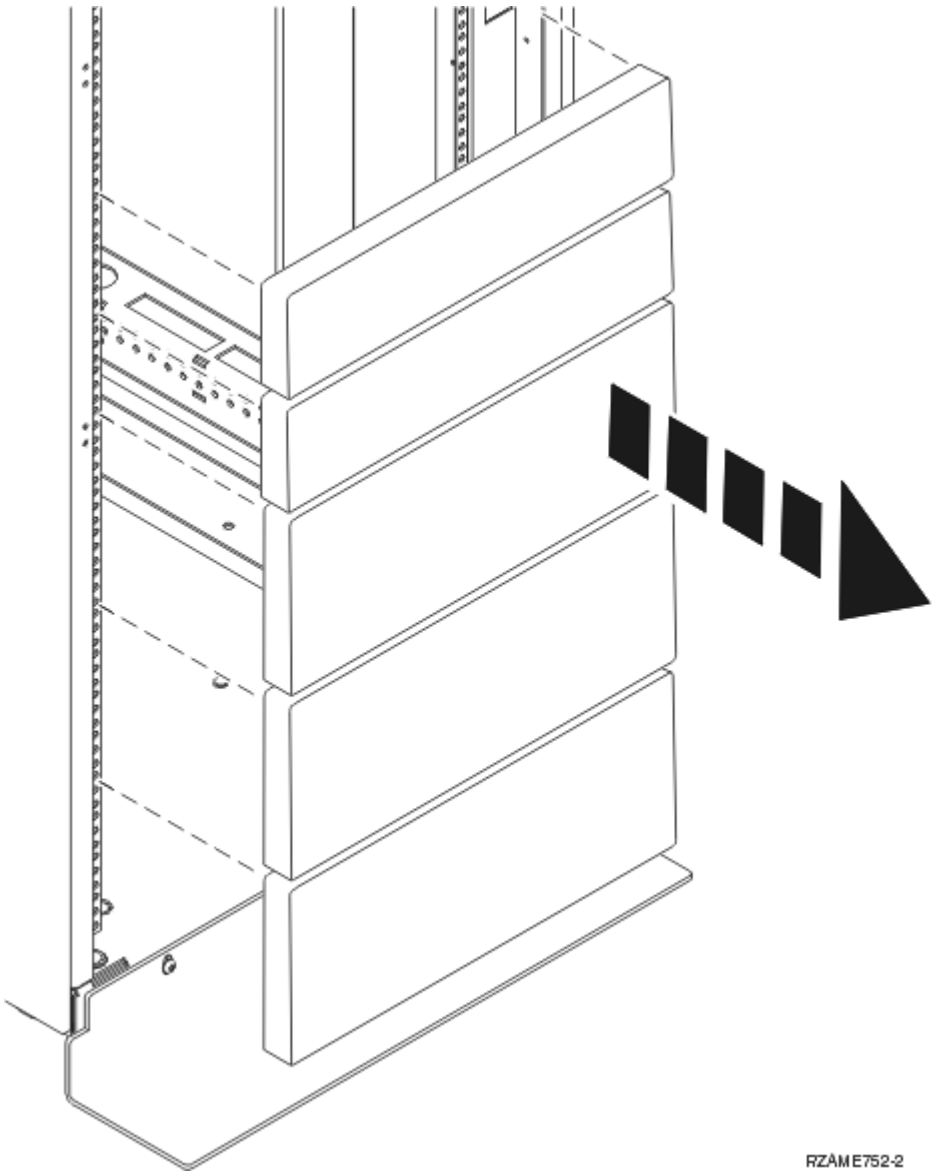


Figura 5. Extracción de los paneles de relleno

4. Determine el lugar donde colocar el sistema en el bastidor. Tome nota de la ubicación de EIA.
5. Con la parte frontal del bastidor orientada hacia usted y comenzando por el lado derecho, utilice una cinta, un rotulador o un lápiz para marcar el agujero inferior de esta unidad EIA.
6. Repita el paso "5" en la página 17 para los agujeros correspondientes que se encuentran en la parte izquierda del bastidor.
7. Vaya a la parte posterior del bastidor.
8. En el lado derecho, localice la unidad EIA que se corresponde con la unidad EIA inferior marcada en la parte frontal del bastidor.
9. Marque la unidad EIA inferior.
10. Marque los orificios correspondientes del lado izquierdo del bastidor.

Fijación de los rieles fijos al chasis del sistema y al bastidor

Debe instalar los rieles en el chasis y en el bastidor. Para realizar esta tarea, siga este procedimiento.

Acerca de esta tarea

Atención: Para evitar una anomalía del riel y posibles daños que el usuario pudiera sufrir y también la unidad, asegúrese de que cuenta con los rieles correctos y la instalación pertinente en su bastidor. Si el bastidor tiene orificios de reborde de soporte cuadrados u orificios de reborde de soporte de rosca, asegúrese de que los rieles y las piezas de ajuste coinciden con los orificios del reborde de soporte utilizados en el bastidor. No instale hardware que no coincida utilizando arandelas o espaciadores. Si no dispone de los rieles y accesorios correctos para su bastidor, póngase en contacto con su distribuidor de IBM.

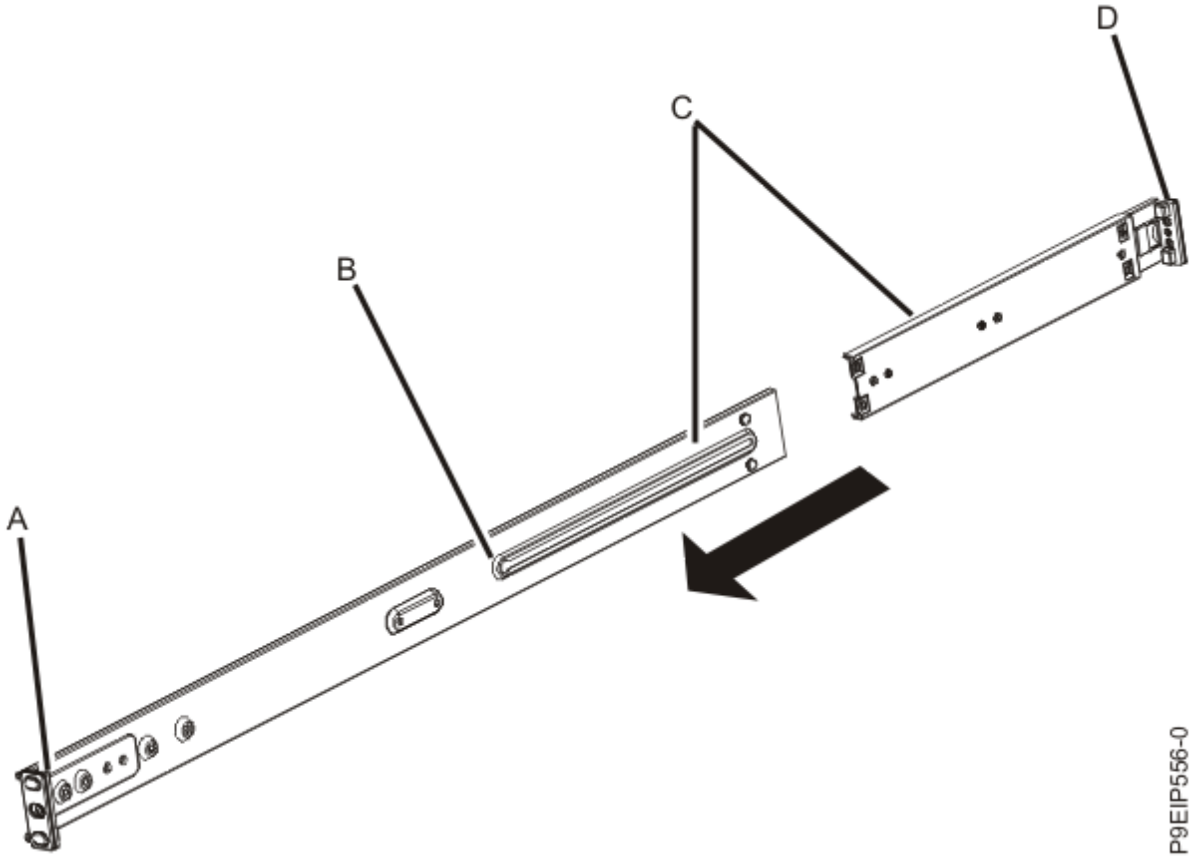
Nota: El sistema requiere 1 unidad de bastidor EIA (1U) de espacio.

Asegúrese de que tiene las piezas que necesita para instalar los rieles. Las piezas siguientes se incluyen con el kit de rieles:

- Tornillos del riel deslizante, que se utilizan para unir las dos partes de cada riel deslizante
- Tornillos del bastidor del riel deslizante, que se utilizan para fijar los rieles al bastidor
- Rieles
- Tornillos 10 - 32 x 0,635 cm (0,25 pulgadas), que se utilizan para fijar los rieles al chasis del sistema

Procedimiento

1. Extraiga del envoltorio las piezas del riel y póngalas sobre la superficie de trabajo.
2. Sustituya las patillas cuadradas del bastidor del riel (**A**) y (**D**) por las patillas redondas del bastidor del riel.
3. Conecte las dos partes de cada riel deslizante del bastidor. Para conectar las dos partes del riel deslizante del bastidor, lleve a cabo las tareas siguientes:
   a. Identifique las dos piezas del riel deslizante del bastidor izquierdo. Alinee las piezas cortas y largas (**C**). Asegúrese de que los pasadores del riel del bastidor apunten a la misma dirección (**A**) y (**D**).



b. La pieza más corta del riel deslizante del bastidor tiene un pasador metálico. Inserte el pasador en el agujero en la pieza más larga del riel deslizante del bastidor (**B**). Deslice la pieza más corta del riel del bastidor en la pieza más larga del riel del bastidor.

c. Alinee los agujeros con las dos piezas de los rieles deslizantes del bastidor. Mediante un destornillador de punta de estrella, una las dos partes aflojando ligeramente los dos tornillos del riel con roscas en los agujeros del riel deslizante del bastidor.

Nota: No apriete los tornillos del riel deslizante del bastidor.

d. Repita estos pasos para el riel deslizante de la derecha.

4. Coloque los rieles deslizantes del bastidor en el bastidor.

a. Sitúese en la parte frontal del bastidor.

b. Seleccione el riel deslizante del bastidor de la izquierda y localice la unidad EIA que ha marcado anteriormente. Cada riel deslizante está marcado también con la palabra **Back**, para designar la parte posterior del bastidor. Asegúrese de sujetar la parte frontal del riel deslizante del bastidor.

c. Extienda el riel desde la parte frontal del bastidor hacia la parte posterior del mismo y alinee las patillas del riel deslizante del bastidor en el reborde del bastidor que ha marcado anteriormente.

d. Presione las patillas del riel del bastidor en el reborde del bastidor posterior hasta que el mecanismo de cierre del bastidor posterior quede fijado en su lugar.

e. Tire de la parte frontal del riel del bastidor hacia la parte frontal del reborde del riel del bastidor. Alinee las patillas del riel deslizante con los orificios en el reborde del riel y tire de ellas hasta que el mecanismo de cierre del riel quede encajado en su lugar.

f. Mediante un destornillador, apriete los tornillos del riel que ha colocado en el paso 2.

Nota: Es posible que necesite 2 unidades (2U) de espacio para acceder y apretar los tornillos del riel.

g. Repita los pasos 4a a 4f para el riel deslizante del lado derecho.

Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación

Instale el sistema en los rieles y conecte y direccione los cables de alimentación.

Acerca de esta tarea

o

o

PRECAUCIÓN:

El peso de esta pieza o unidad está comprendido entre 18 y 32 kg (39,7 y 70,5 libras). Hacen falta dos personas para levantar esta pieza o unidad sin peligro. (C009)

Procedimiento

1. Quite la capa protectora de plástico de la parte superior del chasis del sistema.
2. Sitúese en la parte frontal del bastidor.
3. Con dos personas, levante el sistema y alinee los rieles del chasis del sistema en cada lateral del chasis con los rieles deslizantes del bastidor.
4. Presione suavemente el sistema hacia la parte posterior del bastidor.

5. Fije el sistema al bastidor enroscando un tornillo con arandela a través de las asas de cada lado del chasis del sistema.

   Nota: Debe utilizar arandelas con los tornillos. Deslice una arandela en cada uno de los tornillos más largos (1,5 cm) que van incluidos con el kit del riel. Enrosque el tornillo con la arandela a través del lado derecho e izquierdo del sistema en la parte frontal.
6. Conecte los cables de alimentación a las fuentes de alimentación.

   Nota: No conecte el otro extremo del cable de alimentación a la fuente de alimentación ahora.

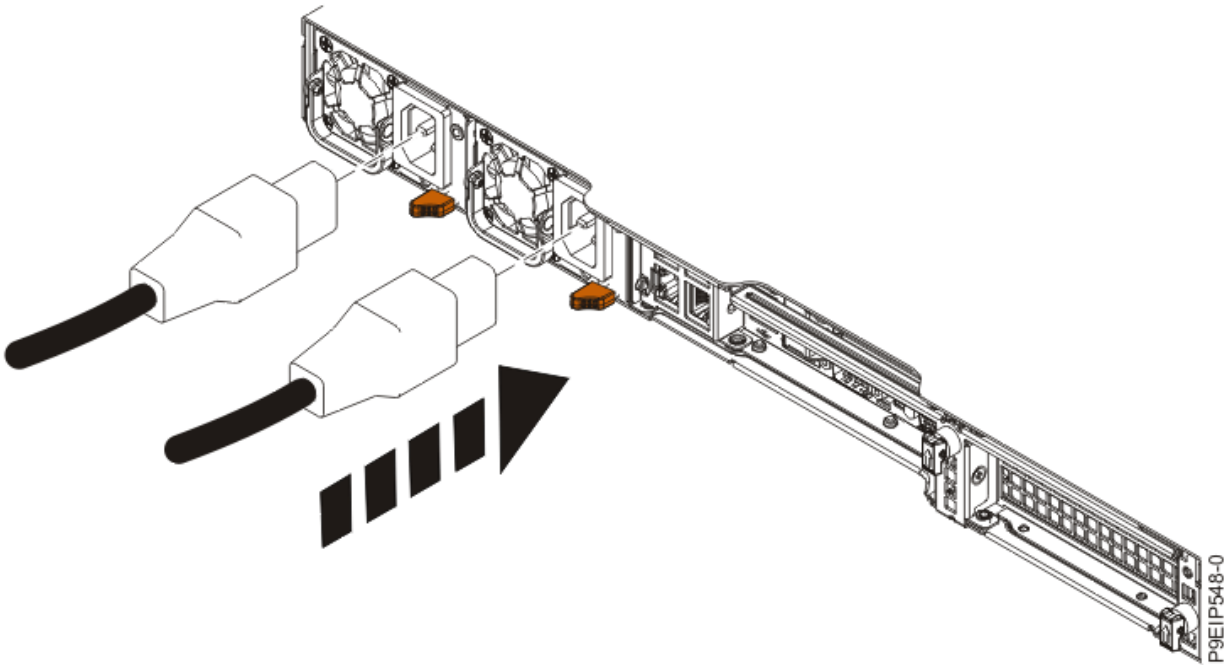


Figura 6. Conexión de los cables de alimentación a las fuentes de alimentación

7. Continúe con "Cableado de la HMC 7063-CR1 montada en bastidor" en la página 20.

Cableado de la HMC 7063-CR1 montada en bastidor

Información sobre cómo instalar de forma física la Hardware Management Console (HMC) montada en bastidor.

Procedimiento

1. Asegúrese de que la HMC está instalada en un bastidor y que los cables de alimentación están enchufados en las fuentes de alimentación. Para obtener más información, consulte "Instalación del sistema en el bastidor y conexión y direccionamiento de los cables de alimentación" en la página 19. Tras instalar la HMC en un bastidor, continúe con el paso siguiente.

   Nota: Si un enchufe cubre un puerto que necesita utilizar en la parte posterior del sistema, extráigalo y descártelo. Las cubiertas de los puertos garantizan que se le recuerde que debe restablecer la contraseña del administrador en el sistema gestionado durante la IPL del sistema inicial.
2. Conecte el teclado, el monitor y el ratón.

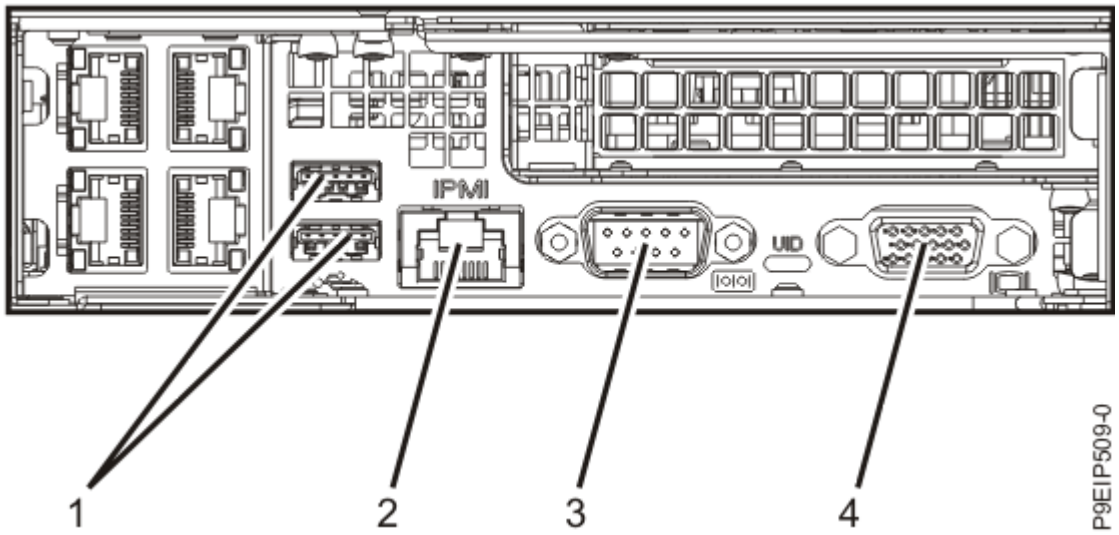


Figura 7. Puertos posteriores

Tabla 7. Puertos de entrada y salida	
Identificador	**Descripción**
1	USB 2.0 utilizado para teclado y ratón
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	IPMI serie
4	La Video Graphics Array (VGA) utilizada para la pantalla. Solo está soportado el valor VGA de 1024 x 768 a 60 Hz. Solo se admite un cable de hasta 3 metros.

Nota: El sistema tiene dos puertos USB frontales que puede utilizar. El puerto serie frontal no es funcional.

3. Conecte el cable Ethernet que está destinado a la conexión con el sistema o los sistemas gestionados.

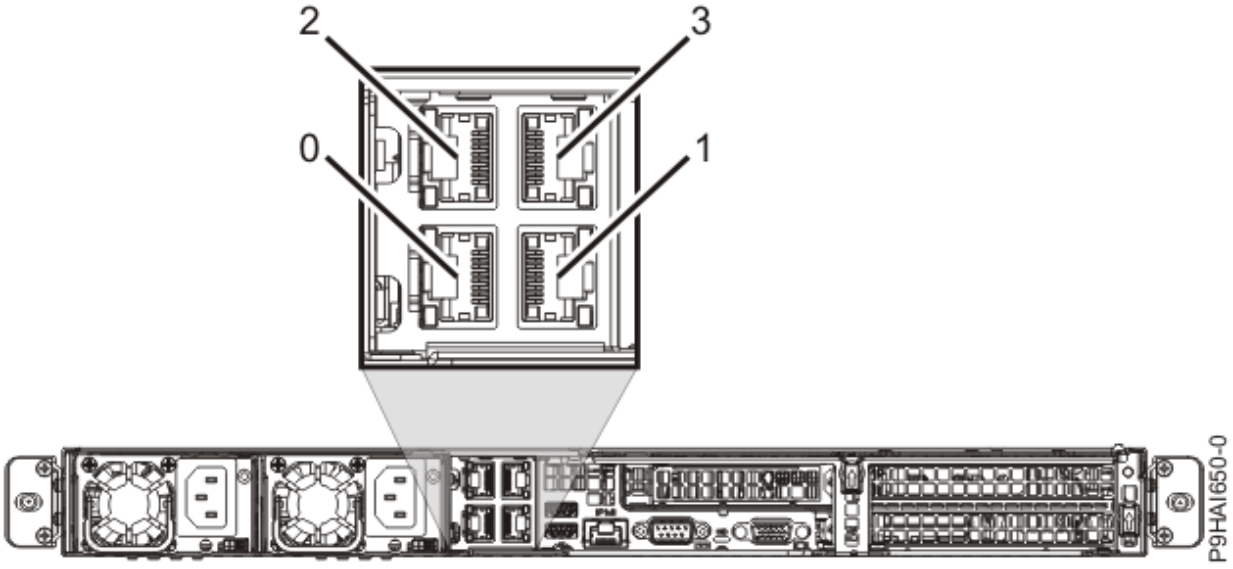


Figura 8. puertos Ethernet

Nota: Para saber más sobre las conexiones de la red HMC, consulte “Conexiones de red de la HMC” en la página 38.

4. Si el sistema gestionado ya está instalado, puede comprobar que la conexión del cable Ethernet está activa observando las luces de estado verdes en los puertos Ethernet de la HMC y el sistema gestionado a medida que avanza la instalación.
5. Conecte el puerto de la Ethernet Intelligent Platform Management Interface (IPMI) a una red.

   Nota: Esta conexión es necesaria para acceder al controlador de gestión de placa base (BMC) en la HMC. Se tiene que acceder a la BMC para obtener las tareas de servicio y para realizar el mantenimiento del firmware de la HMC. Para obtener más información, consulte “Tipos de conexiones de red de la HMC” en la página 39.

6. Conecte los cables de alimentación del sistema y los cables de alimentación para cualquier dispositivo conectado en la fuente de alimentación de corriente alterna (CA).
7. Verifique el estado de la alimentación utilizando los LED de fuente de alimentación como indicadores. Para obtener más información, consulte LED en el sistema 7063-CR1LED en el sistema 7063-CR1.

Resultados

A continuación, tiene que instalar y configurar el software de su HMC. Continúe con “Configuración de la HMC 7063-CR1” en la página 22.

Configuración de la HMC 7063-CR1

Información para instalar y configurar la Hardware Management Console (HMC).

Compruebe la versión de HMC que se suministra con la HMC. Puede descargar la versión más reciente de la HMC que está disponible del sitio web de Fix Central. Utilice soportes de almacenamiento extraíbles (como, por ejemplo, un DVD o USB) para crear un archivo ISO arrancable desde el paquete de la HMC (imagen ISO).

Nota: En la tabla siguiente se describe la información de inicio de sesión predefinida (predeterminada) para las interfaces HMC y BMC.

Tabla 8.

Consola o interfaz	ID predeterminado	Contraseña predeterminada	Descripción
BMC	`ADMIN`	`ADMIN`	El ID de usuario ADMIN y la contraseña se utilizan para iniciar la sesión en la BMC por primera vez.
HMC	`hscroot`	`abc123`	El ID de usuario hscroot y su contraseña se utilizan para iniciar sesión por primera vez en la HMC. Son sensibles a las mayúsculas/minúsculas y solo los puede utilizar un miembro del rol de superadministrador.

Tabla 8. (continuación)

Consola o interfaz	ID predeterminado	Contraseña predeterminada	Descripción
HMC	`raíz`	`passw0rd`	El ID de usuario root y la contraseña los utiliza el proveedor de servicios para realizar procedimientos de mantenimiento. No se pueden utilizar para iniciar sesión en la HMC.

Nota: Las instalaciones siguientes se muestran como ejemplos.

Instalación de la HMC utilizando la unidad flash USB

Para instalar la HMC utilizando la unidad flash USB, lleve a cabo los pasos siguientes para sistemas Linux:

Nota: Por ejemplo, en diferentes sistemas operativos, verá:

- Windows: Soporte de instalación flash USB (Windows)
- Mac: Soporte de instalación flash USB (macOS)

1. Descargue la versión de la HMC que desee del sitio web de Fix Central.
2. Ejecute el mandato siguiente: **`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`** (donde **sdx** es el nombre de la unidad USB).

   Nota: Puede ejecutar el mandato de Linux `lsblk` para determinar el nombre de la unidad USB cuando esté conectada.
3. Inserte la unidad USB y encienda el sistema.

   Nota: La unidad USB debe tener al menos 4 GB. Algunas unidades USB podrían ser demasiada anchas para entrar correctamente en el puerto USB de la parte posterior del sistema. Pruebe el ajuste de la unidad USB antes de continuar.
4. Cuando se visualiza el menú Petitboot, seleccione la opción **Instalar Hardware Management Console** que se encuentra en **USB**.

Instalación de la HMC utilizando soportes remotos desde el visor de la consola

Para instalar la HMC utilizando soportes remotos desde el visor de la consola, lleve a cabo los pasos siguientes:

1. Inicie sesión en la interfaz web del BMC (`http://<bmc-ip>`).
2. Seleccione **Control remoto**.
3. Seleccione **Redirección de la consola**.
4. Pulse **Iniciar consola**.
5. En el Visor iKVM de Java™, seleccione **Medios virtuales** > **Almacenamiento virtual**.
6. En **Tipo de unidad lógica**, seleccione **Archivo ISO**.
7. Pulse **Abrir imagen** y localice el archivo ISO en su sistema.
8. Pulse **Plugin** para montar el archivo ISO.
9. Encienda el sistema.
10. Cuando se visualiza el menú Petitboot, seleccione la opción **Instalar Hardware Management Console** que se encuentra en **CD/DVD**.

Instalación de la HMC mediante una unidad de DVD conectada a USB externa

Para instalar la HMC mediante una unidad de DVD conectada a USB externa, siga estos pasos:

1. Descargue la versión de recuperación de la HMC que desee del sitio web de Fix Central.
2. Grabe la imagen DVD de la recuperación HMC en un soporte DVD-R como imagen. Como alternativa, puede ordenar el soporte de recuperación en DVD.
3. Apague la HMC.
4. Conecte la unidad de DVD USB externa a la HMC e inserte el DVD de recuperación HMC.

   Nota: Puede que necesite conectar la unidad de DVD USB a una fuente de alimentación externa o utilice un cable USB Y para conectarse a un puerto USB adicional que proporcione energía suficiente para la unidad de DVD.
5. Encienda la HMC.

   Nota: Es posible que el monitor de pantalla no muestre señal durante el inicio. El proceso puede tomar 2 o 3 minutos antes de que el supervisor muestre cualquier estado.
6. Cuando se inicia el cargador de arranque Petitboot, vaya al arranque automático.

   Nota: Se impone un tiempo de espera de 10 segundos. Si no se toman medidas en un periodo de 10 segundos, el sistema intenta arrancar desde la unidad de disco duro.
7. Espere hasta que el dispositivo **CD/DVD** aparezca en el menú Petitboot.

   Nota: Este proceso puede tardar hasta un minuto.
8. Seleccione la opción **Instalar Hardware Management Console** que se encuentra en **CD/DVD**.

Instalación de la HMC utilizando el soporte remoto que aloja un servidor de archivos SMB

Para instalar la HMC utilizando soporte remoto que aloja un servidor de archivos Server Message Block (SMB - bloque de mensajes de servidor), complete los pasos siguientes:

1. Copie el archivo ISO de recuperación a un host de compartición en el servidor de archivos compatible con SMB.

   Nota: No se admite la versión 3 de Server Message Block (SMBv3 - bloque de mensajes de servidor).
2. Inicie sesión en la interfaz web del BMC (`http://<bmc-ip>`).
3. Seleccione **Almacenamiento virtual**.
4. Seleccione **Imagen de CD-ROM**.
5. Complete la siguiente información:

   Host de compartición

   La IP del host SMB. Si está utilizando el nombre de host, asegúrese de que el sistema de nombre de dominio (DNS) del BMC se haya configurado correctamente.

   Vía de acceso a la imagen

   La vía de acceso de SMB al sistema. Por ejemplo: `/<nombre compartición>/<resto de vía de acceso>/<nombre de iso>.iso`

   Usuario (opcional)

   El nombre del usuario que se utiliza para iniciar sesión en el host SMB.

   Contraseña (opcional)

   La contraseña del usuario.
6. Pulse **Guardar**.
7. Pulse **Montar**.
8. El dispositivo 1 ahora muestra el mensaje siguiente: **Hay montado un archivo iso.**

Nota: Si el mensaje no aparece, vuelva a comprobar la información y repita los pasos del 6 al 8.

9. Encienda el sistema.
10. Cuando se visualiza el menú Petitboot, seleccione la opción **Instalar Hardware Management Console** que se encuentra en **CD/DVD**.

Opcional: actualizar el nivel de firmware de la HMC utilizando la llave de memoria USB incluida

Nota: Si la configuración incluye una actualización de firmware de la HMC en una llave de memoria USB, siga estos pasos para actualizar el nivel de firmware de la HMC.

Para actualizar el nivel de firmware de la HMC utilizando la llave de memoria USB incluida, siga estos pasos:

1. Inserte la unidad de llave de memoria USB en el puerto USB de la parte posterior del sistema.
2. Encienda el sistema e inicie una sesión en la HMC.
3. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
4. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
5. Siga las instrucciones de la pantalla en el asistente para instalar el servicio corrector de la HMC.

A continuación, tendrá que configurar el software de su HMC. Encontrará las instrucciones en: "Configuración de la HMC" en la página 38.

Conceptos relacionados

Configuración de la conectividad de BMC
Puede configurar o visualizar los valores de red en el BMC para la consola de gestión.

Instalación del dispositivo virtual de la HMC

Información sobre cómo instalar el dispositivo virtual de Hardware Management Console (HMC).

El dispositivo virtual de la HMC se puede instalar en la infraestructura virtualizada x86 o POWER. El dispositivo virtual de la HMC admite los siguientes hipervisores de virtualización x86:

- Máquina virtual basada en kernel (KVM)
- Xen
- VMware

El dispositivo virtual de la HMC soporta los hipervisores de virtualización de POWER siguientes:

- PowerVM

Requisitos mínimos para ejecutar el dispositivo virtual de la HMC:

- 16 GB de memoria
- 4 procesadores virtuales
- 2 interfaces de red (máximo de 4 permitidos)
- 1 unidad de disco que contiene 500 GB de espacio de disco disponible

Notas:

- El procesador en los sistemas que alojan el dispositivo virtual de la HMC debe ser Intel VT-x o un procesador habilitado para la virtualización de hardware AMD-V.
- Los DVD del dispositivo virtual de la HMC que recibe no se pueden arrancar. Primero debe montar el soporte de almacenamiento y luego copiar el archivo `.tgz` del soporte de almacenamiento. El método para montar el DVD puede variar en función del sistema operativo que utilice.

- La sintaxis de mandatos que se utilicen en los ejemplos siguientes pueden variar en función del sistema operativo que utilice.
- El hipervisor de virtualización de PowerVM requiere 160 GB de espacio de disco. No obstante, 500 GB de memoria es lo recomendado.
- El requisito mínimo de procesador PowerVM son 1.0 unidades de procesador y cuatro procesadores virtuales compartidos en modalidad de compartimiento acotado. No es recomendable utilizar procesadores dedicados. El procesador PowerVM también requiere 16 GB de memoria.

Información relacionada

Imágenes e instrucciones de instalación de la versión 8 de la HMC

Instalación del dispositivo virtual de la HMC en x86

Información sobre cómo instalar el dispositivo virtual de Hardware Management Console (HMC) en un entorno x86.

Instalación del dispositivo virtual de la HMC utilizando el hipervisor de KVM

Aprenda a instalar el dispositivo virtual de Hardware Management Console (HMC) utilizando el hipervisor de la máquina virtual basada en kernel (KVM).

Para instalar el dispositivo virtual de la HMC en KVM, siga estos pasos:

Nota: En los pasos siguientes se utiliza la interfaz de línea de mandatos y se requiere autoridad de usuario root. La sintaxis del mandato puede variar en función del sistema operativo.

1. Verifique que los paquetes de virtualización se hayan instalado en los sistemas con Red Hat Enterprise Linux (RHEL) versión 7.0 o posterior.
2. Descargue el archivo `<nombre de archivo de instalación de vHMC de KVM>.tar.gz` en el sistema host.
3. Ejecute el siguiente mandato: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Ejecute el siguiente mandato: `cd /var/lib/libvirt/images/vHMC`.
5. Para extraer las imágenes de disco virtual, ejecute el siguiente mandato: `tar -zxvf <nombre de archivo de instalación de vHMC de KVM>.tgz`

   Nota: En este mandato, especifique la vía de acceso completa del archivo .tar del dispositivo virtual de la HMC.
6. Se proporciona un archivo **domain.xml** en el archivo `<nombre de archivo de instalación de vHMC de KVM>.tar.gz`. Siga estos pasos:
   a. Edite el archivo **domain.xml** y verifique que la vía de acceso al disco sea correcta. Este archivo contiene la serie **DISK_PATH**.
   b. Asegúrese de que se utilice `virtio` en el valor de bus del dispositivo de disco.
   c. Puede elegir otro nombre para la VM. El nombre predeterminado en el archivo **domain.xml** es **vHMC**.
   d. Verifique que la dirección de control de acceso a soportes (MAC) esté establecida en el archivo **domain.xml**. Este archivo contiene la serie **MAC_ADDRESS**.

      Nota: Elimine esta línea si desea que la dirección MAC se genere automáticamente.
   e. Verifique que los puentes coincidan con los dispositivos Ethernet. El archivo **domain.xml** predeterminado especifica un Ethernet.
   f. Si utiliza el motor de activación, sustituya **AEDISK** por el nombre de la imagen del disco virtual del motor de activación. De lo contrario, extraiga el elemento del disco.
7. Para definir la VM, ejecute el siguiente mandato: `virsh define <domain>.xml`.
8. Para verifique que la HMC virtual se haya añadido a la lista de máquinas virtuales definidas, ejecute el mandato siguiente: `virsh list --all`.
9. Para iniciar la VM, ejecute el siguiente mandato: `virsh start vHMC`.

10. Para determinar el número de pantalla de sistema de red virtual (VNC) de la consola, ejecute el siguiente mandato: `virsh vncdisplay vHMC`.
11. Para conectarse a la consola con un visor VNC, ejecute el siguiente mandato: `vncviewer HOSTNAME:ID` (donde ID es el número de pantalla, por ejemplo, `0`).

    Nota: Si requiere acceso remoto, debe descartar o configurar el cortafuegos para permitir el acceso al puerto 5900.

Instalación del dispositivo virtual de la HMC utilizando el hipervisor Xen

Información sobre cómo instalar el dispositivo virtual de Hardware Management Console (HMC) utilizando el hipervisor Xen.

El dispositivo virtual de la HMC admite la versión 4.2 o posterior de Xen.

Para instalar el dispositivo virtual de la HMC utilizando el hipervisor Xen, siga estos pasos:

Nota: En los pasos siguientes se utiliza la interfaz de línea de mandatos y se requiere autoridad de usuario root. La sintaxis del mandato puede variar en función del sistema operativo.

1. Verifique que los paquetes de virtualización se hayan instalado en los sistemas con Red Hat Enterprise Linux (RHEL) versión 6.4 o posterior.
2. Descargue el archivo `<nombre de archivo de instalación de XEN vHMC>.tar.gz` al sistema de host.
3. Ejecute el siguiente mandato: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Ejecute el siguiente mandato: `cd /var/lib/libvirt/images/vHMC`.
5. Para extraer las imágenes de disco virtual, ejecute el mandato siguiente: `tar -zxvf <nombre de archivo de instalación de XEN vHMC>.tgz`

   Nota: En este mandato, especifique la vía de acceso completa del archivo .tar del dispositivo virtual de la HMC.
6. Se proporciona un archivo **vhmc.cfg** en el archivo `<nombre de archivo de instalación vHMC de XEN>.tar.gz`. Abra el archivo **vhmc.cfg** en un editor de texto y edite los valores siguientes:
   a. Cambie el nombre de la HMC virtual (opcional): edite el archivo **vhmc.cfg** y verifique que la vía de acceso a los discos sea correcta. Este archivo contiene la serie **DISK_PATH**.
   b. Sustituya **DISK_PATH** por la vía de acceso de `disk1.img`:

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

   c. Sustituya **adaptador Ethernet** y añada la dirección MAC (opcional):

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

      Dirección MAC opcional:

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

      Nota: Cuando se rearranca la HMC virtual, el hipervisor Xen vuelve a generar automáticamente una dirección MAC. La adición de la dirección MAC opcional resuelve este problema.
   d. Sustituya **FLOPPYPATH** (si está utilizando el motor de activación):

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

7. Para crear e iniciar la máquina virtual, ejecute el mandato siguiente: `xl create vHMC.cfg`.
8. Para comprobar que se ha añadido la máquina virtual en la lista de máquinas virtuales definidas, ejecute el mandato siguiente: `xl list`.
9. Para acceder a la consola local de la máquina virtual, ejecute el mandato siguiente: `vncviewer localhost 0`.

Instalación del dispositivo virtual de la HMC utilizando VMware ESXi

Información sobre cómo instalar el dispositivo virtual de Hardware Management Console (HMC) utilizando VMware ESXi.

Puede instalar el dispositivo virtual de la HMC en VMware ESXi utilizando la interfaz gráfica de usuario en el cliente vSphere para desplegar la plantilla OVF (Open Virtualization Format).

Nota: Puede instalar el dispositivo virtual de la HMC en VMware ESXi versión 6.0 o posterior.

Para instalar el dispositivo virtual de la HMC en VMware ESXi utilizando el cliente vSphere, siga estos pasos:

Nota: La sintaxis del mandato puede variar en función del sistema operativo.

1. Obtenga el archivo de archivado Tar: `<nombre de archivo de instalación de vHMC de VMware>.tgz`.
2. Utilice el mandato `tar` para extraer el archivo OVA del archivo de archivado Tar.
3. Inicie el cliente vSphere e inicie una sesión en el host ESXi.
4. En el menú **Archivo**, seleccione **Desplegar plantilla de OVF**.
5. Pulse **Examinar** y seleccione el archivo OVA.
6. Pulse **Siguiente**.
7. Una vez realizado el despliegue, pulse **Cerrar** y seleccione el icono del dispositivo virtual de la HMC para encender la dispositivo virtual de la HMC.

Instalación del dispositivo virtual de la HMC en POWER

Información sobre cómo instalar el dispositivo virtual de Hardware Management Console (HMC) en un entorno de POWER virtualizado.

Instalación del dispositivo virtual de la HMC en PowerVM (partición lógica)

Información sobre cómo instalar el dispositivo virtual de Hardware Management Console (HMC) en un entorno PowerVM.

El dispositivo virtual de la HMC da soporte a servidores POWER9 en el nivel de firmware FW910 o posterior. Para obtener más información, consulte Distribuciones de Linux para sistemas POWER8 y POWER9 Linux on Power (https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm).

Notas:

1. No puede gestionar el servidor que aloja el dispositivo virtual de la HMC.
2. No puede gestionar el servicio que aloja a otro dispositivo virtual de la HMC que está gestionando el servidor que aloja este dispositivo virtual de la HMC.

   Por ejemplo, dispositivo virtual de la HMC A se ejecuta en el servidor A y dispositivo virtual de la HMC B se ejecuta en el servidor B. dispositivo virtual de la HMC A no puede gestionar el servidor B y dispositivo virtual de la HMC B no puede gestionar el servidor A simultáneamente. Uno del dispositivo virtual de la HMC puede gestionar el otro servidor, pero el dispositivo virtual de la HMC no se pueden gestionar entre sí simultáneamente.

.

Crear imagen de instalación HMC automatizada (opcional)

Puede crear una imagen de instalación HMC automatizada que instala automáticamente el dispositivo virtual de la HMC sin solicitar el asistente de **Instalación de HMC**.

Nota: El dispositivo virtual de la HMC en PowerVM proporciona soporte de adaptador gráfico para adaptadores que están asignados a la partición. Puede utilizar un navegador web soportado para conectar con la HMC para soporte de interfaz de usuario.

Para crear una imagen de instalación automatizada de HMC, siga estos pasos:

1. Cree dos directorios ejecutando los mandatos siguientes: `mkdir -p oldiso` y `mkdir -p newiso`.
2. Monte la imagen de instalación de la HMC en el directorio **oldiso** ejecutando el mandato siguiente: `sudo mount -o loop <vía_acceso_imagen> oldiso`.
3. Copie el contenido del directorio **oldiso** en el directorio **newiso** ejecutando el mandato siguiente: `cp -r oldiso/* newiso`.
4. Edite el archivo Grub para la instalación automatizada ejecutando el mandato siguiente: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Haga que el archivo Grub sea de solo lectura ejecutando el mandato siguiente: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Cree un ISO de instalación HMC nuevo ejecutando el mandato siguiente `mkisofs -o <nuevo_nombre_iso> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso` (donde **etiqueta ISO** debe ser `HMC-<número de release de versión hmc>`, por ejemplo `HMC-8.0.870.0`).

Nota: Para obtener más información sobre cómo configurar el motor de activación y el archivo de configuración, consulte "Utilización del motor de activación para el dispositivo virtual de la HMC" en la página 32.

Configuración de volumen lógico

Para configurar el volumen lógico, realice los pasos siguientes:

1. Seleccione un sistema gestionado.
2. En el pod del menú, seleccione **Acciones del sistema** > **Power VM** > **Almacenamiento virtual**.
3. Seleccione **Gestionar VIOS del sistema** > **Acción** > **Gestionar almacenamiento virtual**.
4. Seleccione la pestaña **Discos virtuales**.
5. Pulse **Crear disco virtual** y especifique la información siguiente:
   - **Nombre disco virtual**: El nombre del disco virtual.
   - **Nombre de la agrupación de almacenamiento**: El nombre de la agrupación de almacenamiento.
   - **Tamaño de disco virtual**: El tamaño del disco virtual.
   - **Partición asignada**: El nombre de la partición lógica.

   Nota: Es necesario un mínimo de 160 GB de espacio de disco (se recomiendan 500 GB de espacio de disco).

Configuración de soporte de instalación - crear biblioteca de soporte

Para crear una biblioteca de soporte, siga estos pasos:

1. Seleccione un sistema gestionado.
2. En el pod del menú, seleccione **Acciones del sistema** > **Power VM** > **Almacenamiento virtual**.
3. Seleccione **Gestionar VIOS del sistema** > **Acción** > **Gestionar almacenamiento virtual**.
4. Seleccione la pestaña **Dispositivos ópticos**.
5. Pulse **Crear biblioteca** y especifique la información siguiente:
   - **Agrupación de almacenamiento**: El nombre de la agrupación de almacenamiento.
   - **Tamaño de biblioteca de soporte**: El tamaño de la biblioteca de soporte.
6. Pulse **Aceptar**.

Configuración de soporte de instalación - cargar soporte en VIOS

Para cargar soporte en Servidor de E/S virtual (VIOS), siga los pasos siguientes:

1. Inicie la sesión en VIOS.
2. En la modalidad raíz VIOS, ejecute el mandato siguiente: `oem_setup_env`.
3. Para permitir la conexión NFS, ejecute el mandato siguiente: `nfso -o nfs_use_reserved_ports=1`.
4. Para montar el NFS en la carpeta local de VIOS, ejecute el mandato siguiente: `mount <ip_servidor>:/Mountpoint <carpeta_local>`.
5. Para verificar que el montaje de NFS incluya la instalación de HMC y la imagen de configuración de ISO y de motor de activación (opcional), ejecute el mandato siguiente: `ls`.

Configuración de soporte de instalación - enlazar soporte con biblioteca de soporte

Para enlazar soporte con la biblioteca de soporte, siga los pasos siguientes:

1. Vaya a **Gestiona VIOS del sistema** > **Acción** > **Gestionar almacenamiento virtual** y seleccione la pestaña **Dispositivos ópticos**.
2. En la sección **Soporte óptico virtual**, seleccione **Añadir soporte** del menú **Acciones**.
3. En la ventana **Añadir soporte virtual**, seleccione **Añadir archivo existente del sistema de archivos VIOS** y entre la información siguiente:
   - **Nombre de soporte**: El nombre del soporte (por ejemplo, `HMCInstall` o `AEDrive`).
   - **Nombre de archivo de soporte óptico**: El nombre del archivo ISO de instalación (por ejemplo, `01234567-ppc64ie.iso`).
4. Pulse **Aceptar**.
5. Si ha creado una imagen de configuración de motor de activación, repita pasos 3 - 4 para añadir la imagen de configuración del motor de activación. De lo contrario, continúe hasta el paso 6.
6. Verifique el soporte óptico se cargue en la biblioteca de soporte verificando que el nombre del soporte aparezca en la lista **Soporte óptico virtual** disponible.

Configuración de la partición lógica

Para configurar la partición lógica, siga estos pasos:

1. Seleccione un sistema gestionado.
2. En el pod del menú, seleccione **Acciones del sistema** > **Particiones** > **Particiones**.
3. Pulse **Crear partición** y especifique la información siguiente:
   - **Nombre de partición**: El nombre de la partición.
   - **ID de partición**: El ID de la partición.
   - **Tipo de partición**: Seleccione el sistema operativo (**AIX/Linux** o **IBM i**).
4. Pulse **Aceptar**.
5. Asigne el número de procesadores y la cantidad de memoria para la partición.

   Nota: Se precisa un mínimo de cuatro procesadores virtuales y 8 GB de memoria.
6. En el pod del menú, seleccione **Acciones de partición** > **E/S virtual** > **Redes virtuales**.
7. Pulse **Conectar red virtual** y seleccione el recuadro de selección **Mostrar y conectar nuevos adaptadores Ethernet virtuales**. En la tabla, seleccione los adaptadores de red virtual que desee conectar a la partición lógica.

   Nota: Está permitido un máximo de cuatro adaptadores de red virtual.
8. En el pod de menú, seleccione **Acciones de partición** > **E/S virtual** > **Almacenamiento virtual**.
9. En la pestaña **Dispositivo óptico virtual**, pulse **Añadir dispositivo óptico virtual**.

10. Especifique el **Nombre de dispositivo** (por ejemplo, `HMCInstall` o `AEDrive`) y seleccione el servidor de E/S virtual buscados de la tabla.

    Nota: La instalación de `AEDrive` es opcional.
11. Pulse **Aceptar**.
12. Verifique que los dispositivos ópticos virtuales que ha añadido en el paso 10 estén listados ahora en la tabla.
13. En el menú **Acción**, pulse **Cargar**.
14. Seleccione el archivo de soporte para asignar a la partición lógica y pulse **Aceptar**.
15. Verifique que los dispositivos ópticos virtuales que ha cargado en el paso 13 estén listados ahora en la tabla.

Iniciar la dispositivo virtual de la HMC

Nota: Cuando instale el dispositivo virtual de la HMC en una partición utilizando el archivo de imagen ISO de la HMC, no tendrá acceso a la consola gráfica local para la interfaz de usuario de la web.

Para iniciar el dispositivo virtual de la HMC en PowerVM, siga estos pasos:

1. Seleccione la partición gestionada.
2. Abra una conexión activa a la partición lógica seleccionando **Acciones** > **Console** > **Abrir ventana terminal**.
3. Active la partición lógica seleccionando **Acciones** > **Activar**.
4. Seleccione **Activar (Normal)** y **Configuración actual**.
5. Pulse **Finalizar**.
6. Vaya a la ventana de terminal.
7. En el menú **Arrancar**, seleccione **1 = Menú SMS**.
8. En el menú **Principal**, seleccione **5 = Seleccionar opciones de arranque**.
9. En el menú de **Arranque múltiple**, seleccione **1 = Seleccionar instalar/dispositivo de arranque**.
10. En el menú **Seleccionar tipo de dispositivo**, seleccione **5 = Lista todos los dispositivos**.
11. Seleccione el dispositivo `HMCInstall` basándose en la ubicación del dispositivo.
12. Seleccione **2. Arranque de modalidad normal**.
13. Seleccione **1. Sí** para confirmar.
14. Siga las instrucciones en la pantalla del asistente **Instalación de HMC**.

    Nota: Omita este paso si ha utilizado una imagen de instalación automatizada de HMC.
15. Una vez finalizada la instalación e iniciado el sistema, debe seleccionar un idioma del recuadro de diálogo **Selección de idioma**.
16. Acepte el acuerdo de licencia.

    Nota: Asegúrese de que el controlador de mandatos esté listo para aceptar mandatos antes de ejecutar ningún mandato. Por ejemplo, ejecute el mandato **`lshmc -V`** hasta que el resultado sea satisfactorio.
17. Inicie sesión como `hscroot` y utilice el mandato **chhmc** para configurar la red.

    En el ejemplo siguiente se muestra la secuencia de los mandatos **chhmc** que se pueden utilizar para configurar la red y habilitar Secure Shell y el acceso web remoto en la HMC.

```
chhmc
-c network -s modify -i ethX -a <dirección ip hmc> -nm <máscara de red hmc> --lparcomm on
chhmc -c network -s modify -h <nombre_host hmc> -d <nombre dominio hmc> -g <ip pasarela>
chhmc -c network -s add -ns <servidor nombres> -ds <buscar en dominio>
chhmc -c ssh -s enable
chhmc -c ssh.name -s add -a <dirección ip>
chhmc -c SecureRemoteAccess.name -s add -a <dirección ip>
```

```
chhmc -c remotewebui -s enable -i ethX
hmcshutdown -r -t now
```

- **ethX** es el nombre de interfaz de red para configurar.
- **dirección ip hmc** es la dirección IP de su HMC.
- **máscara red hmc** es la máscara de red de su HMC.
- **nombre_host hmc** es el nombre de host de su HMC.
- **nombre dominio hmc** es el nombre del dominio de su HMC.
- **ip pasarela** es la dirección IP de la pasarela de su red.
- **servidor nombres** es la dirección del servidor de nombres de su red.
- **buscar dominio** es el nombre de los dominios en los que desea que la HMC efectúe búsquedas.
- Para permitir el acceso a todas las direcciones IP, utilice **-a 0.0.0.0 -nm 0** en lugar de **dirección ip**.

Nota: Cuando utilice varios adaptadores Ethernet virtuales, ejecute el mandato **`cat /etc/sysconfig/network-scripts/ifcfg-ethX`** en el dispositivo virtual de la HMC en cada interfaz. Compare la dirección de control de acceso de soporte (MAC) en la que HMC aparece en la vista de adaptador de la red virtual de la partición. Puede pulsar **Ver valores del adaptador Ethernet virtual** para obtener más información sobre los adaptadores Ethernet virtuales. Este paso le ayuda a determinar la interfaz correcta que se debe utilizar.

18. Reinicie el sistema.

Utilización del motor de activación para el dispositivo virtual de la HMC

Información sobre cómo utilizar el motor de activación para el dispositivo virtual de Hardware Management Console (HMC).

El motor de activación es una infraestructura que permite configurar varios componentes en una máquina virtual durante el arranque del sistema. Para utilizar el motor de activación, debe configurar un perfil de configuración XML para que el dispositivo virtual de la HMC pueda estar en un estado preparado para la gestión desde el primer inicio. Para obtener más información sobre la configuración del perfil de configuración XML, consulte “Configuración del perfil de configuración para el motor de activación” en la página 33. El archivo de configuración puede utilizarse para configurar las siguientes opciones:

- Establecer el teclado predeterminado (EE.UU.)
- Entorno local predeterminado (EE.UU.)
- Inhabilitar la configuración del teclado
- Inhabilitar la configuración de la pantalla
- Acuerdo de licencia y acuerdo de código de máquina
- Inhabilitar el asistente para la configuración
- Inhabilitar el asistente de llamada al centro de soporte
- Configurar hasta cuatro tarjetas de interfaz de red
- Configurar los valores de cortafuegos para cada interfaz
- Configurar interfaz de red como servidor DHCP IPv4
- Configurar interfaz privada y abierta
- Configurar dispositivo de interfaz de pasarela predeterminado

Nota: El número de adaptadores Ethernet que está definido en el archivo de configuración **vHMC-Conf.xml** debe estar correlacionado con los adaptadores de red definidos en el archivo de configuración **domain.xml**, **vHMC.cfg** o **VMWare**.

El motor de activación requiere un disco virtual que contiene una configuración XML. Puede editar el archivo **datos_usuario** con un editor de texto y utilizar la guía de configuración XML que se muestra en el ejemplo siguiente.

Para crear una imagen de disco virtual ISO con la configuración del motor de activación en un entorno de Linux, realice los pasos siguientes:

1. Cree un directorio:

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

2. Copie el archivo **user_data** editado en el directorio:

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

3. Cree una imagen de disco virtual con la configuración del motor de activación:

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

Configuración del perfil de configuración para el motor de activación

Aprenda a configurar el archivo de configuración del motor de activación utilizando etiquetas XML.

Archivo de configuración

Utilice el siguiente ejemplo del archivo de configuración para obtener información sobre las etiquetas XML.

```
<vHMC-Configuration>
   <ConfigurationVersion>2.0</ConfigurationVersion>
   <LicenseAgreement></LicenseAgreement>
   <AcceptLicense>Yes</AcceptLicense>
   <Locale>en_US.UTF-8</Locale>
   <SetupWizard>No</SetupWizard>
   <SetupCallHomeWizard>No</SetupCallHomeWizard>
   <SetupKeyboard>No</SetupKeyboard>
   <SetupDisplay>No</SetupDisplay>
   <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
      <Hostname></Hostname>
      <Domain></Domain>
      <DNSServers></DNSServers>
      <IPV4Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Netmask></Netmask>
         <Gateway></Gateway>
      </IPV4Config>
      <IPV6Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Gateway></Gateway>
      <IPV6Config>
      <Firewall>
         <PEGASUS>Enabled</PEGASUS>
         <RPD>Enabled</RPD>
         <FCS>Enabled</FCS>
         <I5250>Enabled</I5250>
         <PING>Enabled</PING>
         <L2TP>Disabled</L2TP>
         <SLP>Enabled</SLP>
         <RSCT>Enabled</RSCT>
         <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
         <SSH>Enabled</SSH>
         <NTP>Disabled</NTP>
         <SNMPTraps>Disabled</SNMPTraps>
         <SNMPAgents>Disabled</SNMPAgents>
      </Firewall>
   </Ethernet>
   <NTPServers>
      <ntpparam ntpserver="" ntpversion=""/>
   </NTPServers>
</vHMC-Configuration>
```

Etiquetas XML para el archivo de configuración

Las etiquetas XML se utilizan en el archivo de configuración del motor de activación para establecer valores específicos para varios atributos. Puede establecer manualmente estos valores en el archivo de configuración del motor de activación. Utilice la tabla siguiente para ver una descripción de cada etiqueta y los valores permitidos:

Tabla 9. Etiquetas XML

Etiquetas	Descripción	Valores aceptados	Notas
ConfigurationVersion	Elemento necesario que define la versión de configuración que se utilizará.	**2.0**	
LicenseAgreement	Elemento necesario que muestra el acuerdo de licencia del dispositivo virtual de la HMC.		
AcceptLicense	Elemento necesario para aceptar el acuerdo de licencia del dispositivo virtual de la HMC.	• **Sí**: Acepta el acuerdo de licencia HMC. • **No**: Solicitudes de usuario para aceptar el Acuerdo de licencia HMC	Si se especifica un valor no válido, el motor de activación utiliza de forma predeterminada el valor de **No**.
Entorno local	Elemento necesario para definir los valores del entorno local.	**en_US.UTF-8**	Si se especifica un valor no válido, el motor de activación utiliza de forma predeterminada el valor de **US**.
SetupWizard	Elemento necesario para habilitar o inhabilitar el asistente **Configuración de HMC**.	• **Sí**: Muestra el asistente **Configuración de HMC**. • **Sí**: Inhabilita el asistente **Configuración de HMC**.	Si se especifica un valor no válido, el motor de activación utiliza de forma predeterminada el valor de **Yes**.
SetupCallHomeWizard	Elemento necesario para habilitar o inhabilitar el asistente **Llamada al centro de soporte de la HMC**.	• **Sí**: Muestra el asistente **Llamada al centro de soporte de la HMC**. • **No**: Inhabilita el asistente **Llamada al centro de soporte de la HMC**.	Si se especifica un valor no válido, el motor de activación utiliza de forma predeterminada el valor de **Yes**.
SetupKeyboard	Elemento necesario para definir la configuración de teclado.	• **Sí**: Solicita al usuario la configuración del teclado. • **No**: Acepta la configuración predeterminada del teclado (EE.UU.).	Si se especifica un valor no válido, el motor de activación utiliza de forma predeterminada el valor de **Yes**.
SetupDisplay	Elemento necesario para habilitar o inhabilitar la configuración de pantalla.	• **Sí**: Solicita al usuario la configuración de la pantalla. • **No**: Acepta la configuración de visualización predeterminada.	Si se especifica un valor no válido, el motor de activación utiliza de forma predeterminada el valor de **Yes**.

Tabla 9. Etiquetas XML (continuación)

Etiquetas	Descripción	Valores aceptados	Notas
Ethernet	Elemento necesario que contiene los valores para las configuraciones del adaptador Ethernet. Se puede configurar un máximo de cuatro adaptadores Ethernet.	**Habilitar**: • **Sí**: Configure este adaptador. • **No**: No configure este adaptador. **DefaultGatewayDevice**: • **Sí**: Configure este adaptador como adaptador de red principal. • **No**: No configure este adaptador como el adaptador de red principal. **PrivateInterface**: • **Sí**: Configure este adaptador como una interfaz privada.**Sí** es necesario para configurar la interfaz como un servidor DHCP IPv4. • **No**: No configure este adaptador como una interfaz privada.**No** es necesario para configurar la interfaz como tipo IPv4.	El motor de activación ejecuta la configuración predeterminada si no se especifica ningún valor en la sección del adaptador Ethernet o si están definidos varios **Dispositivos de pasarelas predeterminadas**. Los elementos opcionales se pueden omitir desde la configuración. Como mínimo es necesaria una configuración IPV4 o IPV6. Si no especifica una configuración IP, el motor de activación utiliza la configuración predeterminada.
HostName	Elemento opcional para definir el nombre de host de la red.	Cualquier serie de nombre de host válido.	Si el motor no está definido, el motor de activación utiliza el valor **HostName** de host local predeterminado.
Domain	Elemento opcional para definir el dominio de red.	Cualquier valor de dominio válido (por ejemplo, **example.us.com**).	Si el elemento no está definido, el motor de activación utiliza el valor predeterminado vacío **Domain**.
DNSServers	Elemento opcional para definir los servidores DNS de la red.	Es aceptable tener un valor de servidor DNS o hasta tres direcciones IPv4 o IPv6 válidas que están separadas por una coma. • Ejemplo 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • Ejemplo 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • Ejemplo 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844, ::ffff:903:201	Si el elemento no está definido, el motor de activación utiliza el valor predeterminado vacío **DNSServers**.

Tabla 9. Etiquetas XML (continuación)

Etiquetas	Descripción	Valores aceptados	Notas
IP4Config	Elemento opcional para definir los valores de configuración IPv4.	**IPType**: Elemento necesario para definir el tipo de configuración IPv4. • **Static**: Configure este adaptador mediante la configuración estática. • **DHCP**: Configure este adaptador utilizando la configuración DHCP. • **DHCPServer**: Configure este adaptador para que sea el servidor Pv4 DHCP (requiere **PrivateInterface** para que se establezca en **Sí**). **IPAddress**: Elemento opcional que solo se requiere si la configuración **Static** o **DHCPServer** está seleccionada. • **Configuración estática**: Cualquier valor de dirección IPv4 válido. • **Configuración DHCPServer**: Cualquier IP de servidor DHCP en el rango IP. **Mask**: Elemento opcional que es necesario únicamente si se ha seleccionado la configuración **Static**. • Cualquier valor de máscara IPv4 válido. **Gateway**: Elemento opcional que es necesario únicamente si se ha seleccionado la configuración **Static**. • Cualquier valor de máscara IPv4 válido.	
IP6Config	Elemento opcional para definir los valores de configuración IPv6.	**IPType**: Elemento necesario para definir el tipo de configuración IPv6. • **Static**: Configure este adaptador mediante la configuración estática. • **DHCP**: Configure este adaptador utilizando la configuración DHCP. **IPAddress**: Es aceptable tener un formato IPv6 de formato con formato largo o corto y prefijo IPv6 de formato largo o corto. • Ejemplo 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888 • Ejemplo 2: IPv6: 2001:4860:4860::8888 • Ejemplo 3: IPv6: 2001:4860:4860::8888/128 Si no se especifica ningún prefijo, el motor de activación utiliza el valor predeterminado del prefijo /64. **Gateway**: • Cualquier valor de dirección IPv6 válido.	

Tabla 9. Etiquetas XML (continuación)

Etiquetas	Descripción	Valores aceptados	Notas
Firewall	Elemento opcional para definir los valores del cortafuegos.	**PEGASUS**: • **Habilitado**: Permite que se abran los puertos PEGASUS . • **Inhabilitado**: Inhabilita los puertos PEGASUS. **RPD**: • **Inhabilitado**: Permite que se abran los puertos RMC. • **Inhabilitado**: Inhabilita los puertos RMC. **FCS**: • **Habilitado**: Permite que se abran los puertos FCS. • **Inhabilitado**: Inhabilita los puertos FCS. **I5250**: • **Habilitado**: Permite que se abran los puertos 5250. • **Inhabilitado**: Inhabilita los puertos 5250. **PING**: • **Habilitado**: Permite que el puerto Ping se abra. • **Inhabilitado**: Inhabilita el puerto Ping. **L2TP**: • **Habilitado**: Permite que se abran los puertos L2TP. • **Inhabilitado**: Inhabilita puertos L2TP. **SLP**: • **Habilitado**: Permite que se abran los puertos SLP. • **Inhabilitado**: Inhabilita puertos SLP. **RSCT**: • **Habilitado**: Permite que se abran los puertos RSCT. • **Inhabilitado**: Inhabilita puertos RSCT. **SECUREREMOTEACCESS**: • **Habilitado**: Permite que se abra el acceso remoto seguro a los puertos. • **Inhabilitado**: Inhabilita los puertos de acceso remoto seguro. **SSH**: • **Habilitado**: Permite que se abra el puerto SSH. • **Inhabilitado**: Inhabilita el puerto SSH.	

Tabla 9. Etiquetas XML (continuación)

Etiquetas	Descripción	Valores aceptados	Notas
Firewall	Elemento opcional para definir los valores del cortafuegos.	**NTP**: • **Habilitado**: Permite que se abran los puertos NTP. • **Inhabilitado**: Inhabilita puertos NTP. **SMNPTraps**: • **Habilitado**: Permite que se abran los puertos SMNP. • **Inhabilitado**: Inhabilita puertos SMNP. **SMNPAgents**: • **Habilitado**: Permite que se abran los puertos de agentes SMNP. • **Inhabilitado**: Inhabilita los puertos de agentes SMNP.	

NTPServers	La etiqueta **NTPServers** es necesaria si desea configurar hasta cinco servidores NTP en un dispositivo virtual de la HMC.	**NTPServers**: Acepta `<ntpparam ntpserver="server" ntpversion="version"/>`
		ntpparam:
		• **ntpserver**: Acepta cualquier valor IPv4 o IPv6 válido y nombres de host válidos.
		• **ntpversion**: Acepta 1-4 valor numérico
		Ejemplo:
		`<NTPServers>`
		`<ntpparam ntpserver="test.austin.ibm" ntpversion="2"/>`
		`<ntpparam ntpserver="192.168.34.1" ntpversion="4"/>`
		`<ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>`
		`</NTPServers>`	

Configuración de la HMC

Aprenda a configurar las conexiones de red, configurar su HMC, realizar los pasos posteriores a la configuración y actualizar y renovar su HMC.

Elegir los valores de red en la HMC

Conozca los valores de red que puede utilizar en Hardware Management Console (HMC).

Conexiones de red de la HMC

Aprenda cómo Hardware Management Console HMC se puede utilizar en una red.

Puede utilizar distintos tipos de conexiones de red para conectar la HMC a los sistemas gestionados. Para obtener más información sobre cómo configurar la HMC para conectarse a una red, consulte “Configurar la HMC” en la página 55. Para obtener más información sobre cómo utilizar HMC en una red, consulte la información siguiente:

Tipos de conexiones de red de la HMC

Aprenda a utilizar las funciones de servicio y gestión remota de la HMC mediante la red.

La HMC da soporte a los siguientes tipos de comunicaciones lógicas:

HMC con un sistema gestionado
Se utiliza para realizar la mayoría de las funciones de gestión de hardware, en las que la HMC emite peticiones de función de control a través del procesador de servicio del sistema gestionado. En ocasiones la conexión entre la HMC y el procesador de servicios se denomina *red de servicios*. Esta conexión es necesaria para la gestión de sistemas.

HMC con partición lógica
Se utiliza para recopilar información relacionada con la plataforma (sucesos de error de hardware, inventario de hardware) de sistemas operativos que se están ejecutando en particiones lógica, y para coordinar determinadas actividades de plataforma (LPAR dinámica, reparación simultánea) con esos sistemas operativos. Si desea utilizar las características de notificación de errores y el servicio, debe crear esta conexión.

HMC en el BMC

Nota: La conexión del controlador de gestión de placa base (BMC) se aplica solamente a la HMC, modelo 7063-CR1.

Se utiliza para llevar a cabo tareas de servicio y de mantenimiento. La conexión del BMC se utiliza para cargar y mantener el firmware de la HMC en el sistema. Esta conexión es necesaria para acceder al BMC en la HMC.

HMC con usuarios remotos
Ofrece a los usuarios remotos acceso a las funciones de HMC. Los usuarios remotos pueden acceder a la HMC de la siguiente manera:

- Utilizando el navegador web para acceder de forma remota a todas las funciones de GUI de la HMC.
- Utilizando SSH (Secure Socket Shell) para acceder de forma remota a las funciones de línea de mandatos de la HMC.
- Utilizando un servidor de terminal virtual para el acceso remoto a las consolas de partición lógica virtual.

HMC con servicio y soporte
Se utiliza para transmitir datos como, por ejemplo, informes de errores de hardware, datos de inventario y actualizaciones de microcódigo, hacia y desde el proveedor de servicios. Puede utilizar esta vía de acceso de comunicación para realizar llamadas de servicio automáticas.

La HMC puede admitir hasta cuatro interfaces Ethernet físicas diferentes, en función del modelo. La versión autónoma de la HMC sólo admite tres interfaces de HMC con un adaptador Ethernet integrado y hasta dos adaptadores de plug-in. Utilice cada una de estas interfaces de la siguiente manera:

- Puede utilizarse de forma exclusiva una interfaz de red para las comunicaciones de la HMC con los sistemas gestionados, lo que significa que sólo la HMC y los procesadores de servicio de los sistemas gestionados estarán en dicha red. Pueden utilizarse de forma exclusiva una o varias interfaces de red para las comunicaciones de la HMC con los sistemas gestionados, lo que significa que sólo la HMC y los procesadores de servicio de los sistemas gestionados estarán en dicha red. Aunque las interfaces de red en los procesadores de servicio están cifradas para el protocolo SSL (Secure Sockets Layer) y protegidas por contraseña, tener una red dedicada aparte puede proporcionar un mayor nivel de seguridad para las interfaces.
- Normalmente, se utilizará una interfaz de red abierta para la conexión de red entre la HMC y las particiones lógicas en los sistemas gestionados, para las comunicaciones de la HMC con las particiones lógicas. También puede usar esta interfaz de red abierta para gestionar la HMC de forma remota.
- También puede usar una tercera interfaz para conectarse con particiones lógicas y gestionar la HMC de forma remota. Esta interfaz también se puede utilizar como conexión aparte de la HMC con distintos grupos de particiones lógicas. Por ejemplo, puede tener una LAN administrativa aparte de la LAN donde se ejecutan las transacciones de empresa normales. Los administradores remotos pueden acceder a la HMC y a otras unidades gestionadas utilizando este método. A veces, las particiones lógicas están en

distintos dominios de seguridad de red, quizá detrás de un cortafuegos y, si lo desea, puede tener distintas conexiones de red de la HMC en cada uno de estos dos dominios.

Requisitos de navegador Web para la HMC

La HMC (Hardware Management Console) versión 9.1.0 puede utilizarse con Google Chrome versión 57, Microsoft Internet Explorer (IE) versión 11.0, Mozilla Firefox versiones 45 y 52 Extended Support Release (ESR), así como Safari versión 10.1.

Si su navegador está configurado para utilizar un proxy Internet, debe incluirse una dirección IP local en la lista de excepciones. Consulte a su administrador de red para obtener más información acerca de la lista de excepciones. Si sigue necesitando el proxy para acceder a la HMC, habilite la opción Usar HTTP 1.1 a través de conexiones proxy bajo la pestaña Opciones avanzadas de la ventana Opciones de Internet.

Es necesario habilitar las cookies de sesión para que la ASMI funcione al conectarse remotamente a la HMC. El código de proxy asm guarda información de sesión y la utiliza. Siga los pasos necesarios para habilitar las cookies de sesión.

Habilitación de las cookies de sesión en Internet Explorer.

1. Seleccione Herramientas y pulse Opciones de Internet
2. Seleccione Privacidad y pulse Avanzada
3. Asegúrese de que la opción Aceptar siempre las cookies de sesión esté seleccionada. En caso contrario, seleccione las opciones Invalidar la administración automática de cookies y Aceptar siempre las cookies de sesión.
4. Seleccione Preguntar bajo Cookies de origen y Cookies de terceros
5. Pulse Aceptar.

Habilitación de las cookies de sesión en Firefox.

1. Seleccione Herramientas y pulse Opciones
2. Pulse Cookies
3. Seleccione Permitir que los sitios definan cookies.
4. Seleccione Excepciones y añadir la HMC.
5. Pulse Aceptar.

Redes privadas y abiertas en el entorno de la HMC
Hardware Management Console (HMC) se puede configurar para utilizar redes abiertas y privadas. Las redes privadas permiten el uso de un rango seleccionado de direcciones IP no direccionables. Una red *pública* o "abierta" describe una conexión de red entre la HMC y un número cualquiera de particiones lógicas y otros sistemas en la red normal.

Redes privadas

Los únicos dispositivos en la red privada de la HMC son la propia HMC y cada uno de los sistemas gestionados con los que se conecta la HMC. La HMC se conecta al procesador de servicio flexible (FSP) de cada sistema gestionado.

En la mayoría de los sistemas, el FSP proporciona dos puertos Ethernet que están etiquetados como **HMC1** y **HMC2**. Le permite conectar hasta dos HMC.

Algunos sistemas tienen una opción de FSP dual. En esta situación, el segundo FSP actúa como copia de seguridad redundante. Los requisitos de configuración básica de un sistema con dos FSP son básicamente los mismos que los de un sistema sin un segundo FSP. La HMC debe estar conectada a cada FSP, por lo que se necesita hardware de red (por ejemplo, un concentrador o un conmutador de LAN) cuando hay más de un FSP o varios sistemas gestionados.

Nota: Cada puerto FSP en el sistema gestionado debe estar conectado sólo a una HMC.

Redes públicas

La red abierta se puede conectar a un cortafuegos o un direccionador para conectarse a Internet. La conexión con Internet permite que HMC llame al centro de soporte cuando se debe notificar cualquier error de hardware.

La HMC proporciona su propio cortafuegos en cada una de sus interfaces de red. Cuando se ejecuta el asistente de instalación guiada de la HMC, se configura automáticamente un cortafuegos básico, pero se recomienda personalizar más los valores del cortafuegos después de la instalación y configuración inicial de la HMC.

HMC como un servidor DHCP
Puede utilizar Hardware Management Console (HMC) como servidor DHCP (Dynamic Host Configuration Protocol).

Si desea configurar la primera interfaz de red como una red privada, puede seleccionar entre una amplia gama de direcciones IP para que el servidor las asigne a los clientes. Los rangos de direcciones seleccionables incluyen segmentos de los rangos de direcciones IP no direccionables estándar.

Además de estos rangos estándar, también existe un rango especial de direcciones IP que está reservado a este uso. Este rango especial puede utilizarse para evitar conflictos en los casos en que las redes abiertas conectadas a la HMC estén utilizando uno de los rangos de direcciones no direccionables conflictivos. En función del rango seleccionado, a la interfaz de red de HMC en la red privada se le asigna automáticamente la primera dirección IP de dicho rango y, a continuación, a los procesadores de servicio se les asignan direcciones del resto del rango.

El servidor DHCP de HMC utiliza la asignación automática, lo que significa que a cada interfaz Ethernet exclusiva de procesador de servicio se le reasigna exactamente la misma dirección IP cada vez que se inicie. Cada interfaz de Ethernet tiene un identificador exclusivo que se basa en un dirección MAC (Media Access Control) incorporada, que permite al servidor DHCP reasignar los mismos parámetros de IP. Puede configurar los puertos **eth0** y **eth1** de la HMC para proporcionar direcciones DHCP. Puede configurar los puertos **eth0** y **eth1** de la HMC para proporcionar direcciones DHCP.

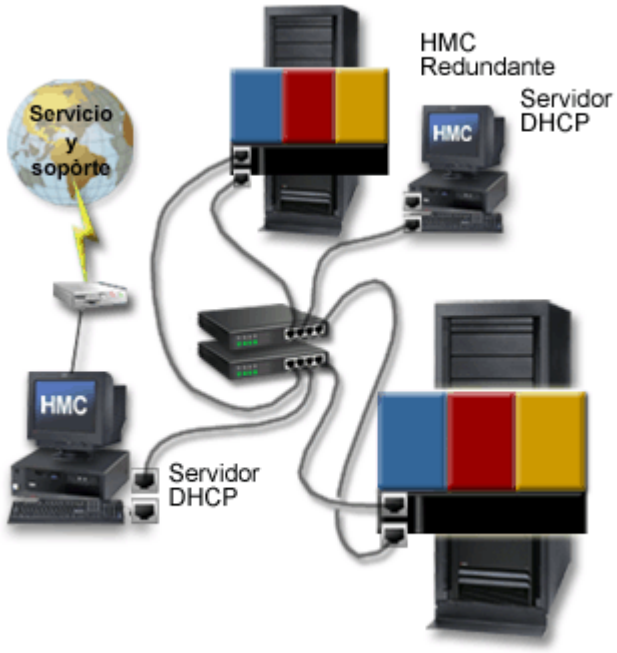
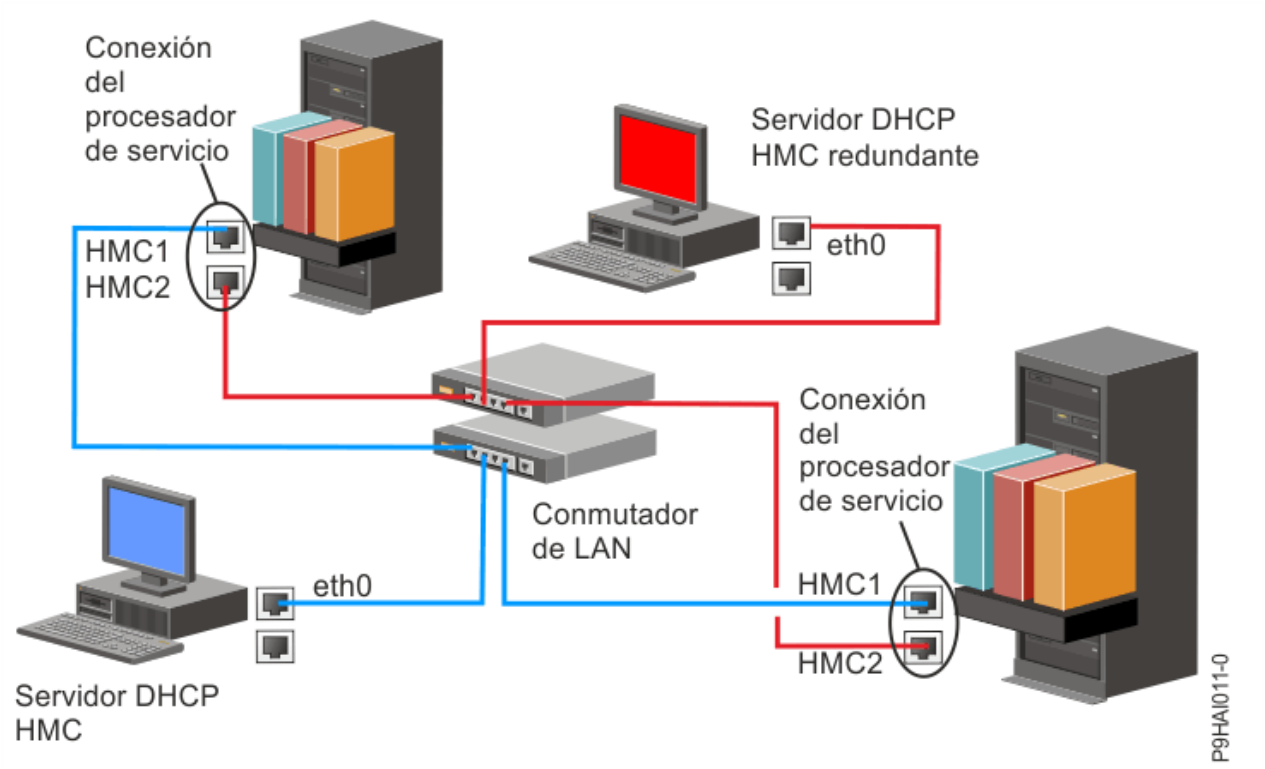


Figura 9. Red privada con una HMC como servidor DHCP

Nota: Si utiliza IPv6, el proceso de descubrimiento debe realizarse manualmente. Para IPv6, la recuperación automática no está disponible.

Para obtener más información sobre cómo configurar la HMC como un servidor DHCP, consulte “Configurar la HMC como un servidor DHCP” en la página 64.

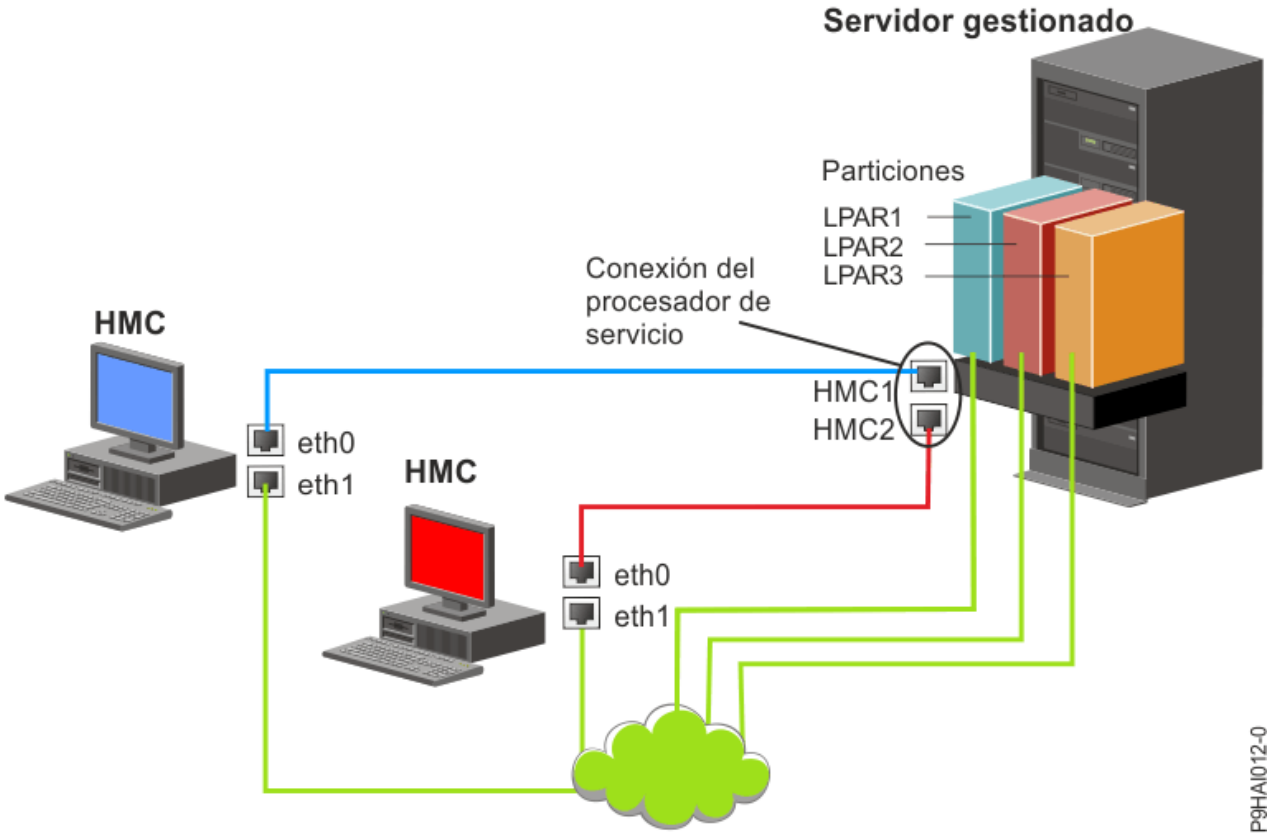


Esta figura muestra un entorno de HMC redundante con dos sistemas gestionados. La primera HMC se conecta al primer puerto de cada FSP y la HMC redundante se conecta al segundo puerto de cada HMC. Cada HMC se configura como servidor DHCP utilizando un rango diferente de direcciones IP. Las conexiones están en redes privadas diferentes. De esta forma, es importante asegurarse de que ningún puerto FSP esté conectado a más de una HMC.

Cada puerto FSP de sistema gestionado que está conectado a una HMC requiere una dirección IP exclusiva. Para asegurarse de que cada FSP tenga una dirección IP exclusiva, utilice la posibilidad de servidor DHCP incorporada de la HMC. Cuando el FSP detecta el enlace de red activo, emite una petición de difusión para localizar un servidor DHCP. Si está configurada correctamente, la HMC responde a dicha petición asignando una entre un rango seleccionado de direcciones.

Si tiene varios FSP, debe tener su propio concentrador o conmutador de LAN para la HMC en la red privada FSP. De manera alternativa, este segmento privado alternativo puede existir como varios puertos en una *LAN virtual* (VLAN) privada en un conmutador gestionado mayor. Si tiene varias VLAN privadas, asegúrese de que estén aisladas y sin tráfico entre ellas.

Si tiene más de una HMC, también debe conectar cada HMC a las particiones lógicas, y entre ellas, en la misma red abierta.



La figura muestra dos HMC conectadas a un servidor gestionado individual en la red privada y a tres particiones lógicas en la red pública. Puede tener un adaptador Ethernet adicional para que la HMC tenga tres interfaces de red. Puede utilizar esta tercera red como red de gestión o conectarla al servidor de gestión CSM (Cluster Systems Manager).

Elegir un método de conectividad para el servidor de llamada al centro de servicio

Contiene información sobre las opciones de conectividad que se ofrecen cuando se utiliza el servidor de llamada al centro de servicio.

Puede configurar Hardware Management Console (HMC) para enviar información relacionada con el servicio de hardware en IBM utilizando una conexión Internet basada en LAN o una conexión de marcación a través de módem.

Dispone de dos posibilidades de comunicación cuando configura la conexión a Internet basada en la LAN. La primera opción es utilizar Secure Sockets Layer (SSL) estándar. La comunicación SSL se puede habilitar para conectarse a Internet a través del servidor proxy. La conectividad SSL es más probable que cumpla las directrices de seguridad corporativa.

Nota: Si la conexión de interfaz de red abierta utiliza únicamente Internet Protocol Versión 6 (IPv6), no puede utilizar la VPN de Internet para la conexión con el centro de soporte. Para obtener más información sobre los protocolos utilizados, consulte “Elegir un protocolo Internet” en la página 45.

Las ventajas de utilizar una conexión a Internet son las siguientes:

- Velocidad de transmisión más rápida
- Gasto reducido del cliente (por ejemplo, el coste de una línea telefónica analógica dedicada)
- Mayor fiabilidad

Están en vigor las siguientes características de seguridad, independientemente del método de conectividad que elija:

- Las peticiones de Recurso de soporte remoto siempre se inician desde la HMC a IBM. Una conexión de entrada nunca se inicia desde el Sistema de soporte de servicio de IBM.

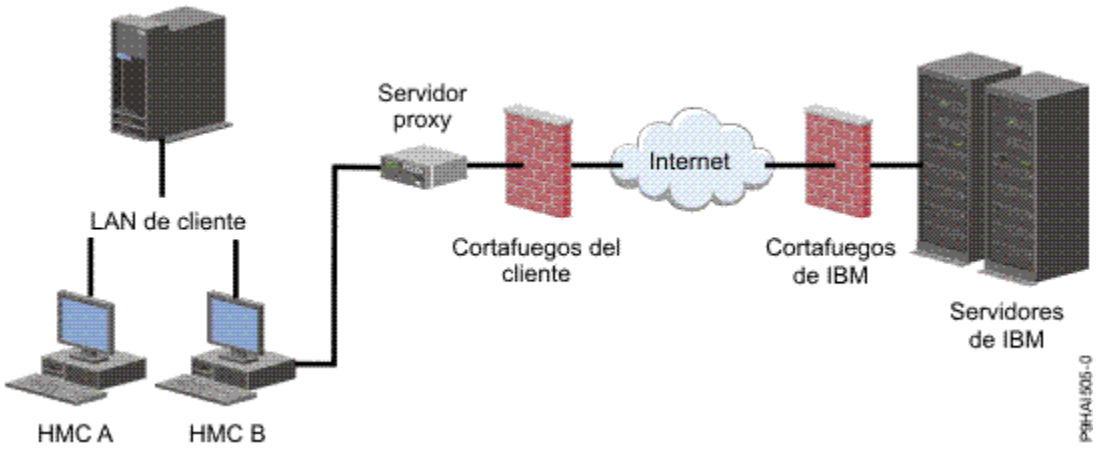
- Todos los datos transferidos entre la HMC y el Sistema de soporte de servicio de IBM se cifran utilizando un cifrado de alto nivel. Dependiendo del método de conectividad elegido, se cifran utilizando SSL o IPSec ESP (Carga útil de seguridad encapsulada).
- Cuando se inicializa la conexión cifrada, la HMC autentica el destino como el del Sistema de soporte de servicio de IBM.

Los datos enviados al Sistema de soporte de servicio de IBM están formados únicamente por información sobre problemas de hardware y configuración. No se transmiten a IBM datos de aplicación o clientes.

Utilización de una conexión a Internet indirecta con un servidor proxy

Si la instalación requiere que la HMC esté en una red privada, puede conectarse directamente a Internet utilizando un proxy SSL, que puede enviar peticiones a Internet. Una de las posibles ventajas de utilizar un proxy SSL es que el proxy puede dar soporte a recursos de registro cronológico y auditoría.

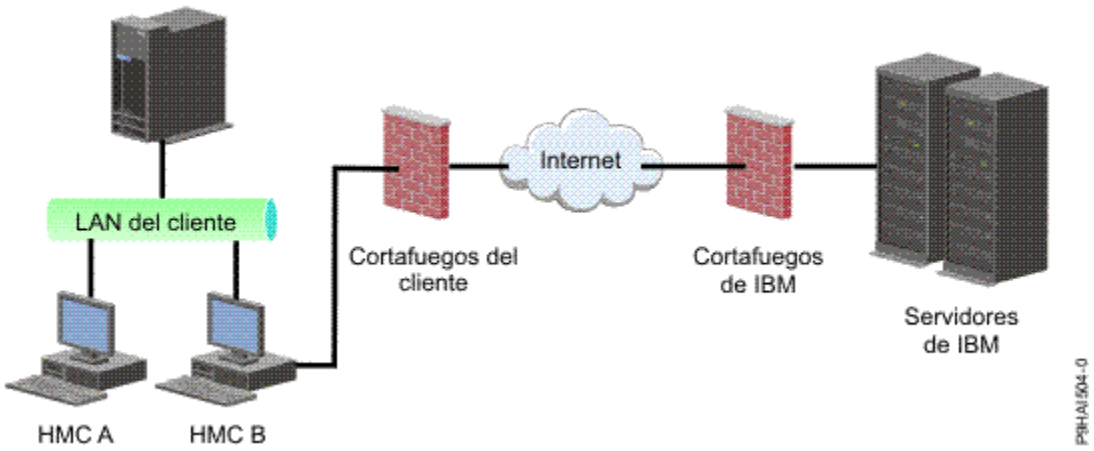
Para enviar sockets SSL, el servidor proxy debe dar soporte a funciones de cabecera proxy básicas (tal como se describe en RFC 2616) y al método CONNECT. De manera opcional, se puede configurar la autenticación de proxy básica (RFC 2617) para que la HMC se autentique antes de intentar enviar sockets a través del servidor proxy.



Para que la HMC se comunique satisfactoriamente, el servidor proxy del cliente debe permitir conexiones con el puerto 443. Puede configurar el servidor proxy para limitar las direcciones IP específicas a las que se puede conectar la HMC. Consulte “Listas de direcciones SSL de Internet” en la página 45 para obtener una lista de las direcciones IP.

Utilizar una conexión SSL a Internet directa

Si la HMC puede conectarse a Internet, y el cortafuegos externo puede configurarse para permitir el flujo de paquetes TCP establecidos hacia los destinos que se describen en “Listas de direcciones SSL de Internet” en la página 45, puede utilizar una Conexión a Internet directa.



Utilizar una conexión SSL de Internet para conectarse al soporte remoto

Todas las comunicaciones se manejan a través de sockets TCP que se han iniciado por la HMC y utilizan una SSL de alto nivel para cifrar los datos que se transmiten. Las direcciones TCP/IP de destino se publican (consulte "Listas de direcciones SSL de Internet" en la página 45) para que se puedan configurar cortafuegos externos para permitir estas conexiones.

Nota: Se utiliza el puerto HTTPS estándar 443 para todas las comunicaciones.

La HMC también se puede habilitar para conectarse directamente a Internet o indirectamente desde un servidor proxy que proporciona el cliente. La decisión sobre cuál enfoque es el idóneo para su instalación depende de los requisitos de red y seguridad de la empresa. La HMC (directamente o mediante el proxy SSL) utiliza las direcciones siguientes cuando se ha configurado para utilizar la conectividad SSL de Internet.

Elegir un protocolo Internet

Determine la versión de la dirección IP que se utiliza cuando se conecta Hardware Management Console (HMC) con el proveedor de servicios.

La mayor parte de los usuarios utilizan Internet Protocol Versión 4 (IPv4) para conectarse a un proveedor de servicios. Las direcciones IPv4 aparecen con el formato que representa los 4 bytes de la dirección IPv4 separados por puntos, (por ejemplo, 9.60.12.123), para acceder a Internet. También puede utilizar Internet Protocol Versión 6 (IPv6) para conectarse a un proveedor de servicios. Los administradores de red suelen utilizar IPv6 para asegurarse un espacio de direcciones exclusivo. Si no está seguro del protocolo Internet que utiliza su instalación, póngase en contacto con el administrador de la red. Para obtener más información sobre el uso de cada versión, consulte los apartados "Configuración de la dirección IPv4" en la página 64 y "Configuración de la dirección IPv6" en la página 65.

Listas de direcciones SSL de Internet

Aprenda las direcciones que la HMC (Hardware Management Console) utiliza cuando la HMC está utilizando la conectividad SSL de Internet.

La HMC utiliza las siguientes direcciones IPv4 para ponerse en contacto con el soporte y el servicio técnico de IBM cuando se configura para utilizar la conectividad SSL de Internet.

Las siguientes direcciones IPv4 son para todas las ubicaciones:

- 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

Las siguientes direcciones IPv4 son para los países americanos:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Las direcciones IPv4 siguientes son para todas las ubicaciones que no se encuentran en el continente americano:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Nota: Cuando configure un cortafuegos para permitir que una HMC se conecte con estos servidores, sólo se necesitan las direcciones IP específicas de la región geográfica.

La HMC utiliza las siguientes direcciones IPv6 para ponerse en contacto con el soporte y el servicio técnico de IBM cuando se configura para utilizar la conectividad SSL de Internet:

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

Utilización de varios servidores de llamada al centro de servicio

Aprenda a saber lo que necesita cuando decide utilizar más de un servidor de llamada al centro de servicio.

Para evitar un punto único de anomalía, configure Hardware Management Console (HMC) de modo que utilice varios servidores de llamada al centro de servicio. El primer servidor de llamada al centro de servicio disponible intenta manejar cada suceso de servicio. Si falla la conexión o la transmisión con este servidor de llamada al centro de servicio, se vuelve a intentar la petición de servicio utilizando otros servidores de llamada al centro de servicio hasta que uno realice la acción correctamente o hasta que se hayan probado todos los servidores.

La HMC conectada que se identifique mediante el análisis de problemas como la consola de análisis principal para un sistema gestionado concreto es la que envíe el informe del problema. Esta consola principal también duplica la notificación de problemas para cualquier HMC secundaria. Esta HMC secundaria debe estar reconocida en la red por la HMC principal. La HMC principal reconoce la HMC secundaria como un servidor de llamada al centro de servicio adicional cuando:

- Se ha configurado la HMC principal para que utilice los servidores de llamada al centro de servicio "detectados" y el servidor de llamada al centro de servicio está en la misma subred que la HMC principal o gestiona el mismo sistema.
- El servidor de llamada al centro de servicio se añade manualmente a la lista de consolas de servidor de llamada al centro de servicio para conexiones de salida.

Preparar la configuración de la HMC

Aprenda los valores de configuración necesarios que debe conocer antes de empezar los pasos de configuración.

Para configurar la HMC debe comprender los conceptos relacionados, tomar decisiones y preparar información.

Conozca la información que necesita para conectar la HMC a las siguientes ubicaciones:

- Procesadores de servicio de los sistemas gestionados
- Particiones lógicas de esos sistemas gestionados
- Estaciones de trabajo remotas
- IBM Service para implementar las funciones de “llamada al centro de servicio”

Para preparar la configuración de la HMC, siga estos pasos:

1. Obtenga e instale el nivel de versión más reciente del código de la HMC que desea instalar.
2. Determine la ubicación física de la HMC en relación con los servidores que gestiona. Si la HMC está a más de 7,6 metros (25 pies) del sistema gestionado, debe proporcionar acceso de navegador web a la HMC desde la ubicación del sistema gestionado para que el personal de servicio pueda acceder a ésta.
3. Identifique los servidores que gestiona la HMC.
4. Determine si utiliza una red privada o abierta para gestionar servidores. Si decide usar una red privada, utilice DHCP, a menos que utilice una configuración CSM (Gestión de sistemas en clúster). CSM no da soporte a IPv6. Para acceder a la CSM, debe tener dos redes. Si desea más información sobre CSM, consulte la documentación que se ha proporcionado con esa función. Para obtener más información sobre las redes abiertas y privadas, consulte “Seleccionar una red privada o abierta” en la página 63.
5. Si utiliza una red abierto para gestionar un FSP, debe establecer la dirección del FSP manualmente mediante los menús de la interfaz de gestión avanzada del sistema. Se recomienda una red privada no direccionable.
6. Si tiene dos HMC, designe una HMC como principal y otra como secundaria. La HMC principal debe estar físicamente más cerca del sistema y debe ser la HMC que se configura para llamadas al centro de servicio.
7. Determine los valores de la red que necesita para conectar la HMC con las estaciones de trabajo remotas, particiones lógicas y dispositivos de red.
8. Defina cómo la HMC llama al centro de servicio. Las opciones de llamada al centro de servicio son a través de una conexión a Internet SSL (Capa de sockets seguros) de salida únicamente, un módem o una conexión VPN (Red privada virtual).
9. Determine los usuarios de la HMC que crea y sus contraseñas, así como las funciones que se les asignarán. Debe asignar una contraseña a los usuarios **hscroot** y **hscpe**.
10. Documente la siguiente información de contacto de la compañía, necesaria al configurar la llamada al centro de servicio:
    - Nombre de la empresa
    - Contacto del administrador
    - Dirección de correo electrónico
    - Números de teléfono
    - Números de fax
    - Dirección postal de la ubicación física de la HMC
11. Si está pensando en utilizar el correo electrónico para avisar a los operadores o administradores de sistemas cuando la información se envía a IBM a través de una llamada al centro de servicio, identifique el servidor SMTP (Protocolo simple de transferencia de correo) y las direcciones de correo electrónico que utiliza.
12. Debe definir las contraseñas siguientes:
    - La contraseña de acceso que se utiliza para autenticar la HMC al FSP.
    - La contraseña de ASMI que se utiliza para el usuario **admin**.
    - La contraseña de ASMI que se utiliza para el usuario **general**.

Cree las contraseñas cuando se conecte desde la HMC a un nuevo servidor por primera vez. Si la HMC es una HMC redundante o secundaria, obtenga la contraseña de usuario de la HMC y esté preparado para especificarla cuando se conecte por primera vez al FSP del servidor gestionado.

Cuando haya realizado estos pasos de preparación, complete "Hoja de trabajo de configuración previa a la instalación para la HMC" en la página 48.

Hoja de trabajo de configuración previa a la instalación para la HMC

Use esta hoja de trabajo para que la información que necesita para la instalación esté preparada.

Política de contraseñas mejorada para HMC

Debe establecer una contraseña nueva en el primer uso para sistemas recién fabricados con la versión HMC 9.940.0 o posterior y después de un restablecimiento de fábrica del sistema. Este cambio de política ayuda a que la HMC no se quede en un estado con una contraseña demasiado conocida.

Con la versión de HMC 9.940.0 y posterior, la contraseña `hscroot` caduca y se debe cambiar antes de poder acceder a las funciones de la HMC. Para obtener más información sobre cómo cambiar la contraseña, consulte https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm. Sin embargo, si está actualizando desde un nivel de HMC anterior o una instalación operativa, no tiene que cambiar la contraseña.

Valores de red

Interfaz de LAN: elija los adaptadores disponibles (como eth0, eth1) que utiliza esta HMC para conectarse a los sistemas gestionados, las particiones lógicas, el soporte y servicio técnico, así como los usuarios remotos. Para obtener más información, consulte "Conexiones de red de la HMC" en la página 38. La conectividad de la HMC puede estar en una red privada o abierta.

Velocidad y modalidad dúplex de adaptador Ethernet

Especifique la velocidad y la modalidad dúplex del adaptador Ethernet que desee. La opción de detección automática determina qué opción es la idónea si no está seguro de qué velocidad y modalidad dúplex producirán resultados óptimos para el hardware. La velocidad de medios Valor predeterminado = Detección automática especifica la velocidad en modalidad dúplex de un adaptador Ethernet. Seleccione Detección automática a menos que deba especificar una velocidad de medios fija. Cualquier dispositivo que esté conectado a FSP (conmutadores/HMC) debe establecerse en la modalidad Auto (Velocidad) / Auto (Dúplex), ya que éste es el valor predeterminado de FSP y no puede cambiarse.

Tabla 10. Velocidad y modalidad dúplex de adaptador Ethernet

Característica	**eth0**	**eth1**	**eth2**	**eth3**
Seleccione la velocidad y la modalidad dúplex				
Velocidad de medios (detección automática, 10/100/1000 dúplex/ semidúplex)				

Para obtener más información sobre las redes abiertas y privadas, consulte "Redes privadas y abiertas en el entorno de la HMC" en la página 40.

Tabla 11. Red privada o abierta				
Característica	**eth0**	**eth1**	**eth2**	**eth3**
Especifique red **Privada** o **Abierta** para cada adaptador.				

El protocolo de configuración de sistema principal dinámico (DHCP) ofrece un método automático para la configuración de clientes dinámicos. Puede especificar esta HMC como un servidor DHCP. Si esta es la primera o la única HMC de la red privada, habilite la HMC como servidor DHCP. Cuando habilita la HMC como servidor DHCP, la HMC configura y detecta automáticamente los sistemas gestionados de la red.

Para los adaptadores Ethernet especificados como redes privadas, complete la tabla siguiente:

Tabla 12. Servidor DHCP		
Características	**eth0**	**eth1**
¿Desea especificar esta HMC como un servidor DHCP? (sí/no)		
Si la respuesta es sí, anote el rango de direcciones IP que desea utilizar.		

Si está utilizando la HMC 7063-CR1, debe conectar el puerto Ethernet **IPMI** para que una red acceda al controlador de gestión de placa base (BMC) en la HMC. Para obtener más información, consulte "Configuración de la conectividad de BMC" en la página 64. Complete las tablas siguientes para su conexión del BMC.

Tabla 13. Conexión del BMC	
Características	**IPMI**
¿Desea configurar esta conexión a través de la modalidad de DHCP? (sí/no)	
Si la respuesta es no, indique las direcciones estáticas especificadas a continuación:	
Dirección IP:	
Máscara de subred:	
Pasarela:	

Para los adaptadores Ethernet especificados como redes *abiertas*, complete las tablas siguientes. Para obtener más información acerca de las diferentes versiones del protocolo Internet, consulte la sección "Configurar los tipos de red de HMC" en la página 58.

Utilización de IPv6

Si está utilizando IPv6, consulte al administrador de la red y decida cómo desea obtener las direcciones IP. A continuación, complete las tablas siguientes:

Tabla 14. IPv6 (estático)				
Característica	**eth0**	**eth1**	**eth2**	**eth3**
¿Está utilizando una dirección IP asignada estáticamente? Si la respuesta es sí, anote aquí la dirección.				

Tabla 15. IPv6 (Servidor DHCP)				
Característica	**eth0**	**eth1**	**eth2**	**eth3**
¿Está obteniendo las direcciones IP desde un servidor DHCP? (sí/no)				

Tabla 16. IPv6 (Direccionador IPv6)				
Característica	**eth0**	**eth1**	**eth2**	**eth3**
¿Está obteniendo las direcciones IP desde un direccionador IPv6?				

Para obtener más información sobre la configuración de direcciones IPv6, consulte el apartado "Configuración de la dirección IPv6" en la página 65. Para obtener más información sobre el uso de las direcciones IPv6, consulte el apartado "Utilización sólo de direcciones IPv6" en la página 65.

Utilización de IPv4

Complete las tablas siguientes para los adaptadores Ethernet que están especificados como redes abiertas mediante IPv4.

Tabla 17. IPv4				
Características	**eth0**	**eth1**	**eth2**	**eth3**
¿Desea obtener una dirección IP automáticamente? (sí/no)				
Si la respuesta es no, indique la dirección especificada a continuación:				
Dirección de interfaz TCP/IP:				
Máscara de red de interfaz TCP/IP:				
Valores de cortafuegos:				
¿Desea configurar los valores de cortafuegos de la HMC? (sí/no)				

Tabla 17. IPv4 (continuación)				
Características	**eth0**	**eth1**	**eth2**	**eth3**
Si la respuesta es sí, liste las aplicaciones y las direcciones IP que se deben permitir a través del cortafuegos:				

Información de TCP/IP
Se necesita una dirección TCP/IP exclusiva para cada nodo, para el Elemento de soporte (SE) y Hardware Management Console (HMC). La máscara de red asignada se utiliza para generar una dirección exclusiva, de forma predeterminada, para la LAN privada local. Si los nodos se conectan a una red mayor con una dirección TCP/IP administrada, puede especificar la dirección TCP/IP que se utilizará. El sistema genera el valor predeterminado.

Valores de cortafuegos
Los valores de cortafuegos de la HMC crean una barrera de seguridad que permite o deniega el acceso a aplicaciones de red en la HMC. Puede especificar estos valores de control de forma individual para cada interfaz de red física, lo que permite controlar a qué aplicaciones de red de la HMC se puede acceder en cada red.

Si configura al menos un adaptador como un adaptador de red abierta, debe proporcionar la siguiente información adicional para habilitar la HMC para acceder a la LAN:

Tabla 18. Adaptador de red abierta	
Información de host local	
Nombre de sistema principal de la HMC:	
Nombre de dominio:	
Descripción de la HMC:	
Información de pasarela	
Dirección de pasarela: (nnn.nnn.nnn.nnn)	
Dispositivo de pasarela:	
Habilitación DNS	
¿Desea utilizar DNS? (sí/no)	
Si la respuesta es “sí”, especifique el orden de búsqueda en el servidor DNS a continuación:	
1.	
2.	
Orden de búsqueda de sufijos de dominio:	
1.	
2.	

Información de host local
Para identificar Hardware Management Console (HMC) en la red, especifique el nombre de host y el nombre de dominio de la HMC. A menos que sólo utilice nombres abreviados de sistema principal en la red, entre un nombre de host totalmente calificado. Ejemplo de nombre de dominio: nombre.suempresa.com

Información de pasarela
Para definir una pasarela predeterminada, rellene la dirección TCP/IP que se va a utilizar para direccionar los paquetes IP. La dirección de pasarela informa a cada sistema o dispositivo de red de cuándo debe enviar los datos si la estación de destino no está en la misma subred que la de origen.

Habilitación DNS
El Sistema de nombres de dominio (DNS) se utiliza para proporcionar un convenio de denominación estándar para localizar los sistemas basados en IP. Mediante la definición de servidores DNS, puede utilizar nombres de host para identificar servidores y consolas de gestión de hardware (HMC), en lugar de direcciones IP.

Orden de búsqueda en el servidor DNS
Especifique las direcciones IP de los servidores DNS en los que se realizarán búsquedas para correlacionar los nombres de sistema principal y las direcciones IP. Este orden de búsqueda sólo está disponible cuando se habilita DNS.

Orden de búsqueda de sufijos de dominio
Especifique los sufijos de dominio que está utilizando. La HMC utiliza sufijos de dominio que se añaden a los nombres no calificados para las búsquedas DNS. Los sufijos se buscan en el orden en el que aparecen. Este orden de búsqueda sólo está disponible cuando se habilita DNS.

Notificación por correo electrónico

Liste la información de contacto de correo electrónico si desea que le notifiquen por correo electrónico si se producen sucesos de problemas de hardware en el sistema.

Tabla 19. Notificación por correo electrónico

Características	**Campo de entrada**
Direcciones de correo electrónico:	
Servidor SMTP:	
Puerto:	
Errores que se deben notificar:	
Sólo sucesos de problemas de llamada automática	
Todos los sucesos de problemas	

Servidor SMTP
Especifique la dirección SMTP (protocolo simple de transferencia de correo) del servidor al que debe notificarse un suceso del sistema. Un ejemplo de nombre de servidor SMTP es `relay.us.ibm.com`.

SMTP es el protocolo que se utiliza para enviar correo electrónico. Cuando se utiliza SMTP, un cliente envía un mensaje y se comunica con el servidor SMTP utilizando el protocolo SMTP.

Si no conoce la dirección SMTP del servidor o no está seguro, póngase en contacto con el administrador de red.

Puerto
Escriba el número de puerto del servidor al que se debe notificar un suceso del sistema, o utilice el puerto predeterminado.

Direcciones de correo electrónico que se deben notificar
Especifique las direcciones de correo electrónico a las que se debe notificar cuando se produzca un suceso del sistema.

- Seleccione **Sólo sucesos de problemas de llamada automática** para recibir notificación solo cuando se producen sucesos que crean una función de llamada al centro de soporte.
- Seleccione **Todos los sucesos de problemas** para recibir una notificación cuando se produzca cualquier suceso.

Información de contacto de servicio

Tabla 20. Información de contacto de servicio	
Características	**Campo de entrada**
Nombre de la empresa	
Nombre del administrador	
Dirección de correo electrónico	
Número de teléfono	
Número de teléfono alternativo	
Número de fax	
Número de teléfono alternativo	
Dirección postal	
Dirección postal 2	
Ciudad o localidad	
Estado	
Código postal	
País o región	
Ubicación de la HMC (si es igual que la dirección de administrador anterior, especifique “ídem”):	
Dirección postal	
Dirección postal 2	
Ciudad o localidad	
Estado	
Código postal	
País o región	

Conectividad y autorización de servicios

Seleccione el tipo de conexión para ponerse en contacto con el proveedor de servicios. Para obtener una descripción de estos métodos, incluidas las características de seguridad y los requisitos de configuración, consulte “Selección de servidores de llamada al centro de servicio para conectar esta HMC con servicio y soporte” en la página 72.

Tabla 21. Conectividad y autorización de servicios	
Características	**Campo de entrada**
Capa de sockets segura (SSL) a través de Internet	_____
Red privada virtual (VPN) a través de Internet	_____

Capa de sockets segura (SSL) a través de Internet:
Si tiene una conexión a Internet existente desde la HMC, puede utilizarla para llamar al proveedor de servicios. Puede conectarse directamente al proveedor de servicios utilizando la Capa de sockets

segura (SSL) a través de la conexión a Internet existente. Seleccione **Utilizar proxy SSL** si desea configurar el uso de la SSL cifrada utilizando una conexión indirecta a través de un proxy SSL.

Tabla 22. SSL	
Características	**Campo de entrada**
¿Utilizar proxy SSL? (sí/no)	
Si la respuesta es sí, indique la información siguiente:	
Dirección:	
Puerto:	
¿Autenticarse con el proxy SSL?	
Si la respuesta es sí, indique la información siguiente:	
Usuario:	
Contraseña:	

Protocolo de conexión Internet utilizado

Para obtener más información acerca de los diversos protocolos de Internet, consulte la sección "Configurar los tipos de red de HMC" en la página 58.

___ IPv4

___ IPv6

___ IPv4 e IPv6

Red privada virtual (VPN)

Si tiene una conexión a Internet existente desde la HMC, puede utilizarla para llamar al proveedor de servicios. Puede conectarse directamente al proveedor de servicios a través de una red privada virtual (VPN) utilizando la conexión a Internet existente.

Nota: Si selecciona la red privada virtual (VPN) a través de Internet, no puede seleccionar ninguna otra opción.

Servidores de llamada al centro de servicio

Determine las HMC que desea configurar para conectar con servicio y soporte como servidores de llamada al centro de servicio. Para obtener más información acerca de cómo utilizar varios servidores de llamada al centro de servicio, consulte la sección "Utilización de varios servidores de llamada al centro de servicio" en la página 46.

___ Esta HMC

___ Otra HMC

Si ha seleccionado **Otra HMC**, liste aquí las demás HMC que se han configurado como servidores de llamada al centro de servicio:

Tabla 23. Otras HMC que se han configurado como servidores de llamada al centro de servicio
Lista de los nombres de host o de las direcciones IP de las HMC que se han configurado como servidores de llamada al centro de servicio

Ventajas de soporte adicionales

Mis sistemas y Búsqueda avanzada

Tabla 24. Mis sistemas y Búsqueda avanzada	
Características	**Campo de entrada**
Listar su ID de IBM	_____
Listar los ID de IBM adicionales	_____

Para poder acceder a información de soporte personalizada de gran valor en las secciones Mis sistemas y Búsqueda avanzada del sitio Web de Electronic Services, los clientes deben registrar su ID de IBM con este sistema. Si no tiene ninguno, puede registrarse para un obtener ID de IBM en: www.ibm.com/account/profile.

Nota: IBM proporciona funciones web personalizadas que utilizan la información que ha recopilado la aplicación de IBM Electronic Service Agent. Para utilizar estas funciones, debe registrarse primero en el sitio Web de IBM Registration en http://www.ibm.com/account/profile.

Para autorizar a los usuarios a que utilicen la información de Electronic Service Agent para personalizar las funciones web, especifique el ID de IBM que ha registrado en el sitio Web de IBM Registration. Vaya a http://www.ibm.com/support/electronic para ver la información de soporte disponible para los clientes que registren un ID de IBM con los sistemas.

Configurar la HMC

Aprenda a configurar conexiones de red, la seguridad, aplicaciones de servicio y algunas preferencias de usuario.

Dependiendo del nivel de personalización que tenga previsto aplicar a la configuración de la HMC, tiene varias opciones para configurar la HMC para que se adapte a sus necesidades. El Asistente de instalación guiada es una herramienta de la HMC diseñada para facilitar la instalación de la HMC. Puede elegir una vía de acceso rápida a través del asistente para crear rápidamente el entorno de HMC recomendado, o puede elegir explorar ampliamente los valores disponibles por los que le guía el asistente. También puede ejecutar los pasos de configuración sin la ayuda del asistente utilizando Configuración de la HMC utilizando los menús.

Antes de empezar, recopile la información de configuración necesaria que necesita para completar los pasos correctamente. Consulte “Preparar la configuración de la HMC” en la página 46 para obtener una lista de la información necesaria. Cuando haya terminado la preparación, asegúrese de haber completado “Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48 y vuelva a este apartado.

Configurar la HMC utilizando la vía de acceso rápida a través del asistente de instalación guiada

En la mayoría de los casos, la HMC puede configurarse para operar de forma eficaz utilizando muchos de los valores predeterminados. Utilice esta lista de comprobación de vía de acceso rápida para preparar la HMC para el servicio. Cuando complete estos pasos, la HMC está configurada como un servidor de protocolo de configuración dinámica de sistemas principales (DHCP) en una red privada (conectada directamente).

Configuración de la HMC utilizando los menús

Esta sección ofrece una lista completa de todas las tareas de configuración de HMC y le guiará por el proceso de configurar su HMC. Elija esta opción si prefiere no utilizar el Asistente de instalación guiada.

Deberá reiniciar la HMC para que se apliquen los cambios de configuración, por lo que se recomienda imprimir esta lista de comprobación y tenerla a mano mientras configura la HMC.

En esta información encontrará referencias a tareas que no están incluidas en este documento. Puede acceder al Información de hardware de IBM Power Systems en la HMC o en la Web. En la HMC, se puede acceder a IBM Knowledge Center desde el ángulo superior derecho de la barra de tareas. En la web, se puede acceder a IBM Knowledge Center en https://www.ibm.com/support/knowledgecenter.

En esta información encontrará referencias a tareas que no están incluidas en este PDF. Puede acceder a materiales de soporte adicionales consultando la sección **Recursos adicionales** en la página de bienvenida de la HMC.

Prerrequisitos

Antes de empezar a configurar la HMC mediante sus propios menús, asegúrese de realizar la actividad de preparación de configuración que se describe en "Preparar la configuración de la HMC" en la página 46.

Tabla 25. Tareas de configuración manual de la HMC y dónde encontrar información relacionada

Tarea	**Dónde encontrar información relacionada**
1. Inicie la HMC.	"Iniciar la HMC" en la página 57
2. Establezca la fecha y la hora.	
3. Cambie las contraseñas predefinidas.	
4. Cree usuarios adicionales y vuelva a esta lista de comprobación cuando haya llevado a cabo este paso.	
5. Configure las conexiones de red.	"Configurar los tipos de red de HMC" en la página 58
6. Para el modelo de HMC 7063-CR1, debe configurar la dirección IP del controlador de gestión de placa base (BMC).	"Configuración de la conectividad de BMC" en la página 64
7. Si está utilizando una red abierta y una dirección IP fija, establezca la información de identificación.	
8. Si está utilizando una red abierta y una dirección IP fija, configure una entrada de direccionamiento como pasarela predeterminada.	"Configurar una entrada de direccionamiento como pasarela predeterminada" en la página 67
9. Si está utilizando una red abierta y una dirección IP fija, configure los servicios de nombres de dominio.	"Configurar servicios de nombre de dominio" en la página 67
10. Si está utilizando una dirección IP fija y tiene habilitado el DNS, configure sufijos de dominio.	"Configurar sufijos de dominio" en la página 68
11. Configure el servidor para conectarse al soporte y servicio técnico de IBM y vuelva a esta lista de comprobación cuando haya llevado a cabo este paso.	"Configuración de la consola local para informar acerca de errores a servicio y soporte " en la página 70
12. Configurar el gestor de sucesos para llamada al centro de soporte.	"Configuración del gestor de sucesos para llamada al centro de soporte" en la página 73
13. Conecte el sistema gestionado a una fuente de alimentación.	
14. Establezca las contraseñas para los sistemas gestionados y cada una de las contraseñas de ASMI (general y admin)	"Establecer contraseñas para el sistema gestionado" en la página 74
15. Acceda a ASMI para establecer la fecha y la hora en el sistema gestionado.	

Tabla 25. Tareas de configuración manual de la HMC y dónde encontrar información relacionada (continuación)	
Tarea	**Dónde encontrar información relacionada**
16. Inicie el sistema gestionado y vuelva a esta lista de comprobación cuando haya llevado a cabo este paso.	
17. Asegúrese de que tiene una partición lógica en el sistema gestionado.	
18. Opcional: añada otro sistema gestionado y vuelva a esta lista de comprobación cuando haya llevado a cabo este paso.	
19. Opcional: si se propone instalar un servidor nuevo con su HMC, configure las particiones lógicas e instale el sistema operativo.	
20. Si no desea instalar un nuevo servidor en estos momentos, ejecute las tareas opcionales de configuración posterior para personalizar aún más la configuración.	"Pasos posteriores a la configuración" en la página 76

Iniciar la HMC

Puede iniciar sesión en la HMC y elegir el idioma que desea mostrar en la interfaz. Utilice el ID de usuario `hscroot` y la contraseña `abc123` predeterminados para iniciar sesión en la HMC por primera vez.

Acerca de esta tarea

Para iniciar la HMC, realice el procedimiento siguiente:

Procedimiento

1. Encienda la HMC pulsando el botón de encendido.
2. Si su idioma de preferencia es el inglés, continúe con el paso 4.

   Si su idioma de preferencia es distinto del inglés, escriba el número **2** cuando se le solicite que cambie el entorno local.

   Nota: Esta solicitud caduca en 30 segundos si no realiza ninguna acción.
3. Seleccione el entorno local que desea que aparezca en la lista en la ventana **Selección de entorno local** y pulse **Aceptar**. El entorno local identifica el idioma que se utiliza en la interfaz de la HMC.
4. Pulse **Iniciar una sesión y lanzar la aplicación Web de Hardware Management Console**.
5. Inicie una sesión en la HMC con el ID de usuario y la contraseña predeterminados siguientes:

   ID: `hscroot`
   Contraseña: `abc123`

   HMC Enhanced
   Muestra la GUI mejorada más reciente con las funciones ampliadas de PowerVM.

   HMC Classic
   Muestra la GUI estándar sin las funciones ampliadas de PowerVM.

   Nota: Cuando la HMC está trabajando como un servidor DHCP, la HMC utiliza la contraseña predeterminada cuando se conecta al procesador de servicios por primera vez.
6. Pulse Intro.

Cambio de la fecha y la hora

El reloj con funcionamiento por batería mantiene la fecha y la hora de la Hardware Management Console (HMC). Puede que tenga que restablecer la fecha y la hora de la consola si sustituye la batería o si mueve físicamente el sistema a un huso horario diferente. Aprenda a cambiar la fecha y hora de la HMC.

Acerca de esta tarea

Si cambia la información de fecha y hora, el cambio no afecta a los sistemas y particiones lógicas que gestiona la HMC.

Para cambiar la fecha y hora de la HMC, siga estos pasos:

Procedimiento

1. Asegúrese de que es miembro de uno de los siguientes roles:
   - Superadministrador
   - Representante del servicio técnico
   - Operador
   - Observador
2. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
3. En el panel de contenido, pulse **Cambiar fecha y hora**.
4. Si selecciona **UTC** en el campo **Reloj**, el valor de hora se ajusta automáticamente según el horario de verano del huso horario que seleccione. Especifique la fecha, la hora y el huso horario y pulse **Aceptar**.

Resultados

Configurar los tipos de red de HMC

Configure la HMC para que se puede comunicar con el sistema gestionado, las particiones lógicas, los usuarios remotos, así como con los recursos de servicio y soporte.

Configurar los valores de la HMC con el fin de usar una red abierta para conectarse con el sistema gestionado

Configure la HMC para que se pueda conectar a un sistema y gestionarlo mediante una red abierta.

Antes de empezar

Para configurar los valores de la red de HMC para que se pueda conectar con el sistema gestionado mediante una red abierta, haga lo siguiente:

Tabla 26. Configurar los valores de la HMC con el fin de usar una red abierta para conectarse con el sistema gestionado

Tarea	**Dónde encontrar información relacionada**
1. Decida qué interfaz desea usar para el sistema gestionado. Es preferible **eth0**.	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48
2. Identifique los puertos Ethernet para la HMC.	“Identificar el puerto Ethernet que está definido como eth0” en la página 61
3. Ejecute estas tareas para configurar el adaptador Ethernet:	

Tabla 26. Configurar los valores de la HMC con el fin de usar una red abierta para conectarse con el sistema gestionado (continuación)	
Tarea	**Dónde encontrar información relacionada**
a. Establezca la velocidad de los medios.	“Establecer la velocidad de medios” en la página 63
b. Seleccione el tipo de red abierta.	“Seleccionar una red privada o abierta” en la página 63
c. Establezca las direcciones estáticas.	“Configuración de la dirección IPv6” en la página 65
d. Establezca el cortafuegos.	“Cambiar los valores de cortafuegos de la HMC” en la página 66
e. Configure la pasarela predeterminada.	“Configurar una entrada de direccionamiento como pasarela predeterminada” en la página 67
f. Configure el DNS.	“Configurar servicios de nombre de dominio” en la página 67
4. Configure los adaptadores adicionales, si dispone de ellos.	
5. Pruebe la conexión entre el servidor gestionado y la HMC.	“Probar la conexión entre la HMC y el sistema gestionado” en la página 75

Configurar los valores de HMC con el fin de usar una red privada para conectarse con el sistema gestionado
Configure la HMC para que se pueda conectar a un sistema y gestionarlo mediante una red privada.

Antes de empezar

Para configurar los valores de la red de HMC para que se pueda conectar con el sistema gestionado mediante una red privada, haga lo siguiente:

Tabla 27. Configurar los valores de HMC con el fin de usar una red privada para conectarse con el sistema gestionado	
Tarea	**Dónde encontrar información relacionada**
1. Decida qué interfaz desea usar para el sistema gestionado.	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48
2. Identifique los puertos Ethernet para la HMC.	“Identificar el puerto Ethernet que está definido como eth0” en la página 61
3. Configure la HMC como un servidor DHCP.	“Configurar la HMC como un servidor DHCP” en la página 64
4. Pruebe la conexión entre el servidor gestionado y la HMC.	“Probar la conexión entre la HMC y el sistema gestionado” en la página 75

Configurar los valores de HMC con el fin de usar una red abierta para conectarse con particiones lógicas

Antes de empezar

Para configurar los valores de la red de HMC para que se pueda conectar con particiones lógicas mediante una red abierta, haga lo siguiente:

Tabla 28. Configurar los valores de HMC con el fin de usar una red abierta para conectarse con particiones lógicas	
Tarea	**Dónde encontrar información relacionada**
1. Decida qué interfaz desea usar para el sistema gestionado.	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48
2. Identifique los puertos Ethernet para la HMC.	“Identificar el puerto Ethernet que está definido como eth0” en la página 61
3. Ejecute estas tareas para configurar el adaptador Ethernet:	
a. Establezca la velocidad de los medios.	“Establecer la velocidad de medios” en la página 63
b. Seleccione el tipo de red abierta.	“Seleccionar una red privada o abierta” en la página 63
c. Establezca las direcciones estáticas.	“Configuración de la dirección IPv6” en la página 65
d. Establezca el cortafuegos.	“Cambiar los valores de cortafuegos de la HMC” en la página 66
e. Configure la pasarela predeterminada.	“Configurar una entrada de direccionamiento como pasarela predeterminada” en la página 67
f. Configure el DNS.	“Configurar servicios de nombre de dominio” en la página 67
4. Configure los adaptadores adicionales, si dispone de ellos.	
5. Pruebe la conexión entre el servidor gestionado y la HMC.	“Probar la conexión entre la HMC y el sistema gestionado” en la página 75

Configurar los valores de HMC con el fin de usar una red abierta para conectarse con usuarios remotos

Antes de empezar

Para configurar los valores de la red de HMC para que se pueda conectar con usuarios remotos mediante una red abierta, haga lo siguiente:

Tabla 29. Configurar los valores de HMC con el fin de usar una red abierta para conectarse con usuarios remotos	
Tarea	**Dónde encontrar información relacionada**
1. Decida qué interfaz desea usar para el sistema gestionado.	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48
2. Identifique los puertos Ethernet para la HMC.	“Identificar el puerto Ethernet que está definido como eth0” en la página 61
3. Ejecute estas tareas para configurar el adaptador Ethernet:	
a. Establezca la velocidad de los medios.	“Establecer la velocidad de medios” en la página 63
b. Seleccione el tipo de red abierta.	“Seleccionar una red privada o abierta” en la página 63

Tabla 29. Configurar los valores de HMC con el fin de usar una red abierta para conectarse con usuarios remotos (continuación)	
Tarea	**Dónde encontrar información relacionada**
c. Establezca las direcciones estáticas.	“Configuración de la dirección IPv6” en la página 65
d. Establezca el cortafuegos.	“Cambiar los valores de cortafuegos de la HMC” en la página 66
e. Configure la pasarela predeterminada.	“Configurar una entrada de direccionamiento como pasarela predeterminada” en la página 67
f. Configure el DNS.	“Configurar servicios de nombre de dominio” en la página 67
g. Configure los sufijos.	“Configurar sufijos de dominio” en la página 68
4. Configure los adaptadores adicionales, si dispone de ellos.	

Configuración de los valores del servidor de llamada al centro de servicio de la HMC

Antes de empezar

Para configurar los valores del servidor de llamada al centro de servicio para que puedan enviarse informes de problemas, siga estos pasos:

Tabla 30. Configuración de los valores del servidor de llamada al centro de servicio de la HMC	
Tarea	**Dónde encontrar información relacionada**
1. Asegúrese de que tiene toda la información del cliente necesaria	“Hoja de trabajo de configuración previa a la instalación para la HMC” en la página 48
2. Configure esta HMC para que informe acerca de los problemas o seleccione un servidor de llamada al centro de servicio existente para informar acerca de los errores	“Configuración de la consola local para informar acerca de errores a servicio y soporte ” en la página 70 “Selección de servidores de llamada al centro de servicio para conectar esta HMC con servicio y soporte” en la página 72
3. Verifique que la configuración de las llamadas al centro de servicio esté funcionando	“Verificación de que la conexión con servicio y soporte está funcionando” en la página 72
4. Autorice a los usuarios a que vean los datos del sistema recopilados	“Autorización de los usuarios para que vean los datos del sistema recopilados” en la página 73
5. Planifique la transmisión de los datos del sistema	“Transmisión de la información de servicio” en la página 73

Identificar el puerto Ethernet que está definido como eth0
La conexión Ethernet con el servidor gestionado debe realizarse utilizando el puerto Ethernet que está definido como `eth0` en su HMC.

Si no ha instalado adaptadores Ethernet adicionales en las ranuras PCI de HMC, entonces el puerto Ethernet integrado primario está siempre definido como `eth0` o `eth1` en la HMC, si intenta utilizar la HMC como un servidor HMC para sus sistemas gestionados.

Si instala adaptadores Ethernet adicionales en las ranuras PCI, el puerto que está definido como `eth0` depende de la ubicación y del tipo de adaptadores Ethernet que están instalados.

Nota: Puede que las siguientes reglas generales no se apliquen a todas las configuraciones.

En la tabla siguiente se describen las normas para la colocación de Ethernet por tipo de HMC.

Tabla 31. Tipos de HMC y reglas asociadas para la colocación de Ethernet

Tipo de HMC	Reglas para la colocación de Ethernet
HMC montadas en bastidor con dos puertos Ethernet integrados.	La HMC sólo soporta un adaptador Ethernet más. • Si se instala un adaptador Ethernet más, dicho puerto se define como `eth0`. En este caso, el puerto Ethernet primario integrado se define como `eth1`, y el puerto Ethernet secundario integrado se define como `eth2`. • Si el adaptador Ethernet es un adaptador Ethernet de puerto dual, el puerto etiquetado como Act/Link A es `eth0`. El puerto que está etiquetado `Act/link B` es `eth1`. En este caso, el puerto Ethernet primario integrado se define como `eth2`, y el puerto Ethernet secundario integrado se define como `eth3`. • Si no hay adaptadores instalados, el puerto Ethernet primario integrado se define como `eth0`.
Modelos autónomos con un solo puerto Ethernet integrado.	Las definiciones dependen del tipo de adaptador Ethernet que se ha instalado: • Si sólo se instala un adaptador Ethernet, dicho adaptador se define como `eth0`. • Si el adaptador Ethernet es un adaptador Ethernet de puerto dual, el puerto que se etiqueta `Act/link A` es `eth0`. El puerto que se etiqueta `Act/link B` sería `eth1`. En este caso, el puerto Ethernet integrado primario se define como `eth2`. • Si no hay adaptadores instalados, el puerto Ethernet integrado se define como `eth0`. • Si se han instalado varios adaptadores Ethernet, consulte “Determinar el nombre de interfaz para un adaptador Ethernet” en la página 62.

Determinar el nombre de interfaz para un adaptador Ethernet
Si configura la HMC como un servidor DHCP, dicho servidor puede funcionar sólo en los conectores de la tarjeta de interfaz de red (NIC) que la HMC identifica como `eth0` y `eth1`. También es posible que necesite determinar qué conector NIC necesita para conectar el cable Ethernet. Más información sobre cómo determinar qué conectores NIC identifica la HMC como `eth0` y `eth1`.

Acerca de esta tarea

Para determinar el nombre que la HMC ha asignado a un adaptador Ethernet, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono **Gestión de la HMC**  y, a continuación, seleccione **Valores de consola**.

2. En el panel de contenido, pulse **Cambiar valores de red**.
3. En la ventana **Cambiar valores de red**, pulse la pestaña **Adaptadores de LAN**. La entrada de ejemplo siguiente muestra que este puerto Ethernet se identifica como `eth0`: `Ethernet eth0 52:54:00:fa:b6:8e (<Dirección IP de HMC>)`.
4. Registre los resultados. Si necesita ver o cambiar los valores del adaptador de LAN, pulse **Detalles**.
5. Pulse **Aceptar**.

Establecer la velocidad de medios
Aprenda a especificar la velocidad de los medios, que incluye la velocidad y la modalidad dúplex del adaptador Ethernet.

Antes de empezar

El valor predeterminado de los valores de adaptador de HMC es **Detección automática**. Si este adaptador se conecta con un conmutador de LAN, los valores de puerto de conmutador deben coincidir. Para establecer la velocidad de los medios y la modalidad dúplex, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**.
3. Pulse la pestaña **Adaptadores de LAN**.
4. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
5. En la página Información de Red de área local (LAN), seleccione **Detección automática** o la combinación adecuada de velocidad de medios y modalidad dúplex.
6. Pulse **Aceptar**.

Seleccionar una red privada o abierta
Una *red de servicio privada* está formada por la HMC (Hardware Management Console) y los sistemas gestionados. Una red de servicio privada está restringida a las consolas y los sistemas que gestionan, y está separada de la red de la empresa. Una *red abierta* está formada por la red de servicio privada y la red de la empresa. Una red abierta puede contener puntos finales de red además de consolas y sistemas gestionados, y puede abarcar varias subredes y varios dispositivos de red.

Acerca de esta tarea

Para seleccionar una red privada o pública, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**.
3. Pulse la pestaña **Adaptadores de LAN**.
4. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
5. Pulse la pestaña **Adaptador de LAN**.
6. En la página de información de red de área local, seleccione **Privada** o **Abierta**.
7. Pulse **Aceptar**.

Configurar la HMC como un servidor DHCP
El protocolo de configuración de sistema principal dinámico (DHCP) ofrece un método automático para la configuración de clientes dinámicos.

Para configurar Hardware Management Console (HMC) como un servidor DHCP, realice los pasos siguientes:

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**. Se abre la ventana Personalizar valores de red.
3. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
4. Seleccione **Privada** y, a continuación, seleccione el tipo de red.
5. En la sección Servidor DHCP, seleccione **Habilitar servidor DHCP** para habilitar la HMC como un servidor DHCP.

   Nota: Puede configurar la HMC para que sea un servidor DHCP en una red privada, únicamente. Si utiliza una red abierta, la opción para seleccionar **Habilitar DHCP** no está disponible.
6. Especifique el rango de direcciones del servidor DHCP.
7. Pulse **Aceptar**.

Si ha configurado la HMC como un servidor DHCP en una red privada, debe comprobar que la red privada DHCP de la HMC está configurada correctamente. Para obtener más información sobre cómo conectar la HMC a una red privada, consulte “Seleccionar una red privada o abierta” en la página 63.

Para obtener más información, consulte “ HMC como un servidor DHCP” en la página 41.

Configuración de la conectividad de BMC
Puede configurar o visualizar los valores de red en el BMC para la consola de gestión.

Nota: Esta tarea se aplica solamente al modelo 7063-CR1. Esta conexión es necesaria para acceder al controlador de gestión de placa base (BMC) en la HMC.

Para configurar la conexión del BMC, siga estos pasos:

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red de BMC/IPMI**.
3. Seleccione la modalidad de conexión (**DHCP** o **Estática**).

   Si selecciona la modalidad **Estática**, complete las direcciones siguientes:

   - **Dirección IP**
   - **Máscara de subred**
   - **Pasarela**
4. Pulse **Aceptar**.

También puede configurar la conexión de red del BMC utilizando la interfaz del cargador de arranque Petitboot. Para obtener más información, consulte Configuración de la dirección IP del firmware.

Configuración de la dirección IPv4
Información sobre cómo configurar la dirección IPv4 en la HMC.

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**.
3. Pulse la pestaña **Adaptadores de LAN**.
4. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
5. Pulse la pestaña de valores básicos.
6. Seleccione una dirección IPv4.
7. Si ha seleccionado especificar una dirección IP, especifique la dirección de la interfaz TCP/IP y la máscara de red de la interfaz TCP/IP.
8. Pulse **Aceptar**.

Configuración de la dirección IPv6
Información sobre cómo configurar la dirección IPv6 en la HMC.

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**.
3. Pulse la pestaña **Adaptadores de LAN**.
4. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
5. Pulse la pestaña de valores IPv6.
6. Seleccione una opción de **Configuración automática** o añada una dirección IP estática.
7. Si añade una dirección IP, especifique la dirección IPv6 y la longitud del prefijo y pulse **Aceptar**.
8. Pulse **Aceptar**.

Utilización sólo de direcciones IPv6
Aprenda a configurar la HMC de modo que sólo utilice direcciones IPv6.

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**.
3. Pulse la pestaña **Adaptadores de LAN**.
4. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
5. Seleccione la opción que indica que no hay dirección IPV4.
6. Pulse la pestaña de valores IPv6.
7. Seleccione **Utilizar DHCPv6 para configurar valores de IP** o añada direcciones IP estáticas, a continuación, pulse **Aceptar**.

Qué hacer a continuación

Tras pulsar **Aceptar**, debe reiniciar la HMC para que estos cambios surtan efecto.

Cambiar los valores de cortafuegos de la HMC

En una red abierta, un cortafuegos se usa para controlar el acceso externo a la red de la empresa. La HMC también tiene un cortafuegos en cada uno de sus adaptadores Ethernet. Si desea controlar la HMC de forma remota o dar acceso remoto a otros, modifique los valores de cortafuegos del adaptador Ethernet en la HMC que está conectada a la red abierta.

Acerca de esta tarea

Para configurar un cortafuegos, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**.
3. Pulse la pestaña **Adaptadores de LAN**.
4. Seleccione el adaptador de LAN con el que desee trabajar y pulse **Detalles**.
5. Pulse la pestaña **Cortafuegos**.
6. Utilizando uno de los métodos siguientes, puede permitir cualquier dirección IP utilizando una determinada aplicación a través del cortafuegos o puede especificar una o varias direcciones IP:
   - Permitir cualquier dirección IP utilizando una determinada aplicación a través del cortafuegos:
     a. En el recuadro superior, resalte la aplicación.
     b. Pulse **Permitir entrada**. La aplicación aparece en el recuadro inferior para indicar que se ha seleccionado.
   - Especificar qué direcciones IP desea permitir a través del cortafuegos:
     a. En el recuadro superior, resalte una aplicación.
     b. Pulse **Permitir entrada por dirección IP**.
     c. En la ventana Sistemas principales permitidos, especifique la dirección IP y la máscara de red.
     d. Pulse **Añadir** y pulse **Aceptar**.
7. Pulse **Aceptar**.

Habilitación del acceso al shell restringido remoto

Puede habilitar el acceso al shell restringido remoto cuando configure un cortafuegos.

Acerca de esta tarea

Para habilitar el acceso al shell restringido remoto, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse **Gestión de la HMC**.
2. Pulse **Ejecución remota de mandatos**.
3. Seleccione **Habilitar ejecución de mandato remoto utilizando el recurso ssh** y, a continuación, pulse **Aceptar**.

Qué hacer a continuación

El acceso al shell restringido remoto ya está habilitado.

Habilitar el acceso web remoto

Puede habilitar el acceso web remoto a Hardware Management Console (HMC).

Acerca de esta tarea

Para habilitar el acceso web remoto, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse **Gestión de la HMC**.
2. Pulse **Operación remota**.
3. Seleccione **Habilitar** y, a continuación, pulse **Aceptar**.

Qué hacer a continuación

El acceso Web remoto ya está habilitado.

Configurar una entrada de direccionamiento como pasarela predeterminada

Aprenda a configurar una entrada de direccionamiento como pasarela predeterminada. Esta tarea está disponible cuando utiliza una red abierta.

Antes de empezar

Para configurar una entrada de direccionamiento como pasarela predeterminada, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**. Se abre la ventana Personalizar valores de red.
3. Pulse la pestaña **Direccionamiento**.
4. En el apartado de información de la pasarela predeterminada, especifique la dirección y el dispositivo de pasarela de la entrada de direccionamiento que desee establecer como pasarela predeterminada.
5. Pulse **Aceptar**.

Configurar servicios de nombre de dominio

Si tiene previsto configurar una red abierta, configure servicios de nombre de dominio.

Acerca de esta tarea

Si tiene previsto configurar una red abierta, configure servicios de nombre de dominio. El Sistema de nombres de dominio (DNS) es un sistema de base de datos distribuida para gestionar nombres de sistema principal y las direcciones IP (Internet Protocol) asociadas. La configuración de servicios de nombres de dominio incluye la habilitación de DNS y la especificación del orden de búsqueda de sufijos de dominio.

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**. Se abre la ventana Cambiar valores de red.
3. Pulse la pestaña **Servicios de nombres**.
4. Seleccione **Habilitado para DNS** para habilitar DNS.
5. Especifique el orden de búsqueda en el servidor DNS y el sufijo de dominio y pulse **Añadir**.
6. Pulse **Aceptar**.

Configurar sufijos de dominio

La lista de sufijos de dominio se utiliza para resolver una dirección IP que empieza por la primera entrada de la lista.

Acerca de esta tarea

El sufijo de dominio es una serie que se añade a un nombre de host que se utiliza para resolver su dirección IP. Por ejemplo, un nombre de host `myname` puede que no se resuelva. No obstante, si la serie `myloc.mycompany.com` es un elemento de la tabla de sufijos de dominio, se intenta resolver `myname.mloc.mycompany.com`.

Para configurar una entrada de sufijo de dominio, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Cambiar valores de red**. Se abre la ventana Personalizar valores de red.
3. Pulse la pestaña **Servicios de nombres**.
4. Entre la serie que se va a utilizar como entrada de sufijo de dominio.
5. Pulse **Añadir** para añadirla a la lista.

Configuración de la HMC para que utilice la autenticación remota LDAP

Puede configurar Hardware Management Console (HMC) de modo que utilice la autenticación remota de LDAP (Lightweight Directory Access Protocol).

Antes de empezar

Cuando un usuario inicia la sesión en la HMC, en primer lugar se realiza la autenticación basándose en un archivo de contraseña local. Si no se encuentra un archivo de contraseña local, la HMC se puede poner en contacto con un servidor LDAP remoto para realizar la autenticación. Debe configurar la HMC de modo que utilice la autenticación remota de LDAP.

Nota: antes de configurar la HMC para que utilice la autenticación remota de LDAP, debe asegurarse de que haya una conexión de red en funcionamiento entre la HMC y los servidores LDAP. Para obtener más información acerca de la configuración de las conexiones de red de la HMC, consulte “Configurar los tipos de red de HMC” en la página 58.

Acerca de esta tarea

Para configurar la HMC de modo que utilice la autenticación LDAP, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono **Usuarios y seguridad**  y, a continuación, seleccione **Seguridad de sistemas y consola**.
2. En el panel de contenido, seleccione **Gestionar LDAP**. Se abre la ventana de definición del servidor LDAP.
3. Seleccione **Habilitar LDAP**.
4. Defina un servidor LDAP para utilizarlo para la autenticación.
5. Defina el atributo LDAP que se utiliza para identificar al usuario que se va a autenticar. El valor predeterminado es **uid**, pero puede utilizar sus propios atributos.

6. Defina el árbol de nombres distinguidos, al que también se conoce como base de búsqueda, para el servidor LDAP.
7. Pulse **Aceptar**.
8. Si un usuario desea utilizar la autenticación LDAP, debe configurar su perfil de modo que utilice la autenticación LDAP remota, en lugar de la autenticación local.

Configuración de la HMC para que utilice los servidores KDC (Key Distribution Center) para la autenticación remota de Kerberos

Puede configurar la HMC para que utilice los servidores KDC (Key Distribution Center) para la autenticación remota de Kerberos.

Antes de empezar

Cuando un usuario inicia la sesión en la HMC, en primer lugar se verifica la autenticación basándose en un archivo de contraseña local. Si no se encuentra un archivo de contraseña local, la HMC se puede poner en contacto con un servidor Kerberos remoto para realizar la autenticación. Debe configurar la HMC de modo que utilice la autenticación remota de Kerberos.

Nota: antes de configurar la HMC para que utilice los servidores KDC para la autenticación remota de Kerberos, debe asegurarse de que haya una conexión de red en funcionamiento entre la HMC y los servidores KDC. Para obtener más información acerca de la configuración de las conexiones de red de la HMC, consulte "Configurar los tipos de red de HMC" en la página 58.

Acerca de esta tarea

Para configurar la HMC de modo que utilice los servidores KDC para la autenticación remota de Kerberos, siga los pasos siguientes:

Procedimiento

1. Habilite el servicio Network Time Protocol (Protocolo de hora de la red) y establezca la HMC y los servidores KDC de modo que se sincronice la hora con el mismo servidor NTP. Para habilitar el servicio NTP en la HMC, siga los pasos siguientes:
   a) En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
   b) En el panel de contenido, seleccione **Cambiar fecha y hora**.
   c) Seleccione la pestaña **Configuración de NTP**.
   d) Seleccione **Habilitar servicio NTP en esta HMC**.
   e) Pulse **Aceptar**.
2. Configure cada perfil de usuario de la HMC remota de modo que utilice la autenticación remota de Kerberos, en lugar de la autenticación local.
3. Opcionalmente, puede importar un archivo de claves de servicio en esta HMC. El archivo de claves de servicio contiene el principal del host que identifica la HMC en el servidor KDC. Los archivos de claves de servicio también se conocen como *archivos de tablas de claves*. Para importar un archivo de claves de servicio a esta HMC, siga los pasos siguientes:
   a) En el área de navegación, pulse el icono **Usuarios y seguridad**  y, a continuación, seleccione **Seguridad de sistemas y consola**.
   b) En el panel de contenido, seleccione **Gestionar KDC**.
   c) Seleccione **Acciones > Importar clave de servicio**. Se abre la ventana de importación de claves de servicio.

d) Escriba la ubicación del archivo de claves de servicio.

e) Pulse **Aceptar**.

4. Añada un nuevo servidor KDC a esta HMC. Para añadir un nuevo servidor KDC a esta HMC, siga los pasos siguientes:

a) En el área de navegación, pulse el icono **Usuarios y seguridad**  y, a continuación, seleccione **Seguridad de sistemas y consola**.

b) En el panel de contenido, seleccione **Gestionar KDC**.

c) Seleccione **Acciones > Añadir servidor KDC**. Se abre la ventana de importación de claves de servicio.

d) Escriba la región y el nombre de host o dirección IP del servidor KDC.

e) Pulse **Aceptar**.

Configuración de la consola local para informar acerca de errores a servicio y soporte

Configuración de esta HMC para que pueda realizar llamadas al centro de servicio para informar de errores mediante conexiones de LAN.

Configuración de la HMC para que se pueda conectar con servicio y soporte utilizando el asistente de configuración de llamada al centro de servicio

Configure la HMC de modo que sea un servidor de llamada al centro de servicio utilizando el asistente de llamada al centro de servicio

Antes de empezar

Este procedimiento describe cómo configurar la HMC como un servidor de llamada al centro de servicio mediante conexiones directas (basadas en LAN) e indirectas (SSL) con Internet.

Antes de empezar esta tarea, asegúrese de que:

- El administrador de red verifica que se permita la conectividad. Para obtener más información, consulte “Preparar la configuración de la HMC” en la página 46.
- Si está configurando el soporte de Internet a través de un servidor proxy, además debe tener la información siguiente:
  - La dirección IP y el puerto del servidor proxy
  - La información de autenticación del proxy
- Se usa el adaptador que se ha designado como **eth1** (el que está designado como red abierta). Para obtener más información, consulte “Elegir los valores de red en la HMC” en la página 38.
- Un cable Ethernet conecta físicamente la HMC con la LAN.

Para configurar la HMC para que sea un servidor de llamada utilizando el asistente de llamada al centro de servicio, realice los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestión de servicio**.
2. En el panel de contenido, pulse **Asistente de configuración de llamada al centro de servicio**. Se abre el asistente de conectividad y servidores de llamada al centro de servicio. Siga las instrucciones del asistente para configurar la llamada al centro de servicio.

Configuración de la consola local para informar acerca de errores a servicio y soporte
Configuración de esta HMC para que pueda realizar llamadas al centro de servicio para informar de errores mediante conexiones de LAN.

Configuración de una HMC para ponerse en contacto con el servicio y soporte a través de Internet basado en LAN y SSL
Describe cómo configurar la HMC como servidor de llamada al centro de servicio mediante conexiones directas (basadas en LAN) e indirectas (SSL) a Internet.

Antes de empezar

Antes de empezar esta tarea, asegúrese de que:

- El administrador de red verifica que se permita la conectividad. Para obtener más información, consulte "Preparar la configuración de la HMC" en la página 46.
- Se ha configurado la información de contacto del cliente. Para verificar la información de contacto, vaya a la interfaz de la HMC y pulse **Disponibilidad de servicio>Gestión de servicio > Gestionar información del cliente**.
- Si está configurando el soporte de Internet a través de un servidor proxy, además debe tener la información siguiente:
  - La dirección IP y el puerto del servidor proxy
  - La información de autenticación del proxy
- Como mínimo necesita tener configurada una interfaz de red abierta. Para obtener más información, consulte "Redes privadas y abiertas en el entorno de la HMC" en la página 40.
- Un cable Ethernet conecta físicamente la HMC con la LAN.

Acerca de esta tarea

Para configurar la HMC como un servidor de centro de soporte utilizando una conexión SSL e Internet basada en LAN, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestión de servicio**.
2. En la sección Conectividad, pulse **Gestionar conectividad de salida**. Se abre la ventana de consolas del servidor de llamada al centro de servicio.
3. Pulse **Configurar.**
4. En la ventana de configuración de la conectividad de salida, seleccione **Habilitar sistema local como un servidor de llamada al centro de servicio**.
5. Acepte el acuerdo.
6. En la ventana de configuración de la conectividad de salida, seleccione la página **Internet**.
7. Seleccione el recuadro **Permitir una conexión a Internet existente para el servicio**.
8. Si utiliza un proxy SSL, seleccione el recuadro **Utilizar proxy SSL**.
9. Si utiliza un proxy SSL, complete la dirección y el puerto del proxy. Esta información se debe obtener del administrador de red.
10. Si ha seleccionado **Utilizar proxy SSL** y el proxy requiere autenticación de ID de usuario y contraseña, seleccione el recuadro **Autenticar con el proxy SSL**. Escriba el ID de usuario y la contraseña. El ID de usuario y la contraseña se obtienen del administrador de red.
11. Seleccione el protocolo para Internet que desea utilizar.
12. En la página **Internet**, pulse **Probar**.
13. En la ventana Probar Internet, pulse **Iniciar**.

14. Verifique que la prueba se realiza satisfactoriamente.
15. En la ventana Probar Internet, pulse **Cancelar**.
16. En la ventana de configuración de la conectividad de salida, pulse **Aceptar**.

Selección de servidores de llamada al centro de servicio para conectar esta HMC con servicio y soporte
Elija los servidores de llamada al centro de servicio de la HMC (Hardware Management Console) existentes que la HMC reconoce o detecta para notificar errores.

Antes de empezar

Las HMC detectadas son las HMC que se han habilitado como servidores de llamada al centro de servicio y están en la misma subred o gestionan el mismo sistema gestionado que esta HMC.

Para seleccionar una HMC detectada para llamadas al centro de servicio cuando la HMC informa de errores, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio** y, a continuación, seleccione **Gestión de servicio**.
2. En el panel de contenido, pulse **Gestionar conectividad de salida**. Se abre la ventana de consolas del servidor de llamada al centro de servicio.
3. Pulse **Utilizar consolas de servidor de llamada al centro de servicio detectadas**. La HMC muestra la dirección IP o el nombre de host de las HMC configuradas para llamadas al centro de servicio
4. Pulse **Aceptar**.

Resultados

También puede añadir manualmente servidores de llamada al centro de servicio de HMC que estén una subred diferente. Seleccione la dirección IP o el nombre de host de la HMC que se ha configurado para llamadas al centro de servicio y pulse **Añadir**; a continuación, pulse **Aceptar**.

Verificación de que la conexión con servicio y soporte está funcionando
Compruebe la notificación de problemas para asegurarse de que la conexión con el servicio y el soporte funciona.

Acerca de esta tarea

Para verificar que la configuración de llamada automática funciona correctamente, realice los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio** y, a continuación, seleccione **Gestión de servicio**.
2. En el área de contenido, pulse **Crear suceso**.
3. Seleccione **Probar notificación automática de problemas** y escriba un comentario.
4. Pulse **Petición de servicio**. Espere unos minutos a que se envíe la petición.
5. En la ventana Gestión de servicio, seleccione **Gestionar sucesos**.
6. Seleccione **Todos los problemas abiertos**.
7. Compruebe que haya un suceso PMH y un número asignados al número de problema que ha abierto.
8. Seleccione ese suceso y pulse **Cerrar**.

9. En la ventana **Cerrar**, escriba el nombre y un breve comentario.

Autorización de los usuarios para que vean los datos del sistema recopilados
Debe autorizar a los usuarios para que puedan ver los datos acerca de los sistemas.

Antes de empezar
Para autorizar a los usuarios para que vean los datos del sistema recopilados, debe obtener un ID de IBM. Para obtener más información acerca de cómo obtener un ID de IBM, consulte el apartado "Hoja de trabajo de configuración previa a la instalación para la HMC" en la página 48.

Acerca de esta tarea
Para autorizar a los usuarios para que vean los datos del sistema recopilados, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestión de servicio**.
2. En el panel de contenido, seleccione **Autorizar usuario**.
3. Escriba su ID de IBM.
4. Pulse **Aceptar**.

Transmisión de la información de servicio
Puede transmitir información de forma inmediata a su proveedor de servicios o puede planificar que la información se envíe con regularidad.

Antes de empezar
IBM proporciona funciones web personalizadas que utilizan la información que ha recopilado IBM Electronic Service Agent. Para utilizar estas funciones, debe registrarse primero en el sitio Web de IBM Registration en http://www.ibm.com/account/profile. Para autorizar a los usuarios de modo que puedan utilizar la información de Electronic Service Agent para personalizar las funciones web, consulte el apartado "Autorización de los usuarios para que vean los datos del sistema recopilados" en la página 73. Para obtener más información acerca de las ventajas de registrar un ID de IBM con los sistemas, consulte http://www.ibm.com/support/electronic.

Nota: Debe transmitir la información del proveedor de servicios así que la HMC esté instalada y configurada para el uso.

Acerca de esta tarea
Para transmitir información de servicio, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestión de servicio**.
2. En el panel de contenido, pulse **Transmitir información de servicio**
3. Complete las tareas de la ventana **Transmitir información de servicio** y pulse **Aceptar**.

Configuración del gestor de sucesos para llamada al centro de soporte
Aprenda a configurar la tarea del gestor de sucesos para llamada al centro de soporte. Puede supervisar y aprobar los datos que se están transmitiendo desde una HMC a IBM a través de esta tarea.

La modalidad del gestor de sucesos para llamada al centro de soporte(habilitado o inhabilitado) se define utilizando la interfaz de línea de mandatos de la HMC. Habilitar la tarea del gestor de sucesos para llamada al centro de soporte bloquea a la HMC de llamar automáticamente a los sucesos a medida que se producen. Para evitar sucesos llamados sin aprobación, todas las HMC que se ejecutan en este entorno deben tener el gestor de sucesos para llamada al centro de soporte habilitado.

Para habilitar o inhabilitar la tarea del gestor de sucesos para llamada al centro de soporte, ejecute el mandato siguiente:

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

Nota: Habilitar la tarea del gestor de sucesos para llamada al centro de soporte retiene los sucesos hasta que los aprueba la tarea de llamada al centro de soporte. Si inhabilita la tarea del gestor de sucesos para llamada al centro de soporte, no habilita automáticamente la función de llamada al centro de soporte. Esta configuración evita cualquier devolución de llamada no deseada al centro de soporte de datos a IBM. Elija entre las siguientes opciones de mandato para realizar la configuración necesaria:

- Para habilitar la tarea del gestor de sucesos para llamada al centro de soporte: **`chhmc -c emch -s enable`**
- Para inhabilitar la tarea del gestor de sucesos para llamada al centro de soporte y volver a habilitar la llamada automática al centro de soporte: **`chhmc -c emch -s disable --callhome enable`**
- Para inhabilitar la tarea del gestor de sucesos para llamada al centro de soporte sin volver a habilitar la llamada automática al centro de soporte: **`chhmc -c emch -s disable --callhome disable`**

Asegúrese de que la HMC se puede comunicar con otras HMC desplegadas en este entorno. El gestor de sucesos para llamada al centro de soporte tiene una función de conexión de prueba cuando una HMC está registrada.

Puede registrar la HMC con el gestor de sucesos para llamada al centro de soporte. Tras registrar la HMC, el gestor de sucesos consulta la HMC registrada para cualquier suceso que esté a la espera de ser llamado en IBM. El gestor de sucesos muestra los datos que se están devolviendo a IBM y aprueba estos sucesos. Tras la aprobación, el gestor de sucesos notifica a la HMC registrada que puede continuar con la operación de llamada al centro de soporte.

La tarea del gestor de sucesos para llamada al centro de soporte se puede ejecutar desde cualquier HMC o varias HMC. Para registrar una consola de gestión con la tarea del gestor de sucesos para llamada al centro de soporte, complete los pasos siguientes:

1. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestor de sucesos para llamada al centro de servicio**.
2. En el panel **Gestor de sucesos para llamada al centro de soporte**, pulse **Gestionar consolas**.
3. Desde la ventana **Gestionar consolas registradas**, pulse **Añadir consola** para entrar información para registrar una consola de gestión con la tarea del gestor de sucesos para llamada al centro de soporte.
4. Pulse **Aceptar** para confirmar los cambios en la lista de consola de gestión registrada.

Nota: El gestor de sucesos para llamada al centro de soporte se puede utilizar con el modo del gestor de sucesos inhabilitado. Puede seguir registrando la HMC y ver los sucesos en el gestor de sucesos, pero el gestor de sucesos no controla cuando se llaman los sucesos.

Establecer contraseñas para el sistema gestionado

Configure contraseñas para su servidor y para Gestión avanzada del sistema (ASM). Obtenga más información sobre cómo utilizar la interfaz de la HMC para establecer estas contraseñas.

Antes de empezar

Si ha recibido el mensaje `Pendiente de autenticación`, la HMC solicita que establezca las contraseñas del sistema gestionado.

Acerca de esta tarea

Si no ha recibido el mensaje Pendiente de autenticación, siga estos pasos para establecer las contraseñas del sistema gestionado.

Actualizar la contraseña del servidor

Antes de empezar

Para actualizar la contraseña del servidor, realice los pasos siguientes:

Procedimiento

1. En el área de navegación, seleccione el sistema gestionado y pulse el icono **Usuarios y seguridad**  y, a continuación, seleccione **Usuarios y roles**.
2. Pulse **Cambiar contraseña**. Se abre la ventana Actualizar contraseña.
3. Escriba la información necesaria y pulse **Aceptar**.

Actualizar la contraseña genérica de ASM (gestión avanzada del sistema)

Antes de empezar

Nota: La contraseña predeterminada para el ID de usuario general es `general` y la contraseña predeterminada para el ID de administrador es `admin`.

Para actualizar la contraseña general de ASM, realice los pasos siguientes:

Procedimiento

1. En el área de navegación del HMC, seleccione el sistema gestionado.
2. En el área de tareas, pulse **Operaciones**.
3. Pulse **gestión avanzada del sistema (ASM)**. Se abre la ventana Lanzar interfaz ASM.
4. Seleccione una dirección IP de procesador de servicio y pulse **Aceptar**. Se abre la interfaz ASM.
5. En el panel de bienvenida de ASMI, especifique el ID de usuario y la contraseña, y pulse **Iniciar sesión**.
6. En el área de navegación, expanda **Perfil de inicio de sesión**.
7. Seleccione **Cambiar contraseña**.
8. Especifique la información necesaria y pulse **Continuar**.

Restablecer la contraseña de administrador de ASM (gestión avanzada del sistema)

Antes de empezar

Para restablecer la contraseña de administrador, póngase en contacto con un proveedor de servicios autorizado.

Probar la conexión entre la HMC y el sistema gestionado

Información sobre cómo verificar que está conectado correctamente a la red.

Acerca de esta tarea

Para probar la conectividad de red, debe ser miembro de uno de estos roles:

- Superadministrador
- Representante del servicio técnico

Para probar la conexión entre la HMC y el sistema gestionado, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Valores de consola**.
2. En el panel de contenido, pulse **Probar conectividad de red**.
3. En la pestaña Ping, escriba el nombre de host o la dirección IP del sistema al que desee conectarse. Para probar una red abierta, escriba la pasarela. Pulse **Ping**.

Resultados

Si no ha creado particiones lógicas, no puede ejecutar el mandato ping en las direcciones. Puede utilizar la HMC para crear particiones lógicas en el servidor. Para obtener más información, consulte Particionamiento lógico.

Para entender cómo puede utilizarse la HMC en una red, consulte “Conexiones de red de la HMC” en la página 38.

Para obtener más información sobre cómo configurar la HMC para conectarse a una red, consulte “Configuración de la HMC utilizando los menús” en la página 55.

Pasos posteriores a la configuración

Tras instalar y configurar la HMC, realice una copia de seguridad de los datos de HMC según convenga.

Copia de seguridad de datos de consola de gestión

Esta tarea realiza una copia de seguridad (o archiva) los datos almacenados en el disco duro de la HMC que son críticos para dar soporte a las operaciones de la HMC.

Antes de empezar

El sistema remoto debe tener configurado NFS (Network File System) o SSH (Secure Shell) y esta red debe ser accesible desde la HMC. Para completar estas tareas, debe concluir y rearrancar la HMC. Use únicamente la HMC para realizar estas tareas.

Acerca de esta tarea

Para hacer una copia de seguridad de la unidad de disco duro de la HMC en un sistema remoto, debe ser miembro de uno de estos roles:

- Superadministrador
- Operador
- Representante del servicio técnico

Realice una copia de seguridad de los datos de la HMC tras realizar cambios en la HMC o en la información asociada a las particiones lógicas.

Los datos de la HMC almacenados en la unidad de disco duro de la HMC se pueden guardar en un DVD-RAM en un sistema local, en un sistema remoto montado en el sistema de archivos de la HMC (como NFS) o enviarlos a un sitio remoto utilizando FTP (File Transfer Protocol).

Nota: Para el modelo de HMC 7063-CR1, puede conectar una unidad de DVD USB externa.

Mediante la HMC, puede hacer una copia de todos los datos importantes, como los siguientes:

- Archivos de preferencias de usuario
- Información de usuario
- Archivos de configuración de plataforma de la HMC
- Archivos de registro de la HMC
- Actualizaciones de la HMC mediante el Servicio correctivo de instalación.

Para realizar una copia de seguridad de la unidad de disco de HMC en un sistema remoto, realice los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Copia de seguridad de datos de consola de gestión**.
3. En la ventana **Copia de seguridad de datos de consola de gestión**, seleccione la opción de archivado que desea realizar.
4. Pulse **Siguiente** y siga las instrucciones adecuadas según la opción que haya elegido.
5. Pulse **Aceptar** para continuar con el proceso de copia de seguridad.

Actualizar, ampliar y migrar el código de máquina de la consola HMC

Se lanzan de forma periódica actualizaciones y ampliaciones para añadir nuevas funciones y mejorar las características existentes de la HMC. Conozca las diferencias entre actualizar, ampliar y migrar el código de máquina de la consola HMC. Aprenda también a ejecutar una actualización, ampliación o migración del código de la máquina HMC.

Cuando haya terminado con cada una de estas tareas, la HMC rearranca pero las particiones no.

Actualizar el código de la HMC
Aplica el mantenimiento a un nivel de HMC existente

No le exige que realice la tarea **Guardar datos de actualización**

Ampliar el código de la HMC
Sustituye el software de la HMC con un nuevo release o nivel de arreglo del mismo programa.

Exige el arranque desde el medio de recuperación

Migrar código de la HMC
Mueve los datos de la HMC de una versión de HMC a otra.

Una migración es un tipo de actualización.

Nota: Para el modelo de HMC 7063-CR1, puede conectar una unidad de DVD USB externa.

Determinar la versión y el release del código de máquina de la HMC

Descubra cómo puede ver la versión y el release del código de máquina de la HMC.

Acerca de esta tarea

El nivel de código de máquina de la HMC determina las características disponibles, incluidos el mantenimiento y las mejoras del firmware del servidor concurrentes para actualizarse a un nuevo release.

Para ver la versión de códigos de la máquina HMC, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera **Información de controlador de HMC actual**, que incluye: la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.

Obtener y aplicar actualizaciones de código de máquina de la HMC con una conexión a Internet

Aprenda a obtener actualizaciones de código de máquina de la HMC cuando la HMC tiene una conexión a Internet.

Acerca de esta tarea

Para obtener actualizaciones de código de máquina de la HMC, realice todos los pasos.

Paso 1. Comprobar que tiene una conexión a Internet

Acerca de esta tarea

Para descargar actualizaciones desde el sitio web o el sistema de servicio y soporte a la HMC o al servidor, debe tener una de las opciones siguientes:

- Conectividad SSL con o sin un proxy SSL
- VPN de Internet

Para comprobar que tiene una conexión a Internet, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestión de servicio**.
2. En el panel de contenido, pulse **Gestionar conectividad de salida**.
3. Seleccione la pestaña correspondiente al tipo de conectividad de salida que ha elegido para la HMC (VPN de Internet o conectividad SSL).

   Nota: Si no existe una conexión con el servicio y soporte, configure la conexión de servicio antes de continuar con este procedimiento. Para obtener instrucciones sobre cómo configurar una conexión con el servicio y el soporte, consulte el apartado sobre la configuración del servidor para conectar con el servicio y soporte de IBM.
4. Pulse **Probar**.
5. Verifique que la prueba se realiza satisfactoriamente.

   Si la prueba no es satisfactoria, resuelva el problema de conectividad antes de continuar con este procedimiento. Como alternativa, puede obtener la actualización en DVD.

   Nota: Para el modelo de HMC 7063-CR1, puede conectar una unidad de DVD USB externa.
6. Continúe con el "Paso 2. Ver el nivel de código de máquina de la HMC existente" en la página 79.

Paso 2. Ver el nivel de código de máquina de la HMC existente

Acerca de esta tarea

Para ver el nivel de código de la máquina HMC siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera Información de controlador de HMC actual, que incluye: la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.
4. Continúe con el "Paso 3. Ver los niveles disponibles de código de máquina de la HMC" en la página 79.

Paso 3. Ver los niveles disponibles de código de máquina de la HMC

Acerca de esta tarea

Para ver los niveles de código de máquina de a HMC siga los pasos siguientes:

Procedimiento

1. Desde un equipo o servidor con una conexión a Internet, vaya a http://www.ibm.com/eserver/support/fixes.
2. Seleccione la familia apropiada en la lista Familia de productos.
3. Seleccione **Hardware Management Console** en la lista Tipo de producto o arreglo.
4. Pulse **Continuar**.

   Se visualiza el sitio de Hardware Management Console.
5. Desplácese hacia abajo hasta el nivel de versión de HMC para ver los niveles de HMC que están disponibles.

   Nota: Si lo prefiere, puede ponerse en contacto con el servicio y soporte.
6. Continúe con el "Paso 4. Aplicar la actualización de código de máquina de la HMC" en la página 79.

Paso 4. Aplicar la actualización de código de máquina de la HMC

Acerca de esta tarea

Para aplicar la actualización del código de máquina de la HMC, realice los pasos siguientes:

Procedimiento

1. Antes de instalar las actualizaciones del código de máquina de la HMC, realice una copia de seguridad de la información más importante de la HMC.

   Encontrará las instrucciones en: "Copia de seguridad de datos de consola de gestión" en la página 76. Después, continúe en el próximo paso.
2. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.

3. En el panel de contenido, pulse **Actualizar Hardware Management Console**. Se abre el asistente para instalar el servicio corrector.
4. Siga las instrucciones del asistente para instalar la actualización.
5. Concluya y reinicie la HMC para que la actualización entre en vigor.
6. Pulse **Iniciar una sesión y lanzar la aplicación Web de Hardware Management Console**.
7. Inicie una sesión en la interfaz HMC.

Paso 5. Verificar que la actualización del código de máquina de la HMC se ha instalado correctamente

Acerca de esta tarea

Para verificar que la actualización del código de máquina de la HMC está instalada correctamente, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera Información de controlador de HMC actual, que incluye: la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.
4. Verifique que la versión y el release coinciden con la actualización que ha instalado.
5. Si el nivel de código que se visualiza no es el nivel que ha instalado, siga estos pasos.
   a. Seleccione la conexión de red en la HMC.
   b. Reintente la actualización del firmware utilizando un repositorio distinto.
   c. Si el problema persiste, póngase en contacto con el siguiente nivel de soporte.

Obtener y aplicar actualizaciones de código de máquina de la HMC mediante un DVD o un servidor FTP

Aprenda a obtener las actualizaciones de código de máquina de Hardware Management Console (HMC) utilizando un DVD o un servidor FTP.

Acerca de esta tarea

Para obtener actualizaciones de código de máquina de la HMC, realice todos los pasos.

Nota: Para el modelo de HMC 7063-CR1, puede conectar una unidad de DVD USB externa.

Paso 1. Ver el nivel de código de máquina de la HMC existente

Antes de empezar

Para ver el nivel de código de la máquina HMC siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.

2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera Información de controlador de HMC actual, que incluye: la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.
4. Continúe con el "Paso 2. Ver los niveles disponibles de código de máquina de la HMC" en la página 81.

Paso 2. Ver los niveles disponibles de código de máquina de la HMC

Antes de empezar

Para ver los niveles de código de máquina de a HMC siga los pasos siguientes:

Acerca de esta tarea

Procedimiento

1. Desde un equipo o servidor con una conexión a Internet, vaya al sitio web de Fix Central.
2. Desplácese hacia abajo hasta el nivel de versión de HMC para ver los niveles de HMC que están disponibles.

   Nota: Si lo prefiere, puede ponerse en contacto con el servicio y soporte de IBM .
3. Continúe con el "Paso 3. Obtener la actualización de código de máquina de la HMC" en la página 81.

Paso 3. Obtener la actualización de código de máquina de la HMC

Antes de empezar

Para obtener la actualización del código de máquina de la HMC, realice los pasos siguientes:

Acerca de esta tarea

Puede solicitar la ampliación de código de máquina de la HMC a través del sitio web de Fix Central, poniéndose en contacto con el servicio y soporte o descargándola a un servidor FTP.

Solicitar la actualización de código de máquina de la HMC a través del sitio de Fix Central

1. Desde un equipo o servidor con una conexión a Internet, vaya al sitio web de Fix Central.
2. En Productos HMC soportados, seleccione el nivel de HMC más reciente.
3. Desplácese hacia abajo hasta el área Nombres de archivo / Paquete y localice la actualización que desea pedir.
4. En la columna Pedir, seleccione **Ir**.
5. Pulse **Continuar** para iniciar la sesión con el ID de IBM.
6. Siga las indicaciones de la pantalla para someter el pedido.

Descargar la actualización de código de máquina de la HMC en un soporte extraíble

1. Desde un equipo o servidor con una conexión a Internet, vaya al sitio web de Fix Central.
2. En Productos HMC soportados, seleccione el nivel de HMC más reciente.
3. Desplácese hacia abajo hasta el área Nombres de archivo / Paquete y localice la actualización que desea descargar.
4. Pulse la actualización que desee descargar.
5. Acepte el acuerdo de licencia y guarde la actualización en el medio extraíble.

Qué hacer a continuación

Cuando haya terminado, continúe con el "Paso 4. Aplicar la actualización de código de máquina de la HMC" en la página 82.

Paso 4. Aplicar la actualización de código de máquina de la HMC

Antes de empezar

Para aplicar la actualización del código de máquina de la HMC, realice los pasos siguientes:

Procedimiento

1. Antes de instalar las actualizaciones del código de máquina de la HMC, realice una copia de seguridad de los datos de la HMC. Para obtener más información, consulte "Copia de seguridad de datos de consola de gestión" en la página 76.
2. Si ha obtenido o creado la actualización en DVD-RAM, insértelo en la unidad de DVD de la HMC. Si ha obtenido o creado la actualización en un dispositivo de memoria USB, insértelo.
3. Antes de instalar las actualizaciones del código de máquina de la HMC, realice una copia de seguridad de la información más importante de la HMC.

   Encontrará las instrucciones en: "Copia de seguridad de datos de consola de gestión" en la página 76. Después, continúe en el próximo paso.
4. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
5. En el panel de contenido, pulse **Actualizar Hardware Management Console**. Se abre el asistente para instalar el servicio corrector.
6. Siga las instrucciones del asistente para instalar la actualización.
7. Concluya, reinicie y vuelva a iniciar una sesión en la HMC para que la actualización entre en vigor.
8. Continúe con el "Paso 5. Verificar que la actualización del código de máquina de la HMC se ha instalado correctamente" en la página 82.

Paso 5. Verificar que la actualización del código de máquina de la HMC se ha instalado correctamente

Antes de empezar

Para verificar que la actualización del código de máquina de la HMC está instalada correctamente, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera Información de controlador de HMC actual, que incluye: la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.
4. Verifique que la versión y el release coinciden con la actualización que ha instalado.
5. Si el nivel de código que se visualiza no es el nivel que ha instalado, siga los pasos siguientes.
   a. Vuelva a intentar la actualización del código de máquina. Si ha creado un DVD para este procedimiento, utilice un medio nuevo.

b. Si el problema persiste, póngase en contacto con el siguiente nivel de soporte.

Actualización del software de la HMC

Aprenda a actualizar el software en una HMC de un release al siguiente mientras mantiene los datos de configuración de la HMC.

Acerca de esta tarea

Para actualizar el código de máquina en una HMC, realice todos los pasos.

Nota: Para los modelos de HMC 7063-CR1 y 7063-CR2, puede conectar una unidad de DVD USB externa.

Paso 1. Obtener la actualización

Acerca de esta tarea

Puede solicitar la actualización de código de máquina de la HMC a través del sitio web de Fix Central.

Para obtener la actualización a través del sitio web de Fix Central, realice los pasos siguientes:

Procedimiento

1. Desde un equipo o servidor con una conexión a Internet, vaya al sitio web de Hardware Management Console, en http://www-933.ibm.com/support/fixcentral/.
2. Pulse **Continuar**.

   Se visualiza el sitio de Hardware Management Console.
3. Desplácese hasta la versión de HMC a la que desee actualizar.
4. Localice la sección de descarga y pedido.

   Nota: Si no tiene acceso a Internet, póngase en contacto con el servicio y soporte de IBM para pedir la actualización en DVD.
5. Siga las indicaciones de la pantalla para someter el pedido.
6. Una vez tenga la actualización, continúe con el “Paso 2. Ver el nivel de código de máquina de la HMC existente” en la página 83.

Paso 2. Ver el nivel de código de máquina de la HMC existente

Acerca de esta tarea

Para determinar el nivel existente del código de máquina en una HMC, siga estos pasos:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.En el área de navegación, pulse **Actualizaciones**.
2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera Información de controlador de HMC actual, incluida la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.
4. Continúe con el “Paso 3. Hacer copia de seguridad de los datos de perfil del sistema gestionado” en la página 84.

Paso 3. Hacer copia de seguridad de los datos de perfil del sistema gestionado

Acerca de esta tarea

Para hacer una copia de seguridad de los datos del perfil del sistema, realice los pasos siguientes:

Procedimiento

1. Seleccione el sistema del que desea guardar los datos del perfil.
2. Pulse **Acciones** > **Ver todas las acciones** > **Legado** > **Gestionar datos de partición** > **Copia de seguridad**.
3. Escriba un nombre de archivo de copia de seguridad y anote esta información.
4. Pulse **Aceptar**.
5. Repita estos pasos para cada sistema.
6. Continúe con el "Paso 4. Haga una copia de seguridad de los datos de la HMC" en la página 84.

Paso 4. Haga una copia de seguridad de los datos de la HMC

Acerca de esta tarea

Realice una copia de seguridad de los datos de la HMC antes de instalar una nueva versión del software de HMC de modo que puedan restaurarse los niveles anteriores en caso de que se produzca un problema durante la actualización del software. No utilice estos datos críticos de la consola después de que haya finalizado satisfactoriamente una actualización a una nueva versión del software de HMC.

Nota: Para realizar una copia de seguridad en un soporte extraíble, debe tener a mano el medio.

Para realizar una copia de seguridad de los datos de la HMC, siga los pasos siguientes:

Procedimiento

1. Si tiene la intención de realizar la copia de seguridad en un soporte, lleve a cabo los pasos siguientes para formatear el medio:
   a. Inserte el medio en la unidad.
   b. En el área de navegación, pulse el icono **Disponibilidad de servicio**  y, a continuación, seleccione **Gestión de servicio**.
   c. En el panel de contenido, pulse **Formato de medio**.
   d. Seleccione el tipo de medio.
   e. Seleccione el tipo de formato.
   f. Pulse **Aceptar**.
2. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
3. En el panel de contenido, pulse **Copia de seguridad de datos de consola de gestión**.
   Se abre la ventana **Copia de seguridad de datos de consola**.
4. Seleccione una opción de archivado.
   Puede realizar la copia de seguridad en un soporte en un sistema local, en un sistema remoto que está montado en el sistema de archivos de la HMC (por ejemplo, NFS) o enviar la copia de seguridad a un sitio remoto utilizando el protocolo de transferencia de archivos (FTP).
   - Para realizar la copia de seguridad en un sistema local, elija **Hacer copia de seguridad en un soporte del sistema local** y siga las instrucciones.

- Para realizar la copia de seguridad en un sistema remoto montado, elija **Hacer copia de seguridad en sistema remoto montado** y siga las instrucciones.
- Para realizar la copia de seguridad en un sitio FTP remoto, elija **Enviar datos críticos de copia de seguridad a sitio remoto** y siga las instrucciones.

5. Continúe con el "Paso 5. Anotar la información de configuración actual de la HMC" en la página 85.

Paso 5. Anotar la información de configuración actual de la HMC

Acerca de esta tarea

Antes de actualizar a una nueva versión del software de HMC, como medida de precaución, anote la información de configuración de la HMC.

Para grabar la configuración de HMC actual, realice los pasos siguientes:

Procedimiento

1. Seleccione un sistema gestionado o las particiones para las que desea grabar información de configuración de HMC.
2. En el pod del menú, seleccione **Acciones** > **Planificar operaciones**.
   Se visualizan todas las operaciones planificadas para el destino que ha seleccionado.
3. Seleccione **Ordenar** > **Por objeto**.
4. Seleccione cada objeto y anote los siguientes detalles:
   - Nombre de objeto
   - Fecha de planificación
   - Hora de la operación (visualizada en formato de 24 horas)
   - Repetitiva (si es Sí, realice los pasos siguientes):
     a. Seleccione **Ver** > **Detalles de la planificación**.
     b. Anote la información de intervalo.
     c. Cierre la ventana Operaciones planificadas.
     d. Repita el proceso para cada operación planificada.
5. Cierre la ventana **Personalizar operaciones planificadas**.
6. Continúe con el "Paso 6. Anotar estado de mandato remoto" en la página 85.

Paso 6. Anotar estado de mandato remoto

Acerca de esta tarea

Para anotar el estado de mandato remoto, siga los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono **Usuarios y seguridad**  y, a continuación, seleccione **Seguridad de sistemas y consola**.
2. En el panel de contenido, pulse **Habilitar ejecución de mandatos remota**.
3. Anote si el recuadro de selección **Habilitar ejecución de mandato remoto utilizando el recurso ssh** está seleccionado.
4. Pulse **Cancelar**.
5. Continúe con el "Paso 7. Guardar datos de actualización" en la página 86.

Paso 7. Guardar datos de actualización

Acerca de esta tarea

Puede guardar la configuración actual de la HMC en una partición de disco designada de la HMC o en un soporte local. Guarde solamente los datos de actualización inmediatamente antes de actualizar el software de HMC a un nuevo release. Puede restaurar los valores de configuración de HMC tras la actualización.

Nota: Sólo se permite una nivel de datos de copia de seguridad. Cada vez que guarde datos de actualización, se sobrescribirá el nivel anterior.

Para guardar los datos, realice los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Guardar datos de actualización**. Se abre el asistente **Guardar datos de actualización**.
3. Seleccione el soporte en el que desea guardar los datos de actualización. Si opta por guardar en un soporte extraíble, insértelo ahora. Pulse **Siguiente**.
4. Pulse **Finalizar**.
5. Espere a que finalice la tarea.

   Si la tarea Guardar datos de ampliación no se realiza satisfactoriamente, póngase en contacto con el personal de soporte técnico de siguiente nivel antes de continuar.

   Nota: Si la tarea Guardar datos de ampliación no se realiza satisfactoriamente, no continúe con el proceso de ampliación.
6. Pulse **Aceptar**.
7. Continúe con el "Paso 8. Actualizar el software de la HMC" en la página 86.

Paso 8. Actualizar el software de la HMC

Acerca de esta tarea

Para actualizar el software de la HMC, reinicie el sistema con el medio extraíble en la unidad de DVD.

Procedimiento

1. Inserte el medio de instalación de productos de la HMC en la unidad de DVD.
2. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
3. En el panel de contenido, seleccione **Concluir o reiniciar la consola de gestión**.
4. Asegúrese de que **Reiniciar la HMC** esté seleccionado.
5. Pulse **Aceptar**.

   La HMC se reinicia y la información del sistema aparece en la pantalla.
6. Seleccione **Ampliar** y pulse **Siguiente**.
7. Elija una de estas opciones:
   - Si ha guardado los datos de actualización durante la tarea anterior, continúe con el paso siguiente.
   - Si no ha guardado los datos de actualización al principio de este procedimiento, debe guardar los datos de actualización ahora antes de continuar.

8. Seleccione **Actualizar desde medio** y pulse **Siguiente**.
9. Confirme los valores y pulse **Finalizar**.
10. Siga las indicaciones.

    Nota:

    - Si la pantalla se pone en blanco, pulse la barra espaciadora para ver la información.
    - El primer DVD puede tardar aproximadamente 20 minutos en instalarse.
11. En el indicador de inicio de sesión, conéctese utilizando su ID de usuario y contraseña.

    La instalación del código de la HMC ha finalizado.
12. Continúe con el "Paso 9. Verificar que la actualización de código de máquina de la HMC se ha instalado satisfactoriamente" en la página 87.

Paso 9. Verificar que la actualización de código de máquina de la HMC se ha instalado satisfactoriamente

Acerca de esta tarea
Para verificar que la actualización de la HMC se haya instalado correctamente, realice los pasos siguientes:

Procedimiento

1. En el área de navegación, pulse el icono Gestión de la **HMC**  y, a continuación, seleccione **Gestión de la consola**.
2. En el panel de contenido, pulse **Actualizar Hardware Management Console**.
3. En la nueva ventana, visualice y anote la información que aparece en la cabecera Información de controlador de HMC actual, incluida la versión de HMC, el release, el nivel de mantenimiento, el nivel de build y las versiones base.
4. Verifique que la versión y el release coinciden con la actualización que ha instalado.
5. Si el nivel de código que se visualiza no es el nivel que ha instalado, intente de nuevo la tarea de actualización con un nuevo DVD. Si el problema persiste, póngase en contacto con el siguiente nivel de soporte.

Actualización de la HMC desde una ubicación remota utilizando imágenes de actualización de red

Aprenda a actualizar el software en una HMC desde una ubicación remota utilizando imágenes de actualización de red.

Acerca de esta tarea
Aprenda a actualizar el software en una HMC desde una ubicación remota utilizando imágenes de actualización de red.

Procedimiento

1. Desde un equipo o servidor con una conexión a Internet, vaya al Sitio web de Hardware Management Console (http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html)
2. Descargue las imágenes de red V9 de HMC adecuadas y guárdelas en un servidor FTP.

   No puede descargar estos archivos directamente en la HMC. Debe descargar los archivos de imagen en un servidor que acepte solicitudes FTP.
3. Asegúrese de que descarga los archivos siguientes:

   - img2a

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

4. Guarde los datos de actualización en la HMC. Ejecute los mandatos siguientes para guardar los datos de actualización:
   - Para guardar los datos en DVD y HDD, ejecute los mandatos siguientes:

     mount /media/cdrom

     saveupgdata -r diskdvd
   - Para guardar los datos en HDD, ejecute el mandato siguiente:

     saveupgdata -r disk
5. Copie los archivos de actualización en la partición de disco que se puede volver a arrancar en la HMC. Ejecute el mandato **getupgfiles** para copiar los archivos.

   Ejemplo: **getupgfiles -h <ftp server> -u <user id> -d <directorio remoto>**

   Donde,
   - **ftp server** es el nombre de host o la dirección IP del servidor FTP donde descarga las imágenes de red HMC.
   - **user id** es un ID de usuario válido en el servidor FTP. Si no especifica la contraseña con el argumento `--passwd`, se le solicitará una contraseña.
   - **remote directory** es el directorio del servidor FTP en que se han guardado las imágenes de red de HMC.
6. Reinicie la HMC para actualizar el código que se copia en la partición de disco reiniciable. Ejecute **chhmc -c altdiskboot -s enable --mode upgrade** para reiniciar la HMC.
7. Reinicie la HMC e inicie la actualización. Ejecute el mandato **hmcshutdown -r -t now** para iniciar la actualización.

Protección de la HMC

Información sobre cómo mejorar la seguridad de Hardware Management Console (HMC) que se basa en los estándares de seguridad corporativa.

La configuración predeterminada de la HMC proporciona seguridad de ejemplo para la mayoría de los usuarios de empresa. Con Hardware Management Console (HMC) Versión 8.4.0 o posterior, puede mejorar más la seguridad de la HMC que se basa en los estándares de seguridad corporativa. Para mejorar la seguridad de la HMC, debe establecer la HMC a un mínimo de seguridad de nivel 1. Puede elegir la seguridad de nivel 2 y nivel 3 en función de los requisitos del entorno y de seguridad corporativa.

Nota: Antes de cambiar el nivel de seguridad, compruebe con el equipo de conformidad con la seguridad corporativa.

Seguridad de nivel 1

Para fijar la HMC (seguridad de nivel 1), complete los pasos siguientes:

1. Cambie la contraseña predefinida para el usuario `hscroot` predeterminado. Para obtener más información sobre la política de contraseñas, consulte “Política de contraseñas ampliada” en la página 90.
2. Si la HMC no pertenece a un entorno protegido físicamente, establezca la contraseña `grub` ejecutando el mandato siguiente: `chhmc -c grubpasswd -s enable --passwd <nueva contraseña grub>`
3. Si ha configurado el módulo de gestión integrada (IMM) en la HMC, establezca una contraseña IMM sólida.

4. Establezca una contraseña fuerte para el usuario *admin* y los usuarios generales en todos los servidores.
5. Actualice la HMC con los últimos arreglos de seguridad publicados. Para obtener más información sobre los arreglos de seguridad, consulte IBM Fix Central.

Seguridad de nivel 2

Si tiene varios usuarios, complete los pasos siguientes para mejorar la seguridad para la HMC:

1. Cree una cuenta para cada usuario en la HMC y asigne los roles y los recursos necesarios a los usuarios. Para obtener más información sobre los diferentes roles en la HMC, consulte Tareas de la consola HMC, roles e ID de usuario, y mandatos asociados.

   Nota: Asegúrese de que solo asigne los recursos y los roles necesarios para los usuarios que se creen en la HMC. Si es necesario, también puede crear roles personalizados.
2. Habilite la réplica de datos de usuarios entre diferentes consolas de gestión de hardware. La réplica de datos de usuarios se puede realizar en modalidad de maestro-esclavo o modalidad de igual a igual. Para obtener más información sobre réplica de datos de usuario, consulte Gestionar la réplica de datos.
3. Importe un certificado que esté firmado por la autoridad emisora de certificados.

Seguridad de nivel 3

Si tiene varias consolas de gestión de hardware y administradores de sistemas, complete los pasos siguientes para mejorar la seguridad para la HMC:

1. Utilice la autenticación centralizada como Lightweight Directory Access Protocol (LDAP) o Kerberos. Para obtener más información sobre la configuración de LDAP, consulte cómo configurar LDAP en HMC.
2. Habilite la réplica de datos de usuarios entre diferentes consolas de gestión de hardware.
3. Asegúrese de que la HMC se encuentra en la modalidad NIST SP 800-131A para que la HMC solo utilice cifrados sólidos.
4. Bloquee los puertos que no son necesarios en el cortafuegos. Para obtener más información sobre los puertos HMC que se pueden utilizar, consulte la tabla siguiente:

Tabla 32. Puerto que utiliza el usuario para su interacción con HMC

Puerto	**Descripción**	**Tipo**	**Versión de protocolo (modalidad predeterminada)**	**Versión de protocolo (modalidad NIST)**
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	Agente SNMP	UDP	SNMP v3	SNMP v3
162	Condición de excepción de SNMP	UDP	SNMP v3	SNMP v3
427	SLP	UDP	N/D	N/D
443	HMC GUI y API REST	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (Texto sin formato + hash y signo)	RSCT (Texto sin formato + hash y signo)

Tabla 32. Puerto que utiliza el usuario para su interacción con HMC (continuación)

Puerto	Descripción	Tipo	Versión de protocolo (modalidad predeterminada)	Versión de protocolo (modalidad NIST)
2300	Terminal 5250 para IBM i	TCP	Texto sin formato	Texto sin formato
2301	Terminal protegido 5250 para IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (puerto heredado, no funcional)	TCP	No funcional	No funcional
9900	FCS: Descubrimiento de HMC a HMC	UDP	FCS	FCS
9920	FCS: Comunicación de HMC a HMC	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	Applet VTerm en GUI	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	API REST HMC (puerto heredado)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	Dominio de iguales RSCT	UDP	RSCT (Texto sin formato + hash y signo)	RSCT (Texto sin formato + hash y signo)
12348	Dominio de iguales RSCT	UDP	RSCT (Texto sin formato + hash y signo)	RSCT (Texto sin formato + hash y signo)

Notas:

- Debe utilizar únicamente SSH (puerto 22), HTTPS (puerto 443 y puerto 12443), terminal protegido 5250 para IBM i (puerto 2301) y VTerm (puerto 9960) que están expuestos a una intranet. Todos los demás puertos deben utilizarse en una red privada o aislada. Puede utilizar un puerto Ethernet separado y VLAN para el control y supervisión de recursos (RMC) (puerto 657), FCS (puerto 9900 y puerto 9920) y dominio de iguales RSCT (puerto 12347 y puerto 12348).
- Los puertos listados en el mandato **`netstat`** se utilizan para procesos internos únicamente.

Política de contraseñas ampliada

Puede imponer requisitos de contraseña para los usuarios autenticados localmente utilizando la Hardware Management Console (HMC). La función de política de contraseñas ampliada permite al administrador del sistema establecer restricciones de contraseña. La política de contraseñas ampliada se aplica a los sistemas en los que se ha instalado una HMC.

Los administradores del sistema pueden utilizar la política de contraseña mejorada para definir una única política de contraseñas para todos los usuarios. La HMC proporciona una política de contraseñas de seguridad media, que los administradores del sistema pueden activar para establecer restricciones de contraseña. El administrador del sistema también puede elegir activar la política de seguridad media o una nueva política definida por el usuario. La política de contraseñas de seguridad media de HMC no

puede eliminarse del sistema. En la tabla siguiente se enumeran los atributos de la política de seguridad media y los valores predeterminados.

Tabla 33. Los atributos de contraseña para la política de contraseñas de seguridad media de HMC

Atributo	Descripción	Valor predeterminado
`min_pwage`	El número mínimo de días para la que una contraseña debe seguir activa.	1
`pwage`	El número máximo de días para el que una contraseña debe seguir activa.	180
`min_length`	La longitud mínima de una contraseña.	8
`hist_size`	El número de contraseñas guardadas anteriormente que no se puede reutilizar.	10
`warn_pwage`	Cuando la contraseña está a punto de caducar, el número de días antes de que se avise a un usuario que la contraseña está a punto de caducar.	7
`min_digits`	El número mínimo de dígitos que se precisa utilizar en la contraseña.	Ninguno
`min_uppercase`	El número mínimo de caracteres en mayúscula.	1
`min_lowercase`	El número mínimo de caracteres en minúscula.	6
`min_special_chars`	El número mínimo de caracteres especiales que se debe utilizar en la contraseña.	Ninguno

Tenga en cuenta los elementos siguientes sobre la política de contraseñas de seguridad media HMC:

- La política no se aplica a los ID de usuario **hscroot**, **hscpe** y **root**.
- La política solo afecta a los usuarios autenticados localmente que gestiona la HMC así como la política no se puede aplicar a usuarios LDAP o Kerberos.
- La política de contraseñas de seguridad media de la HMC o la política definida por el usuario permite que los administradores del sistema establezcan restricciones sobre reutilización de contraseña.
- La contraseña de seguridad media de HMC es de sólo lectura y los atributos de la contraseña de seguridad media de HMC no pueden cambiarse. Puede crear una nueva contraseña definida por el usuario para establecer la restricción de contraseñas.

Puede utilizar los mandatos siguientes para configurar la política de contraseñas de seguridad media de HMC:

mkpwdpolicy
: Importa la política de contraseñas a partir de un archivo, que contiene todos los parámetros o crea una política de contraseñas.

lspwdpolicy
: Lista todos los perfiles de política de contraseñas disponibles y busca parámetros específicos. También puede ver la política de contraseñas que está activa actualmente.

rmpwdpolicy
: Elimina una política de contraseñas inactiva existente.

  Nota: No puede eliminar una política de seguridad media y la política de contraseña de solo lectura predeterminada.

chpwdpolicy
: Cambia parámetros de una política de contraseña inactiva.

Perfiles de seguridad: Reglamento general de protección de datos (RGPD) y Normas de Seguridad de Datos para la Industria de tarjetas de pago (PCI-DSS)

Aprenda cómo Hardware Management Console (HMC) maneja la información sobre privacidad de los usuarios.

Hardware Management Console (HMC) es un dispositivo cerrado que no almacena ningún dato de titular de la tarjeta. Por ello, únicamente un subconjunto de requisitos y procedimientos de evaluación de la seguridad de la IT que están definidos por PCI-DSS se pueden aplicar a la HMC. Solo se puede instalar en la HCM código de confianza que distribuye IBM. Cuando se conoce alguna vulnerabilidad mediante el proceso PSIRT de IBM, se publican los arreglos temporales. Los requisitos y las recomendaciones incluyen los elementos siguientes:

Consultas RGPD

Tabla 34. Consultas RGPD. La tabla proporciona información sobre las preguntas relacionadas con GDPR

Preguntas	**Respuestas**
¿Qué tipo de datos se almacena en la HMC?	HMC almacena hardware de información de configuración de Power, virtualización de PowerVM e información sobre métricas de rendimiento.
¿Tiene el proceso HMC algún dato personal?	Puede proporcionar información de contacto para la función de llamada al centro de soporte. El suministro de información de contacto para la función de llamada al centro de soporte es opcional.
¿Qué cuentas predefinidas se utilizan para la administración del sistema de la HMC?	El usuario administrador del sistema utiliza el nombre de usuario *hscroot*.
¿Alguna de las cuentas en la HMC están relacionadas con una persona específica?	No.
¿Es obligatorio proporciona datos personales en la HMC?	No. No necesita proporcionar información de datos personales. No obstante, el suministro de esta información es opcional.
¿El archivo de registro de HMC tiene información de datos personales?	No.
¿Es posible suprimir datos personales completa y permanentemente?	Sí. Desconfigure la función de llamada al centro de soporte.

Consultas PCI-DSS

Tabla 35. Consultas PCI-DSS. La tabla proporciona información sobre las preguntas relacionadas con PCI-DSS

Preguntas	**Respuestas**
¿Cómo puedo instalar y mantener una configuración del cortafuegos para proteger los datos del titular?	La HMC no almacena ningún dato del titular de la tarjeta ni tiene acceso a ellos. No obstante, la HMC tiene una configuración del cortafuegos y el usuario puede controlar y habilitar puertos específicos.

Tabla 35. Consultas PCI-DSS. La tabla proporciona información sobre las preguntas relacionadas con PCI-DSS *(continuación)*	
Preguntas	**Respuestas**
¿Puedo utilizar el valor predeterminado suministrado por el proveedor para contraseñas del sistema y otros parámetros de seguridad?	Antes de instalar un sistema en la red, cambie todas las contraseñas predefinidas en el usuario *hscroot*.
¿Cómo la HMC protege los datos almacenados del titular?	La HMC no almacena ningún dato del titular de la tarjeta ni tiene acceso a ellos.
¿Cómo la HMC cifra los datos del titular cuando los datos se transmiten a través de redes públicas?	La HMC no almacena ningún dato del titular de la tarjeta ni tiene acceso a ellos.
¿Cómo puedo utilizar programas de software antivirus de forma regular?	La HMC es un dispositivo cerrado. Por consiguiente, el programa malicioso no puede infectar a la HMC.
¿Cómo puedo desarrollar y mantener sistemas y aplicaciones seguros?	Debe instalar los parches necesarios para el sistema manualmente desde el sitio web IBM Fix Central. Solo se puede instalar en la HCM código de confianza que distribuye IBM.
¿La HMC limita el acceso a los datos del titular?	La HMC no almacena ningún dato del titular de la tarjeta ni tiene acceso a ellos.
¿Cómo puedo asignar un ID exclusivo a cada persona que tiene acceso al sistema?	Puede implementar este requisito asegurando de que no haya ningún ID compartido y mediante las políticas de contraseña siguientes:
¿Cómo puedo limitar el acceso físico a los datos del titular?	La HMC no almacena ningún dato del titular de la tarjeta ni tiene acceso a ellos
¿Cómo puedo monitorizar y supervisar el acceso a recursos de la red y a datos del titular?	La HMC no almacena ningún dato del titular de la tarjeta ni tiene acceso a ellos.
¿Cómo prueba la HMC la seguridad y los procesos del sistema?	Se utilizan herramientas de exploración para ejecutar exploraciones de seguridad de todas las versiones publicadas de HMC. Las herramientas de exploración incluyen: *Qualys*, *Nessus*, *testssl*, *sslscan* y *ASoC*.
¿Cómo puedo mantener una política de seguridad que incluya seguridad de la información para empleados y contratistas?	El administrador del sistema inhabilita el inicio de sesión de usuario remoto, activa el inicio de sesión de usuario según sus necesidades y desactiva el inicio de sesión de usuario cuando ya no se precisa el acceso.

Cómo resolver problemas comunes al fijar la HMC

Aprenda a resolver problemas comunes que pueden surgir al fijar la HMC.

Cómo fijar la conexión entre la Hardware Management Console (HMC) y el sistema?

La HMC se conecta al sistema a través del procesador de servicio flexible (FSP). Un protocolo binario de cliente denominado protocolo de cliente de red (NETC) se utiliza para gestionar FSP y el hipervisor de Power. En la tabla siguiente se listan puertos que utiliza la HMC:

Tabla 36. Puertos en FSP que se utilizan para interactuar con HMC			
Puerto en FSP	**Descripción**	**Versión de protocolo (modalidad predeterminada)**	**Versión de protocolo (modalidad NIST)**
443	Interfaz de gestión avanzada del sistema	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). Recurre a SSLv3 para soporte de firmware más antiguo.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). Recurre a SSLv3 para soporte de firmware más antiguo.	NETC (TLS 1.2)

¿Cómo puedo bloquear la HMC?

Si desea mejorar la seguridad para la infraestructura, puede utilizar un dispositivo Intrusion Prevention System (IPS) o añada todas las HMC (Hardware Management Console) y servidores de IBM Power Systems tras un cortafuego. Además, puede inhabilitar servicios de red en la HMC si no la utiliza de forma remota o si desea bloquear la HMC. Para inhabilitar los servicios de red en la HMC, complete los pasos siguientes:

1. Inhabilite la ejecución de mandato remoto utilizando el puerto SSH.
2. Inhabilite el terminal virtual remoto (puerto VTerm).
3. Inhabilite el acceso web remoto (interfaz gráfica de usuario HMC y API REST).
4. Bloquee puertos en el cortafuego utilizando los valores de red HMC para cada puerto Ethernet configurado.

Cómo establecer la HMC en modalidad de conformidad con NIST SP 800-131A?

Con HMC Versión 8.1.0 o posterior, cuando establece la HMC en modalidad de conformidad, solo se da soporte a cifrados sólidos que aparecen listados en NIST SP 800-131A. Es posible que no se pueda conectar a servidores anteriores de Power Systems tales como servidores POWER5 que no dan soporte a Transport Layer Security (TLS 1.2). Para obtener más información sobre cómo cambiar la modalidad de seguridad, consulte Modalidad HMC V8R8 NIST.

¿Cómo puedo ver y cambiar cifrados que utilizan la HMC?

Con HMC Versión 8.1.0 o posterior, la HMC da soporte a conjuntos de cifrados más seguros que están definidos en NIST 800-131A. Los cifrados que se utilizan en la modalidad predeterminada son sólidos. Para obtener más información sobre cifras de cifrados que utiliza la HMC, ejecute el mandato **lshmcencr**. Si los estándares corporativos requieren el uso de un conjunto de cifrados diferente, ejecute el mandato **chhmcencr** para modificar las cifras de cifrados.

Para listar las cifras de cifrados que utiliza la HMC para cifrar la contraseña de usuario, ejecute el mandato siguiente:

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

Para listar las cifras de cifrado que utiliza actualmente la interfaz de usuario web de HMC y la API REST, ejecute el mandato siguiente:

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

Para listar las cifras de cifrado que utiliza actualmente la interfaz de usuario SSH de HMC y la API REST, ejecute el mandato siguiente:

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

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

¿Cómo puedo comprobar la solidez del certificado en la HMC?

Los certificados autofirmados en la HMC utilizan SHA256 con cifrado RSA de 2048 bits, que es robusto. Si utiliza certificados firmados por CA, asegúrese de que no utilice el cifrado de 1024 bits, que es poco seguro. Los certificados siguientes se pueden utilizar para la HMC:

- El certificado firmado por CA se puede utilizar para la interfaz gráfica de usuario HMC y la API REST (puertos 443 y 12443).
- El puerto 9920 se utiliza para comunicación de HMC a HMC. No puede sustituir este certificado por su propio certificado.

¿Cómo puedo elegir entre un certificado autofirmado (valor predeterminado) o un certificado firmado por CA?

La HMC genera automáticamente un certificado durante la instalación. No obstante, puede generar una solicitud de firma de certificado (CSR) desde la HMC y obtener un nuevo certificado que emita la entidad emisora de certificados. Puede importar este certificado a HMC. Asegúrese de que también obtenga un nombre de dominio para la HMC. Para obtener más detalles sobre la gestión de los certificados en HMC, consulte Gestionar certificados.

¿Cómo puedo auditar la HMC?

La auditoría sobre las consolas HMC se centra en cifras configuradas y el uso de actividad de los diversos usuarios de HMC. Utilice los mandatos siguientes para ver la actividad de uso de varios usuarios de HMC:

Tabla 37. Cifrados que se utilizan en la HMC

Finalidad	**Mandato**
Cifrado de contraseña (valor global)	`lshmcencr -c passwd -t c`
Cifrado de contraseña para cada usuario	`lshmcusr -Fname:password_encryption`
Cifrados SSH	`lshmcencr -c ssh -t c`
SSH MAC	`lshmcencr -c sshmac -t c`
Cifrado que se utiliza para la interfaz gráfica de usuario HMC y la API REST	`lshmcencr -c webui -t c`

Utilice los mandatos siguientes para supervisar información sobre diversos sucesos susceptibles de servicios y de consola para usos en la HMC:

Tabla 38. Mandatos para ver los usuarios registrados e información sobre los sucesos susceptibles de servicios y de consola para usos en la HMC: HMC

Información	**Mandato**
Usuarios de la GUI	`lslogon –r webui –u`
Tareas de la GUI	`lslogon –r webui –t`
Usuarios de la CLI	`lslogon –r ssh –u`
Tareas de la CLI	`lslogon –r ssh –t`
Operaciones en HMC	`lssvcevents -t console -d <número de días>`

Tabla 38. Mandatos para ver los usuarios registrados e información sobre los sucesos susceptibles de servicios y de consola para usos en la HMC: HMC (continuación)	
Información	**Mandato**
Operaciones en System	`lssvcevents –t hardware –m <sistema gestionado> -d <número de días>`

Sucesos de supervisión centralizados para la HMC: Si tiene muchas consolas de gestión de hardware (HMC), establezca el archivo `rsyslog` para recopilar todos los datos de uso.

¿Cómo puede IBM arreglar las vulnerabilidades de seguridad de HMC?

IBM tiene un proceso de respuesta a incidentes de seguridad denominado IBM Product Security Incident Response Team (PSIRT). El equipo de IBM Product Security Incident Response Team (PSIRT) es un equipo global que gestiona la recepción, la investigación y la coordinación interna de la información sobre vulnerabilidad de seguridad relacionada con las ofertas de IBM. Los componentes de código abierto e IBM que se suministran con la HMC están supervisados y analizados de forma activa. Los arreglos temporales y los arreglos de seguridad los proporciona IBM para todos los releases soportados de la HMC.

¿Cómo puedo rastrear nuevos arreglos internos en la HMC?

El boletín de seguridad contiene información sobre la vulnerabilidad y arreglos temporales para versiones HMC soportadas. Para rastrear arreglos temporales en la HMC, puede:

- Busque los últimos boletines de seguridad en IBM Security Bulletin.
- Siga @IBMPowereSupp en Twitter en busca de notificaciones.
- Suscríbase a notificaciones de correo electrónico en IBM Support.

Ubicaciones de los puertos de la HMC

Puede encontrar las ubicaciones de puerto mediante códigos de ubicación. Utilice las ilustraciones de las ubicaciones de los puertos de la HMC para correlacionar un código de ubicación con la posición del puerto de la HMC en el servidor.

Ubicaciones de los puertos de la HMC en el modelo 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H y 9223-22S

Utilice este diagrama y esta tabla para correlacionar los puertos de la HMC en el 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H y 9223-22S.

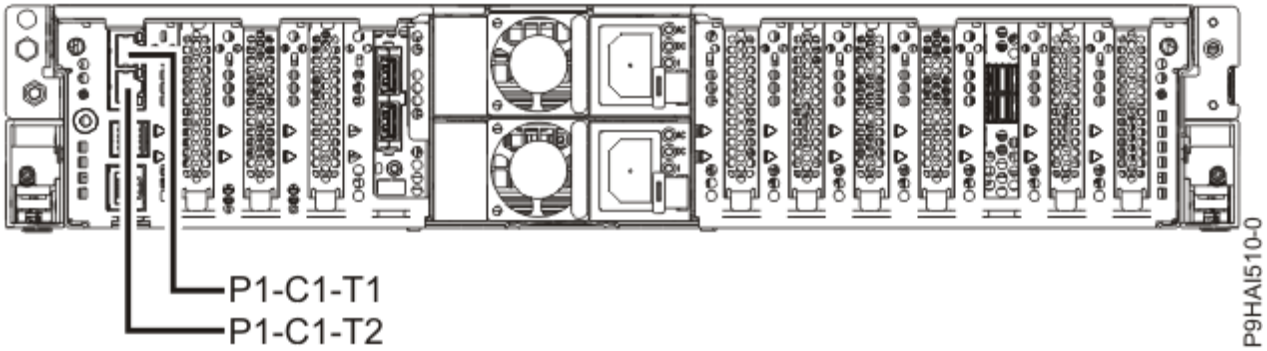


Figura 10. Ubicaciones de los puertos de la HMC en el modelo 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H y 9223-22S

Tabla 39. Ubicaciones de los puertos de la HMC en el modelo 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H y 9223-22S		
Puerto	**Código de ubicación física**	**LED de identificación**
Puerto HMC 1	Un-P1-C1-T1	No
Puerto HMC 2	Un-P1-C1-T2	No
Para obtener más información sobre ubicaciones de puertos HMC en 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H o 9223-22S, consulte Ubicaciones de piezas y códigos de ubicación para 9008-22L, 9009-22A, 9009-22G, 9223-22H o 9223-22S.		

Ubicaciones de los puertos de la HMC en el modelo 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H y 9223-42S

Utilice este diagrama y esta tabla para correlacionar los puertos de la HMC en el 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H y 9223-42S.

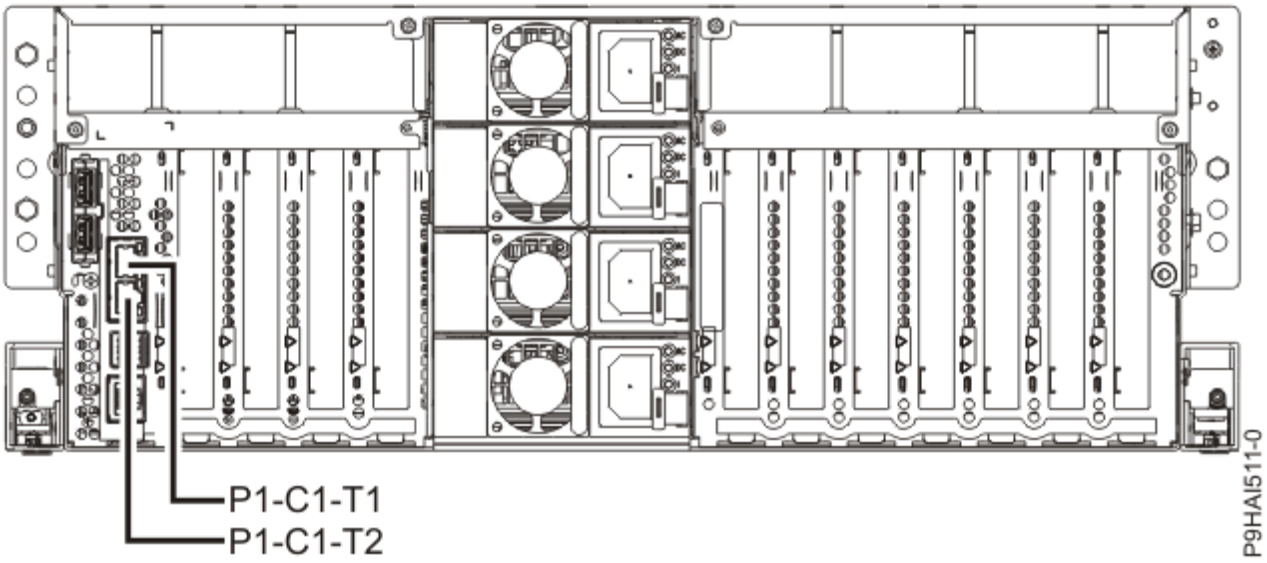


Figura 11. Ubicaciones de los puertos de la HMC en el modelo 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H y 9223-42S

Tabla 40. Ubicaciones de los puertos de la HMC en el modelo 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H y 9223-42S		
Puerto	**Código de ubicación física**	**LED de identificación**
Puerto HMC 1	Un-P1-C1-T1	No
Puerto HMC 2	Un-P1-C1-T2	No
Para obtener más información sobre ubicaciones de puertos HMC en 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H o 9223-42S, consulte Ubicaciones de piezas y códigos de ubicación para 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H o 9223-42S.		

Ubicaciones de los puertos de la HMC en el modelo 9040-MR9

Utilice este diagrama y la tabla para correlacionar los puertos de HMC en 9040-MR9.

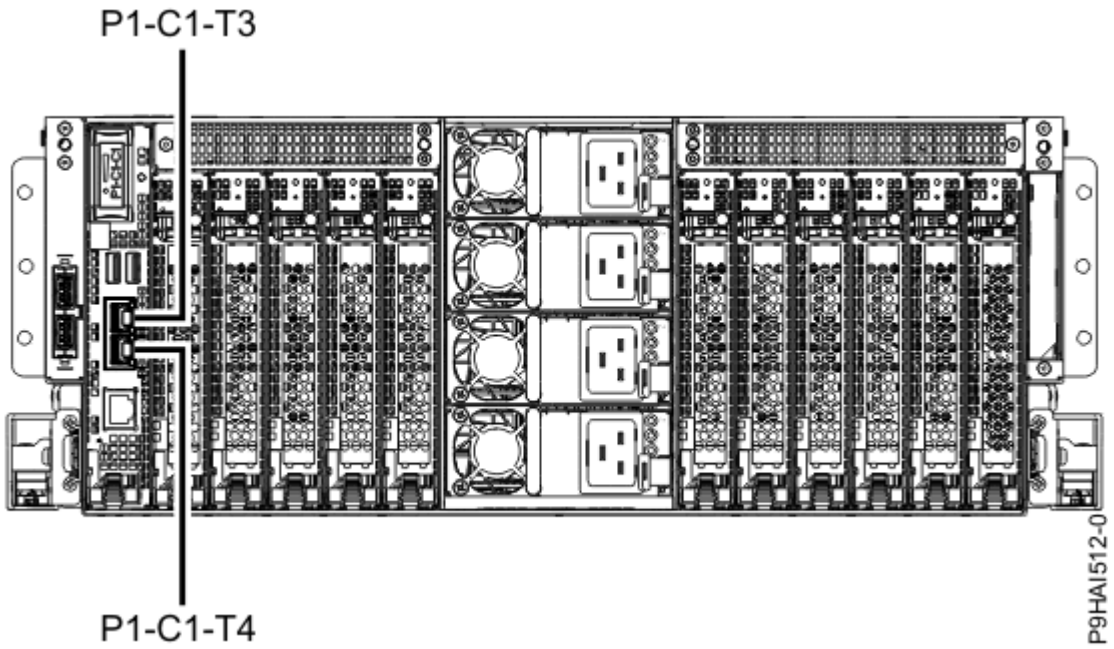


Figura 12. Ubicaciones de puertos de HMC de 9040-MR9

Tabla 41. Ubicaciones de puertos de HMC de 9040-MR9		
Puerto	**Código de ubicación física**	**LED de identificación**
Puerto HMC 1	Un-P1-C1-T3	No
Puerto HMC 2	Un-P1-C1-T4	No
Para obtener más información sobre las ubicaciones de los puertos de la HMC en 9040-MR9, consulte Ubicaciones de piezas y códigos de ubicación.		

Ubicaciones de los puertos de la HMC en el modelo 9080-M9S

Utilice este diagrama y la tabla para correlacionar los puertos de HMC en 9080-M9S.

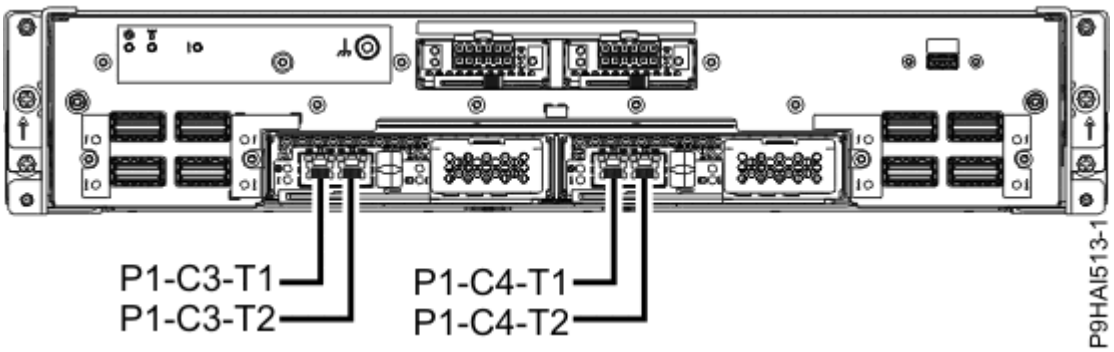


Figura 13. Ubicaciones de puertos de HMC de 9080-M9S

Tabla 42. Ubicaciones de puertos de HMC de 9080-M9S		
Puerto	**Ubicación de puerto físico**	**LED de identificación**
Tarjeta del procesador de servicios 1 - Puerto de HMC 1	Un-P1-C3-T1	No
Tarjeta del procesador de servicios 1 - Puerto de HMC 2	Un-P1-C3-T2	No

Tabla 42. Ubicaciones de puertos de HMC de 9080-M9S (continuación)		
Puerto	**Ubicación de puerto físico**	**LED de identificación**
Tarjeta del procesador de servicios 2 - Puerto de HMC 1	Un-P1-C4-T1	No
Tarjeta del procesador de servicios 2 - Puerto de HMC 2	Un-P1-C4-T2	No
Para obtener más información sobre las ubicaciones de los puertos de la HMC en 9080-M9S, consulte Ubicaciones de piezas y códigos de ubicación.		

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU.

Es posible que IBM no ofrezca en otros países los productos, servicios o características descritos en este documento. Solicite información al representante local de IBM acerca de los productos y servicios disponibles actualmente en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPRESAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunas jurisdicciones no permiten la renuncia de garantías expresas o implícitas en ciertas transacciones, por lo que esta declaración podría no ser aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información incluida en este documento está sujeta a cambios periódicos, que se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en el producto(s) y/o el programa(s) descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios web que no sean de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de dichos sitios web. Los materiales de estos sitios web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le suministre de cualquier modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los ejemplos de datos de rendimiento y de clientes citados se presentan solamente a efectos ilustrativos. Los resultados reales de rendimiento pueden variar en función de configuraciones específicas y condiciones de operación.

La información concerniente a productos que no sean de IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad o cualquier otra afirmación relacionada con productos que no son de IBM. Las consultas acerca de las prestaciones de los productos que no sean de IBM deben dirigirse a las personas que los suministran.

Las declaraciones relacionadas con las futuras directrices o intenciones de IBM están sujetas a cambios o a su retirada sin previo aviso y sólo representan metas u objetivos.

Todos los precios IBM que se muestran son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambios sin previo aviso. Los precios de los distribuidores pueden variar.

Esta documentación se suministra sólo a efectos de planificación. La información que aquí se incluye está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres reales de personas o empresas es mera coincidencia.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Los gráficos y especificaciones contenidos aquí no deben reproducirse total ni parcialmente sin el permiso escrito de IBM.

IBM ha preparado esta información para que se utilice con las máquinas especificadas indicadas. IBM no garantiza que sea adecuada para ningún otro propósito.

Los sistemas informáticos de IBM contienen mecanismos diseñados para reducir la posibilidad de que haya una alteración o pérdida de datos sin detectar. Sin embargo, este riesgo no se puede descartar. Los usuarios que experimentan cortes energéticos no planificados, anomalías del sistema, fluctuaciones o interrupciones de alimentación o averías de componentes, deben verificar la exactitud de las operaciones realizadas y de los datos guardados o transmitidos por el sistema en el momento más aproximado posible de producirse el corte o la anomalía. Además, los usuarios deben establecer procedimientos para garantizar que existe una verificación de datos independiente antes de fiarse de esos datos en las operaciones críticas o confidenciales. Los usuarios deben visitar periódicamente los sitios web de soporte de IBM para comprobar si hay información actualizada y arreglos que deban aplicarse al sistema y al software relacionado.

Declaración de homologación

Es posible que este producto no esté certificado para la conexión a través de algún medio, sea cual sea, a las interfaces de las redes públicas de telecomunicaciones. Es posible que la ley requiera más certificación antes de realizar una conexión de ese estilo. Si tiene alguna consulta, póngase en contacto con un representante o distribuidor de IBM.

Funciones de accesibilidad para servidores IBM Power Systems

Las funciones de accesibilidad ayudan a los usuarios con discapacidades como, por ejemplo, movilidad restringida o visión limitada, a la hora de utilizar el contenido de las tecnologías de la información de forma correcta.

Visión general

Los servidores IBM Power Systems incluyen estas funciones de accesibilidad principales:

- Funcionamiento solo con teclado
- Operaciones que utilizan un lector de pantalla

Los servidores IBM Power Systems utilizan el estándar W3C más reciente, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), con el fin de garantizar la conformidad con la US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) y las directrices Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para aprovechar las funciones de accesibilidad, utilice la versión más reciente del su lector de pantalla y el navegador web más reciente que admitan los servidores IBM Power Systems.

La documentación en línea de productos de servidores IBM Power Systems de IBM Knowledge Center está habilitada para las funciones de accesibilidad. Las funciones de accesibilidad de IBM Knowledge Center se describen en la Sección de accesibilidad de la ayuda de IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Navegación con teclado

Este producto utiliza las teclas de navegación estándar.

Información sobre la interfaz

Las interfaces de usuario de los servidores IBM Power Systems no disponen de contenido que parpadee entre 2 y 55 veces por segundo.

La interfaz de usuario de web de los servidores IBM Power Systems se basan en hojas de estilo en cascada para representar el contenido correctamente y para ofrecer una experiencia útil. La aplicación proporciona una forma equivalente para que los usuarios con visión reducida utilicen los valores de visualización del sistema, incluida la modalidad de alto contraste. Puede controlar la medida de la letra mediante los valores del dispositivo o del navegador web.

La interfaz de usuario de los servidores IBM Power Systems incluye puntos de referencia de navegación WAI-ARIA que se pueden utilizar para navegar de forma rápida a áreas funcionales de la aplicación.

Software de proveedores

Los servidores IBM Power Systems incluyen software de determinados proveedores que no está cubierto en el acuerdo de licencia de IBM. IBM no se hace responsable de las funciones de accesibilidad de estos productos. Póngase en contacto con el proveedor si necesita información sobre la accesibilidad en estos productos.

Información relacionada con la accesibilidad

Además del centro de atención al cliente de IBM y de los sitios web de ayuda técnica, IBM dispone de un servicio telefónico de teletipo para que las personas sordas o con dificultades auditivas puedan acceder a los servicios de ventas y soporte técnico:

Servicio TTY
800-IBM-3383 (800-426-3383)
(en Norteamérica)

Para obtener más información sobre el compromiso de IBM en cuanto a la accesibilidad, consulte IBM Accessibility (www.ibm.com/able).

Consideraciones de la política de privacidad

Los productos de IBM Software, incluido el software como soluciones de servicio, (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se describe información específica sobre la utilización de cookies por parte de esta oferta.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilan el nombre de cada usuario y la dirección IP para fines de gestión de sesiones. Estas cookies pueden inhabilitarse, pero su inhabilitación también eliminará la funcionalidad que habilitan.

Si las configuraciones desplegadas para esta oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, que incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de las diversas tecnologías, incluidas las cookies, para estos fines, consulte la política de privacidad de IBM en https://www.ibm.com/es-es/privacy y la Declaración de Privacidad Online en https://www.ibm.com/es-es/privacy/details en la sección “Cookies, balizas web y otras tecnologías”.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras empresas. Puede encontrar una lista actualizada de las marcas registradas IBM en Copyright and trademark information.

La marca registrada Linux se utiliza de acuerdo con una sublicencia de Linux Foundation, el titular exclusivo de la licencia de Linus Torvalds, propietario de la marca en todo el mundo.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph y Gluster son marcas registradas de Red Hat, Inc. o sus filiales en Estados Unidos y en otros países.

Microsoft y Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o de sus filiales.

Avisos de emisiones electrónicas

Avisos para la Clase A

Las siguientes declaraciones de Clase A se aplican a los servidores de IBM que contienen el procesador POWER9 y sus características a menos que se designe como de Clase B de compatibilidad electromagnética (EMC) en la información de características.

Cuando conecte un monitor al equipo debe utilizar el cable de monitor correspondiente y los dispositivos para la eliminación de interferencias suministrado por su fabricante.

Aviso de Canadá

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

Aviso de la Comunidad Europea y Marruecos

Este producto cumple con los requisitos de protección de la Directiva 2014/30/EU del Parlamento Europeo y del Consejo sobre la armonización de la legislación de los Estados miembros en relación con la compatibilidad electromagnética. IBM declina toda responsabilidad por el incumplimiento de los requisitos de protección resultante de una modificación no recomendada del producto, incluida la instalación de tarjetas de opciones que no son de IBM.

Este producto puede causar interferencias si se utiliza en zonas residenciales. Dicho uso debe evitarse a menos que el usuario tome medidas especiales para reducir las emisiones electromagnéticas con el fin de evitar interferencias con la recepción de difusiones de radio y televisión.

Aviso: Este equipo es compatible con la Clase A de CISPR 32. En un entorno residencial, este equipo puede provocar interferencias de radio.

Aviso de Alemania

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

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

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

Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

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

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

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

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Alemania
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.

Aviso de Japan Electronics and Information Technology Industries Association (JEITA)

（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

Esta declaración se aplica a productos inferiores o iguales a 20 A por fase.

高調波電流規格 JIS C 61000-3-2 適合品

Esta declaración se aplica a productos con más de 20 A de una sola fase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

Esta sentencia se aplica a productos superiores a 20 A por fase, tres fases.

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

Aviso del Consejo de Control Voluntario de Interferencias (VCCI) de Japón

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

Aviso de Corea

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

Aviso de la República Popular de China

声 明

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

Aviso de Rusia

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

Aviso de Taiwán

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。

Información de contacto de IBM Taiwán:

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

Aviso de la comisión FCC (Federal Communications Commission) de EE.UU.

Este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase A, en conformidad con la Sección 15 de las normas de la FCC. Estos límites están diseñados para ofrecer una protección adecuada contra interferencias nocivas cuando el equipo se utiliza en un entorno comercial. Este equipo genera, utiliza y puede irradiar energía de frecuencia de radio y, si no se instala y utiliza de acuerdo con el manual de instrucciones, puede provocar interferencias perjudiciales para las comunicaciones de radio. El funcionamiento de este equipo en una zona residencial podría provocar interferencias perjudiciales, en cuyo caso el usuario deberá corregir las interferencias por su cuenta.

Hay que utilizar cables y conectores debidamente protegidos y con toma de tierra para cumplir con los límites de emisión de la FCC. Los cables y conectores adecuados están disponibles en los distribuidores autorizados de IBM. IBM no se responsabiliza de ninguna interferencia de radio o televisión ocasionada por la utilización de cables y conectores que no sean los recomendados o por la realización de cambios o modificaciones no autorizados en este equipo. Los cambios o modificaciones no autorizados pueden anular la autorización del usuario sobre el uso del equipo.

Este dispositivo está en conformidad con la Sección 15 de las
normas de la FCC. Su funcionamiento está sujeto a dos condiciones:
(1) este dispositivo
no puede causar interferencias perjudiciales y (2) este dispositivo debe
aceptar las interferencias que se reciban, incluidas
aquellas que pueden causar un funcionamiento no deseado.

Parte responsable:
International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
Contacto para obtener información sobre la conformidad con FCC únicamente: fccinfo@us.ibm.com

Avisos para la Clase B

Las siguientes declaraciones de Clase B se aplican a las características designadas como Clase B de compatibilidad electromagnética (EMC) en la información de instalación de características.

Cuando conecte un monitor al equipo debe utilizar el cable de monitor correspondiente y los dispositivos para la eliminación de interferencias suministrado por su fabricante.

Aviso de Canadá

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

Aviso de la Comunidad Europea y Marruecos

Este producto cumple con los requisitos de protección de la Directiva 2014/30/EU del Parlamento Europeo y del Consejo sobre la armonización de la legislación de los Estados miembros en relación con la compatibilidad electromagnética. IBM declina toda responsabilidad por el incumplimiento de los requisitos de protección resultante de una modificación no recomendada del producto, incluida la instalación de tarjetas de opciones que no son de IBM.

Aviso en alemán

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

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

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

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

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

Generelle Informationen:

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

Aviso de Japan Electronics and Information Technology Industries Association (JEITA)

（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

Esta declaración se aplica a productos inferiores o iguales a 20 A por fase.

高調波電流規格 JIS C 61000-3-2 適合品

Esta declaración se aplica a productos con más de 20 A de una sola fase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

Esta sentencia se aplica a productos superiores a 20 A por fase, tres fases.

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

Aviso del Consejo de Control Voluntario de Interferencias (VCCI) de Japón

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

Aviso de Taiwán

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

Aviso de la comisión FCC (Federal Communications Commission) de EE.UU.

Este equipo ha sido probado y ha sido declarado conforme con los límites para dispositivos digitales de Clase B, en conformidad con la Sección 15 de las Normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable ante interferencias perjudiciales en una instalación residencial.Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con las instrucciones, puede producir interferencias perjudiciales en las comunicaciones de radio. Sin embargo, no hay ninguna garantía de que no se produzcan interferencias en una instalación determinada.Si este equipo produce interferencias perjudiciales en la recepción de radio o televisión, lo cual se puede determinar apagando y encendiendo el equipo, se aconseja al usuario que intente corregir las interferencias tomando una o varias de las siguientes medidas:

- Reorientar o volver a ubicar la antena receptora.
- Aumentar la separación entre el equipo y el receptor.
- Conectar el equipo a una toma de alimentación de un circuito distinto de aquél al que está conectado el receptor.

- Consultar con un distribuidor autorizado de IBM o con el representante de servicio para obtener asistencia.

Hay que utilizar cables y conectores debidamente protegidos y con toma de tierra para cumplir con los límites de emisión de la FCC. Los cables y conectores adecuados están disponibles en los distribuidores autorizados de IBM. IBM no se responsabiliza de ninguna interferencia de radio o televisión ocasionada por la utilización de cables y conectores que no sean los recomendados o por la realización de cambios o modificaciones no autorizados en este equipo. Los cambios o modificaciones no autorizados pueden anular la autorización del usuario sobre el uso del equipo.

Este dispositivo está en conformidad con la Sección 15 de las normas de la FCC. Su funcionamiento está sujeto a dos condiciones:

(1) este dispositivo
no puede causar interferencias perjudiciales y (2) este dispositivo debe
aceptar las interferencias que se reciban, incluidas
aquellas que pueden causar un funcionamiento no deseado.

Parte responsable:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
Contacto para obtener información sobre la conformidad con FCC únicamente: fccinfo@us.ibm.com

Términos y condiciones

El permiso para utilizar estas publicaciones se otorga de acuerdo con los siguientes términos y condiciones.

Aplicabilidad: estos términos y condiciones son adicionales a los términos de uso del sitio web de IBM.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Derechos: Excepto lo expresamente concedido en este permiso, no se conceden otros permisos, licencias ni derechos, explícitos o implícitos, sobre las publicaciones ni sobre ninguna información, datos, software u otra propiedad intelectual contenida en el mismo.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer de IBM, no se sigan debidamente las instrucciones anteriores.

No puede descargar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.