

Power Systems

*Instalar e configurar a Consola de Gestão  
de Hardware*



**Nota**

Antes de utilizar as informações e o produto que suporta, leia as informações em “[Informações sobre segurança](#)” na página v, “[Avisos](#)” na página 115, no manual *IBM Systems Safety Notices*, G229-9054, e no manual *IBM Environmental Notices and User Guide*, Z125-5823.

Esta edição aplica-se à Consola de Gestão de Hardware da IBM® Versão 9 Edição 2 Nível de Manutenção 950 e a todas as edições e modificações subsequentes até indicação em contrário em novas edições.

© **Copyright International Business Machines Corporation 2018, 2021.**

---

# Índice

<b>Informações sobre segurança.....</b>	<b>V</b>
<b>Instalar e configurar a Consola de Gestão de Hardware.....</b>	<b>1</b>
Novidades na Instalação e configuração da HMC.....	1
Tarefas de instalação e configuração.....	2
Instalar e configurar uma nova HMC com um novo servidor.....	2
Actualizar e aperfeiçoar o código da HMC.....	3
Adicionar uma segunda HMC a uma instalação existente.....	3
Preparar a HMC.....	4
Instalar o IBM Power Systems HMC (7063-CR2) num bastidor.....	4
Instalar a 7063-CR1 num bastidor.....	15
Instalar a HMC 7042-CR9 num bastidor.....	25
Instalar a Dispositivo virtual da HMC .....	37
Configurar a HMC.....	52
Seleção de definições de rede na HMC.....	52
Configurar a HMC.....	69
Passos de Pós-configuração.....	91
Actualizar, aperfeiçoar e migrar o código máquina da HMC.....	92
Proteger a HMC.....	104
Política aperfeiçoada de palavras-passe.....	106
Resolver problemas comuns enquanto protege a HMC.....	107
Perfis de segurança: Security profiles: Regulamentação de Protecção de Dados Globais (GDPR, Global Data Protection Regulation) e Padrão de Segurança de Dados de Indústria de Cartões de Pagamento (PCI-DSS, Payment Card Industry Data Security Standard) .....	110
Localizações das portas HMC.....	111
<b>Avisos.....</b>	<b>115</b>
Funções de acessibilidade para servidores IBM Power Systems.....	116
Considerações da política de privacidade .....	117
Marcas comerciais.....	118
Avisos de emissão electrónica.....	118
Informações da Classe A.....	118
Avisos da Classe B.....	121
Termos e condições.....	124



# Informações sobre segurança

---

As informações sobre segurança podem estar em qualquer lugar deste guia:

- Os avisos de **PERIGO** chamam a atenção para uma situação potencialmente letal ou bastante perigosa para as pessoas.
- Os avisos de **CUIDADO** chamam a atenção para uma situação potencialmente perigosa para as pessoas devido a alguma condição em particular.
- Os avisos de **Atenção** chamam a atenção para a possibilidade de causar danos ao programa, dispositivo, sistema ou dados.

## Informações sobre segurança para comércio internacional

Alguns países requerem que as informações sobre segurança contidas nas publicações do produto estejam no idioma nacional. Se este requisito se aplica no seu país, a documentação com as informações de segurança está incluída no pacote de publicações (tal como a documentação impressa, em DVD ou como parte do produto) enviada com o produto. A documentação contém informações sobre segurança no idioma nacional com referências para a versão em Inglês dos EUA. Antes de utilizar uma publicação em Inglês do EUA para instalar, operar ou efectuar reparações sobre o produto, leia atentamente as informações sobre segurança associadas na documentação. Deverá também consultar esta documentação quando não perceber claramente qualquer informação sobre segurança nas publicações em Inglês dos EUA.

A substituição ou cópias adicionais de informações sobre segurança pode ser obtida através de um telefona para a Linha de Apoio da IBM (1-800-300-8751 apenas para os EUA).

## Informações sobre segurança do Laser

Os servidores IBM podem utilizar placas de E/S ou funções com base em fibra óptica e que utilizem lasers ou LEDs.

### Conformidade do Laser

Podem ser instalados servidores IBM dentro ou fora de um bastidor do equipamento de TI.



**Perigo:** Quando trabalhar no sistema ou em volta do sistema, tenha em atenção os seguintes cuidados:

A tensão eléctrica e a corrente dos cabos de alimentação, telefone e dados são perigosas. Para evitar uma situação de risco de choque eléctrico: Se a IBM forneceu o(s) cabo(s) de alimentação, ligue a alimentação a esta unidade apenas com o cabo de alimentação fornecido pela IBM. Não utilize o cabo de alimentação fornecido pela IBM para qualquer outro produto. Não abra nem repare qualquer conjunto da fonte de alimentação. Não ligue nem desligue quaisquer cabos nem execute instalações, manutenções ou reconfigurações deste produto durante uma trovoadas.



- O produto pode estar equipado com vários cabos de alimentação. Para remover todas as tensões perigosas, desligue todos os cabos de alimentação. Para alimentação CA, desligue todos os cabos de alimentação da respectiva fonte de alimentação de CA. Para bastidores com um painel de distribuição de potência em CC (PDP), desligue a fonte de alimentação CC do cliente para o PDP.
- Ao ligar a alimentação ao produto certifique-se de que todos os cabos de alimentação estão devidamente ligados. Para bastidores com alimentação CA, ligue todos os cabos de alimentação a uma tomada com ligação à terra correctamente estabelecida. Certifique-se de que a tomada fornece a tensão e rotação física adequadas de acordo com a placa de classificação do sistema. Para bastidores

com um painel de distribuição de potência em CC (PDP), ligue a fonte de alimentação CC do cliente para o PDP. Certifique-se de que é utilizada a polaridade correcta quando ligar a alimentação CC e a cablagem de retorno de alimentação CC.

- Ligue todos os equipamentos que serão utilizados com este produto a tomadas correctamente instaladas.
- Sempre que possível, utilize apenas uma mão para ligar ou desligar os cabos de sinal.
- Nunca ligue equipamento em caso de incêndio, inundação ou danos estruturais.
- Não tente ligar a alimentação à máquina até que todas as possíveis condições de insegurança estejam corrigidas.
- Ao realizar uma inspecção à máquina: Assuma que existem sempre perigos de segurança eléctricos. Efectue todas as verificações de continuidade, ligação à terra e alimentação especificadas durante os procedimentos de instalação do subsistema para garantir que a máquina corresponde aos requisitos de segurança. Não tente ligar a alimentação à máquina até que todas as possíveis condições de insegurança estejam corrigidas. Antes de abrir as tampas dos dispositivos, a menos que lhe sejam dadas instruções diferentes nos procedimentos de instalação e configuração: Desligue os cabos de alimentação CA ligados, desligue os disjuntores aplicáveis localizados no painel de distribuição de alimentação (PDP) do bastidor e desligue todos os sistemas de telecomunicações, redes e modems.
- Ligue e desligue cabos conforme descrito nos procedimentos seguintes ao instalar, mover ou abrir tampas neste produto ou dispositivos ligados.

Para desligar: 1) Desligue tudo (excepto em caso de instruções contrárias). 2) Para alimentação CA, remova os cabos de alimentação das tomadas. 3) Para bastidores com um painel de distribuição de alimentação em CC (PDP), desligue os disjuntores localizados no PDP e remova a alimentação da fonte de alimentação CC do cliente. 4) Remova os cabos de sinal dos conectores. 5) Remova todos os cabos dos dispositivos.

Para ligar: 1) Desligue tudo (excepto em caso de instruções contrárias). 2) Ligue todos os cabos aos dispositivos. 3) Ligue os cabos de sinal aos conectores. 4) Para alimentação CA, ligue os cabos de alimentação às tomadas. 5) Para bastidores com um painel de distribuição de alimentação em CC (PDP), reponha a alimentação a partir da fonte de alimentação CC do cliente e ligue os disjuntores localizados no PDP. 6) Ligue os dispositivos.



- Pode verificar-se a presença de extremidades, arestas e juntas cortantes no sistema ou na proximidade do mesmo. Manuseie o equipamento cuidadosamente para evitar cortes ou quaisquer outras lesões. (D005)

#### **(R001 parte 1 de 2):**



**Perigo:** Tenha em atenção os seguintes cuidados quando trabalhar no sistema do bastidor de TI ou em volta do sistema:

- Equipamento pesado – caso seja manipulado incorrectamente, pode resultar em lesões pessoais ou danos no equipamento.
- Baixe sempre os niveladores no armário de bastidor.
- Se fornecidos, instale sempre os suportes estabilizadores no armário de bastidor, a menos que seja para instalar a opção de tremor de terra.
- Para evitar condições perigosas devido a carregamento mecânico irregular, instale sempre os dispositivos mais pesados na parte inferior do armário de bastidor. Instale sempre os servidores e dispositivos opcionais começando pela parte inferior do armário de bastidor.
- Dispositivos montados em bastidor não devem ser utilizados como prateleiras ou espaços de trabalho. Não coloque objectos sobre os dispositivos montados em bastidor. Adicionalmente, não se apoie em dispositivos montados em bastidores e não os utilize para estabilizar a sua posição do corpo (por exemplo, quando trabalha numa escada).



- Perigo de estabilidade:
  - O bastidor pode tombar provocando lesões pessoais graves.
  - Antes de expandir o bastidor para a posição de instalação, leia as instruções de instalação.
  - Não coloque qualquer carga no equipamento montado nas calhas deslizantes instalado na posição de instalação.
  - Não deixe o equipamento montado nas calhas deslizantes na posição de instalação.
- Cada armário de bastidor poderá ter mais do que um cabo de alimentação.
  - Para bastidores alimentados com CA, certifique-se de que desliga todos os cabos de alimentação no armário de bastidor quando for instruído para desligar a alimentação durante a assistência.
  - Para bastidores com um painel de distribuição de alimentação em CC (PDP), desligue o disjuntor que controla a alimentação às unidades dos sistema ou desligue a fonte de alimentação de CC, quando lhe for indicado para desligar a alimentação durante a assistência.
- Ligue todos os dispositivos instalados num armário de bastidor a dispositivos de alimentação instalados no mesmo armário de bastidor. Não ligue um cabo de alimentação de um dispositivo instalado num armário de bastidor a um dispositivo de alimentação instalado noutra armário de bastidor.
- Uma tomada que não tenha ligações correctas à corrente e à terra pode colocar tensões perigosas nos componentes de metal do sistema ou nos dispositivos ligados ao sistema. É da responsabilidade do cliente garantir que a tomada tem ligações correctas à corrente e à terra para prevenir um choque eléctrico. (R001 parte 1 de 2)

**(R001 parte 2 de 2):**



**Cuidado:**

- Não instale uma unidade num bastidor onde as temperaturas ambiente internas excedam as recomendadas pelo fabricante para todos os dispositivos montados em bastidor.
- Não instale uma unidade num bastidor onde a circulação do ar seja insuficiente. Assegure-se de que a circulação do ar não está bloqueada ou reduzida nas partes laterais, anterior ou posterior de um dispositivo utilizado para ventilar o ar através da unidade.
- Deve ter em consideração a ligação do equipamento ao circuito eléctrico de alimentação para que a sobrecarga de circuitos não comprometa a protecção contra sobrecargas de corrente ou ligações de alimentação. Para fornecer a ligação de alimentação correcta a um bastidor, consulte as etiquetas de tensão nominal localizadas no equipamento do bastidor para determinar todos os requisitos de alimentação do circuito eléctrico de alimentação.
- *(Para gavetas deslizantes.)* Não puxe para fora nem instale qualquer gaveta ou componente se os suportes estabilizadores não estiverem instalados no bastidor ou se o bastidor não estiver aparafusado ao chão. Não puxe para fora mais do que uma gaveta de cada vez. O bastidor pode tornar-se instável se puxar para fora mais do que uma gaveta de cada vez.



- (Para gavetas fixas.) Esta gaveta é fixa e não deve ser movida para assistência a não ser que esse procedimento seja especificado pelo fabricante. A tentativa de mover a gaveta parcial ou totalmente para fora do bastidor pode causar instabilidade no mesmo ou fazer com que a gaveta caia do bastidor. (R001 parte 2 de 2)



**Cuidado:** A remoção dos componentes das posições superiores do armário de bastidor permite melhorar a estabilidade do bastidor durante a relocalização. Siga estas directrizes gerais sempre que recolocar um armário de bastidor preenchido numa sala ou edifício.

- Reduza o peso do armário de bastidor removendo o equipamento, começando pela parte superior do armário de bastidor. Quando for possível, restaure a configuração do armário de bastidor para a que tinha quando foi recebido. Se esta configuração não for conhecida, tem de observar os seguintes cuidados:
  - Remova todos os dispositivos da posição 32U e superiores.
  - Certifique-se de que os dispositivos mais pesados são instalados na parte inferior do armário de bastidor.
  - Certifique-se de que não existem quaisquer níveis U vazios entre dispositivos instalados no armário de bastidor abaixo do nível 32U, a não ser que a configuração recebida permita esta situação de forma específica.
- Se o armário de bastidor que estiver a relocalizar fizer parte de um conjunto de armários de bastidor, desligue o armário de bastidor do conjunto.
- Se o armário de bastidor que está a recolocar tiver sido facultado com extensões estabilizadores removíveis, estas têm de ser reinstaladas antes do armário ser recolocado.
- Inspeccione o percurso que pretende utilizar para eliminar potenciais situações de risco.
- Verifique se o percurso escolhido suporta o peso do armário de bastidor carregado. Consulte a documentação fornecida com o armário de bastidor, para obter o peso de um armário de bastidor carregado.
- Verifique se todas as aberturas das portas têm no mínimo 760 x 2083 mm (30 x 82 pol).
- Certifique-se de que todos os dispositivos, prateleiras, gavetas, portas e cabos estão seguros.
- Certifique-se de que os quatro niveladores estão colocados na respectiva posição mais elevada.
- Certifique-se de que não está instalado qualquer suporte estabilizador no armário de bastidor durante a deslocação.
- Não utilize uma rampa com uma inclinação superior a 10 graus.
- Quando o armário de bastidor estiver na nova localização, complete os seguintes passos:
  - Baixe os quatro niveladores.
  - Instale os suportes estabilizadores no armário de bastidor ou num ambiente de terramotos aparafuse o bastidor ao chão.
  - Se remover quaisquer dispositivos do armário de bastidor, encha novamente o armário de bastidor começando pela posição mais baixa até à posição mais elevada.

- Se for necessária uma realocação de longa distância, restaure a configuração original do armário de bastidor. Embale o armário de bastidor com o material da embalagem original ou equivalente. Além disso, baixe os niveladores para que os rodízios fiquem salientes na paleta e aparafuse o armário de bastidor à paleta.

(R002)

**(L001)**



**Perigo:** Um componente que possua esta etiqueta possui tensões, correntes ou níveis de energia perigosos. Não abra uma tampa ou barreira que contenha esta etiqueta. (L001)

**(L002)**

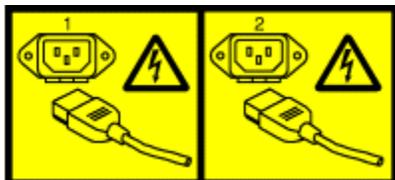


**Perigo:** Dispositivos montados em bastidor não devem ser utilizados como prateleiras ou espaços de trabalho. Não coloque objectos sobre os dispositivos montados em bastidor. Adicionalmente, não se apoie em dispositivos montados em bastidores e não os utilize para estabilizar a sua posição do corpo (por exemplo, quando trabalha numa escada). Perigo de estabilidade:

- O bastidor pode tombar provocando lesões pessoais graves.
- Antes de expandir o bastidor para a posição de instalação, leia as instruções de instalação.
- Não coloque qualquer carga no equipamento montado nas calhas deslizantes instalado na posição de instalação.
- Não deixe o equipamento montado nas calhas deslizantes na posição de instalação.

(L002)

**(L003)**



ou



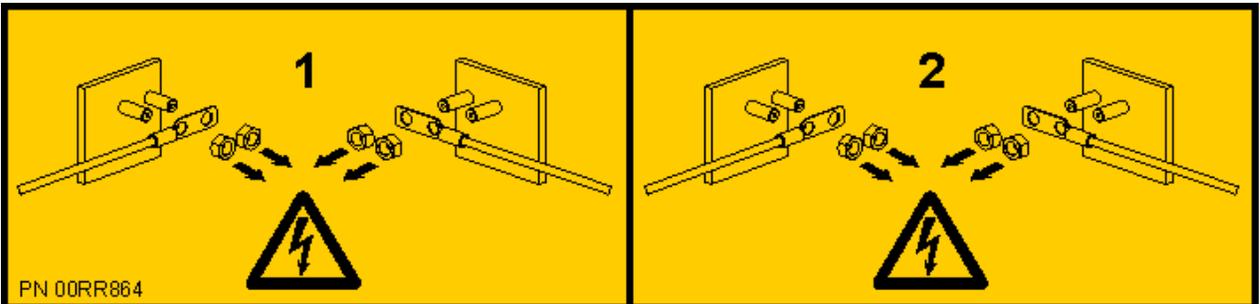
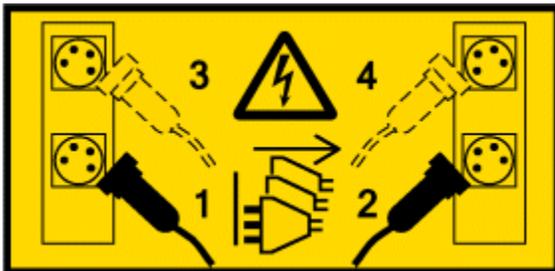
ou



ou



ou



**Perigo:** Múltiplos cabos de alimentação. O produto pode estar equipado com múltiplos cabos de alimentação de CA ou com múltiplos cabos de alimentação de CC. Para remover todas as tensões perigosas, desligue todos as linhas e cabos de alimentação. (L003)

(L007)



**Cuidado:** Existência de uma superfície quente. (L007)

(L008)



**Cuidado:** Movimentação de componentes perigosos perto. (L008)

Todos os lasers são certificados nos EUA de acordo com os requisitos da norma DHHS 21 CFR sub-capítulo J para produtos laser de classe 1. Fora dos EUA, são certificados de acordo com a norma IEC 60825 para produtos laser de classe 1. Consulte a etiqueta de cada componente para identificar os números de certificação laser e as informações de aprovação.



**Cuidado:** Este produto pode conter um ou mais dos seguintes dispositivos: unidade CD-ROM, unidade DVD-ROM, unidade DVD-RAM ou módulo laser, que são produtos laser de Classe 1. Tenha em atenção as seguintes informações:

- Não remova as tampas. A remoção das tampas de um produto laser pode resultar na exposição a radiações laser perigosas. Não existem quaisquer componentes no interior do dispositivo passíveis de assistência.
- A utilização de controlos ou realização de ajustes ou de procedimentos diferentes dos contidos nesta publicação pode resultar na exposição a radiações laser perigosas.

(C026)



**Cuidado:** Os ambientes de processamento de dados podem conter equipamentos que efectuem transmissões em ligações do sistema com módulos laser que funcionem em níveis de alimentação superiores aos níveis da Classe 1. Por este motivo, nunca olhe para a extremidade de um cabo de fibra óptica nem para uma caixa de ligação aberta. Apesar do facto de projectar luz para uma extremidade e de olhar para outra extremidade de uma fibra óptica desligada, para verificar a continuidade das fibras ópticas, poder não ferir no olho, este procedimento é potencialmente perigoso. Assim, não é recomendado verificar a continuidade das fibras ópticas ao projectar luz para uma extremidade enquanto olha para a outra extremidade. Para verificar a continuidade de um cabo de fibra óptica, utilize uma fonte de luz óptica e um wattómetro. (C027)



**Cuidado:** Este produto contém laser da Classe 1M. Não visualize directamente com instrumentos ópticos. (C028)



**Cuidado:** Alguns produtos laser contêm um díodo laser da Classe 3A ou da Classe 3B incorporado. Tenha em atenção as seguintes informações:

- Presença de radiações laser quando a unidade se encontra aberta.
- Não olhe fixamente para o raio laser, não visualize directamente com instrumentos ópticos e evite a exposição directa ao raio laser. (C030)

(C030)



**Cuidado:** A bateria contém lítio. Para evitar o perigo de explosão, não incendeie nem sobrecarregue a bateria.

*Não:*

- Molhe ou mergulhe na água
- Aqueça a mais de 100 graus C (212 graus F)
- Repare nem desmonte a bateria

Substitua apenas pelo componente aprovado pela IBM. Recicle ou deite fora a bateria, tal como indicado pelos regulamentos locais. Em Portugal, o sistema de recolha e reciclagem de baterias é assegurado pelo governo. As baterias usadas são recolhidas nos estabelecimentos comerciais de revenda onde existem baterias à venda, bem como em pontos de recolha municipais. Para mais informações, contacte as autoridades municipais da sua área. Para qualquer contacto sobre este assunto, tenha disponível o part number que consta na bateria. (C003)



**Cuidado:** Sobre a FERRAMENTA DE ELEVAÇÃO DO FORNECEDOR fornecida pela IBM:

- Operação da FERRAMENTA DE ELEVAÇÃO apenas por pessoal autorizado.
- A FERRAMENTA DE ELEVAÇÃO destina-se a prestar assistência, levantar, instalar, remover unidades (carregadas) em elevações de bastidores. Não deve ser utilizada carregada como transporte em rampas de acesso de grandes dimensões nem como substituição de determinadas ferramentas como carros, empilhadoras, carregadores de paletes nem para outras práticas de recolocação relacionadas. Quando esta situação não for praticável, deverão ser utilizadas pessoas ou serviços especializados (como, por exemplo, transportadoras ou funcionários de empresas de mudanças).
- Leia e compreenda totalmente o conteúdo do manual de funcionamento da FERRAMENTA DE ELEVAÇÃO antes de a utilizar. Não ler, compreender, obedecer às regras de segurança e seguir às instruções à risca poderá resultar em danos na propriedade e/ou em lesões nas pessoas. Se existirem questões, contacte o suporte e a assistência do fornecedor. O manual impresso local facultado deverá permanecer juntamente com a máquina na área da pasta de armazenamento facultada. O manual com a revisão mais recente está disponível no sítio da Web do fornecedor.
- Teste e verifique a função de travão do estabilizador antes de cada utilização. Não force o movimento ou o deslocamento vertical da FERRAMENTA DE ELEVAÇÃO com o travão estabilizador activado.
- Não levante, baixe ou deslize a prateleira de carregamento da plataforma a não ser que o estabilizador (pedal de travão) esteja totalmente preso. Mantenha o travão do estabilizador preso quando não estiver em utilização ou movimento.
- Não mova a FERRAMENTA DE ELEVAÇÃO enquanto a plataforma está elevada, excepto para posicionamentos menores.
- Não exceda a capacidade de carga nominal. Consulte o GRÁFICO DE CAPACIDADE DE CARGA relativamente às cargas máximas no centro face às extremidades da plataforma expandida.
- Apenas eleve a carga caso esteja devidamente centrada na plataforma. Não coloque mais de 200 lb (91 kg) na extremidade da plataforma prateleira da plataforma deslizante e tenha também em conta o centro de massa/gravidade (CoG) da carga.
- Não carregue os cantos das plataformas, incline a placa de expansão, use uma cunha de instalação para a unidade angular ou outras opções de acessórios semelhantes. Prenda essas plataformas -- as opções da placa de expansão, a cunha, etc, para manter a barra lateral levantada ou forquilha em todas as quatro localizações (x4 ou outra instalação aprovada) apenas com o hardware fornecido, antes da utilização. Os objectos de carga são concebidos para deslizar para dentro e fora de plataformas de forma suave sem ser necessário aplicar muita força e, por essa razão, não tente empurrar ou inclinar. Mantenha a opção da placa de expansão plana [ajustável ao ângulo da plataforma] em todos os momentos, excepto para pequenos ajustes de ângulo finais quando necessário.
- Não fique por baixo de carga suspensa.
- Não utilize numa superfície irregular, inclinação ou declive (grandes rampas).

- Não empilhe cargas.
- Não opere sob a influência de fármacos ou álcool.
- Não apoie escadas contra FERRAMENTA DE ELEVAÇÃO (a não ser que seja dada a permissão específica para um dos seguintes procedimentos qualificados para trabalhar com elevações com esta FERRAMENTA).
- Perigo de queda. Não empurre ou incline-se contra a carga com a plataforma elevada.
- Não utilize como plataforma de elevação de pessoal ou degrau. Sem penduras.
- Não se apoie em qualquer parte do elevador. Não é um degrau.
- Não suba para o mastro.
- Não opere uma máquina da FERRAMENTA DE ELEVAÇÃO danificada ou avariada.
- Perigo de esmagamento e beliscadura abaixo da plataforma. Desça apenas a carga em áreas desimpedidas de pessoal e de obstruções. Mantenha as mãos e os pés livres durante a operação.
- Sem forquilhas. Nunca levante ou mova a MÁQUINA DA FERRAMENTA DE ELEVAÇÃO descoberta com um porta-paletes, carregadora ou empilhadora.
- O mastro estende-se acima da plataforma. Tenha cuidado com a altura do tecto com as calhas dos cabos eléctricos, extintores, luzes e outros objectos que se encontrem elevados.
- Não deixe a FERRAMENTA DE ELEVAÇÃO abandonada com uma carga elevada.
- Tenha atenção e mantenha as mãos, dedos e roupa afastados quando o equipamento estiver em movimento.
- Vire o guincho apenas com a força das mãos. Se não for possível rodar a facilmente a pega do cabrestante com uma mão, é sinal de que poderá estar sobrecarregado. Não continue a rodar o cabrestante para lá do ponto superior ou inferior da plataforma. Um desenrolar excessivo irá desmontar a pega e danificar o cabo. Segure sempre na pega ao baixar, ao desenrolar. Garanta sempre que o cabrestante está a reter a carga antes de libertar a pega do cabrestante.
- Um acidente com o guincho poderá provocar lesões graves. Não foi concebido para mover pessoas. Certifique-se de que ouve o som de um clique à medida que o equipamento está a ser elevado. Certifique-se de que o cabrestante está bloqueado na posição antes de libertar a pega. Leia a página de instruções antes de operar este cabrestante. Nunca permita que o cabrestante se desenrole livremente. O desenrolar livre irá causar um embrulho do cabo desigual à volta do tambor do cabrestante, irá danificar o cabo e poderá causar ferimentos graves.
- Esta FERRAMENTA deve ser mantida de forma correcta para que o pessoal de assistência da IBM a possa utilizar. A IBM deverá inspeccionar as condições e verificar o histórico de manutenção antes da operação. O pessoal da assistência reserva-se ao direito de não utilizar a FERRAMENTA caso esta não esteja em conformidade. (C048)

## **Informações sobre alimentação e cablagem para NEBS (Network Equipment-Building System) GR-1089-CORE**

Os comentários seguintes aplicam-se aos servidores IBM que tenham sido designados como estando em conformidade com NEBS (Network Equipment-Building System) GR-1089-CORE:

O equipamento é adequado para instalação no seguinte:

- Instalações de telecomunicações de rede
- Localizações onde o NEC (National Electrical Code) é aplicável

As portas dentro deste equipamento são adequadas para ligação a sistemas de cablagem ou de ligações internos ou não expostos apenas. As portas dentro deste equipamento *não podem* ser ligadas de modo metálico às interfaces que ligam à OSP (planta exterior) ou respectivo sistema de ligações. Estas interfaces foram concebidas para utilização como interfaces internas apenas (portas do Tipo 2 ou Tipo 4, conforme descrito no GR-1089-CORE) e requerem isolamento da cablagem da OSP exposta. A adição dos protectores primários não é uma protecção suficiente para ligar estas interfaces de modo metálico ao sistema de ligações da OSP.

**Nota:** Todos os cabos de Ethernet têm de estar protegidos e ligados à terra em ambas as extremidades.

O sistema com alimentação de ca não requer a utilização de um dispositivo protector contra oscilações de tensão (SPD) externo.

O sistema com alimentação de cc emprega uma concepção de retorno de cc isolado (DC-I). O terminal de retorno da bateria de CC *não deverá* ser ligado ao chassis ou estrutura.

O sistema de alimentação CC tem como intuito ser instalado numa Common Bonding Network (CBN) tal como é descrito em GR-1089-CORE.

---

# Instalar e configurar a Consola de Gestão de Hardware

Saiba como instalar o hardware da Consola de Gestão de Hardware (HMC), ligá-lo ao sistema gerido e configurá-lo para utilização. O utilizador pode executar estas tarefas ou contactar o fornecedor de serviços para que as execute. É possível que o prestador de assistência exija o pagamento de uma taxa por este serviço.

## Novidades na Instalação e configuração da HMC

---

Conheça as novidades e alterações significativas no tópico Instalação e configuração da HMC desde a anterior actualização da colecção de tópicos.

### Abril de 2021

- Foram adicionados os seguintes tópicos:
  - [“Instalar o IBM Power Systems HMC \(7063-CR2\) num bastidor”](#) na página 4
  - [“Pré-requisitos para instalar o sistema 7063-CR2 instalada em bastidor”](#) na página 4
  - [“Concluir o inventário para o sistema”](#) na página 5
  - [“Determinar e marcar a localização no bastidor para o sistema 7063-CR2”](#) na página 5
  - [“Fixar as calhas ajustáveis ao chassis do sistema e ao bastidor”](#) na página 7
  - [“Fixar as calhas fixas ao chassis do sistema e ao bastidor”](#) na página 9
  - [“Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação”](#) na página 10
  - [“Ligar a HMC 7063-CR2 instalada em bastidor”](#) na página 11
  - [“Configurar a HMC 7063-CR2”](#) na página 12

### Novembro de 2020

- Foram actualizados os seguintes tópicos:
  - [“Tarefas de instalação e configuração”](#) na página 2
  - [“Instalar a HMC 7042-CR9 num bastidor”](#) na página 25
  - [“Proteger a HMC”](#) na página 104
  - [“Localizações das portas HMC”](#) na página 111

### Julho de 2020

- Foram actualizados os seguintes tópicos:
  - [“Instalar a Dispositivo virtual da HMC ”](#) na página 37
  - [“Localizações das portas HMC”](#) na página 111

### Outubro de 2019

- Foram actualizados os seguintes tópicos:
  - [“Instalar a Dispositivo virtual da HMC ”](#) na página 37
  - [“Proteger a HMC”](#) na página 104

## Fevereiro de 2019

- Foram adicionados os seguintes tópicos:
  - [“Proteger a HMC” na página 104](#)
  - [“Política aperfeiçoada de palavras-passe” na página 106](#)
  - [“Resolver problemas comuns enquanto protege a HMC” na página 107](#)
  - [“Perfis de segurança: Security profiles: Regulamentação de Protecção de Dados Globais \(GDPR, Global Data Protection Regulation\) e Padrão de Segurança de Dados de Indústria de Cartões de Pagamento \(PCI-DSS, Payment Card Industry Data Security Standard\) ” na página 110](#)

## Agosto de 2018

- Foram actualizados os seguintes tópicos:
  - [“Configurar a HMC 7063-CR1” na página 22](#)
  - [“Localizações das portas HMC” na página 111](#)

## Dezembro de 2017

- Informações adicionadas para os servidores IBM Power Systems que contenham o processador POWER9.

## Tarefas de instalação e configuração

Saiba mais sobre as tarefas associadas a diferentes tarefas de instalação e configuração da HMC.

Saiba mais sobre, a um alto nível, as tarefas que é necessário concluir quando instalar e configura a HMC. É possível instalar e configurar a HMC de formas diferentes. Encontre a situação que melhor corresponde à tarefa que pretende concluir.

### Notas:

- Caso esteja a gerir servidores baseados em processadores POWER9, a HMC tem de se encontrar na Versão 9.1.0 ou posterior. Para obter mais informações, consulte [“Determinar a versão e a edição do código máquina da HMC” na página 92](#).
- A Consola de Gestão de Hardware (Hardware Management Console) Versão 9.2.950 ou posterior não é suportada no Tipo de Máquina HMC 7042. Para obter mais informações sobre as versões da HMC para a sua HMC 7042, consulte as notas de edição que se encontram disponíveis no sítio da [Web Central de Correções \(Fix Central\)](#).

## Instalar e configurar uma nova HMC com um novo servidor

Saiba mais sobre as tarefas de alto nível que é necessário concluir quando instala e configura uma nova HMC com um novo servidor.

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Recolha informações e conclua o Esquema de Configuração de Pré-Instalação.	<a href="#">“Esquema de configuração da pré-instalação para a HMC” na página 62</a> <a href="#">“Preparar a configuração da HMC” na página 60</a>
2. Descompacte o hardware.	
3. Ligue o hardware da HMC.	<a href="#">“Ligar a HMC 7063-CR1 instalada em bastidor” na página 20</a>

*Tabela 1. Tarefas que é necessário concluir quando instalar e configura uma nova HMC com um novo servidor (continuação)*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
4. Ligue a HMC ao premir o botão de alimentação.	
5. Inicie sessão e inicie a aplicação da Web da HMC.	
6. Acesse ao Assistente de Instalação Assistida ou utilize os menus da HMC para configurar a HMC.	<p>“Configurar a HMC utilizando o caminho rápido através do Assistente de Instalação Assistida” na página 69</p> <p>“Configurar a HMC através da utilização dos menus” na página 70</p>
7. Anexe o servidor à HMC.	

## Actualizar e aperfeiçoar o código da HMC

Saiba mais sobre as tarefas de alto nível que é necessário concluir quando actualiza e aperfeiçoa o código da HMC.

Se tiver uma HMC existente e pretender actualizar ou aperfeiçoar o código da HMC, deve concluir as seguintes tarefas de alto nível:

*Tabela 2. Tarefas que é necessário concluir quando actualiza ou aperfeiçoa o código da HMC*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Obtenha o aperfeiçoamento.	<p>“Actualizar o software da HMC” na página 98</p>
2. Veja o nível de código máquina da HMC existente.	
3. Faça cópia de segurança dos dados de perfil do sistema gerido.	
4. Faça cópia de segurança dos dados da HMC.	
5. Registe as informações de configuração da HMC actuais.	
6. Registe o estado do comando remoto.	
7. Guarde os dados de aperfeiçoamento.	
8. Aperfeiçoe o software da HMC.	
9. Verifique se o aperfeiçoamento do código máquina da HMC foi instalado com sucesso	

## Adicionar uma segunda HMC a uma instalação existente

Saiba mais sobre as tarefas de alto nível que é necessário concluir quando adiciona uma segunda HMC ao sistema gerido.

Caso possua uma HMC e sistema gerido existentes e pretende adicionar uma segunda HMC a esta configuração, conclua os seguintes passos:

*Tabela 3. Tarefas que é necessário concluir quando adiciona uma segunda HMC a uma instalação existente*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Certifique-se de que o hardware da HMC suporta o código da HMC Versão 7.	
2. Recolha informações e conclua o Esquema de Configuração de Pré-Instalação.	<a href="#">“Esquema de configuração da pré-instalação para a HMC” na página 62</a>
3. Descompacte o hardware.	
4. Ligue o hardware da HMC.	<a href="#">“Ligar a HMC 7063-CR1 instalada em bastidor” na página 20</a>
5. Ligue a HMC ao premir o botão de alimentação.	
6. Inicie a sessão na HMC.	
7. Os níveis de código da HMC têm de corresponder. Altere o código de uma das HMCs para coincidir com o da outra.	<a href="#">“Determinar a versão e a edição do código máquina da HMC” na página 92</a> <a href="#">“Actualizar o software da HMC” na página 98</a>
8. Aceda ao Assistente de Instalação Assistida ou utilize os menus da HMC para configurar a HMC.	<a href="#">“Configurar a HMC através da utilização dos menus ” na página 70</a>
9. Configure esta HMC para assistência através da utilização do assistente de Configuração de Comunicação de Retorno.	<a href="#">“Configurar a HMC de forma a que seja possível ligar à assistência e suporte através da utilização do assistente de configuração de comunicação de retorno” na página 85</a>
10. Anexe o servidor à HMC.	

## Preparar a HMC

Tem de preparar o hardware da HMC antes de configurar o software da HMC. Saiba mais acerca da preparação de uma HMC vertical ou de uma HMC instalada em bastidor.

### Instalar o IBM Power Systems HMC (7063-CR2) num bastidor

Saiba como instalar a IBM Power Systems HMC (7063-CR2) num bastidor.

Poderá visualizar a documentação de instalação online ou poderá imprimir a versão PDF das mesmas informações. Para visualizar ou imprimir a versão PDF, consulte [Instalar e configurar a Consola de Gestão de Hardware](#).

### Pré-requisitos para instalar o sistema 7063-CR2 instalada em bastidor

Utilize a informação para compreender os pré-requisitos que são requeridos para instalar o sistema.

#### Sobre esta tarefa



**Cuidado:** Este componente ou unidade é pesado mas tem um peso inferior a 18 kg (39,7 lb). Proceda com cuidado ao levantar, remover ou instalar este componente ou unidade. (C008)

Poderá precisar de ler os seguintes documentos antes de iniciar a instalação do servidor:

- A versão mais recente deste documento é mantida online, consulte [Instalar o 7063-CR2 num bastidor](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm) ([http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai\\_install7063cr2\\_kickoff.htm](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm)).
- Para planear a instalação do servidor, consulte [Planeamento das instalações e do hardware](#).

## Procedimento

1. Certifique-se de que tem os seguintes itens antes de iniciar a instalação:

- Chave de parafusos Phillips tamanho 2
- Chave de fendas de cabeça plana
- Chave de fendas T25
- X-acto
- Fita de pulso de descarga electrostática (ESD, Electrostatic discharge)
- Bastidor com uma unidade (1U) de Associação das Indústrias de Electrónica (EIA, Electronic Industries Association) de espaço.

### Notas:

- Caso não tenha um bastidor instalado, instale o mesmo. Para obter mais instruções, consulte [Bastidores e funcionalidades de bastidores](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm) ([http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf\\_9xx\\_kickoff.htm](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm)).
- As classificações de fornecimento de energia são 100 a 127 V ca, 9 A (x2), 200 a 240 V ca, 4,5 A (x2); 50 ou 60 Hz.

2. Avance para [“Concluir o inventário para o sistema”](#) na página 5.

## Concluir o inventário para o sistema

Utilize esta informação para concluir o inventário para o sistema.

## Procedimento

1. Verifique se recebeu todas as caixas que encomendou.
2. Desempacote os componentes do servidor conforme necessário.
3. Conclua um inventário dos componentes e verifique se recebeu todos os componentes que encomendou antes de instalar cada componente do servidor.

### Nota:

As informações de encomenda estão incluídas com o produto. Também pode obter as informações da encomenda pelo representante comercial ou Parceiro de Negócios IBM.

Se existirem componentes incorrectos, em falta ou danificados, contacte uma das seguintes entidades:

- O revendedor IBM.
- A linha de Informação Automática da IBM, Rochester Manufacturing (R-MAIL). Se reside nos E.U.A., marque 1-800-300-8751.
- O [sítio da Web Directório de Contactos Mundiais](http://www.ibm.com/planetwide) (<http://www.ibm.com/planetwide>). Seleccione a sua localização para visualizar as informações de contacto de assistência e suporte.

4. Avance para [“Determinar e marcar a localização no bastidor para o sistema 7063-CR2”](#) na página 5.

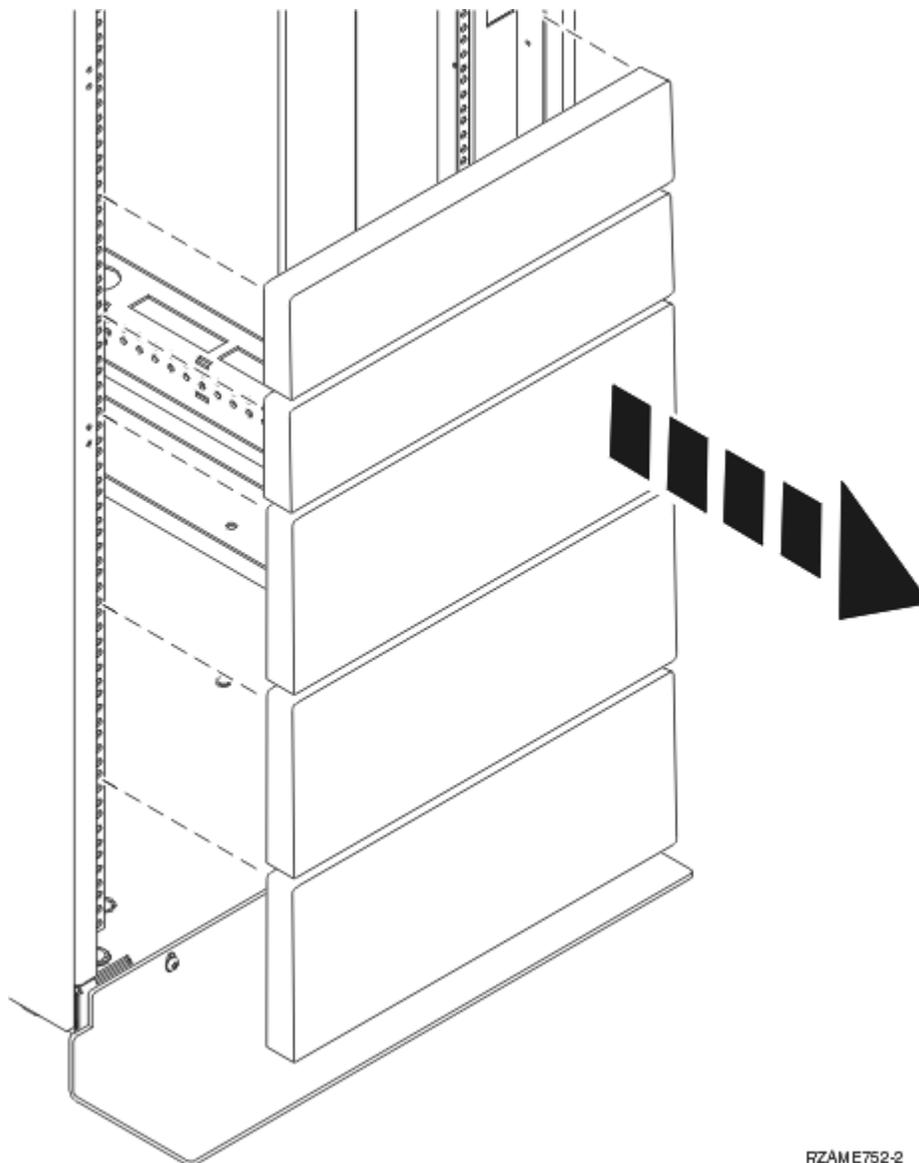
## Determinar e marcar a localização no bastidor para o sistema 7063-CR2

É necessário que determine onde instalar a unidade de sistema no bastidor.

## Procedimento

1. Leia as [Informações sobre a segurança do bastidor](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm) ([http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf\\_racksafety.htm](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm)).
2. Determine onde colocar a unidade de sistema no bastidor. Se planear instalar a unidade de sistema num bastidor, considere a seguinte informação:
  - Organize as unidades maiores e mais pesadas na parte inferior do bastidor.

- Planeie primeiro a instalação das unidades de sistema na parte inferior do bastidor.
  - Registe as localizações de Aliança das Indústrias Electrónicas (EIA, Electronic Industries Alliance) no planeamento.
3. Caso seja necessário, remova os painéis de enchimento para permitir o acesso ao interior da estrutura do bastidor onde planeia colocar a unidade, conforme demonstrado em [Figura 1](#) na [página 6](#).



*Figura 1. Remover os painéis de enchimento*

4. Determine onde colocar o sistema no bastidor. Registe a localização EIA.
5. Voltado de frente para a parte anterior do bastidor e a trabalhar a partir do lado direito, utilize a fita-cola, um marcador ou lápis para marcar o orifício inferior de cada unidade EIA.
6. Repita o passo "5" na [página 6](#) para as posições correspondentes localizadas no lado esquerdo do bastidor.
7. Passe para a parte posterior do bastidor.
8. No lado direito, localize a unidade EIA que corresponde à unidade EIA inferior assinalada na parte anterior do bastidor.
9. Marque a parte inferior da unidade EIA.
10. Assinale os orifícios correspondentes no lado esquerdo do bastidor.

11. Continue com “Fixar as calhas ajustáveis ao chassis do sistema e ao bastidor” na página 7 para fixar as calhas ajustáveis ou continue com “Fixar as calhas fixas ao chassis do sistema e ao bastidor” na página 9 para fixar as calhas fixas.

## Fixar as calhas ajustáveis ao chassis do sistema e ao bastidor

Tem de instalar as calhas no chassis e no bastidor. Utilize este procedimento para executar esta tarefa.

### Sobre esta tarefa



**Atenção:** Para evitar problemas na calha e colocar em risco o utilizador e a unidade, assegure-se de que utiliza as calhas e os encaixes correctos para o bastidor. Se o bastidor tiver orifícios de reforço de suporte quadrados ou orifícios de reforço de suporte de rosca de parafusos, certifique-se de que as calhas e os encaixes correspondem aos orifícios de reforço que são utilizados no bastidor. Não instale hardware não correspondente utilizando anilhas ou espaçadores. Caso não possua as calhas e encaixes correctos para o bastidor, contacte o revendedor IBM.

**Nota:** As unidades 1 EIA nos bastidores são medidas em incrementos verticais de 44,45 mm (1,75 pol.) cada. Cada incremento de 44,45 mm (1,75 pol.) é designado um “EIA.” Nalguns países, o mesmo incremento pode ser designado como “U.”

**Nota:** O sistema requer 1 unidade de bastidor EIA (1U) de espaço.

Assegure-se de que tem os componentes necessários para instalar as calhas. Os seguintes componentes estão incluídos com o Conjunto de Calhas:

- 4 - parafusos Philips 6,35 mm (0,25 pol.)
- 2 - conjuntos de calha de suporte de deslizamento e bastidor
- 2 - suportes de deslizamento de HMC
- 10 - porcas de mola para orifícios de montagem de EIA quadrados
- 10 - porcas de mola para orifícios de montagem de EIA redondos
- 10 - parafusos de bordo sextavado M5

### Procedimento

1. Remova os elementos da calha do pacote e coloque-os numa superfície de trabalho.
2. Identificar o espaço 1U no bastidor da HMC.
3. Para fixar os suportes de deslizamento à HMC, execute as seguintes tarefas:
  - a. Identifique o suporte de deslizamento da direita.
  - b. Alinhe os orifícios no suporte de deslizamento da direita com os pinos do suporte de deslizamento do lado direito da HMC. Certifique-se de que todos os pinos estão alinhados com os orifícios do suporte.
  - c. Empurre o suporte de deslizamento da HMC em direcção à parte de trás da HMC até que fique totalmente encaixado na posição.
  - d. Fixe o suporte de deslizamento da direita ao lado direito da estação de trabalho da HMC através da colocação de dois parafusos Philips de 6,35 mm (0,25 pol.) nos orifícios dos parafusos.
  - e. Repita os passos “3.a” na página 7 a “3.d” na página 7 para instalar o suporte de deslizamento da esquerda ao lado esquerdo da estação de trabalho da HMC.
4. Mova-se para a frente do bastidor.
  - a. No lado esquerdo, instale três porcas de mola nos três orifícios no bordo da frente do bastidor na ranhura 1U que foi designada para a HMC.

**Nota:** O conjunto de calhas inclui porcas de mola para orifícios de bastidor quadrados e redondos. Certifique-se de que utiliza as porcas de mola apropriadas que correspondem aos orifícios no bastidor.

- b. Repita o passo “4.a” na página 7 do lado direito do bastidor.
5. Mova a parte posterior do bastidor.
- a. No lado esquerdo, instale duas porcas de mola nos dois orifícios no bordo da frente do bastidor na ranhura 1U que foi designada para a HMC.
- Nota:** O orifício do meio tem de ficar vazio.
- b. Repita o passo “5.a” na página 8 do lado direito do bastidor.
6. Para instalar as calhas deslizantes da HMC no bastidor, execute os seguintes passos:
- a. Meça a profundidade do bastidor. A profundidade tem de ser entre 558,8 mm (22 pol.) e 863,6 mm (34 pol.).
- b. Coloque as calhas deslizantes da HMC numa superfície plana e localize os parafusos pré-instalados.
- Nota:** As calhas deslizantes têm quatro orifícios para parafusos.
- c. Desaperte os parafusos pré-instalados nas calhas deslizantes o suficiente para que as calhas possam ser movidas para dentro e para fora com facilidade.
- d. Com base na profundidade do bastidor medida no passo “6.a” na página 8, tem de ajustar os parafusos nas calhas.
- i) Se a profundidade do bastidor estiver entre 558,8 mm (22 pol.) e 698,5 mm (27,5 pol.), coloque os parafusos no primeiro e terceiro orifício.
- ii) Se a profundidade do bastidor estiver entre 698,5 mm (27,5 pol.) e 863,6 mm (34 pol.), coloque os parafusos no segundo e quarto orifício.
- Notas:**
- O primeiro orifício é sempre o orifício mais perto da extremidade da calha deslizante. O terceiro e quarto orifício estão localizados perto um do outro.
  - Certifique-se de que os parafusos estão suficientemente desapertados para que o comprimento da calha deslizante possa ser ligeiramente ajustado enquanto esta está a ser instalada no bastidor.
7. Na frente do bastidor, instale as calhas deslizantes da HMC no bastidor, através da execução dos seguintes passos:
- a. Localize o conjunto da calha deslizante da esquerda.
- b. Oriente o conjunto da calha de forma a que a extremidade com o orifício de parafuso mais perto (o primeiro orifício) entre no bastidor primeiro. Certifique-se de que as cabeças dos parafusos estão viradas para o lado de dentro do bastidor. A ranhura aberta do conjunto da calha está mais perto da frente do bastidor.
- c. No lado esquerdo do bastidor, ligue a flange na extremidade da calha deslizante ao bordo da frente do bastidor com dois parafusos M5, deixando o orifício do meio aberto. Certifique-se de que o conjunto da calha fica ligeiramente solto na parte da frente do bastidor para permitir que a HMC seja inserida.
8. Na parte de trás do bastidor, no lado direito, puxe a extremidade livre da calha deslizante em direcção à parte de trás e fixe a flange da calha deslizante ao bastidor com dois parafusos M5, deixando o orifício do meio aberto.
9. Repita o passo “7” na página 8 e o passo “8” na página 8 para instalar o conjunto da calha deslizante da direita no lado direito do bastidor.
10. Na frente do bastidor, instale a estação de trabalho da HMC no bastidor através da execução dos seguintes passos:
- a. Enquanto mantém a estação de trabalho da HMC nivelada, insira os suportes de deslizamento nas calhas deslizantes da HMC que instalou no passo anterior. Empurre a HMC para a frente até que as flanges na frente da HMC estejam niveladas com os orifícios abertos dos parafusos na frente do bastidor.

- b. Fixe a HMC ao lado esquerdo da estrutura com um parafuso M5. Repita este passo do lado direito do bastidor.
11. Avance para [“Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação”](#) na página [10](#).

## Fixar as calhas fixas ao chassis do sistema e ao bastidor

Tem de instalar as calhas no chassis e no bastidor. Utilize este procedimento para executar esta tarefa.

### Sobre esta tarefa



**Atenção:** Para evitar problemas na calha e colocar em risco o utilizador e a unidade, assegure-se de que utiliza as calhas e os encaixes correctos para o bastidor. Se o bastidor tiver orifícios de reforço de suporte quadrados ou orifícios de reforço de suporte de roscas de parafusos, certifique-se de que as calhas e os encaixes correspondem aos orifícios de reforço que são utilizados no bastidor. Não instale hardware não correspondente utilizando anilhas ou spacejadores. Caso não possua as calhas e encaixes correctos para o bastidor, contacte o revendedor IBM.

**Nota:** As unidades 1 EIA nos bastidores são medidas em incrementos verticais de 44,45 mm (1,75 pol.) cada. Cada incremento de 44,45 mm (1,75 pol.) é designado um “EIA.” Nalguns países, o mesmo incremento pode ser designado como “U.”

**Nota:** O sistema requer 1 unidade de bastidor EIA (1U) de espaço.

Assegure-se de que tem os componentes necessários para instalar as calhas. Os seguintes componentes estão incluídos com o Conjunto de Calhas:

- 4 - Parafusos Philips 6,35 mm (0,25 pol.)
- 2 - Calhas interiores
- 2 - Calhas de suporte da HMC
- 2 - Porcas de mola para orifícios de montagem de EIA quadrados
- 2 - Porcas de mola para orifícios de montagem de EIA redondos
- 8 - Parafusos de bordo sextavado M5

### Procedimento

1. Remova os elementos da calha do pacote e coloque-os numa superfície de trabalho.
2. Identificar o espaço 1U no bastidor da HMC.
3. Para fixar as calhas interiores à HMC, execute as seguintes tarefas:
  - a. Identifique a calha interior da direita.
  - b. Alinhe os orifícios na calha interior da direita com os pinos da calha interior localizados no lado direito da HMC. Certifique-se de que todos os pinos estão alinhados com os orifícios da calha interior.
  - c. Empurre a calha interior da HMC em direcção à frente da HMC até que esta encaixe totalmente na respectiva posição.
  - d. Fixe a calha interior da direita ao lado direito da estação de trabalho da HMC através da colocação de dois parafusos Philips de 6,35 mm (0,25 pol.) nos orifícios dos parafusos.
  - e. Repita os passos 3.a a “3.d” na página 9 para instalar a calha interior da esquerda ao lado esquerdo da estação de trabalho da HMC.
4. Mova-se para a frente do bastidor. No lado esquerdo, instale uma porca de mola no orifício no bordo da frente do bastidor na ranhura 1U que foi designada para a HMC.

**Nota:** O conjunto de calhas inclui porcas de mola para orifícios de bastidor quadrados e redondos. Certifique-se de que utiliza as porcas de mola apropriadas que correspondem aos orifícios no bastidor.

5. Mova a parte posterior do bastidor. No lado esquerdo, instale uma porca de mola no orifício do meio no bordo da frente do bastidor na ranhura 1U que foi designada para a HMC.
  6. Na frente do bastidor, instale os suporte de deslizamento da HMC no bastidor, através da execução dos seguintes passos:
    - a. Alinhe os pino das calhas de suporte acima e abaixo da porca de mola que instalou no passo anterior.
    - b. No lado direito do bastidor, fixe a flange na extremidade da calha de suporte ao bordo da frente do bastidor com dois parafusos M5 nos orifícios de parafusos superior e inferior, deixando o orifício do meio aberto. Certifique-se de que o conjunto da calha fica ligeiramente solto na parte da frente do bastidor para permitir que a HMC seja inserida.
  7. Na parte de trás do bastidor, no lado direito, puxe a extremidade livre da calha de suporte em direcção à parte de trás e fixe a flange da calha de suporte ao bastidor com dois parafusos M5, deixando o orifício do meio aberto.
  8. Repita o passo “6” na página 10 e o passo “7” na página 10 para instalar o conjunto da calha deslizante da esquerda no lado esquerdo do bastidor.
  9. Na frente do bastidor, instale a estação de trabalho da HMC no bastidor através da execução dos seguintes passos:
    - a. Enquanto mantém a estação de trabalho da HMC nivelada, insira as calhas interiores nas calhas de suporte da HMC que instalou no passo anterior. Empurre a HMC para a frente até que as flanges na frente da HMC estejam niveladas com os orifícios abertos dos parafusos na frente do bastidor.
    - b. Fixe a HMC ao lado esquerdo da estrutura com um parafuso M5. Repita este passo do lado direito do bastidor.
- Nota:** Se existirem, remova os suportes de transporte cor de laranja que estão ligados à parte de trás do sistema e volte a colocar o parafuso.
10. Avance para “[Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação](#)” na página 10.

## Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação

Instalar o sistema no bastidor e ligar e encaminhas os cabos de alimentação.

### Sobre esta tarefa



**Cuidado:** Este componente ou unidade é pesado mas tem um peso inferior a 18 kg (39,7 lb). Proceda com cuidado ao levantar, remover ou instalar este componente ou unidade. (C008)

### Procedimento

1. Remova a película plástica protectora da parte superior do chassis do sistema.
2. Ligue os cabos de alimentação às fontes de alimentação.

**Nota:** Não ligue a outra extremidade do cabo de alimentação à fonte de alimentação agora.

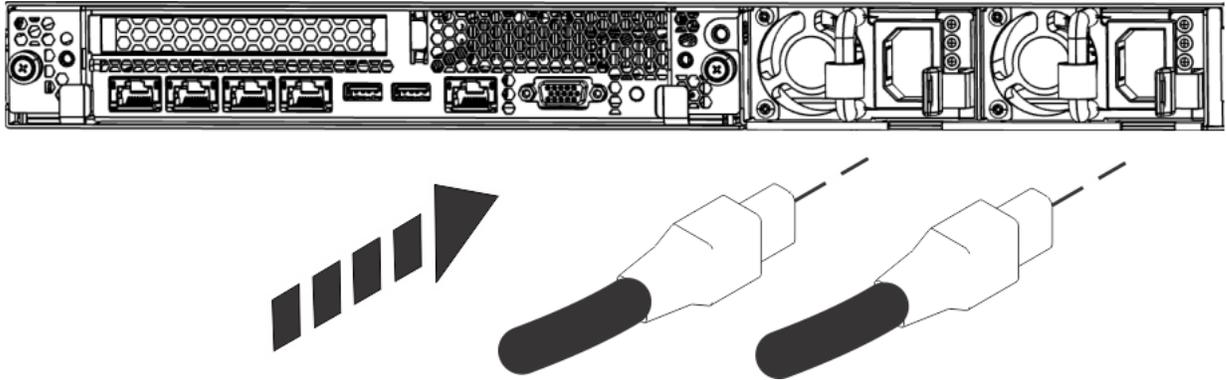


Figura 2. Ligue os cabos de alimentação às fontes de alimentação

3. Aperte os fixadores de velcro para fixar os cabos de alimentação.
4. Avance para [“Ligar a HMC 7063-CR2 instalada em bastidor”](#) na página 11.

## Ligar a HMC 7063-CR2 instalada em bastidor

Saiba como instalar fisicamente a Consola de gestão de hardware (HMC, Hardware Management Console) instalada em bastidor.

### Procedimento

1. Certifique-se de que a HMC está instalada num bastidor e de que os cabos de alimentação estão ligados às fontes de alimentação. Para obter mais informações, consulte [“Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação”](#) na página 10. Após instalar a HMC num bastidor, prossiga com o passo seguinte.
2. Ligue o teclado, o monitor e o rato.

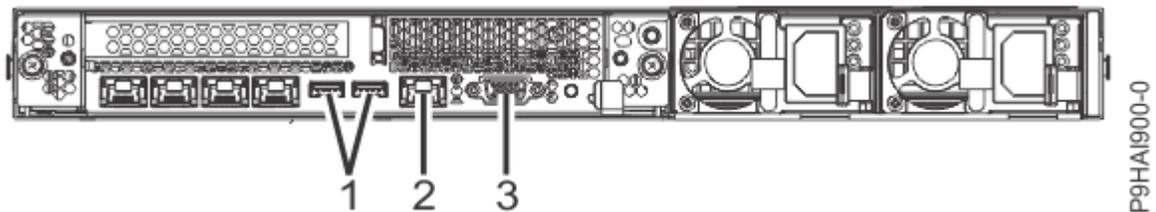


Figura 3. Portas da parte posterior

Identificador	Descrição
1	USB 2.0 utilizada para o teclado e rato
2	Interface de Gestão de Plataformas Inteligente (IPMI, Intelligent Platform Management Interface) da Ethernet
3	Matriz de gráficos de ecrã (VGA, Video Graphics Array) que é utilizada para o monitor. Apenas é suportada a definição 1024 x 768 a 60 Hz VGA. Apenas é suportado até 3 metros de cabo.

**Nota:** O sistema possui duas portas USB frontais que poderá utilizar.

3. Ligue a porta Interface de Gestão de Plataformas Inteligente (IPMI, Intelligent Platform Management Interface) da Ethernet a uma rede.

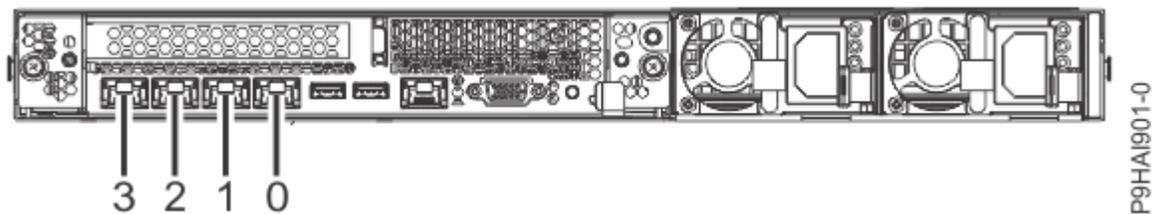


Figura 4. Portas de Ethernet

Identificador	Descrição
0	Ligação de rede de Ethernet de Interface de Gestão de Plataformas Inteligente (IPMI, Intelligent Platform Management Interface) e HMC partilhada
1, 2 e 3	Ligação de rede da HMC

**Nota:** Esta ligação é requerida para aceder ao Controlador de Gestão de Placas de Sistema (BMC, baseboard management controller) na HMC. É requerido acesso ao BMC para tarefas de assistência service e para manter o software proprietário da HMC. Para obter mais informações, consulte [“Tipos de ligações de rede da HMC”](#) na página 53.

**Aviso:** Este produto poderá não estar certificado no seu país para ligações, seja por que meio for, a interfaces de redes de telecomunicações públicas. Poderá ser necessária uma certificação adicional, de acordo com a lei, antes de efectuar algum destes tipos de ligação. Entre em contacto com a IBM para obter mais informações.

4. Ligue o cabo de Ethernet destinado para a ligação ao sistema ou sistemas geridos.

**Notas:**

- Se estiver a utilizar uma ligação partilhada para IPMI e HMC, um único cabo na porta 0 na Figura 2 pode satisfazer ambos os requisitos para IPMI e HMC.
  - Para obter mais informações sobre as ligações de rede da HMC, consulte [“Ligações de rede da HMC”](#) na página 52.
5. Se o sistema gerido já estiver instalado, é possível verificar se a ligação de cabos Ethernet está activa observando as luzes de estado verdes tanto na HMC como nas portas de Ethernet do sistema gerido, à medida que continua a instalação.
  6. Ligue os cabos de alimentação do sistema e os cabo de alimentação de quaisquer outros dispositivos fixados à fonte de alimentação de corrente alternada (AC, alternating current).
  7. Verifique o estado da alimentação através da utilização dos LEDs da fonte de alimentação como indicadores. Para obter mais informações, consulte [LEDs no sistema 7063-CR2](#) no sistema 7063-CR2.
  8. Prima o botão de alimentação para iniciar o sistema. O indicador de alimentação ligada para de estar intermitente e permanece ligado, indicando que a alimentação do sistema está ligada.

**Resultados**

Em seguida, precisará de instalar e configurar o software da HMC. Avance para [“Configurar a HMC 7063-CR2”](#) na página 12.

**Configurar a HMC 7063-CR2**

Saiba como instalar e configurar a Consola de Gestão de Hardware (HMC, Hardware Management Console).

Verifique a versão da HMC que é enviada com a HMC. Para saber como visualizar a versão e edição do código máquina da HMC, consulte [Verifique a versão da HMC que é enviada com a HMC](#). É possível descarregar a versão mais recente da HMC que se encontra disponível a partir do sítio da Web da Fix Central. Utilize o suporte amovível (como um DVD ou USB) para criar um ficheiro ISO passível de arranque do pacote da HMC (imagem ISO).

**Nota:** A seguinte tabela descreve as informações de início de sessão predefinidas para as interfaces da HMC e BMC.

<i>Tabela 6.</i>			
<b>Consola ou Interface</b>	<b>ID Predefinido</b>	<b>Palavra-passe Predefinida</b>	<b>Descrição</b>
BMC (OpenBMC)	root	0penBmc	O ID de utilizador e palavra-passe de root são utilizados para iniciar sessão no BMC pela primeira vez.
HMC	hscroot	abc123	O ID de utilizador e palavra-passe de hscroot são utilizados para iniciar sessão na HMC pela primeira vez. São sensíveis a maiúsculas e minúsculas e apenas podem ser utilizados por um membro da função Super Administrador.
HMC	root	passw0rd	O ID de utilizador e palavra-passe root são utilizados pelo fornecedor de serviços para efectuar procedimentos de manutenção. Não podem ser utilizados para iniciar sessão na HMC.

**Nota:** As seguintes instalações são apresentadas como exemplos.

### **Instalar a HMC ao utilizar a unidade USB**

Para instalar a HMC ao utilizar a unidade USB, conclua os seguintes passos para sistemas Linux®:

**Nota:** Para obter exemplos em diferentes sistemas operativos, consulte:

- Windows: [Suporte de instalação flash USB \(Windows\)](#)
- Mac: [Suporte de instalação flash USB \(macOS\)](#)

1. Descarregue a versão da HMC que pretende no sítio da Web Fix Central.
2. Execute o seguinte comando: **dd bs=4M if=/path/to/HMC\_ISO\_FILE.iso of=/dev/sdx status=progress && sync** (onde **sdx** é o nome da unidade USB).

**Nota:** É possível executar o comando `lsblk` do Linux para determinar o nome do dispositivo da unidade USB quando esta está ligada.

3. Insira a unidade USB e ligue o sistema.

**Nota:** A unidade USB tem de ter pelo menos 8 GB. Certas unidades USB podem ser demasiado largas para encaixar devidamente na porta USB na parte posterior do sistema. Teste o ajuste da unidade USB antes de prosseguir.

4. Quando o menu Petitboot é apresentado, seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **USB**.

## Instalar a HMC através de suportes virtuais a partir da BMC

Para instalar a HMC através de suporte virtual a partir da BMC, execute os seguintes passos:

1. Abra um navegador da web suportado. Na barra de endereço, introduza o endereço de IP da BMC à qual se pretende ligar. Por exemplo, pode utilizar o formato `https://<IP da BMC>` na barra de endereço do navegador da Web.
2. A partir da janela de **Início de sessão OpenBMC**, introduza o endereço do **Sistema** da BMC e o **Nome de utilizador** e **Palavra-passe** que lhe foram atribuídos.

**Nota:** O ID de utilizador predefinido é `root` e a palavra-passe predefinida é `OpenBmc`.

Se estiver a utilizar o nível de software proprietário OP940.01, ou posterior, a palavra-passe de root está expirada por predefinição. Tem de alterar a palavra-passe predefinida antes de poder aceder à BMC. Para obter mais informações sobre como alterar a palavra-passe predefinida expirada, consulte [Definir a palavra-passe](#).

Se se tiver esquecido da sua palavra-passe, pode executar uma reposição de fábrica do sistema para restaurar a palavra-passe predefinida. Para repor o sistema, consulte [Executar uma reposição de fábrica](#).

3. Clique em **Iniciar sessão**.
4. Seleccione **Controlo de servidor**.
5. Seleccione **Suporte virtual**.
6. Clique em **Escolher ficheiro**.
7. Localize o ISO do suporte de Recuperação da HMC e clique em **Abrir**.
8. Clique em **Iniciar**.
9. Ligue o sistema.
10. Quando o menu Petitboot é apresentado, seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **USB**.

## Instalar a HMC através da utilização de uma unidade de DVD ligada através de USB

Para instalar a HMC através da utilização de uma unidade de DVD ligada através de USB, conclua os seguintes passos:

1. Descarregue a versão de recuperação da HMC que pretende a partir do sítio da Web [Fix Central](#).
2. Grave a imagem do DVD de recuperação da HMC para um suporte DVD-R DL como uma imagem.
3. Desligue a HMC.
4. Ligue a unidade de DVD USB externa à HMC e insira o DVD de recuperação da HMC.

**Nota:** Poderá ser necessário ligar a unidade de DVD USB a uma fonte de alimentação externa ou utilizar um cabo USB Y para ligar a uma porta USB adicional para facultar alimentação suficiente à unidade de DVD.

5. Ligue a HMC.

**Nota:** O monitor de apresentação poderá não mostrar qualquer sinal durante o arranque. O processo poderá demorar 2 ou 3 minutos antes de o monitor de apresentação mostrar qualquer estado.

6. Quando o Petitboot bootloader iniciar, navegue para parar o arranque automático.

**Nota:** É imposto um tempo de espera de 10 segundos. Caso não seja efectuada qualquer acção dentro de 10 segundos, o sistema tenta arrancar a partir da unidade de disco rígido.

7. Aguarde até que o dispositivo de **CD/DVD** surja no menu Petitboot.

**Nota:** Este processo poderá demorar até um minuto.

8. Seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **CD/DVD**.

## Instalar a 7063-CR1 num bastidor

Saiba como instalar a Consola de Gestão de Hardware (HMC, Hardware Management Console) 7063-CR1 num bastidor.

Poderá visualizar a documentação de instalação online ou poderá imprimir a versão PDF das mesmas informações. Para visualizar ou imprimir a versão PDF, consulte [Instalar e configurar a Consola de Gestão de Hardware](#).

### Pré-requisitos para instalar o sistema 7063-CR1 instalada em bastidor

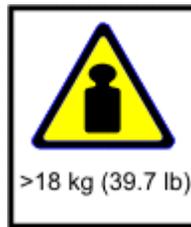
Utilize a informação para compreender os pré-requisitos que são requeridos para instalar o sistema.

#### Sobre esta tarefa



**Cuidado:**

ou



ou



O peso deste componente ou unidade situa-se entre 18 e 32 kg (39,7 e 70,5 lb). São necessárias duas pessoas para levantar com segurança este componente ou unidade. (C009)

Poderá precisar de ler os seguintes documentos antes de iniciar a instalação do servidor:

- A versão mais recente deste documento é mantida online, consulte [Instalar o 7063-CR1 num bastidor](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm) ([http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai\\_install7063\\_kickoff.htm](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm)).
- Para planear a instalação do servidor, consulte [Planeamento das instalações e do hardware](#).

### Procedimento

Certifique-se de que tem os seguintes itens antes de iniciar a instalação:

- Chave de parafusos Phillips tamanho 2
- Chave de fendas de cabeça plana
- X-acto
- Fita de pulso de descarga electrostática (ESD, Electrostatic discharge)
- Bastidor com uma unidade (1U) de Associação das Indústrias de Electrónica (EIA, Electronic Industries Association) de espaço.

**Nota:** Caso não tenha um bastidor instalado, instale o mesmo. Para obter mais instruções, consulte [Bastidores e funcionalidades de bastidores](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm) ([http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf\\_9xx\\_kickoff.htm](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm)).

### Concluir o inventário para o sistema

Utilize esta informação para concluir o inventário para o sistema.

## Procedimento

1. Verifique se recebeu todas as caixas que encomendou.
2. Desempacote os componentes do servidor conforme necessário.
3. Conclua um inventário dos componentes e verifique se recebeu todos os componentes que encomendou antes de instalar cada componente do servidor.

### Nota:

As informações de encomenda estão incluídas com o produto. Também pode obter as informações da encomenda pelo representante comercial ou Parceiro de Negócios IBM.

Se existirem componentes incorrectos, em falta ou danificados, contacte uma das seguintes entidades:

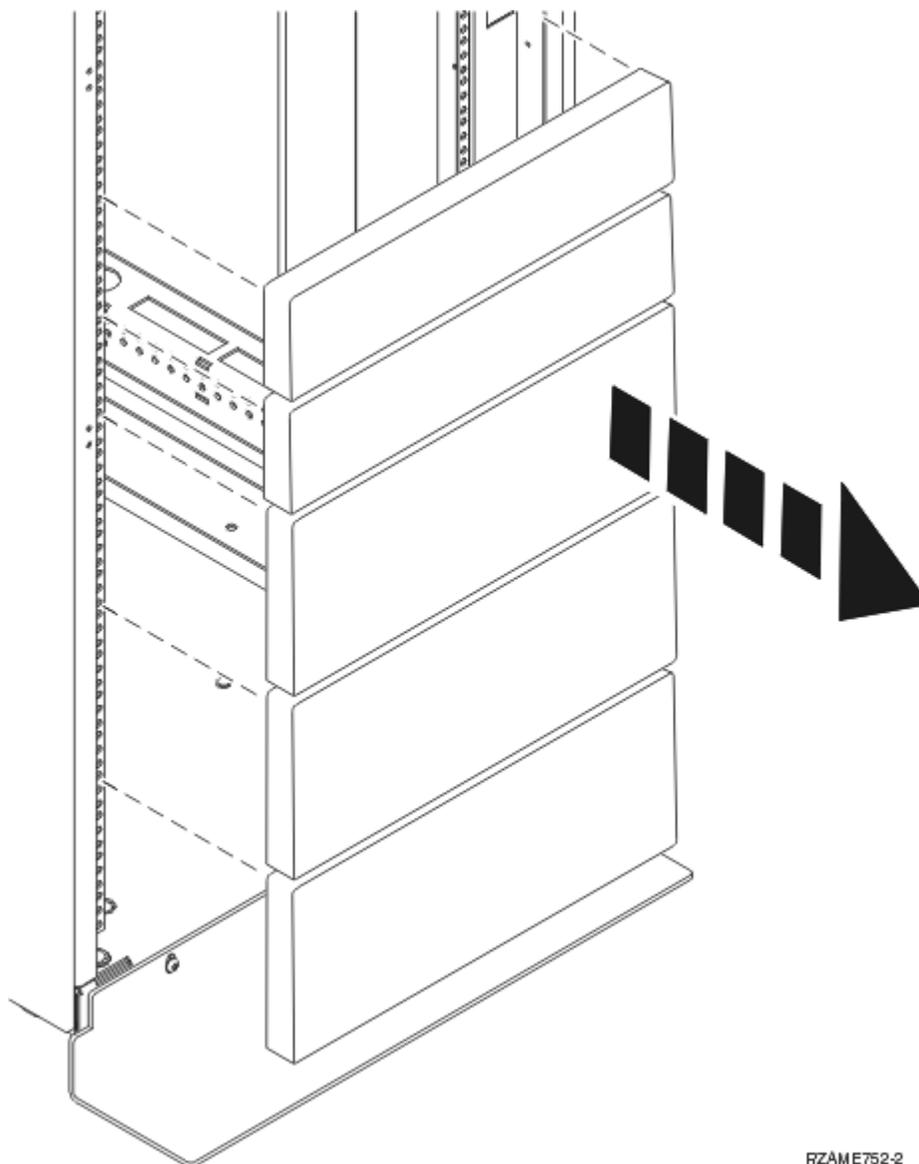
- O revendedor IBM.
- A linha de Informação Automática da IBM, Rochester Manufacturing (R-MAIL). Se reside nos E.U.A., marque 1-800-300-8751.
- O [sítio da Web Directório de Contactos Mundiais](http://www.ibm.com/planetwide) (<http://www.ibm.com/planetwide>). Seleccione a sua localização para visualizar as informações de contacto de assistência e suporte.

## Determinar e marcar a localização no bastidor para o sistema 7063-CR1

Poderá ser necessário determinar onde instalar a unidade de sistema no bastidor.

## Procedimento

1. Leia as [Informações sobre a segurança do bastidor](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm) ([http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf\\_racksafety.htm](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm)).
2. Determine onde colocar a unidade de sistema no bastidor. Se planejar instalar a unidade de sistema num bastidor, considere a seguinte informação:
  - Organize as unidades maiores e mais pesadas na parte inferior do bastidor.
  - Planeie primeiro a instalação das unidades de sistema na parte inferior do bastidor.
  - Registe as localizações de Aliança das Indústrias Electrónicas (EIA, Electronic Industries Alliance) no planeamento.
3. Caso seja necessário, remova os painéis de enchimento para permitir o acesso ao interior da estrutura do bastidor onde planeia colocar a unidade, conforme demonstrado em [Figura 5 na página 17](#).



RZAME752-2

*Figura 5. Remover os painéis de enchimento*

4. Determinar para colocar o sistema no bastidor. Registe a localização EIA.
5. Voltado de frente para a parte anterior do bastidor e a trabalhar a partir do lado direito, utilize a fita-cola, um marcador ou lápis para marcar o orifício inferior de cada unidade EIA.
6. Repita o passo “5” na página 17 para as posições correspondentes localizadas no lado esquerdo do bastidor.
7. Passe para a parte posterior do bastidor.
8. No lado direito, localize a unidade EIA que corresponde à unidade EIA inferior assinalada na parte anterior do bastidor.
9. Marque a parte inferior da unidade EIA.
10. Assinale os orifícios correspondentes no lado esquerdo do bastidor.

### **Fixar as calhas fixas ao chassis do sistema e ao bastidor**

Tem de instalar as calhas no chassis e no bastidor. Utilize este procedimento para executar esta tarefa.

## Sobre esta tarefa



**Atenção:** Para evitar problemas na calha e colocar em risco o utilizador e a unidade, assegure-se de que utiliza as calhas e os encaixes correctos para o bastidor. Se o bastidor tiver orifícios de reforço de suporte quadrados ou orifícios de reforço de suporte de roscas de parafusos, certifique-se de que as calhas e os encaixes correspondem aos orifícios de reforço que são utilizados no bastidor. Não instale hardware não correspondente utilizando anilhas ou espacejadores. Caso não possua as calhas e encaixes correctos para o bastidor, contacte o revendedor IBM.

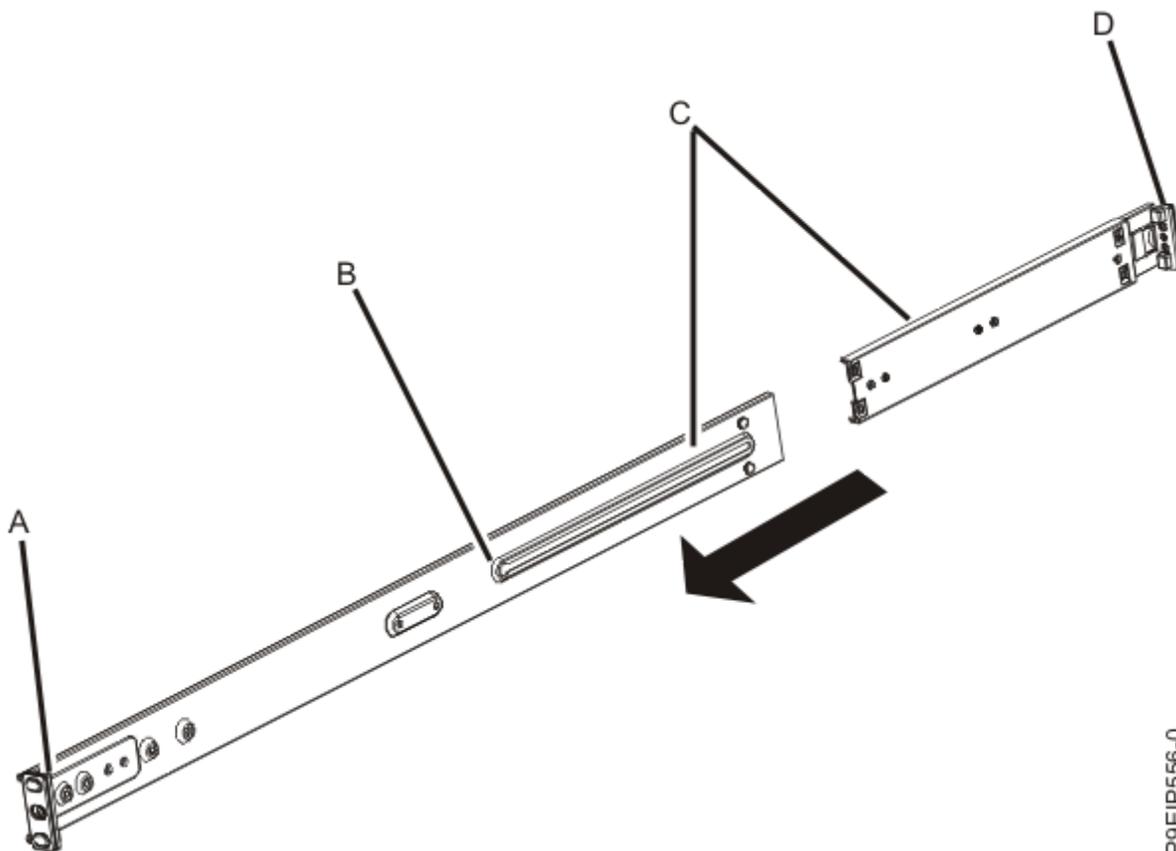
**Nota:** O sistema requer 1 unidade de bastidor EIA (1U) de espaço.

Assegure-se de que tem os componentes necessários para instalar as calhas. Os seguintes componentes estão incluídos com o Conjunto de Calhas:

- Parafusos de calhas deslizantes, utilizados para fixar os dois componentes de cada calha deslizante
- Parafusos do bastidor da calha deslizante, utilizados para fixar as calhas ao bastidor
- Calhas
- Parafusos de 10 - 32 x 0.635 cm (0.25 pol.), utilizados para fixar as calhas ao chassis do sistema

## Procedimento

1. Remova os elementos da calha do pacote e coloque-os numa superfície de trabalho.
2. Substitua os pinos quadrados do bastidor da calha (A) e (D) pelos pinos redondos do bastidor da calha.
3. Ligue os dois componentes a cada calha deslizante do bastidor. Para ligar os dois componentes da calha deslizante do bastidor, execute as seguintes tarefas:
  - a. Identifique os dois componentes da calha deslizante esquerda do bastidor. Alinhe os componentes pequeno e longo (C). Assegure-se de que os pinos da calha do bastidor estão a apontar na mesma direcção (A) e (D).



P9EIP556-0

- b. A parte mais pequena da calha deslizante do bastidor tem um pino de metal. Insira o pino no orifício na parte mais pequena da calha deslizante do bastidor (**B**). Deslize a parte mais curta da calha do bastidor na parte mais comprida da calha do bastidor.
- c. Alinhe os orifícios das duas partes das calhas deslizantes do bastidor. Com uma chave de parafusos de cabeça Philips, fixe as duas partes ao apertar levemente dois parafusos de calha de roscas através dos orifícios na calha deslizante do bastidor.

**Nota:** Não aperte os parafusos da calha deslizante do fixar.

- d. Repita estes passos para a calha deslizante direita.
4. Instale as calhas deslizantes do bastidor no bastidor.
- a. Mova-se para a frente do bastidor.
  - b. Seleccione a calha deslizante esquerda do bastidor e localize a unidade EIA que marcou anteriormente. Cada calha deslizante também é marcada **Posterior (Back)**, para designar a parte posterior do bastidor. Assegure-se de que está a suportar a parte anterior da calha deslizante do bastidor.
  - c. Expanda a calha da parte anterior do bastidor para a parte posterior e alinhe os pinos da calha deslizante do bastidor com os orifícios no bordo do bastidor que marcou anteriormente.
  - d. Empurre os pinos da calha do bastidor para o bordo do bastidor posterior até que o trinco da calha do bastidor da parte posterior se encaixe.
  - e. Puxe a parte anterior da calha do bastidor para a parte anterior do bordo da calha do bastidor. Alinhe os pinos da calha deslizante com os orifícios no bordo da calha e puxe-os até o fecho da calha se encaixar.
  - f. Utilize uma chave de fendas para apertar os parafusos da calha que instalou no passo 2.
- Nota:** Poderá necessitar de 2U de espaço para aceder e apertar os parafusos da calha.
- g. Repita os passos 4a a 4f para a calha deslizante da direita.

## Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação

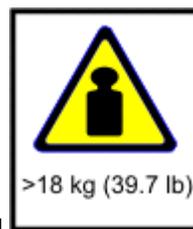
Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação.

### Sobre esta tarefa



**Cuidado:**

ou



ou



O peso deste componente ou unidade situa-se entre 18 e 32 kg (39,7 e 70,5 lb). São necessárias duas pessoas para levantar com segurança este componente ou unidade. (C009)

### Procedimento

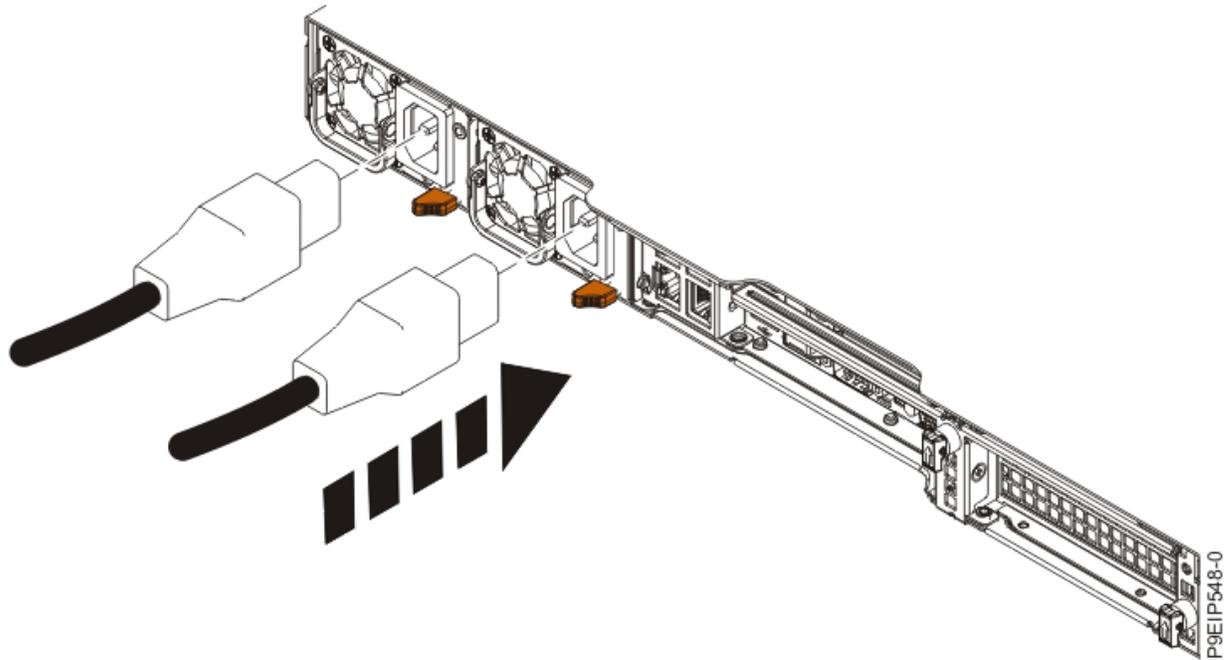
1. Remova a película plástica protectora da parte superior do chassis do sistema.
2. Mova-se para a frente do bastidor.
3. Recorrendo a duas pessoas, uma de cada lado do sistema, levante o sistema e alinhe as calhas do chassis do sistema em cada lado do chassis com as calhas deslizantes do bastidor.
4. Empurre devagar o sistema na direcção da parte posterior do bastidor.

5. Prenda o sistema ao bastidor ao apertar um parafuso com uma anilha através das pegas em cada lado do chassis do sistema.

**Nota:** É necessário utilizar anilhas com os parafusos. Deslize uma anilha para cada um dos dois parafusos mais longos (1.5 cm (0.59 pol.)) incluídos com o conjunto de calhas. Aperte o parafuso com a anilha através do lado direito e esquerdo do sistema na parte anterior.

6. Ligue os cabos de alimentação às fontes de alimentação.

**Nota:** Não ligue a outra extremidade do cabo de alimentação à fonte de alimentação agora.



*Figura 6. Ligue os cabos de alimentação às fontes de alimentação*

7. Avance para [“Ligar a HMC 7063-CR1 instalada em bastidor”](#) na página 20.

## Ligar a HMC 7063-CR1 instalada em bastidor

Saiba como instalar fisicamente a Consola de gestão de hardware (HMC, Hardware Management Console) instalada em bastidor.

### Procedimento

1. Certifique-se de que a HMC está instalada num bastidor e de que os cabos de alimentação estão ligados às fontes de alimentação. Para obter mais informações, consulte o tópico [“Instalar o sistema no bastidor e ligar e encaminhar os cabos de alimentação”](#) na página 19. Após instalar a HMC num bastidor, prossiga com o passo seguinte.

**Nota:** Se uma ficha estiver a cobrir uma porta na parte de trás do sistema, remova-a e elimine-a. As coberturas das portas asseguram que não se esquece de que tem que repor a palavra-passe de administrador no seu sistema gerido após o IPL inicial do sistema.

2. Ligue o teclado, o monitor e o rato.

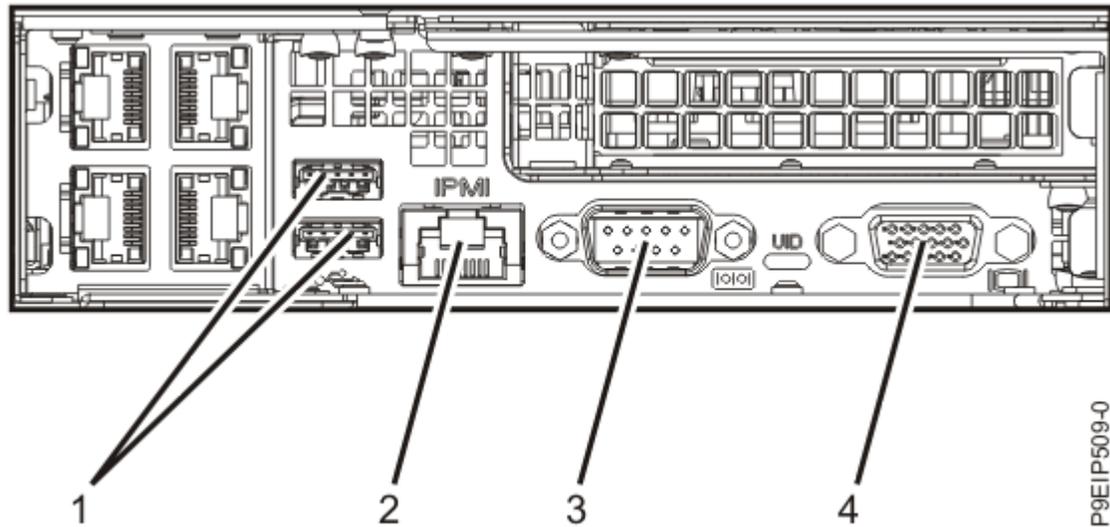


Figura 7. Portas da parte posterior

Tabela 7. Portas de entrada e de saída

Identificador	Descrição
1	USB 2.0 utilizada para o teclado e rato
2	Interface de Gestão de Plataformas Inteligente (IPMI, Intelligent Platform Management Interface) da Ethernet
3	IPMI em série
4	Matriz de gráficos de ecrã (VGA, Video Graphics Array) que é utilizada para o monitor. Apenas é suportada a definição 1024 x 768 a 60 Hz VGA. Apenas é suportado até 3 metros de cabo.

**Nota:** O sistema possui duas portas USB frontais que poderá utilizar. A porta série frontal não é funcional.

3. Ligue o cabo de Ethernet destinado para a ligação ao sistema ou sistemas geridos.

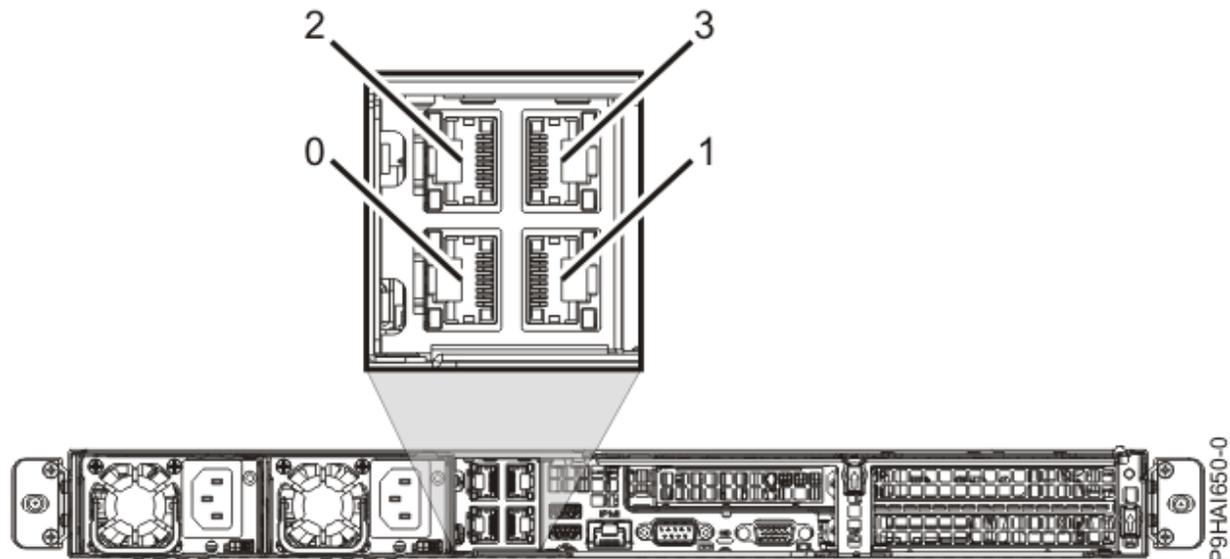


Figura 8. Portas de Ethernet

**Nota:** Para obter mais informações sobre as ligações de rede da HMC, consulte [“Ligações de rede da HMC”](#) na página 52.

4. Se o sistema gerido já estiver instalado, é possível verificar se a ligação de cabos Ethernet está activa observando as luzes de estado verdes tanto na HMC como nas portas de Ethernet do sistema gerido, à medida que continua a instalação.
5. Ligue a porta Interface de Gestão de Plataformas Inteligente (IPMI, Intelligent Platform Management Interface) da Ethernet a uma rede.

**Nota:** Esta ligação é requerida para aceder ao Controlador de Gestão de Placas de Sistema (BMC, baseboard management controller) na HMC. É requerido acesso ao BMC para tarefas de assistência service e para manter o software proprietário da HMC. Para obter mais informações, consulte [“Tipos de ligações de rede da HMC”](#) na página 53.

6. Ligue os cabos de alimentação do sistema e os cabo de alimentação de quaisquer outros dispositivos fixados à fonte de alimentação de corrente alternada (AC, alternating current).
7. Verifique o estado da alimentação através da utilização dos LEDs da fonte de alimentação como indicadores. Para obter mais informações, consulte [LEDs no sistema 7063-CR1](#) LEDs no sistema 7063-CR1.

## Resultados

Em seguida, precisará de instalar e configurar o software da HMC. Avance para [“Configurar a HMC 7063-CR1”](#) na página 22.

## Configurar a HMC 7063-CR1

Saiba como instalar e configurar a Consola de Gestão de Hardware (HMC, Hardware Management Console).

Verifique a versão da HMC que é enviada com a HMC. É possível descarregar a versão mais recente da HMC que se encontra disponível a partir do sítio da Web da [Fix Central](#). Utilize o suporte amovível (como um DVD ou USB) para criar um ficheiro ISO passível de arranque do pacote da HMC (imagem ISO).

**Nota:** A seguinte tabela descreve as informações de início de sessão predefinidas para as interfaces da HMC e BMC.

Consola ou Interface	ID Predefinido	Palavra-passe Predefinida	Descrição
BMC	ADMIN	ADMIN	O ID de utilizador e palavra-passe de ADMIN são utilizados para iniciar sessão no BMC pela primeira vez.
HMC	hscroot	abc123	O ID de utilizador e palavra-passe de hscroot são utilizados para iniciar sessão na HMC pela primeira vez. São sensíveis a maiúsculas e minúsculas e apenas podem ser utilizados por um membro da função Super Administrador.

Tabela 8. (continuação)

Consola ou Interface	ID Predefinido	Palavra-passe Predefinida	Descrição
HMC	root	passwd	O ID de utilizador e palavra-passe root são utilizados pelo fornecedor de serviços para efectuar procedimentos de manutenção. Não podem ser utilizados para iniciar sessão na HMC.

**Nota:** As seguintes instalações são apresentadas como exemplos.

### Instalar a HMC ao utilizar a unidade USB

Para instalar a HMC ao utilizar a unidade USB, conclua os seguintes passos para sistemas Linux:

**Nota:** Para obter exemplos em diferentes sistemas operativos, consulte:

- Windows: [Suporte de instalação flash USB \(Windows\)](#)
- Mac: [Suporte de instalação flash USB \(macOS\)](#)

1. Descarregue a versão da HMC que pretende no sítio da [Web Fix Central](#).
2. Execute o seguinte comando: `dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync` (onde `sdx` é o nome da unidade USB).

**Nota:** É possível executar o comando `lsblk` do Linux para determinar o nome do dispositivo da unidade USB quando esta está ligada.

3. Insira a unidade USB e ligue o sistema.

**Nota:** A unidade USB tem de ter pelo menos 4 GB. Certas unidades USB podem ser demasiado largas para encaixar devidamente na porta USB na parte posterior do sistema. Teste o ajuste da unidade USB antes de prosseguir.

4. Quando o menu Petitboot é apresentado, seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **USB**.

### Instalar a HMC ao utilizar suportes remotos a partir das vistas da consola

Para instalar a HMC ao utilizar suportes remotos a partir das vistas da consola, conclua os seguintes passos:

1. Inicie sessão na interface da Web BMC (<http://<bmc-ip>>).
2. Seleccione **Controlo remoto (Remote Control)**.
3. Seleccione **Redireccionamento da consola (Console Redirection)**.
4. Faça clique em **Iniciar consola (Launch Console)**.
5. No visualizador iKVM Java™, seleccione **Suporte Virtual (Virtual Media) > Memória Virtual (Virtual Storage)**.
6. Sob **Tipo de unidade lógica (Logical Drive Type)**, seleccione **Ficheiro ISO (ISO File)**.
7. Faça clique em **Abrir imagem (Open Image)** e localize o ficheiro ISO no sistema.
8. Prima **Suplemento (Plugin)** para instalar o ficheiro ISO.
9. Ligue o sistema.

10. Quando o menu Petitboot é apresentado, seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **CD/DVD**.

## Instalar a HMC através da utilização de uma unidade de DVD ligada através de USB

Para instalar a HMC através da utilização de uma unidade de DVD ligada através de USB, conclua os seguintes passos:

1. Descarregue a versão de recuperação da HMC que pretende a partir do sítio da Web [Fix Central](#).
2. Grave a imagem do DVD da recuperação da HMC para um suporte DVD-R como uma imagem. Em alternativa, é possível encomendar o suporte de recuperação em DVD.
3. Desligue a HMC.
4. Ligue a unidade de DVD USB externa à HMC e insira o DVD de recuperação da HMC.

**Nota:** Poderá ser necessário ligar a unidade de DVD USB a uma fonte de alimentação externa ou utilizar um cabo USB Y para ligar a uma porta USB adicional para facultar alimentação suficiente à unidade de DVD.

5. Ligue a HMC.

**Nota:** O monitor de apresentação poderá não mostrar qualquer sinal durante o arranque. O processo poderá demorar 2 ou 3 minutos antes de o monitor de apresentação mostrar qualquer estado.

6. Quando o Petitboot bootloader iniciar, navegue para parar o arranque automático.

**Nota:** É imposto um tempo de espera de 10 segundos. Caso não seja efectuada qualquer acção dentro de 10 segundos, o sistema tenta arrancar a partir da unidade de disco rígido.

7. Aguarde até que o dispositivo de **CD/DVD** surja no menu Petitboot.

**Nota:** Este processo poderá demorar até um minuto.

8. Seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **CD/DVD**.

## Instalar a HMC através da utilização de suportes remotos alojados por um servidor de ficheiros SMB

Para instalar a HMC através da utilização de suportes remotos alojados por um servidor de ficheiros de Bloco de Mensagens de Servidor (SMB, Server Message Block), conclua os seguintes passos:

1. Copie o ficheiro ISO de recuperação para um sistema central de partilha no servidor de ficheiros em conformidade com SMB.

**Nota:** Bloco de Mensagens de Servidor versão 3 (SMBv3, Server Message Block version 3) não é suportado.

2. Inicie sessão na interface da Web BMC (<http://<bmc-ip>>).
3. Seleccione **Suporte virtual**.
4. Seleccione **Imagem de CD-ROM (CD-ROM Image)**.
5. Conclua as seguintes informações:

### Sistema central de partilha

O IP do sistema central SMB. Se estiver a utilizar o nome do domínio, assegure-se de que o sistema de nomes de domínio (DNS, domain name system) no BMC está configurado correctamente.

### Caminho para a imagem

O caminho SMB para o sistema. Por exemplo: `/<share name>/<rest of path>/<name of iso>.iso`

### Utilizador (opcional)

O nome de utilizador que é utilizado para iniciar sessão no sistema central SMB.

### Palavra-passe (opcional)

A palavra-passe do utilizador.

6. Faça clique em **Guardar (Save)**.
7. Faça clique em **Montar (Mount)**.
8. O dispositivo 1 mostra agora a seguinte mensagem: **Há um ficheiro ISO instalado (There is an iso file mounted.)**

**Nota:** Caso a mensagem não seja apresentada, volte a verificar as informações e repita os passos 6 - 8.

9. Ligue o sistema.
10. Quando o menu Petitboot é apresentado, seleccione a opção **Instalar Consola de Gestão de Hardware (Install Hardware Management Console)** que se encontra localizada sob **CD/DVD**.

## Opcional: Actualizar o nível de software proprietário da Consola de gestão de hardware (HMC) através da chave de armazenamento USB incluída

**Nota:** Se a configuração incluiu uma actualização de software proprietário da HMC numa chave de memória USB, execute os seguintes passos para actualizar o nível de software proprietário da HMC.

Para actualizar o nível de software proprietário da HMC através da chave de armazenamento USB, execute os seguintes passos:

1. Insira a unidade de chave de armazenamento USB na porta USB localizada na parte posterior do sistema.
2. Ligue o sistema e inicie sessão na HMC.

3. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, seleccione **Gestão da Consola**.
4. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.
5. Siga as instruções no ecrã no assistente Instalar Serviço Correctivo da HMC (Install HMC Corrective Service).

Em seguida, necessita de configurar o software da HMC. Para obter instruções, consulte [“Configurar a HMC” na página 52](#).

### Conceitos relacionados

[Configurar a conectividade do BMC](#)

Pode configurar ou visualizar as definições de rede no BMC para a consola de gestão.

## Instalar a HMC 7042-CR9 num bastidor

Saiba como instalar a Consola de Gestão de Hardware (HMC, Hardware Management Console) 7042-CR9 num bastidor.

### Antes de começar

#### Nota:

A Consola de Gestão de Hardware (Hardware Management Console) Versão 9.2.950 ou posterior não é suportada na HMC 7042-CR9. Para obter mais informações sobre as versões da HMC para a sua HMC 7042-CR9, consulte as notas de edição que se encontram disponíveis no sítio da [Web Central de Correções \(Fix Central\)](#).

Preencha um inventário de componentes. As ilustrações seguintes mostram os itens de que necessita para instalar o servidor no armário do bastidor. Caso faltem itens ou estejam danificados, contacte o local de compra.

#### Conteúdo da caixa do Braço de gestão de cabos

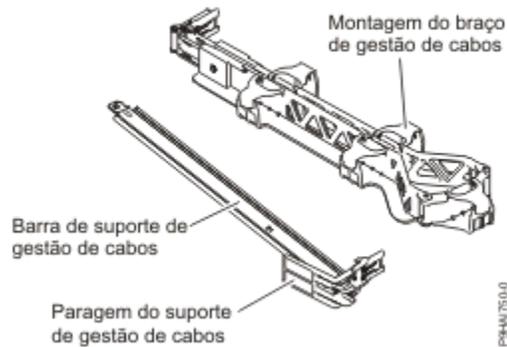


Figura 9. Conteúdos da caixa do braço de gestão de cabos

#### Conteúdo da caixa das calhas

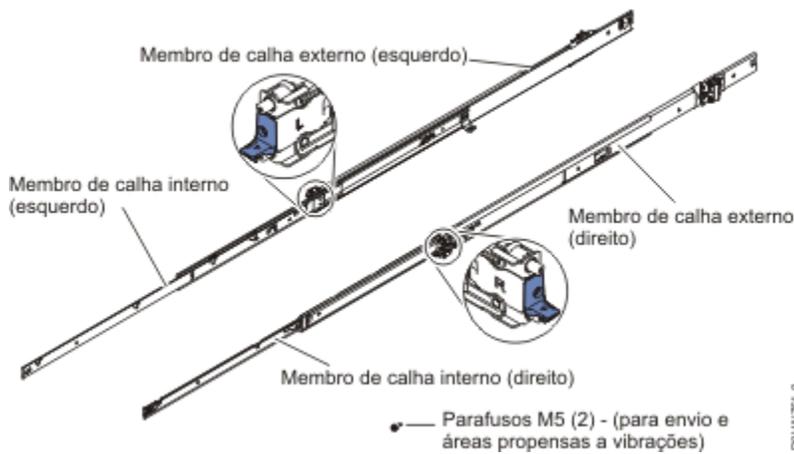


Figura 10. Conteúdos da caixa das calhas

**Nota:** Precisa da caixa da calha deslizante e da caixa do braço de gestão de cabos para esta instalação.

### Sobre esta tarefa

Para instalar uma HMC 7042-CR9 num bastidor, conclua os seguintes passos:

### Procedimento

1. Seleccione um espaço disponível (dependendo do servidor que está a instalar) no bastidor para instalar o servidor.

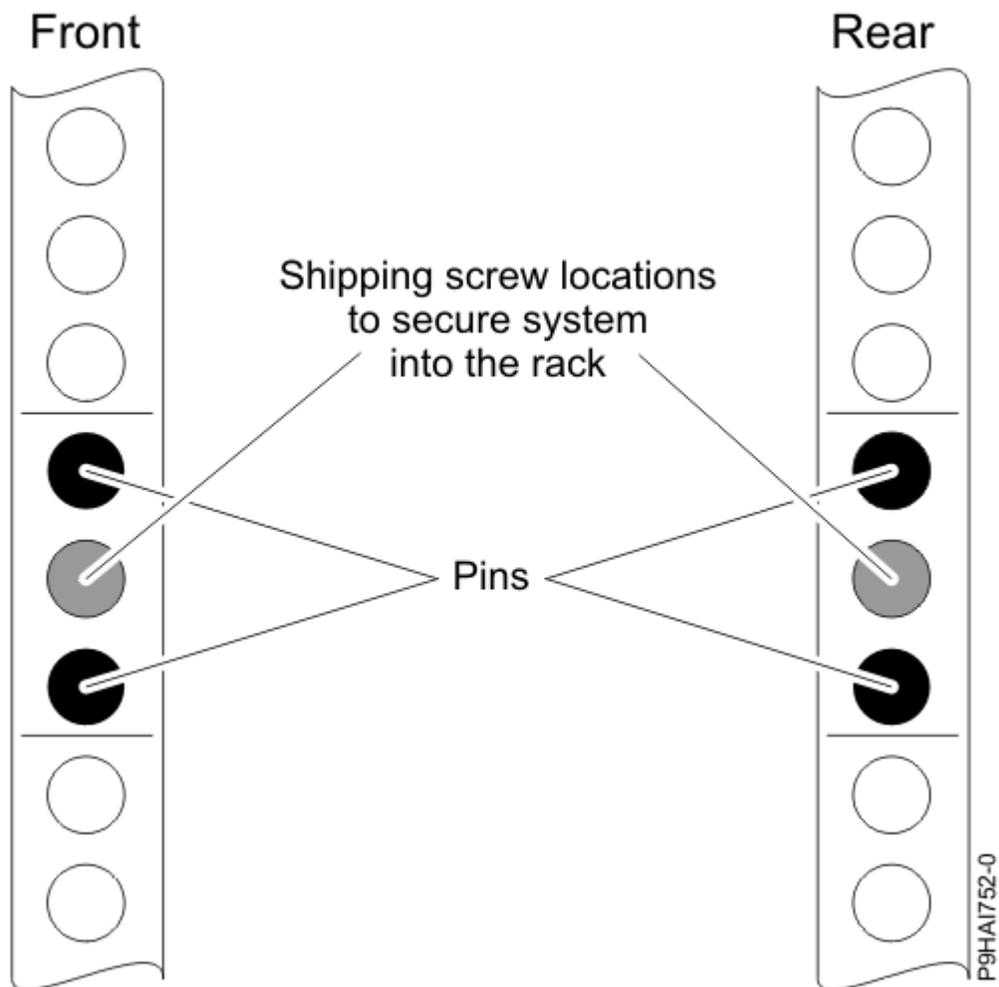


Figura 11. Identificar um espaço de bastidor

**Nota:** Necessita de uma unidade (1 U) de espaço e as calhas deslizantes estão instaladas na unidade (U) inferior da uma unidade de espaço.

2. Expanda o membro da calha exterior completamente até à parte posterior até ouvir um clique audível. O suporte de montagem em bastidor posterior está agora rodada na posição de desbloqueio.

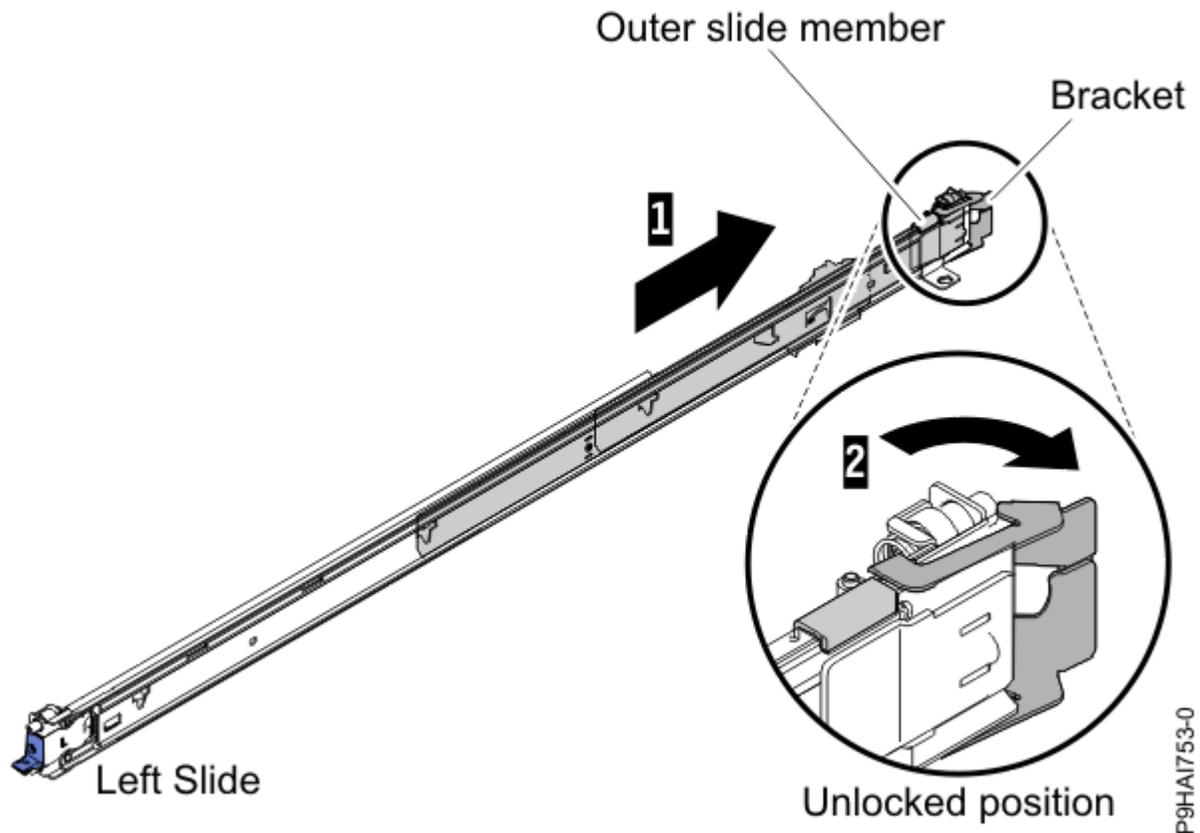
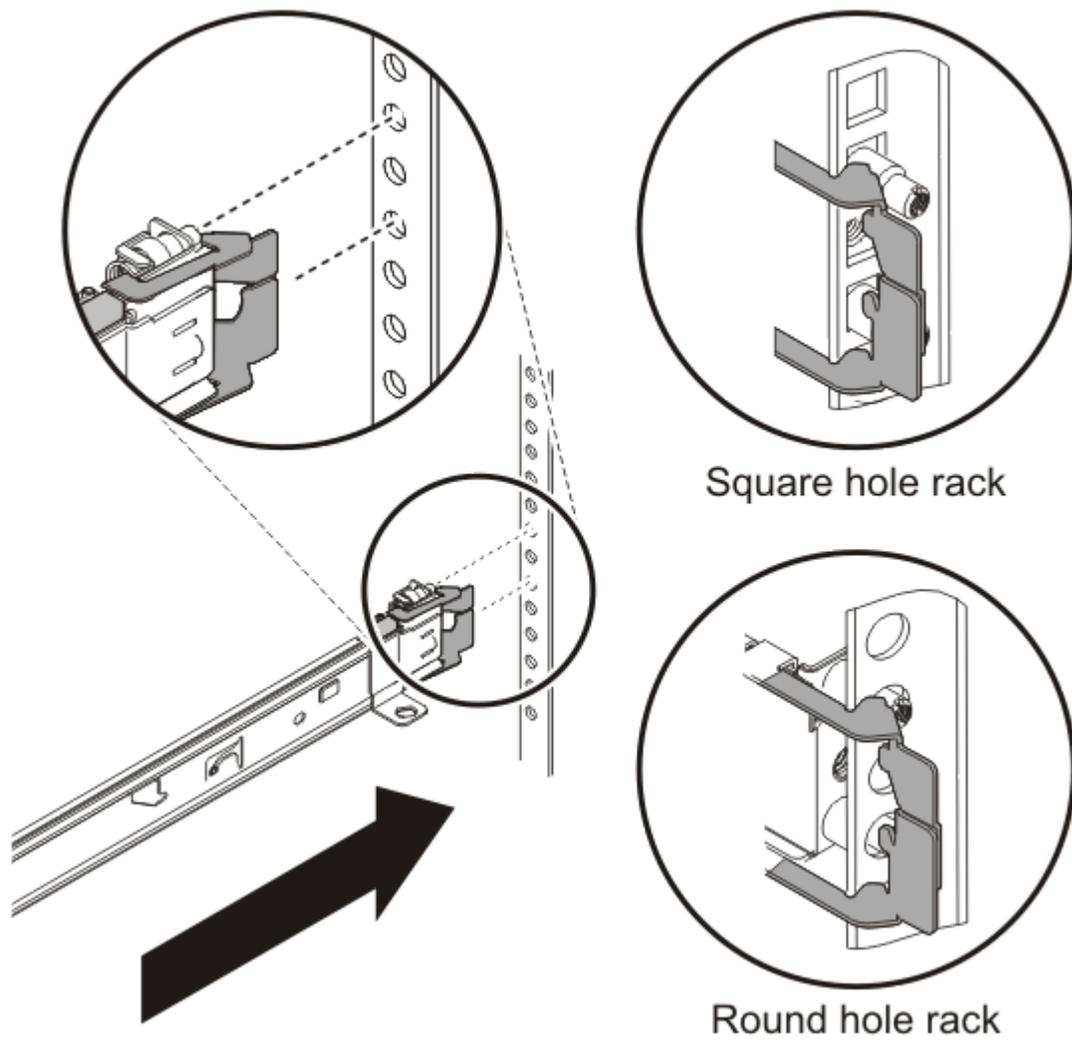


Figura 12. Calha deslizante e o membro de calha externo

**Nota:** Cada calha deslizante está marcada como **R (direita)** ou **L (esquerda)** na respectiva parte posterior.

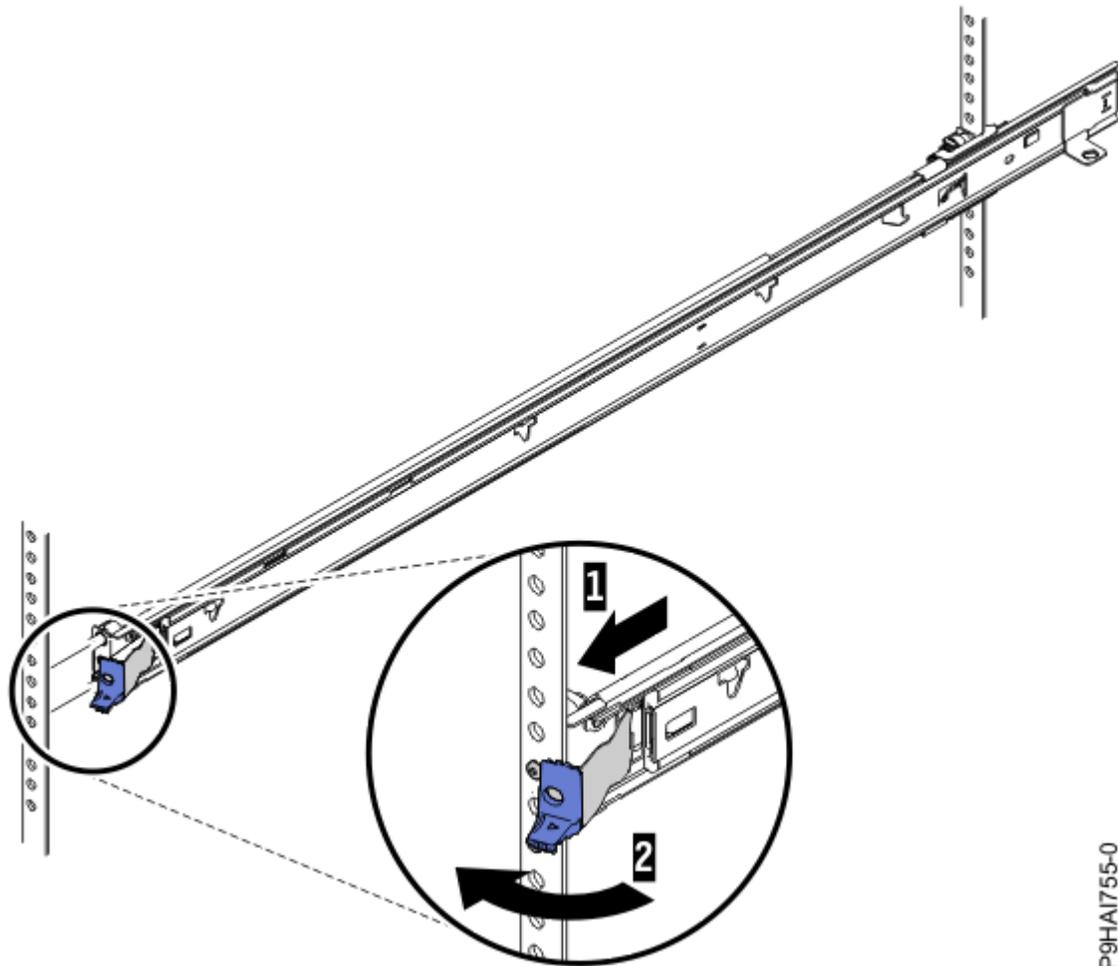
3. Alinhe a parte posterior do membro de calha externo contra os buracos na parte posterior do bastidor. Alinhe os pinos e empurre a calha para dentro de forma a que os pinos entrem nos buracos. Os dois pinos da calha sobressaem através dos buracos superior e inferior no bordo EIA. Empurre a calha na direcção da parte posterior do bastidor até que o suporte de montagem em bastidor posterior bloqueie no sítio.



P9HAI754-0

*Figura 13. Alinhe os pinos com os orifícios na parte de trás do bastidor*

4. Rode o fecho frontal para a posição de aberto e alinhe a parte anterior do membro de calha externo contra os buracos na frente do bastidor. Alinhe os pinos com buracos nos bordos EIA e puxe a calha para a frente de forma a que os pinos sobressaiam através dos buracos. Bloqueie a parte anterior da calha ao permitir que a fecho frontal rode para a posição de fechado. Repita os passos 2- 4 para o outro membro de calha externo.



P9HA1755-0

Figura 14. Patilha da calha deslizante anterior

5. Prima os fechos **(1)**. Quando mover o armário do bastidor ou caso instale o armário do bastidor numa área propensa a vibrações, aperte os parafusos M5 fixos **(2)** na parte anterior do servidor.

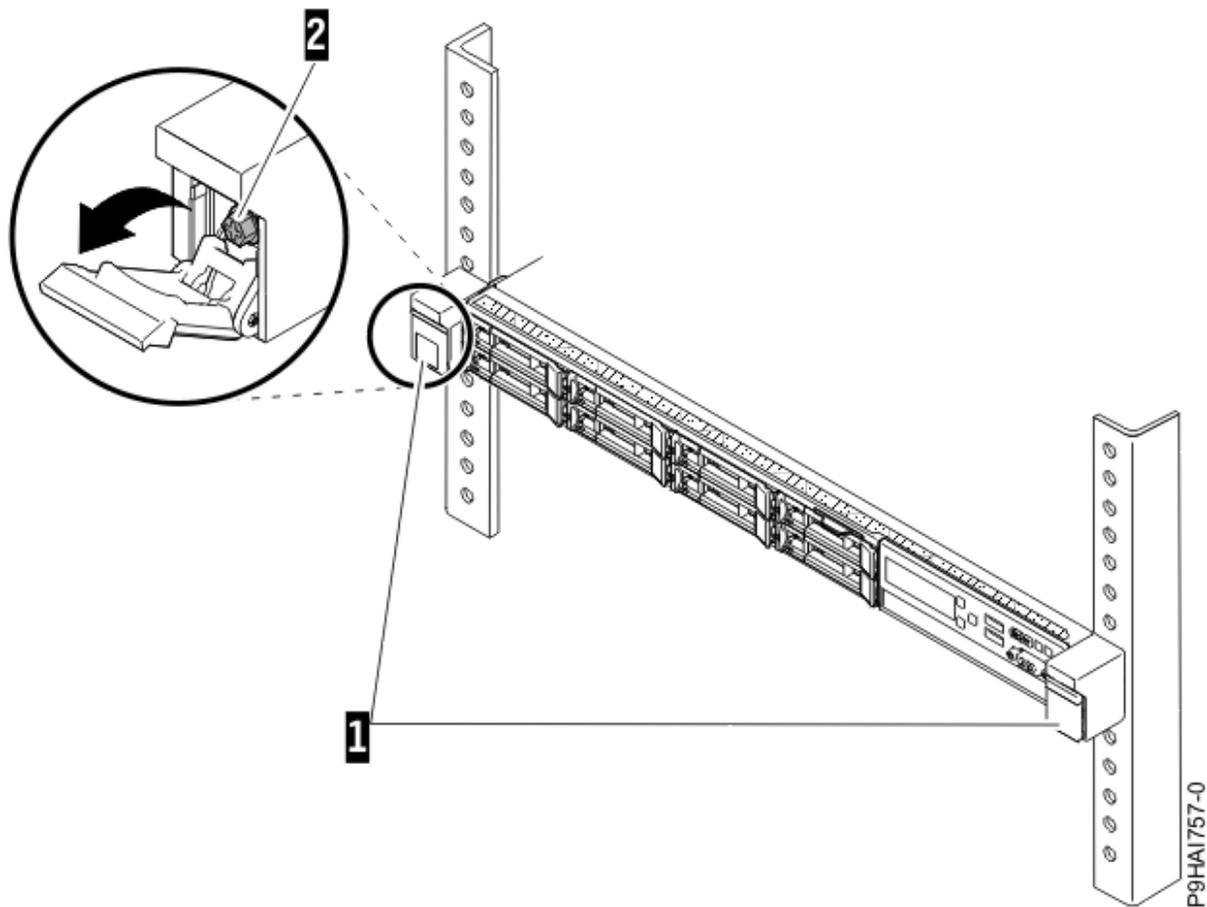


Figura 15. Calha deslizante frontal e pinos

6. Empurre as calhas deslizantes para a frente **(1)** até encaixarem com um duplo estalido. Com cuidado, levante o servidor e incline-o na posição sobre as calhas deslizantes de forma a que o parafuso de trás fique alinhado **(2)** no servidor com as ranhuras de trás nas calhas deslizantes. Baixe o servidor até que a cabeça do parafuso de trás deslize para as duas ranhuras de trás e, em seguida, baixe devagar a parte da frente do servidor **(3)** até que as outras cabeças dos parafusos entrem nas ranhuras nos carris laterais. Certifique-se de que o trinco frontal cobre a cabeça dos parafusos de forma a que o sistema fique trancado nas calhas deslizantes.

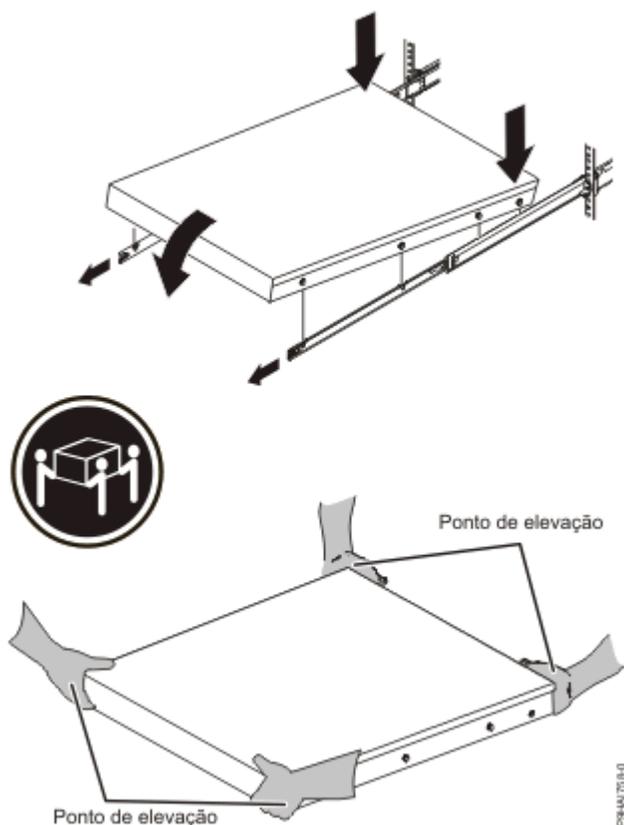


Figura 16. Calhas deslizantes expandidas, cabeças dos parafusos alinhadas com as ranhuras na calha deslizante e pontos de elevação

**Nota:** Utilize as práticas de segurança ao levantar. Se estiver a instalar um servidor 1 U, certifique-se de que tem duas pessoas quando levanta o servidor. As mãos devem estar posicionadas tal como é demonstrado em [Figura 16 na página 32](#).

7. Levante as alavancas de bloqueio **(1)** nas calhas deslizantes e empurre o servidor **(2)** no bastidor até que se encaixe.

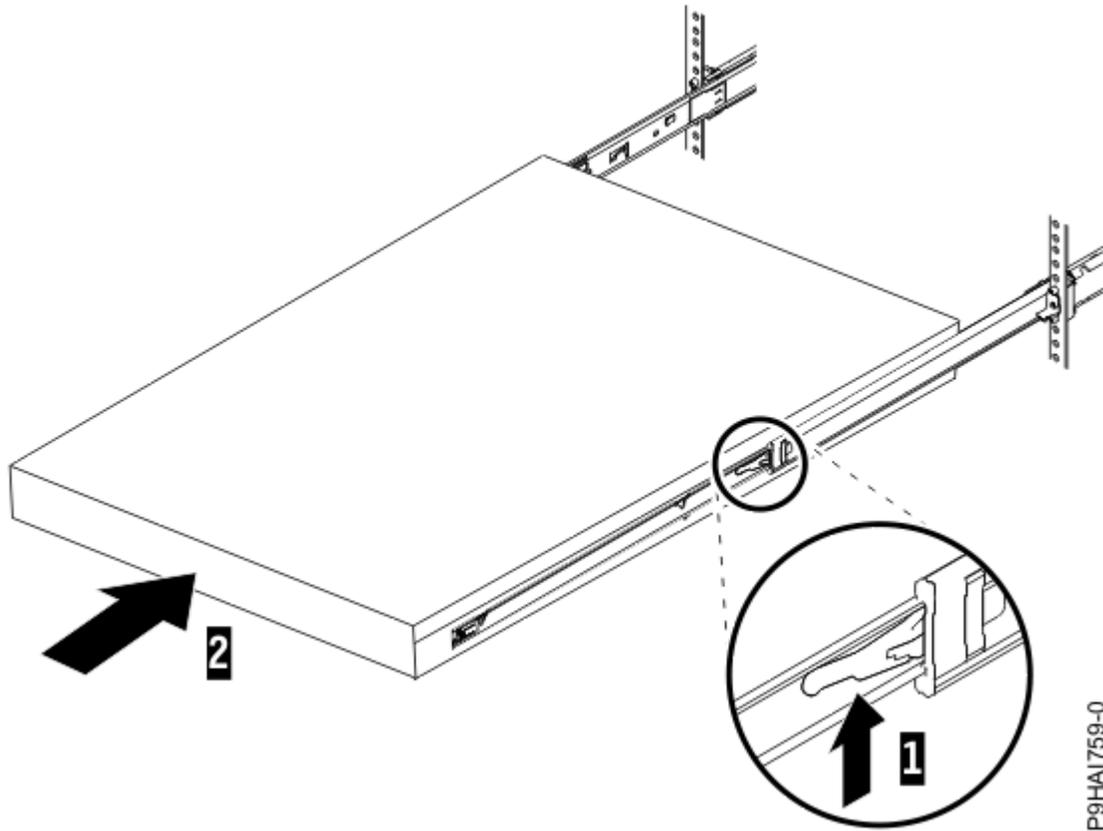
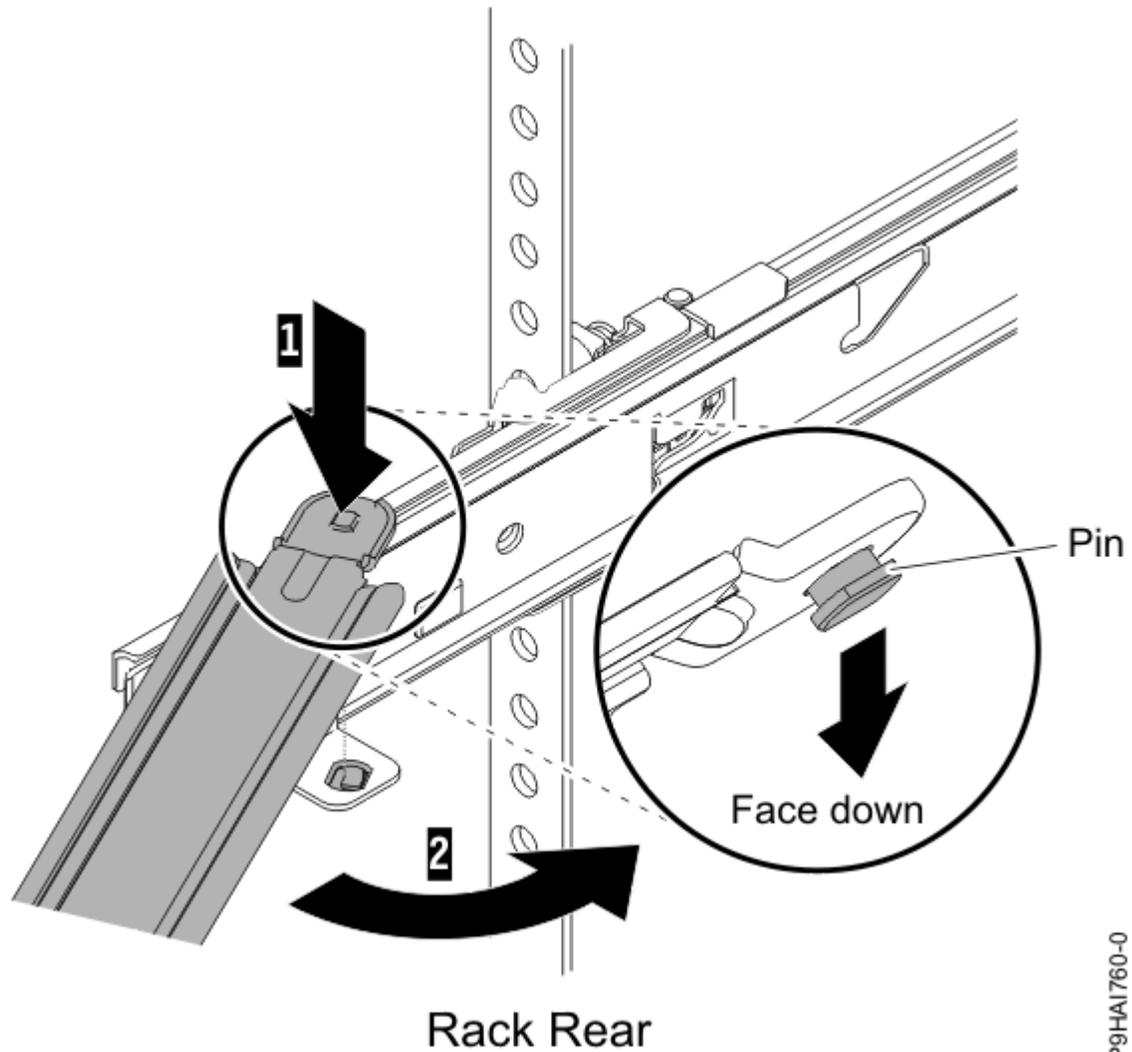


Figura 17. Fechos e o servidor

8. O braço de gestão de cabos pode ser instalado em qualquer um dos lados do servidor. Figura 18 na página 34 demonstra a instalação do mesmo no lado esquerdo. É melhor instalar o braço de gestão de cabos de forma a que fique apoiado no lado oposto às fontes de alimentação para facilitar acesso às mesmas. Para instalar o braço de gestão de cabos no lado direito, siga as instruções e instale o hardware do lado oposto. Coloque o pino (1) na ranhura horizontal na parte posterior das calhas deslizantes. Em seguida, rode a outra extremidade da barra no sentido do bastidor (2) no sentido do bastidor.

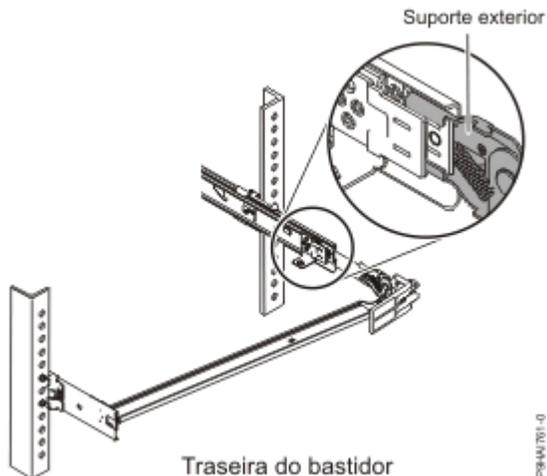


P9HAI760-0

Figura 18. Ligação do braço de suporte

**Nota:** A barra de suporte de gestão de cabos tem de se encontrar no cimo do separador da calha para funcionar correctamente.

9. Instale o suporte de paragem de gestão de cabos (com a letra maiúscula **O**) na extremidade desligada do braço de suporte. Certifique-se de que o braço de suporte está correctamente instalado.

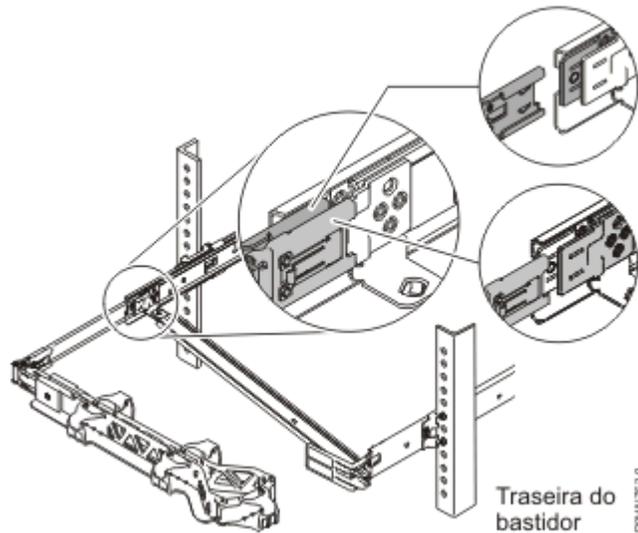


P9HAI761-0

Figura 19. Ligar o suporte de paragem à calha deslizante

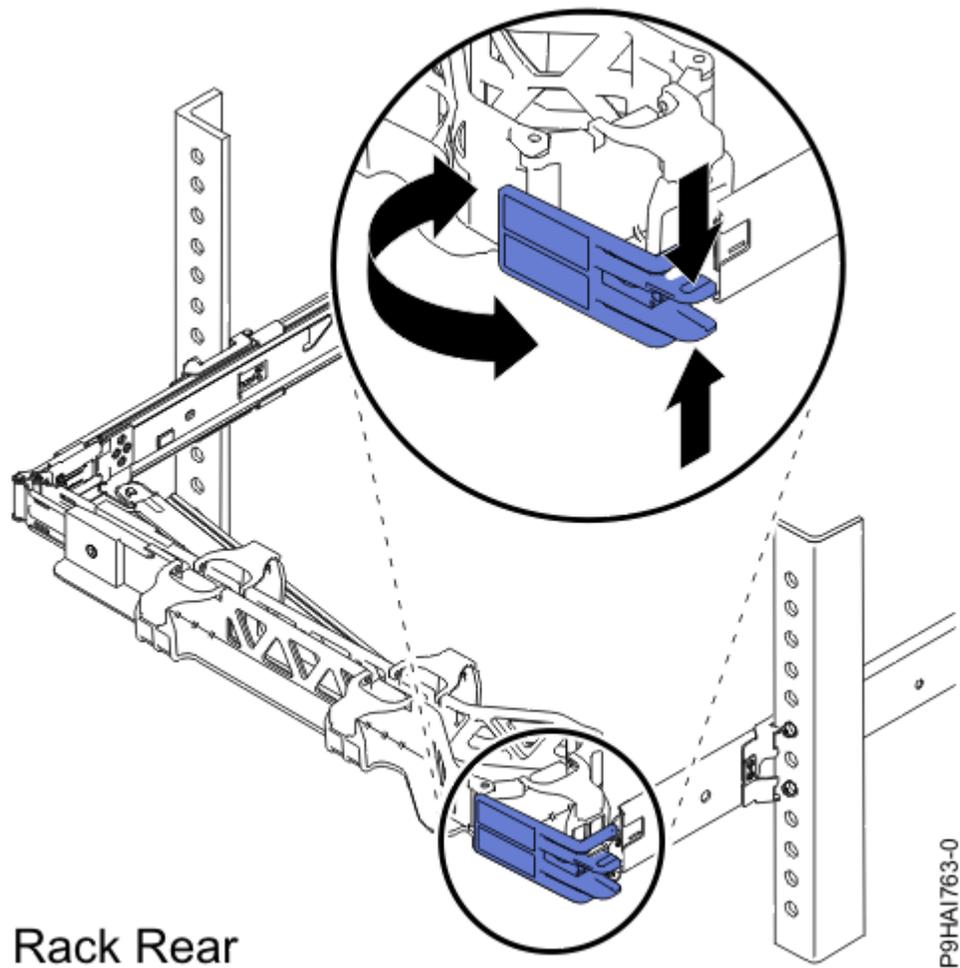
**Nota:** A letra maiúscula **O** está marcada nos pinos do braço de gestão de cabos para identificar os pinos exteriores.

10. Colocar o braço de gestão de cabos no braço de suporte. Deslize os separadores do braço de gestão de cabos para as ranhuras interiores e exteriores da calha deslizante. Empurre os separadores até estes ficarem encaixados no respectivo lugar.



*Figura 20. Ligação do braço de gestão de cabos*

11. Para facilitar a rotação do braço de gestão de cabos para dentro e para fora do braço de gestão de cabos, é possível abrir o suporte de paragem ao puxar os separadores para cima e para baixo do suporte de gestão de cabos.



## Rack Rear

Figura 21. Suporte de paragem do suporte de gestão de cabos

12. Ligue os cabos de alimentação e outros cabos à parte de trás do servidor incluindo teclado, monitor e cabos do rato, caso seja necessário). Passe os cabos e os cabos de alimentação no braço de gestão de cabos e prenda-os aos laços dos cabos ou a presilhas que os podem segurar.

**Nota:** A localização das fitas de cabos poderão ser ligeiramente diferentes em sistemas diferentes. Utilize as fitas de cabos fornecidas na parte posterior do sistema para prender os cabos e para prevenir que os mesmos fiquem soltos.

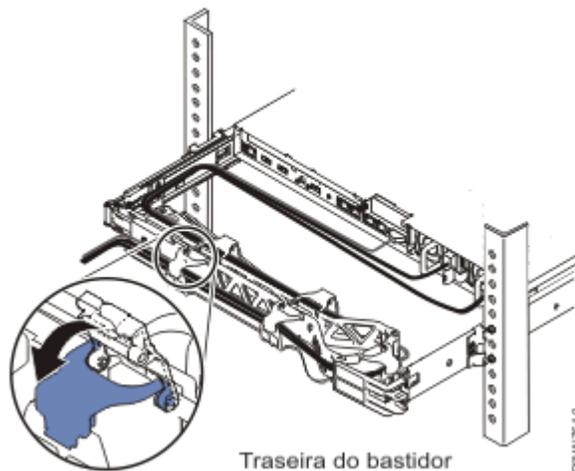


Figura 22. Anexar o cabo Power e encaminhar o cabo

13. Os cabos têm de estar agrupados com a fita para cabos para uma movimentação correcta do braço de gestão de cabos.

**Nota:** Certifique-se de que os cabos não se soltam abaixo do espaço U para que não fiquem presos nas partes inferiores dos sistemas. Permita o ajuste interno de todos os cabos para evitar tensão nos cabos à medida que se move o braço de gestão de cabos.

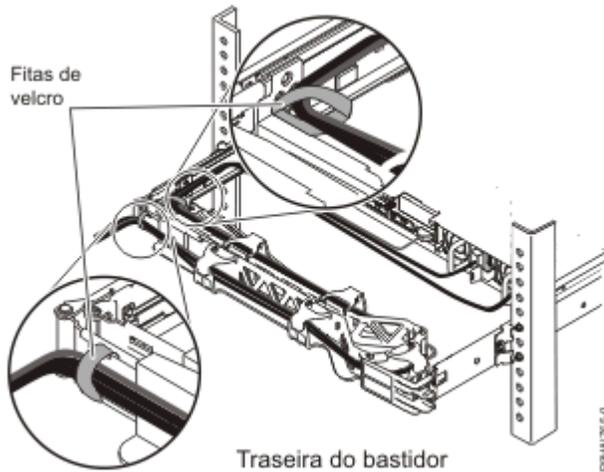


Figura 23. Presilha

14. Caso esteja a transportar o bastidor com o sistema instalado ou caso esteja numa área propícia a vibrações, insira os parafusos M5 na parte posterior das calhas deslizantes. Utilize uma braçadeira de cabos para fixar a extremidade livre do braço de gestão de cabos ao bastidor, caso seja necessário.

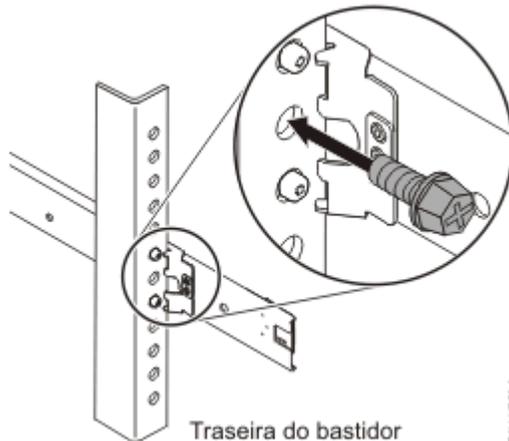


Figura 24. Fixar o servidor para transporte

## Instalar a Dispositivo virtual da HMC

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC).

É possível instalar a Dispositivo virtual da HMC na infra-estrutura virtualizada x86 ou POWER existente. A Dispositivo virtual da HMC suporta os seguintes hipervisores de virtualização x86:

- Máquina virtual baseada em Kernel (KVM, Kernel-based virtual machine)
- Xen
- VMware

A Dispositivo virtual da HMC suporta os seguintes hipervisores de virtualização POWER:

- PowerVM

Requisitos mínimos para executar a Dispositivo virtual da HMC:

- 16 GB de memória
- 4 processadores virtuais
- 2 interfaces de rede (máximo permitido de 4)
- 1 unidade de disco que contém 500 GB de espaço em disco disponível

#### Notas:

- O processador nos sistemas que alojam a Dispositivo virtual da HMC têm de ser um processador Intel VT-x ou um processador AMD-V de virtualização de hardware activada.
- Não é possível arrancar a partir dos DVDs da Dispositivo virtual da HMC que recebe. É necessário montar o suporte primeiro e, em seguida, copiar o ficheiro .tgz do suporte. O método para montar o DVD poderá variar dependendo do sistema operativo que utilizar.
- A sintaxe de comando utilizada nos seguinte exemplos poderá variar dependendo do sistema operativo que utilizar.
- O hipervisor de virtualização PowerVM requer 160 GB de espaço em disco. No entanto, é recomendado 500 GB de memória.
- O processador PowerVM requer pelo menos 1.0 unidades de processamento e quatro processadores virtuais partilhados no modo de partilha com limite definido. Não se recomenda a utilização de processadores dedicados. O processador PowerVM também requer 16 GB de memória.

#### Informações relacionadas

[Instruções de instalação e imagens de instalação em rede da HMC V8](#)

## Instalar a Dispositivo virtual da HMC no x86

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC) num ambiente x86.

### ***Instalar a Dispositivo virtual da HMC através da utilização do hipervisor de KVM***

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC) através da utilização do hipervisor da máquina virtual baseada em Kernel (KVM, kernel-based virtual machine).

Para instalar a Dispositivo virtual da HMC em KVM, conclua os seguintes passos:

**Nota:** Os seguintes passos utilizam a interface da linha de comandos e requerem autoridade de utilizador raiz. A sintaxe de comandos poderá variar dependendo do sistema operativo.

1. Verifique se os pacotes de virtualização estão instalados em sistemas com Red Hat Enterprise Linux (RHEL) versão 7.0 ou posterior.
2. Descarregue o ficheiro <KVM vHMC installation filename>.tar.gz para o sistema central.
3. Execute o seguinte comando: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Execute o seguinte comando: `cd /var/lib/libvirt/images/vHMC`.
5. Para extrair as imagens de disco virtuais, execute o seguinte comando: `tar -zxvf <KVM vHMC installation filename>.tgz`

**Nota:** Neste comando, especifique o caminho completo do ficheiro .tar da Dispositivo virtual da HMC.

6. É facultado um ficheiro **domain.xml** no ficheiro <KVM vHMC installation filename>.tar.gz. Conclua os seguintes passos:
  - a. Edite o ficheiro **domain.xml** e verifique se o caminho para os discos está correcto. Este ficheiro contém a cadeia **DISK\_PATH**.
  - b. Certifique-se de que **virtio** é utilizado no valor de barramento para o dispositivo de discos.
  - c. É possível optar por ter um nome diferente para a VM. O nome predefinido no ficheiro **domain.xml** é **vHMC**.
  - d. Verifique se o endereço Controlo de Acesso de Suportes (MAC, media access control) está definido no ficheiro **domain.xml**. Este ficheiro contém a cadeia **MAC\_ADDRESS**.

**Nota:** Remova esta linha caso pretenda que um endereço MAC seja criado automaticamente.

- e. Verifique se as pontes correspondem aos dispositivos de Ethernet. O ficheiro **domain.xml** predefinido especifica uma Ethernet.
  - f. Caso esteja a utilizar o Activation Engine, substitua **AEDISK** pelo nome da imagem de disco virtual do Activation Engine. Caso contrário, remova o elemento de disco.
7. Para definir a VM, execute o seguinte comando: `virsh define <domain>.xml`.
  8. Para verificar se a HMC Virtual foi adicionada à lista de máquinas virtuais definidas, execute o seguinte comando: `virsh list --all`.
  9. Para iniciar a VM, execute o seguinte comando: `virsh start vHMC`.
  10. Para determinar o número de apresentação de Processamento de Redes Virtuais (VNC, Virtual Network Computing) da consola, execute o seguinte comando: `virsh vncdisplay vHMC`.
  11. Para estabelecer ligação à consola com um visualizador de VNC, execute o seguinte comando: `vncviewer HOSTNAME:ID`(Onde ID corresponde ao número de apresentação, por exemplo 0).
- Nota:** Caso requeira de acesso remoto, é necessário largar ou configurar a firewall para permitir acesso à porta 5900.

### ***Instalar a Dispositivo virtual da HMC através da utilização do hipervisor de Xen***

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC) através da utilização do hipervisor de Xen.

A Dispositivo virtual da HMC suporta Xen versão 4.2 ou posterior.

Para instalar a Dispositivo virtual da HMC através da utilização do hipervisor de Xen, conclua os seguintes passos:

**Nota:** Os seguintes passos utilizam a interface de linha de comandos e requerem autoridade de utilizador raiz. A sintaxe de comandos poderá variar dependendo do sistema operativo.

1. Verifique se os pacotes de virtualização estão instalados em sistemas com Red Hat Enterprise Linux (RHEL) versão 6.4 ou posterior.
2. Descarregue o ficheiro `<XEN vHMC installation filename>.tar.gz` para o sistema central.
3. Execute o seguinte comando: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Execute o seguinte comando: `cd /var/lib/libvirt/images/vHMC`.
5. Para extrair as imagens de disco virtuais, execute o seguinte comando: `tar -zxvf <XEN vHMC installation filename>.tgz`

**Nota:** Neste comando, especifique o caminho completo do ficheiro .tar da Dispositivo virtual da HMC.

6. É facultado um ficheiro **vhmc.cfg** no ficheiro `<XEN vHMC installation filename>.tar.gz`. Abra o ficheiro **vhmc.cfg** num editor de texto e edite os seguintes valores:
  - a. Altere o nome da HMC virtual (opcional): Edite o ficheiro **vhmc.cfg** e verifique se o caminho para os discos está correcto. Este ficheiro contém a cadeia **DISK\_PATH**.
  - b. Substitua **DISK\_PATH** pelo caminho para `disk1.img`:

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

- c. Substitua **ethernet adapter** e adicione o endereço MAC (opcional):

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

Endereço MAC Opcional:

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

**Nota:** Quando a HMC Virtual é reiniciada, o hipervisor de Xen recria automaticamente um endereço MAC. A adição do Endereço MAC opcional resolve esta questão.

d. Substitua **FLOPPYPATH** (se estiver a utilizar o Activation Engine):

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

7. Para criar e iniciar a VM, execute o seguinte comando: `xl create vHMC.cfg`.
8. Para verificar se a VM foi adicionada à lista de máquinas virtuais definidas, execute o seguinte comando: `xl list`.
9. Para aceder à consola local da VM, execute o seguinte comando: `vncviewer localhost 0`.

### ***Instalar a Dispositivo virtual da HMC através da utilização de VMware ESXi***

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC) através da utilização de VMware ESXi.

É possível instalar a Dispositivo virtual da HMC em VMware ESXi através da utilização da interface gráfica de utilizador no cliente vSphere para implementar o modelo OVF (Open Virtualization Format).

**Nota:** É possível instalar a Dispositivo virtual da HMC em VMware ESXi versão 6.0 ou posterior.

Para instalar a Dispositivo virtual da HMC em VMware ESXi através da utilização do cliente vSphere, conclua os seguintes passos:

**Nota:** A sintaxe de comandos poderá variar dependendo do sistema operativo.

1. Obtenha o ficheiro de arquivo Tar: `<VMware vHMC installation file name>.tgz`.
2. Utilize o comando `tar` para extrair o ficheiro OVA a partir do ficheiro de arquivo Tar.
3. Inicie o cliente vSphere e inicie sessão no sistema central ESXi.
4. A partir do menu **Ficheiro (File)**, seleccione **Implementar modelo OVF (Deploy OVF template)**.
5. Faça clique em **Pesquisar (Browse)** e seleccione o ficheiro OVA.
6. Faça clique em **Seguinte (Next)**.
7. Após a conclusão da implementação, faça clique em **Fechar (Close)** e seleccione o ícone da Dispositivo virtual da HMC para iniciar a Dispositivo virtual da HMC.

### **Instalar a Dispositivo virtual da HMC em POWER**

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC) num ambiente POWER virtualizado.

#### ***Instalar a Dispositivo virtual da HMC no PowerVM (partição lógica)***

Saiba como instalar a Dispositivo virtual da Consola de Gestão de Hardware (HMC) num ambiente PowerVM.

A Dispositivo virtual da HMC suporta servidores POWER9 no nível de software proprietário FW910 ou posterior. Para obter mais informações, consulte [Distribuições Linux suportadas para POWER8 e POWER9 Linux em sistemas Power](https://www.ibm.com/support/knowledgecenter/en/linuxonibm/iaam/iaamdistros.htm) (<https://www.ibm.com/support/knowledgecenter/en/linuxonibm/iaam/iaamdistros.htm>).

#### **Notas:**

1. Não é possível gerir o servidor que aloja a Dispositivo virtual da HMC.
2. Não é possível gerir o servidor que aloja outra Dispositivo virtual da HMC que está a gerir o servidor que aloja esta Dispositivo virtual da HMC.

Por exemplo, a Dispositivo virtual da HMC A encontra-se em execução no servidor A e a Dispositivo virtual da HMC B encontra-se em execução no Servidor B. A Dispositivo virtual da HMC A não pode gerir o servidor B e a Dispositivo virtual da HMC B não pode gerir o servidor A ao mesmo tempo. Uma das Dispositivo virtual da HMC pode gerir o outro servidor, mas ambas as Dispositivo virtual da HMC não podem gerir-se uma à outra ao mesmo tempo.

## Criar uma imagem de instalação da HMC automatizada (opcional)

É possível criar uma imagem de instalação da HMC automatizada que instala a Dispositivo virtual da HMC automaticamente sem pedir pelo assistente de **Instalação da HMC (HMC Installation)**.

**Nota:** A Dispositivo virtual da HMC em PowerVM não faculta suporte de adaptador de gráficos para adaptadores atribuídos à partição. É possível utilizar um navegador da Web suportado para estabelecer ligação à HMC para obter suporte da interface de utilizador.

Para criar uma imagem de instalação da HMC automatizada, conclua os seguintes passos:

1. Crie dois directórios através da execução dos seguintes comandos: `mkdir -p oldiso` e `mkdir -p newiso`.
2. Instale a imagem de instalação da HMC no directório **oldiso** através da execução do seguinte comando: `sudo mount -o loop <image_path> oldiso`.
3. Copie o conteúdo do directório **oldiso** para o directório **newiso** através da execução do seguinte comando: `cp -r oldiso/* newiso`.
4. Edite o ficheiro Grub para a instalação automatizada através da execução do seguinte comando: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Torne o ficheiro Grub só de leitura através da execução do seguinte comando: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Crie um novo ISO de instalação da HMC através da execução do seguinte comando: `mkisofs -o <new_iso_name> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrip-boot -iso-level 4 -part -no-desktop -quiet newiso` (onde **Etiqueta ISO (ISO label)** tem de ser HMC-<número de edição da versão da hmc>, por exemplo, HMC-8.0.870.0).

**Nota:** Para obter mais informações sobre a configuração do Activation Engine e do ficheiro de configuração, consulte [“Utilizar o Activation Engine para a Dispositivo virtual da HMC”](#) na página 44.

## Configuração do volume lógico

Para configurar o volume lógico, conclua os seguintes passos:

1. Seleccione um sistema gerido.
2. A partir do pod do menu, seleccione **Ações do Sistema (System Actions) > Power VM (Power VM) > Memória Virtual (Virtual Storage)**.
3. Seleccione **Gerir VIOS do Sistema (Manage System VIOS) > Acção (Action) > Gerir Memória Virtual (Manage Virtual Storage)**.
4. Seleccione o separador **Discos Virtuais (Virtual Disks)**.
5. Faça clique em **Criar disco virtual (Create virtual disk)** e introduza as seguintes informações:
  - **Nome do disco virtual (Virtual disk name):** O nome do disco virtual.
  - **Nome do conjunto de memória (Storage pool name):** O nome do conjunto de memória.
  - **Tamanho do disco virtual (Virtual disk size):** O tamanho do disco virtual.
  - **Partição atribuída (Assigned partition):** O nome da partição lógica.

**Nota:** É requerido um mínimo de 160 GB de espaço em disco (recomendam-se 500 GB de espaço em disco).

## Configuração do suporte de instalação - criar biblioteca de suportes

Para criar uma biblioteca de suportes, conclua os seguintes passos:

1. Seleccione um sistema gerido.
2. A partir do pod do menu, seleccione **Ações do Sistema (System Actions) > Power VM (Power VM) > Memória Virtual (Virtual Storage)**.

3. Selecione **Gerir VIOS do Sistema (Manage System VIOS) > Acção (Action) > Gerir Memória Virtual (Manage Virtual Storage)**.
4. Selecione o separador **Dispositivos Ópticos (Optical Devices)**.
5. Faça clique em **Criar Biblioteca (Create Library)** e introduza as seguintes informações:
  - **Conjunto de memória (Storage pool)**: O nome do conjunto de memória.
  - **Tamanho da biblioteca de suportes (Media library size)**: O tamanho da biblioteca de suportes.
6. Faça clique em **OK**.

## Configuração do suporte de instalação - carregar suportes para VIOS

Para carregar suportes para o Servidor de E/S Virtual (VIOS, Virtual I/O Server), conclua os seguintes passos:

1. Inicie sessão no VIOS.
2. No modo de raiz do VIOS, execute o seguinte comando: `oem_setup_env`.
3. Para permitir a ligação NFS, execute o seguinte comando: `nfs -o nfs_use_reserved_ports=1`.
4. Para instalar o NFS na pasta local do VIOS, execute o seguinte comando: `mount <server_ip>:/ Mountpoint <local_folder>`.
5. Para verificar se a instalação do NFS inclui o ISO de instalação da HMC e imagem de configuração do Activation Engine (opcional), execute o seguinte comando: `ls`.

## Configuração do suporte de instalação - ligar suportes à biblioteca de suportes

Para ligar suportes à biblioteca de suportes, conclua os seguintes passos:

1. Navegue de volta para **Gerir VIOS do Sistema (Manage System VIOS) > Acção (Action) > Gerir Memória Virtual (Manage Virtual Storage)** e selecione o separador **Dispositivos Ópticos (Optical Devices)**.
2. A partir da secção **Suporte Óptico Virtual (Virtual Optical Media)**, selecione **Adicionar Suporte (Add Media)** a partir do menu **Acções (Actions)**.
3. A partir da janela **Adicionar Suporte Virtual (Add Virtual Media)**, selecione **Adicionar ficheiro existente a partir de sistema de ficheiros VIOS (Add existing file from VIOS filesystem)** e introduza as seguintes informações:
  - **Nome do suporte (Media name)**: O nome do suporte (por exemplo, HMCInstall ou AEDrive).
  - **Nome do ficheiro do suporte óptico (Optical media file name)**: O nome de ficheiro do ficheiro ISO de instalação (por exemplo, 01234567-ppc64ie.iso).
4. Faça clique em **OK**.
5. Caso tenha criado uma imagem de configuração do Activation Engine, repita os passos 3 - 4 para adicionar a imagem de configuração do Activation Engine. Caso contrário, avance para o passo 6.
6. Verifique se o suporte óptico é carregado para a biblioteca de suportes através da verificação se o nome do suporte é apresentado na lista de **Suportes Ópticos Virtuais (Virtual Optical Media)** disponíveis.

## Configuração da partição lógica

Para configurar a partição lógica, conclua os seguintes passos:

1. Selecione um sistema gerido.
2. A partir do pod do menu, selecione **Acções do Sistema (System Actions) > Partições (Partitions) > Partições (Partitions)**.
3. Faça clique em **Criar Partição (Create Partition)** e introduza as seguintes informações:
  - **Nome da Partição (Partition Name)**: O nome da partição.

- **ID da Partição (Partition ID):** O ID da partição.
  - **Tipo de Partição (Partition Type):** Seleccione o sistema operativo (**AIX/Linux** ou **IBM i**).
4. Faça clique em **OK**.
  5. Atribua o número de processadores e a quantidade de memória para a partição.  
**Nota:** É necessário um mínimo de quatro processadores virtuais e 8 GB de memória.
  6. A partir do pod do menu, seleccione **Ações de Partições (Partition Actions) > E/S Virtual (Virtual I/O) > Redes Virtuais (Virtual Networks)**.
  7. Faça clique em **Ligar Rede Virtual (Attach Virtual Network)** e seleccione a caixa de verificação **Mostrar e ligar novos adaptadores de Ethernet virtuais (Show and attach new virtual ethernet adapters)**. A partir da tabela, seleccione os adaptadores da rede virtual que pretende ligar à partição lógica.  
**Nota:** É permitido um máximo de quatro adaptadores de rede virtual.
  8. A partir do pod do menu, seleccione **Ações de Partições (Partition Actions) > E/S Virtual (Virtual I/O) > Memória Virtual (Virtual Storage)**.
  9. A partir do separador **Dispositivo Óptico Virtual (Virtual Optical Device)**, faça clique em **Adicionar Dispositivo Óptico Virtual (Add Virtual Optical Device)**.
  10. Introduza o **Nome do Dispositivo (Device Name)** (por exemplo, HMCInstall ou AEDrive) e seleccione o Servidor de E/S Virtual pretendido a partir da tabela.  
**Nota:** A instalação de AEDrive é opcional.
  11. Faça clique em **OK**.
  12. Verifique se os dispositivos ópticos virtuais que adicionou do passo [10](#) se encontram agora listados na tabela.
  13. A partir do menu **Ação (Action)**, faça clique em **Carregar (Load)**.
  14. Seleccione o ficheiro de suporte para atribuir à partição lógica e faça clique em **OK**.
  15. Verifique se os dispositivos ópticos virtuais que carregou do passo [13](#) se encontram agora listados na tabela.

## Iniciar a Dispositivo virtual da HMC

**Nota:** Quando instala a Dispositivo virtual da HMC numa partição através da utilização do ficheiro de imagem ISO da HMC, não possuirá acesso de consola gráfica local à interface de utilizador da Web.

Para iniciar a Dispositivo virtual da HMC em PowerVM, conclua os seguintes passos:

1. Seleccione a partição gerida.
2. Abra uma ligação activa à partição lógica através da selecção de **Ações (Actions) > Consola (Console) > Abrir Janela do Terminal (Open Terminal Window)**.
3. Active a partição lógica através da selecção de **Ações (Actions) > Activar (Activate)**.
4. Seleccione **Activar (Normal) (Activate (Normal))** e **Configuração Actual (Current Configuration)**.
5. Faça clique em **Terminar (Finish)**.
6. Mude para a janela do terminal.
7. A partir do menu **Arranque (Boot)**, seleccione **1 = Menu SMS (1 = SMS Menu)**.
8. A partir do menu **Principal (Main)**, seleccione **5 = Seleccionar Opções de Arranque (5 = Select Boot Options)**.
9. A partir do menu **Arranque múltiplo (Multiboot)**, seleccione **1 = Seleccionar Dispositivo de Instalação/Arranque (1 = Select Install/Boot Device)**.
10. A partir do menu **Seleccionar Tipo de Dispositivo (Select Device Type)**, seleccione **5 = Listar todos os dispositivos (5 = List all devices)**.
11. Seleccione o dispositivo HMCInstall com base na localização do dispositivo.

12. Selecione **2. Arranque em Modo Normal (2. Normal Mode Boot)**.

13. Selecione **1. Sim (1. Yes)** para confirmar.

14. Siga as instruções no ecrã a partir do assistente de **Instalação da HMC (HMC Install)**.

**Nota:** Ignore este passo caso tenha utilizado uma imagem de instalação da HMC automatizada.

15. Após a instalação concluir e o sistema iniciar, tem de seleccionar um idioma a partir da caixa de diálogo **Seleção do idioma (language selection)**.

16. Aceite o acordo de licença.

**Nota:** Assegure-se de que o controlador de comandos está pronto a aceitar comandos antes de executar quaisquer comandos. Por exemplo, executar o comando **lshmc -V** até que seja bem sucedido.

17. Inicie sessão como `hscroot` e utilize o comando **chhmc** para configurar a rede.

O seguinte exemplo demonstra a sequência de comandos **chhmc** que poderão ser utilizados para configurar a rede e activar acesso Secure Shell (SSH) e remoto da Web na HMC.

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

- **ethX** é o nome da interface de rede a configurar.
- **hmc ip address** é o endereço de IP da HMC.
- **hmc network mask** é a máscara de rede da HMC.
- **hmc hostname** é o nome do sistema central da HMC.
- **hmc domain name** é o nome do domínio da HMC.
- **gateway ip** é o endereço de IP da porta de ligação na rede.
- **name server** é o endereço do servidor de nomes da rede.
- **domain search** é o nome dos domínios em que pretende que a HMC procure.
- Para permitir o acesso em todos os endereços de IP, utilize **-a 0.0.0.0 -nm 0** em vez do **endereço de ip (ip address)**.

**Nota:** Quando utilizar múltiplos adaptadores de Ethernet virtuais, execute o comando **cat /etc/sysconfig/network-scripts/ifcfg-ethX** na Dispositivo virtual da HMC em cada interface. Compare o endereço de Controlo de Acesso de Suportes (MAC, media access control) com o que a HMC apresenta na vista de adaptador da rede virtual da partição. É possível fazer clique em **Visualizar Definições do Adaptador de Ethernet Virtual (View Virtual Ethernet Adapter Settings)** para obter mais informações sobre os adaptadores de Ethernet virtuais. Este passo ajuda o utilizador a determinar a interface correcta a utilizar.

18. Reinicie o sistema.

## Utilizar o Activation Engine para a Dispositivo virtual da HMC

Saiba como utilizar o Activation Engine para a Dispositivo virtual da Consola de Gestão de Hardware (HMC).

O Activation Engine é uma estrutura que permite a configuração de vários componentes dentro de uma máquina virtual durante o arranque do sistema. Para utilizar o Activation Engine, é necessário configurar um perfil de configuração XML para permitir que a Dispositivo virtual da HMC se encontre num estado pronto a gerir no primeiro início. Para obter mais informações sobre a configuração do perfil de configuração XML, consulte [“Definir o perfil de configuração para o Activation Engine” na página 45](#). É possível utilizar o ficheiro de configuração para configurar as seguintes opções:

- Definir Teclado Predefinido (E.U.A.)
- Locale Predefinido (E.U.A.)
- Desactivar a Configuração do Teclado
- Desactivar a Configuração da Apresentação
- Acordo de Licença e Acordo de Código Máquina
- Desactivar o Assistente de Configuração
- Desactivar o Assistente de Chamada de Assistência
- Configurar até quatro Placas de Interface de Rede
- Configurar Definições de Firewall para cada Interface
- Configurar a interface de rede como Servidor de DHCP IPv4
- Configurar a Interface Privada e Aberta
- Configurar o Dispositivo de Interface de Porta de Ligação Predefinido

**Nota:** O número de adaptadores de Ethernet que é definido no ficheiro de configuração **vHMC-Conf.xml** tem de se correlacionar com os adaptadores de Rede definidos no ficheiro de configuração **domain.xml**, **vHMC.cfg** ou **VMWare**.

O Activation Engine requer um disco virtual que contenha uma configuração XML. É possível editar o ficheiro **user\_data** com um editor de texto e utilizar o manual de configuração XML que é apresentado no seguinte exemplo.

Para criar uma imagem de disco ISO virtual com a configuração do Activation Engine num ambiente Linux, conclua os seguintes passos:

1. Crie um directório:

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

2. Copie o ficheiro **user\_data** editado para o directório:

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

3. Crie uma imagem de disco virtual com a configuração do Activation Engine:

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

## **Definir o perfil de configuração para o Activation Engine**

Saiba como definir o ficheiro de configuração do Activation Engine através da utilização de etiquetas XML.

## **Ficheiro de configuração**

Utilize o seguinte exemplo do ficheiro de configuração para obter mais informações sobre as 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 o ficheiro de configuração

As etiquetas XML são utilizadas no ficheiro de configuração do Activation Engine para definir valores específicos para vários atributos. É possível definir manualmente estes valores no ficheiro de configuração do Activation Engine. Utilize a seguinte tabela para visualizar uma descrição de cada etiqueta e respectivos valores permitidos:

Tabela 9. Etiquetas XML			
Etiquetas	Descrição	Valores aceitáveis	Notas
ConfigurationVersion	Elemento requerido que define a versão da configuração a utilizar.	<b>2.0</b>	
LicenseAgreement	Elemento requerido que apresenta o acordo de licença da Dispositivo virtual da HMC.		
AcceptLicense	Elemento requerido para aceitar o acordo de licença da Dispositivo virtual da HMC.	<ul style="list-style-type: none"> <li>• <b>Sim (Yes):</b> Aceita o acordo de licença da HMC.</li> <li>• <b>Não (No):</b> Pede ao Utilizador para Aceitar o Acordo de Licença da HMC</li> </ul>	Caso seja introduzido um valor não válido, o Activation Engine utilizará a predefinição de <b>Não (No)</b> .
Locale	Elemento requerido para definir definições de locale.	<b>en_US.UTF-8</b>	Caso seja introduzido um valor não válido, o Activation Engine utilizará a predefinição de <b>US</b> .
SetupWizard	Elemento requerido para activar ou desactivar o assistente de <b>Configuração da HMC (HMC Setup)</b> .	<ul style="list-style-type: none"> <li>• <b>Sim (Yes):</b> Apresenta o assistente de <b>Configuração da HMC (HMC Setup)</b>.</li> <li>• <b>Não (No):</b> Desactiva o assistente de <b>Configuração da (HMC Setup)</b>.</li> </ul>	Caso seja introduzido um valor não válido, o Activation Engine utilizará a predefinição de <b>Sim (Yes)</b> .

Tabela 9. Etiquetas XML (continuação)

Etiquetas	Descrição	Valores aceitáveis	Notas
SetupCallHomeWizard	Elemento requerido para activar ou desactivar o assistente de <b>Chamada de Assistência da HMC (HMC Call Home)</b> .	<ul style="list-style-type: none"> <li>• <b>Sim (Yes)</b>: Apresenta o assistente de <b>Chamada de Assistência da HMC (HMC Call Home)</b>.</li> <li>• <b>Não (No)</b>: Desactiva a apresentação do assistente de <b>Chamada de Assistência da HMC (HMC Call Home)</b>.</li> </ul>	Caso seja introduzido um valor não válido, o Activation Engine utilizará a predefinição de <b>Sim (Yes)</b> .
SetupKeyboard	Elemento requerido para definir a configuração do teclado.	<ul style="list-style-type: none"> <li>• <b>Sim (Yes)</b>: Pede ao utilizador a configuração do teclado.</li> <li>• <b>Não (No)</b>: Aceita a configuração predefinida do teclado (US).</li> </ul>	Caso seja introduzido um valor não válido, o Activation Engine utilizará a predefinição de <b>Sim (Yes)</b> .
SetupDisplay	Elemento requerido para activar ou desactivar a configuração da apresentação.	<ul style="list-style-type: none"> <li>• <b>Sim (Yes)</b>: Pede ao utilizador a configuração da apresentação.</li> <li>• <b>Não (No)</b>: Aceita a configuração predefinida da apresentação.</li> </ul>	Caso seja introduzido um valor não válido, o Activation Engine utilizará a predefinição de <b>Sim (Yes)</b> .
Ethernet	Elemento requerido que detém valores para configurações de adaptadores de Ethernet. É possível configurar um máximo de quatro adaptadores de Ethernet.	<p><b>Activar (Enable):</b></p> <ul style="list-style-type: none"> <li>• <b>Sim (Yes)</b>: Configurar este adaptador.</li> <li>• <b>Não (No)</b>: Não configurar este adaptador.</li> </ul> <p><b>DefaultGatewayDevice:</b></p> <ul style="list-style-type: none"> <li>• <b>Sim (Yes)</b>: Configurar este adaptador como o adaptador de rede principal.</li> <li>• <b>Não (No)</b>: Não configurar este adaptador como o adaptador de rede principal.</li> </ul> <p><b>PrivateInterface:</b></p> <ul style="list-style-type: none"> <li>• <b>Sim (Yes)</b>: Configurar este adaptador como uma interface privada. <b>Sim (Yes)</b> é requerido para configurar a interface como um Servidor de DHCP IPv4.</li> <li>• <b>Não (No)</b>: Não configurar este adaptador como uma interface privada. <b>Não (No)</b> é requerido para configurar a interface como um tipo estático de IPv4.</li> </ul>	O Activation Engine executará a configuração predefinida caso sejam introduzidos quaisquer valores não válidos dentro da secção do adaptador de Ethernet ou caso sejam definidos múltiplos <b>Dispositivos de Porta de Ligação Predefinidos (Default Gateway Devices)</b> . É possível omitir elementos opcionais da configuração. É necessária pelo menos uma configuração IPV4 ou IPV6. Caso não especifique uma configuração de IP, o Activation Engine utilizará a configuração predefinida.

Tabela 9. Etiquetas XML (continuação)

Etiquetas	Descrição	Valores aceitáveis	Notas
HostName	Elemento opcional para definir o nome do sistema central da rede.	Qualquer cadeia válida de nome do sistema central.	Caso o elemento não seja definido, o Activation Engine utilizará o valor <b>HostName</b> do sistema central local predefinido.
Domain	Elemento opcional para definir o domínio de rede.	Qualquer valor de domínio válido (por exemplo, <b>exemplo.pt.com</b> ).	Caso o elemento não seja definido, o Activation Engine utilizará o valor <b>Domínio (Domain)</b> vazio predefinido.
DNSServers	Elemento opcional para definir os servidores de DNS da rede.	É aceitável possuir um valor de Servidor de DNS ou até três endereços IPv4 ou IPv6 separados por uma vírgula. <ul style="list-style-type: none"> <li>Exemplo 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888</li> <li>Exemplo 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844</li> <li>Exemplo 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</li> </ul>	Caso o elemento não seja definido, o Activation Engine utilizará o valor <b>DNSServers</b> vazio predefinido.

Tabela 9. Etiquetas XML (continuação)

Etiquetas	Descrição	Valores aceitáveis	Notas
IP4Config	Elemento opcional para definir definições de configuração de IPv4.	<p><b>IPType:</b> Elemento requerido para definir o tipo de configuração de IPv4.</p> <ul style="list-style-type: none"> <li>• <b>Estática (Static):</b> Configurar este adaptador através da utilização da configuração estática.</li> <li>• <b>DHCP:</b> Configurar este adaptador através da utilização da configuração de DHCP.</li> <li>• <b>DHCPServer:</b> Configurar este adaptador para ser um servidor de DHCP IPv4 (requer que <b>PrivateInterface</b> seja definido para <b>Sim (Yes)</b>).</li> </ul> <p><b>IPAddress:</b> Elemento opcional que apenas é requerido caso seja seleccionada a configuração <b>Estática (Static)</b> ou <b>DHCPServer</b>.</p> <ul style="list-style-type: none"> <li>• <b>Configuração Estática (Static Configuration):</b> Qualquer valor válido do endereço IPv4.</li> <li>• <b>Configuração DHCPServer (DHCPServer Configuration):</b> Qualquer IP de servidor DHCP dentro do intervalo de IP.</li> </ul> <p><b>Máscara de rede (Netmask):</b> Elemento opcional que apenas é requerido caso seja seleccionada a configuração <b>Estática (Static)</b>.</p> <ul style="list-style-type: none"> <li>• Qualquer valor válido de máscara de rede IPv4.</li> </ul> <p><b>Porta de Ligação (Gateway):</b> Elemento opcional que apenas é requerido caso seja seleccionada a configuração <b>Estática (Static)</b>.</p> <ul style="list-style-type: none"> <li>• Qualquer valor válido de máscara de rede IPv4.</li> </ul>	

Tabela 9. Etiquetas XML (continuação)

Etiquetas	Descrição	Valores aceitáveis	Notas
IP6Config	Elemento opcional para definir definições de configuração de IPv6.	<p><b>IPType:</b> Elemento requerido para definir o tipo de configuração de IPv6.</p> <ul style="list-style-type: none"> <li>• <b>Estática (Static):</b> Configurar este adaptador através da utilização da configuração estática.</li> <li>• <b>DHCP:</b> Configurar este adaptador através da utilização da configuração de DHCP.</li> </ul> <p><b>IPAddress:</b> É aceitável possuir um formato de IPv6 de forma longa ou abreviada e um prefixo de IPv6 de forma longa ou abreviada.</p> <ul style="list-style-type: none"> <li>• Exemplo 1: IPv6: 2001:4860:4860:0000:0000:0000:8888</li> <li>• Exemplo 2: IPv6: 2001:4860:4860::8888</li> <li>• Exemplo 3: IPv6: 2001:4860:4860::8888/128</li> </ul> <p>Caso não seja especificado qualquer prefixo, o Activation Engine utilizará a predefinição do prefixo /64.</p> <p><b>Porta de Ligação (Gateway):</b></p> <ul style="list-style-type: none"> <li>• Qualquer valor válido de endereço IPv6.</li> </ul>	

Tabela 9. Etiquetas XML (continuação)

Etiquetas	Descrição	Valores aceitáveis	Notas
Firewall	Elemento opcional para definir as definições de firewall.	<p><b>PEGASUS:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas PEGASUS sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas PEGASUS.</li> </ul> <p><b>RPD:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas RMC seja abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas RMC.</li> </ul> <p><b>FCS:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas FCS sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas FCS.</li> </ul> <p><b>I5250:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas 5250 sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas 5250.</li> </ul> <p><b>PING:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que a porta Ping seja aberta.</li> <li>• <b>Desactivado:</b> Desactiva a porta Ping.</li> </ul> <p><b>L2TP:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas L2TP sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas L2TP.</li> </ul> <p><b>SLP:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas SLP sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas SLP.</li> </ul> <p><b>RSCT:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas RSCT sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas RSCT.</li> </ul> <p><b>SECUREREMOTEACCESS:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas de acesso remoto seguro sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas de acesso remoto seguro.</li> </ul> <p><b>SSH:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que a porta SSH seja aberta.</li> <li>• <b>Desactivado:</b> Desactiva a porta SSH.</li> </ul>	

Tabela 9. Etiquetas XML (continuação)

Etiquetas	Descrição	Valores aceitáveis	Notas
Firewall	Elemento opcional para definir as definições de firewall.	<p><b>NTP:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas NTP sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas NTP.</li> </ul> <p><b>SNMPTraps:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas SNMP traps sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas SNMP traps.</li> </ul> <p><b>SNMPAgents:</b></p> <ul style="list-style-type: none"> <li>• <b>Activado:</b> Permite que as portas SNMP agents sejam abertas.</li> <li>• <b>Desactivado:</b> Desactiva as portas Disables SNMP.</li> </ul>	
NTPServers	A etiqueta <b>NTPServers</b> será necessária caso pretenda configurar até cinco servidores NTP dentro de uma Dispositivo virtual da HMC.	<p><b>NTPServers:</b> Aceita &lt;ntpparam ntpserver="server" ntpversion="version"/&gt;</p> <p><b>ntpparam:</b></p> <ul style="list-style-type: none"> <li>• <b>ntpserver:</b> Aceita quaisquer valores válidos de IPv4 ou IPv6 e nomes do sistema central válidos.</li> <li>• <b>ntpversion:</b> Aceita o valor numérico 1-4</li> </ul> <p>Exemplo:</p> <pre>&lt;NTPServers&gt;   &lt;ntpparam     ntpserver="test.austin.ibm.com"     ntpversion="2"/&gt;   &lt;ntpparam     ntpserver="192.168.34.1"     ntpversion="4"/&gt;   &lt;ntpparam     ntpserver="::ffff:903:201"     ntpversion="3"/&gt; &lt;/NTPServers&gt;</pre>	

## Configurar a HMC

Saiba como configurar as ligações de rede, configurar a HMC, concluir passos de pós-configuração e actualizar e renovar a HMC.

### Seleção de definições de rede na HMC

Obtenha informações sobre as definições de rede que poderá utilizar na Consola de Gestão de Hardware (HMC, Hardware Management Console).

### Ligações de rede da HMC

Saiba como é possível utilizar a Consola de Gestão de Hardware HMC numa rede.

Pode utilizar diferentes tipos de ligações de rede para ligar a HMC aos sistemas geridos. Para mais informações sobre como configurar a HMC para ligar a uma rede, consulte [“Configurar a HMC”](#) na página 69. Para obter mais informações sobre como utilizar a HMC numa rede, consulte as seguintes informações:

### **Tipos de ligações de rede da HMC**

Saiba como utilizar a gestão remota e funções de assistência da HMC ao utilizar a rede.

A HMC suporta os seguintes tipos de comunicações lógicas:

#### **HMC para o sistema gerido**

Utilizado para executar a maioria das funções de gestão de hardware, nas quais a HMC envia pedidos de função de controlo através do processador de serviço do sistema gerido. A ligação entre a HMC e o processador de serviço é por vezes referido como a *rede de serviço*. Esta ligação é necessária para gestão do sistema gerido.

#### **HMC para a partição lógica**

Utilizado para recolher informações relacionadas com plataformas (eventos de erros de hardware, inventário de hardware) de sistemas operativos que estão a executar em partições lógicas e para coordenar certas actividades de plataforma (LPAR dinâmica, reparação simultânea) com esses sistemas operativos. Se pretende utilizar componentes de notificação de assistência e erro, deve criar esta ligação.

#### **HMC para o BMC**

**Nota:** A ligação do Controlador de Gestão de Placas de Sistema (BMC, baseboard management controller) é aplicável apenas ao modelo 7063-CR1 da HMC.

Utilizado para executar tarefas de assistência e manutenção. A ligação BMC é utilizada para carregar e manter o software proprietário da HMC no sistema. Esta ligação é requerida para aceder ao BMC na HMC.

#### **HMC para utilizadores remotos**

Fornece aos utilizadores remotos acesso a funções da HMC. Os utilizadores remotos podem aceder à HMC nos seguintes modos:

- Ao utilizar o navegador da Web para aceder a todas as funções GUI da HMC remotamente.
- Ao utilizar a SSH (Secure Socket Shell) para aceder a funções da linha de comandos da HMC remotamente.
- Ao utilizar um servidor de terminal virtual para acesso remoto a consolas de partições lógicas virtuais.

#### **HMC para a assistência e suporte**

Utilizado para transmitir dados, tal como relatórios de erro no hardware, inventário de dados e actualizações de microcódigo, de e a partir do fornecedor de serviços. Pode utilizar este caminho de comunicações para efectuar chamadas de assistência automáticas.

A HMC suporta até quatro interfaces físicas de Ethernet diferentes, dependendo do modelo. A versão autónoma da HMC suporta apenas três interfaces da HMC, ao utilizar um adaptador Ethernet integrado e até dois adaptadores de suplemento. Utilize cada uma destas interfaces do seguinte modo:

- Uma interface de rede pode ser utilizada exclusivamente para comunicações da HMC para o sistema gerido, o que significa que apenas a HMC e os processadores de assistência dos sistemas geridos se encontram nessa rede. Uma ou mais interfaces podem ser utilizadas exclusivamente para comunicações entre a HMC e sistemas geridos, o que significa que apenas a HMC e os processadores de serviço dos sistemas geridos estão nessa rede. Embora as interfaces de rede dos processadores de assistência estejam codificadas para o Protocolo Secure Sockets Layer (SSL) e protegidas por palavra-passe, ter uma rede dedicada em separado poderá fornecer um nível de segurança mais elevado a estas interfaces.
- Uma interface de rede aberta será normalmente utilizada para a ligação de rede entre a HMC e as partições lógicas nos sistemas geridos, para as comunicações entre a HMC e as partições lógicas. Pode igualmente utilizar esta interface de rede aberta para gerir a HMC remotamente.

- Opcionalmente, pode utilizar uma terceira interface para ligar a partições lógicas e gerir a HMC remotamente. Esta interface pode ser igualmente utilizada como uma diferente ligação da HMC a diferentes grupos de partições lógicas. Por exemplo, o utilizador poderá pretender ter uma LAN administrativa separada da LAN em que estão a ser executadas todas as transacções comerciais normais. Administradores remotos podem aceder à HMC e a outras unidades geridas ao utilizar este método. Por vezes, as partições lógicas encontram-se em diferentes domínios de segurança de Rede, talvez por trás de uma firewall e pode ser conveniente ter diferentes ligações de rede da HMC a cada um dos dois domínios.

## Requisitos do navegador da web para a HMC

A Consola de Gestão de Hardware (HMC, Hardware Management Console) versão 9.1.0 é suportada pelo Google Chrome versão 57, Microsoft Internet Explorer (IE) versão 11.0, Mozilla Firefox versões 45 e 52 Extended Support Release (ESR) e Safari versão 10.1.

Caso o navegador do utilizador esteja configurado para utilizar um proxy da Internet, um endereço de IP local deve ser incluído na lista de excepções. Consulte o administrador de redes para obter mais informações sobre a lista de excepções. Se ainda precisar de utilizar o proxy para aceder à HMC, active a opção Utilizar HTTP 1.1 através de ligações proxy no separador Avançadas na janela Opções de Internet.

Os cookies de sessão têm de estar activados para que a ASMI funcione quando ligada remotamente à HMC. O código de proxy asm guarda informações de sessão e utiliza-as. Siga os passos para activar os cookies da sessão.

Activar os cookies da sessão no Internet Explorer.

1. Seleccione Ferramentas (Tools) e faça clique em Opções de Internet (Internet Options)
2. Seleccione Privacidade (Privacy) e faça clique em Avançadas (Advanced)
3. Certifique-se de que a caixa de verificação Permitir cookies de sessão sempre (Always allow session cookies) está marcada. Caso não esteja, seleccione Ignorar a manipulação automática de cookies (Override automatic cookie handling) e Permitir cookies de sessão sempre (Always allow session cookies).
4. Seleccione o pedido de confirmação em Cookies originais (First-party Cookies) e Cookies de terceiros (Third-party Cookies)
5. Faça clique em OK.

Activar cookies de sessão no Firefox.

1. Seleccione Ferramentas (Tools) e faça clique em Opções (Options)
2. Faça clique em Cookies
3. Seleccione Permitir que os sítios definam cookies (Allow sites to set cookies).
4. Seleccione Excepções (Exceptions) e adicione HMC.
5. Faça clique em OK.

### *Redes privadas e abertas no ambiente da HMC*

É possível configurar a Consola de Gestão de Hardware (HMC, Hardware Management Console) para utilizar redes abertas e privadas. As redes privadas permitem a utilização de um intervalo seleccionado de endereços de IP não encaminháveis. Uma rede *pública* (*public*) ou "aberta" descreve a ligação de rede entre a HMC para quaisquer partições lógicas e para outros sistemas na rede regular.

## Redes privadas

Os únicos dispositivos na rede privada da HMC são a própria HMC e cada um dos sistemas geridos a que essa HMC se encontra ligada. A HMC encontra-se ligada ao FSP (Flexible Service Processor) de cada sistema gerido.

Na maioria dos sistemas, o FSP faculta duas portas de Ethernet identificadas como **HMC1** e **HMC2**. Tal permite ao utilizador ligar até duas HMCs.

Alguns sistemas têm uma opção de FSP dupla. Neste situação, o segundo FSP age como uma cópia de segurança redundante. Os requisitos de configuração básicos para um sistema com dois FSPs são essencialmente os mesmos que de um sistema sem um segundo FSP. A HMC tem de estar ligada a cada FSP e, como tal, é necessário mais hardware de rede (por exemplo, um comutador ou concentrador de rede local) quando existe mais de um FSP ou múltiplos sistemas geridos.

**Nota:** Cada porta de FSP no sistema gerido só pode ser ligada a uma HMC.

## Redes públicas

É possível ligar a rede aberta a uma firewall ou encaminhador para ligar à Internet. A ligação à Internet permite à HMC efectuar uma comunicação de retorno quando é necessário comunicar quaisquer erros de hardware.

A própria HMC fornece a sua própria firewall em cada uma das suas interfaces de rede. É automaticamente configurada uma firewall básica quando executa o Assistente de Instalação Assistida da HMC, mas deve personalizar as definições da firewall após a instalação e configuração iniciais da HMC.

### *A HMC como servidor de DHCP*

É possível utilizar a Consola de Gestão de Hardware (HMC) como um servidor de DHCP (Dynamic Host Configuration Protocol).

Se pretender configurar a primeira interface de rede como rede privada, pode optar entre um intervalo de endereços de IP para o servidor de DHCP atribuir aos respectivos clientes. Os intervalos de endereços seleccionáveis incluem segmentos dos intervalos de endereços de IP não encaminháveis padrão.

Para além destes intervalos padrão, existe um intervalo especial de endereços de IP reservado a endereços de IP. É possível utilizar este intervalo especial para evitar conflitos em casos onde as redes abertas ligadas da HMC estão a utilizar um dos intervalos de endereços não encaminháveis. Com base no intervalo seleccionado, o primeiro endereço de IP desse intervalo é automaticamente atribuído à interface de rede da HMC na rede privada e os endereços do resto do intervalo são então atribuídos aos processadores de serviço.

O servidor de DHCP na HMC utiliza a atribuição automática, o que significa que o mesmo endereço de IP é atribuído a cada interface de Ethernet do processador de serviço única de cada vez que esta é iniciada. Cada interface de Ethernet possui um identificador exclusivo baseado num endereço de Controlo de Acesso de Suportes (MAC, Media Access Control) incorporado, o que permite ao servidor de DHCP voltar a atribuir os mesmos parâmetros de IP. Pode configurar as portas HMC **eth0** e **eth1** para servirem endereços de DHCP. Pode configurar as portas HMC **eth0** e **eth1** para servirem endereços de DHCP.

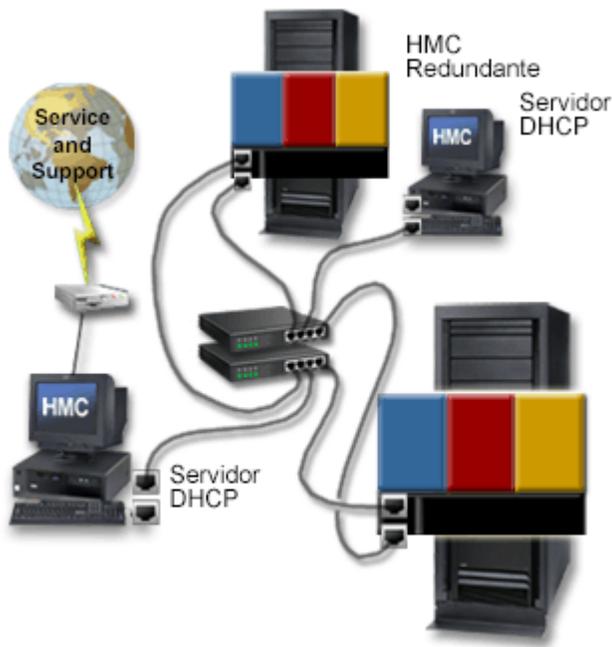
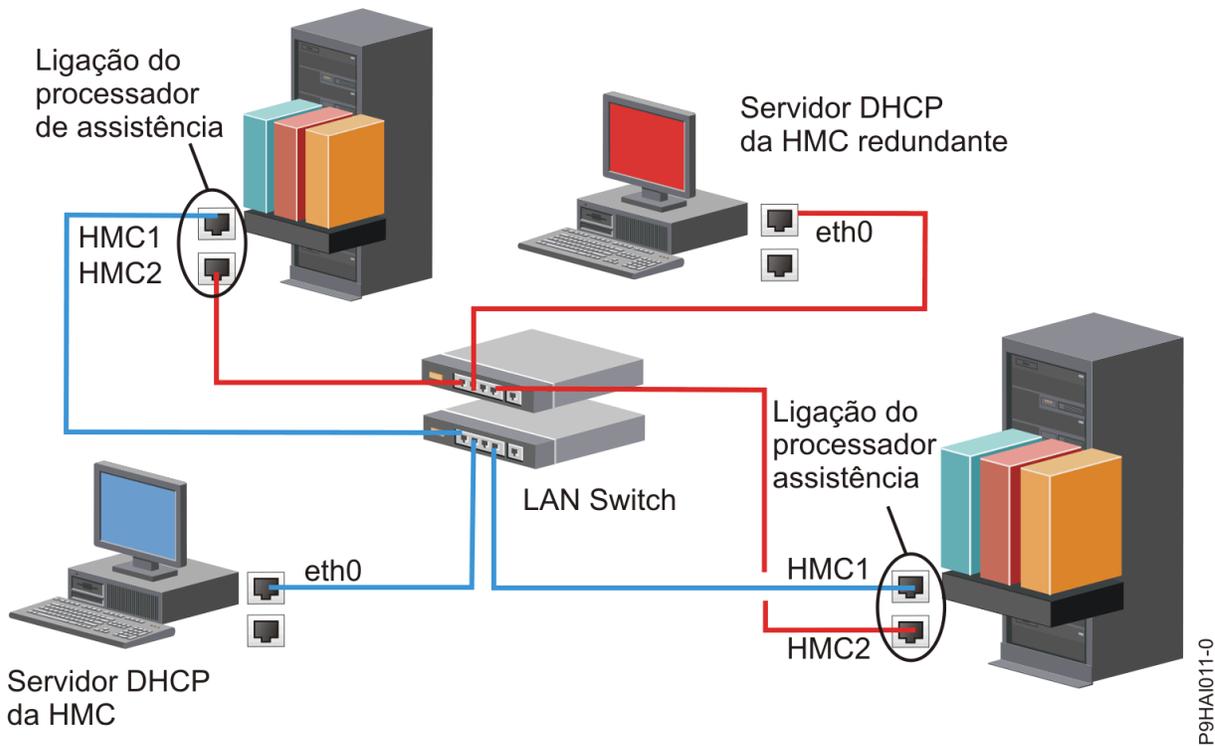


Figura 25. Rede privada com uma HMC como servidor de DHCP

**Nota:** Se estiver a usar IPv6, o processo de identificação tem de ser feito manualmente. Para IPv6, a identificação automática não se encontra disponível.

Para obter mais informações sobre como configurar a HMC como um servidor de DHCP, consulte [“Configurar a HMC como um servidor de DHCP”](#) na página 78.



Esta figura apresenta um ambiente redundante da HMC com dois sistemas geridos. A primeira HMC está ligada à primeira porta em cada FSP e a HMC redundante está ligada à segunda porta em cada HMC. Cada HMC está configurada como um servidor de DHCP através da utilização de um intervalo diferente de

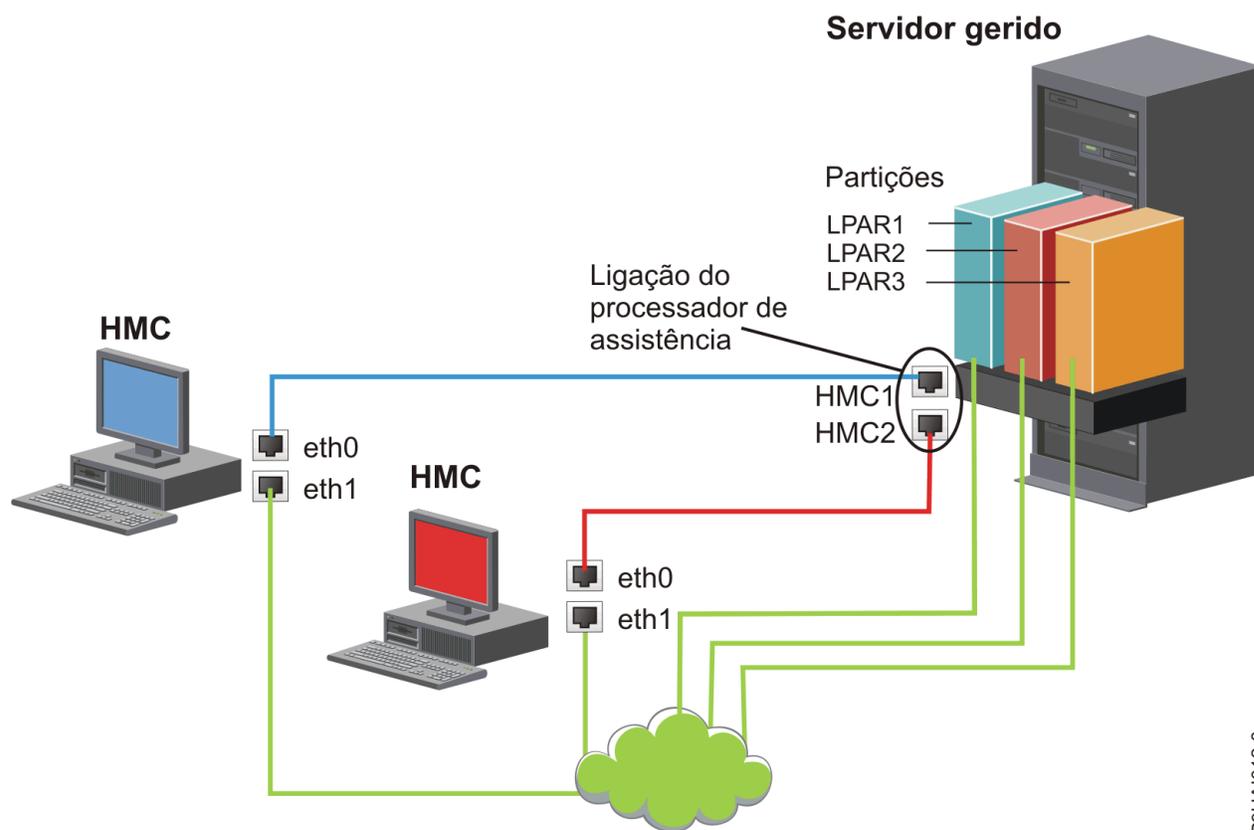
P9HA1011-0

endereços de IP. As ligações encontram-se em redes privadas separadas. Desta forma, é importante garantir que nenhuma porta de FSP está ligada a mais do que uma HMC.

Cada porta de FSP do sistema gerido que está ligada a uma HMC requer um endereço de IP exclusivo. Para garantir que cada FSP detém um endereço de IP exclusivo, utilize a capacidade do servidor de DHCP incorporado. Quando o FSP detecta a ligação de rede activa, envia um pedido de difusão para localizar um servidor de DHCP. Quando correctamente configurada, a HMC responde a esse pedido atribuindo um de um intervalo de endereços seleccionado.

Se tiver múltiplos FSPs, tem de ter o seu próprio concentrador ou comutador LAN para a rede privada da HMC para FSP. Alternadamente, este segmento privado pode existir como várias portas numa LAN virtual privada (VLAN) num comutador com maiores capacidades de gestão. Caso possua múltiplas VLANs privadas, será necessário garantir que estão isoladas e sem qualquer tráfego de cruzamento.

Se tiver mais do que uma HMC, é necessário também ligar cada HMC às partições lógicas e umas às outras, na mesma rede aberta.



Esta figura mostra duas HMCs ligadas a um único servidor gerido na rede privada e a três partições lógicas na rede pública. É possível possuir um adaptador de Ethernet adicional para que a HMC possua três interfaces de rede. É possível utilizar esta terceira rede como uma rede de gestão ou ligá-la ao Servidor de Gestão de CSM (Cluster Systems Manager).

### ***Decidir que método de conectividade utilizar para o servidor de comunicação de retorno***

Saiba mais sobre as opções de conectividade disponíveis através da utilização do servidor de comunicação de retorno.

É possível configurar a Consola de Gestão de Hardware (HMC, Hardware Management Console) para enviar informações relacionadas com assistência de hardware para a IBM através da utilização de uma ligação à Internet baseada em rede local ou uma ligação de acesso telefónico através de um modem.

Possui duas opções de comunicação quando configura a ligação à Internet baseada em rede local. A primeira opção é utilizar o Secure Sockets Layer (SSL) padrão. É possível activar a comunicação SSL para

ligar à Internet através do servidor proxy. A conectividade SSL é mais provável que esteja em conformidade com as directrizes de segurança da empresa.

**Nota:** Caso a ligação de rede aberta utilize apenas o Protocolo da Internet Versão 6 (IPv6), não será possível utilizar a VPN da Internet para estabelecer ligação ao suporte. Para obter mais informações sobre os protocolos utilizados, consulte [“Escolher um Protocolo de Internet”](#) na página 59.

As vantagens de utilizar uma ligação à Internet poderão incluir:

- Velocidade de transmissão mais rápida
- Custos do cliente reduzidos (por exemplo, o custo de uma linha de telefone analógica dedicada)
- Maior fiabilidade

As características de segurança que se seguem estão activas, independentemente do método de conectividade escolhido:

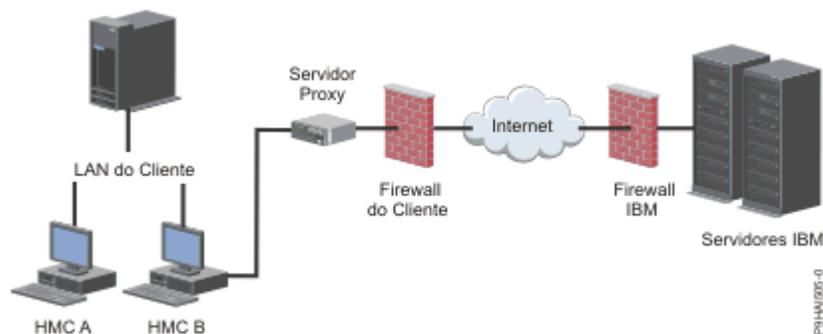
- Os pedidos de Função de Suporte Remoto são sempre iniciados na HMC para a IBM. Uma ligação de recepção nunca é iniciada a partir do Sistema de Suporte de Assistência IBM.
- Todos os dados que são transferidos entre a HMC e o Sistema de Suporte de Assistência da IBM são codificados através da utilização de uma codificação de alto nível. Dependendo do método de conectividade que é seleccionado, são encriptados através da utilização de SSL ou IPsec Encapsulating Security Payload (ESP).
- Quando inicializa a ligação codificada, a HMC autentica o alvo de destino como o Sistema de Suporte de Assistência da IBM.

Os dados enviados para o Sistema de Suporte de Assistência IBM consistem apenas em informações sobre problemas de hardware e configuração. Não são transmitidos dados da aplicação ou do cliente para a IBM.

## Utilizar uma ligação à Internet indirecta com um servidor proxy

Caso a instalação requiera que a HMC se encontre numa rede privada, poderá conseguir estabelecer ligação à Internet indirectamente através da utilização de um proxy SSL, que poderá encaminhar pedidos para a Internet. Uma das outras potenciais vantagens de utilizar um proxy SSL é que o proxy pode suportar utilitários de registo e de auditoria.

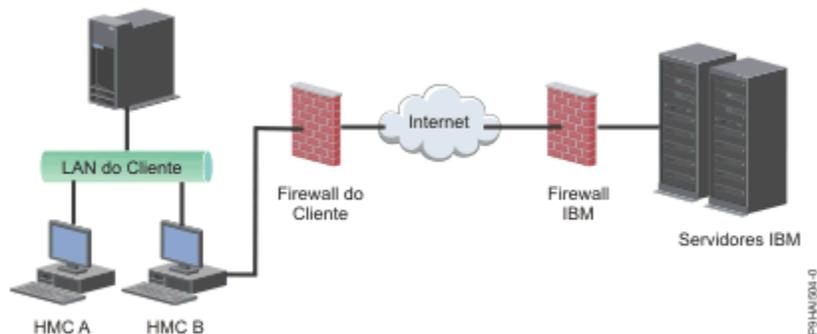
Para reencaminhar sockets SSL, o servidor proxy deve suportar as funções de cabeçalho proxy básicas (como descrito em RFC 2616) e o método LIGAR (CONNECT). Opcionalmente, é possível configurar a autenticação de proxy básica (RFC 2617) de forma a que a HMC autentique antes de tentar encaminhar sockets através do servidor proxy.



Para que a HMC comunique com sucesso, o servidor proxy do cliente tem de permitir ligações à porta 443. Pode configurar o servidor proxy para limitar os endereços de IP específicos aos quais a HMC pode ligar. Consulte o tópico [“Listas de endereços Internet SSL”](#) na página 59 para uma lista de endereços de IP.

## Utilizar uma ligação à Internet SSL directa

Caso seja possível ligar a HMC à Internet e configurar a firewall externa para permitir que pacotes TCP estabelecidos saiam para os destinos descritos em [“Listas de endereços Internet SSL”](#) na página 59, poderá utilizar uma ligação à Internet directa.



## Utilizar Internet SSL para ligar ao suporte remoto

Todas as comunicações são processadas através de sockets de TCP iniciados pela Consola de Gestão de Hardware (HMC, Hardware Management Console) e utilizam um SSL de alto nível para codificar os dados transmitidos. Os endereços de TCP/IP de destino são publicados (consultar [“Listas de endereços Internet SSL”](#) na página 59) para que as firewalls externas possam ser configuradas para permitir estas ligações.

**Nota:** A porta padrão 443 de HTTPS é utilizada para todas as comunicações.

É possível activar a HMC para ligar directamente à Internet ou para ligar indirectamente a partir de um servidor proxy facultado pelo cliente. A decisão sobre qual abordagem é a melhor para a instalação depende da segurança e requisitos de rede da empresa. A HMC (directamente ou através do proxy de SSL) utiliza os seguintes endereços quando é configurada para utilizar a conectividade de Internet SSL.

## Escolher um Protocolo de Internet

Determine a versão do endereço de IP utilizada quando a Consola de Gestão de Hardware (HMC, Hardware Management Console) estabelece ligação ao fornecedor de serviços.

A maior parte dos utilizadores usa o Protocolo de Internet Versão 4 (IPv4) para estabelecer ligação com o fornecedor de serviços de assistência. Os endereços IPv4 surgem no formato que representa os 4 bytes do endereço de IPv4, que está separado por pontos (por exemplo, 9.60.12.123) para aceder à Internet. Pode igualmente usar o Protocolo de Internet Versão 6 (IPv6) para estabelecer ligação com o fornecedor de serviços de assistência. A IPv6 é normalmente utilizada por administradores de rede de forma a garantir um espaço de endereço único. Se não tem a certeza de qual é o Protocolo de Internet utilizado pela instalação, contacte o seu administrador de rede. Para obter mais informações sobre a utilização de cada versão, consulte [“Definir o endereço de IPv4”](#) na página 79 e [“Definir o endereço de IPv6”](#) na página 79.

## Listas de endereços Internet SSL

Saiba mais sobre os endereços que a Consola de Gestão de Hardware (HMC, Hardware Management Console) utiliza quando a HMC está a utilizar conectividade de Internet SSL.

A HMC utiliza os seguintes endereços de IPv4 para contactar a assistência e suporte da IBM quando está configurada para utilizar a conectividade de Internet SSL.

Os endereços de IPv4 que se seguem são para todos os locais:

- 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

Os endereços de IPv4 que se seguem são para todo o continente americano:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Os endereços de IPv4 que se seguem são para todos os locais, excepto os do continente americano:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

**Nota:** Quando configurar a firewall para permitir que uma HMC estabeleça ligação a estes servidores, apenas serão requeridos os endereços de IP específicos da região geográfica.

A HMC utiliza os seguintes endereços de IPv6 para contactar a assistência e suporte da IBM quando está configurada para utilizar a conectividade de Internet SSL.

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

### ***Utilizar múltiplos servidores de comunicação de retorno***

Saiba o que tem de fazer quando decide utilizar mais de um servidor de comunicação de retorno.

Para evitar um ponto único de falha, configure a Consola de Gestão de Hardware (HMC, Hardware Management Console) para utilizar múltiplos servidores de comunicação de retorno. O primeiro servidor de comunicação de retorno disponível tenta processar cada evento de assistência. Caso a ligação ou transmissão falhe com este servidor de comunicação de retorno, o pedido de assistência é obtido através da utilização dos outros servidores de comunicação de retorno disponíveis até um ter êxito ou até ter tentado utilizar todos os servidores.

A HMC ligada que é identificada pela análise de problemas como sendo a consola de análise principal para um determinado sistema gerido que comunica o problema. Este consola principal também replica o relatório do problema para qualquer HMC secundária. A HMC principal tem de reconhecer a HMC secundária na rede. Uma HMC secundária é reconhecida pela HMC principal como um servidor de comunicação de retorno adicional quando:

- A HMC principal é configurada para utilizar servidores de comunicação de retorno "identificados" e o servidor de comunicação de retorno se encontra na mesma sub-rede que a HMC principal ou gere o mesmo sistema.
- O servidor de comunicação de retorno é adicionado manualmente à lista de consolas de servidor de comunicação de retorno disponíveis para conectividade de transmissão.

## **Preparar a configuração da HMC**

Obtenha informações sobre as definições de configuração requeridas que necessita de saber antes de iniciar os passos de configuração.

Para configurar a HMC, tem de compreender os conceitos relacionados, tomar decisões e preparar informações.

Saiba sobre as informações de que necessita para ligar a HMC às seguintes localizações:

- Processadores de serviço nos seus sistemas geridos

- Partições lógicas nesses sistemas geridos
- Estações de trabalho remotas
- Assistência da IBM para implementar as funções de “comunicação de retorno”

Para preparar para a configuração da HMC, conclua os seguintes passos:

1. Obtenha e instale o último nível da versão do código HMC que pretende instalar.
2. Determine a localização física da HMC em relação aos servidores que gere. Se a HMC estiver a mais de 7,5 metros de distância do sistema gerido, deve fornecer acesso de navegador da Web à HMC a partir da localização do sistema gerido para que o pessoal de assistência possa aceder à HMC.
3. Identifique os servidores que a HMC gere.
4. Determine se utiliza uma rede privada ou aberta para gerir servidores. Se decidir utilizar uma rede privada, utilize DHCP, excepto se estiver a utilizar uma configuração Cluster Systems Management (CSM). Esta CSM não suporta IPv6. Para aceder à CSM, tem de ter duas redes. Para mais informação sobre CSM, consulte a documentação que foi fornecida com esse componente. Para mais informação sobre redes privadas e abertas, consulte [“Seleccionar uma rede privada ou aberta”](#) na página 77.
5. Caso utilize uma rede aberta para gerir um FSP, será necessário definir manualmente o endereço do FSP através dos menus da Interface de Gestão de Sistemas Avançada. É recomendada uma rede privada, não encaminhável.
6. Se tiver duas HMCs, indique qual é a HMC principal e qual é a secundária. A HMC principal necessita de estar fisicamente mais próxima do sistema e tem de ser a HMC que se encontra configurada para efectuar a comunicação de retorno.
7. Determine as definições de rede necessárias para ligar a HMC a estações de trabalho remotas, partições lógicas e dispositivos de rede.
8. Defina como a HMC efectua a comunicação de retorno. As opções de comunicação de retorno incluem uma ligação à Internet de SSL (Secure Socket Layer) apenas de saída, um modem ou uma ligação de Rede Privada Virtual (VPN, Virtual Private Network).
9. Determine os utilizadores da HMC que irá criar e respectivas palavras-passe, bem como as funções que lhes são atribuídas. É necessário atribuir uma palavra-passe aos utilizadores **hscroot** e **hscpe**.
10. Documente as seguintes informações de contacto da empresa necessárias quando configurar a chamada de retorno:
  - Nome da empresa
  - Contacto do administrador
  - Endereço de correio electrónico
  - Números de telefone
  - Números de fax
  - O endereço postal da localização física da HMC
11. Caso planeie utilizar o correio electrónico para notificar operadores ou administradores do sistema quando forem enviadas informações para a Assistência da IBM através da comunicação de retorno, identifique o servidor de Protocolo Simples para Transferência de Correio (SMTP, Simple Mail Transfer Protocol) e os endereços de correio electrónico que utilizar.
12. Tem de definir as seguintes palavras-passe:
  - A palavra-passe de acesso que é utilizada para autenticar a HMC para o FSP.
  - A palavra-passe da ASMI que é utilizada para o utilizador **admin**.
  - A palavra-passe da ASMI que é utilizada para o utilizador **general**.

Crie as palavras-passe quando ligar a partir da HMC a um novo servidor pela primeira vez. Caso a HMC seja redundante ou uma segunda HMC, obtenha a palavra-passe de Utilizador da HMC e esteja preparado para introduzir a mesma quando ligar pela primeira vez ao FSP do servidor gerido.

Quando concluir estes passos de preparação, conclua o [“Esquema de configuração da pré-instalação para a HMC”](#) na página 62.

## Esquema de configuração da pré-instalação para a HMC

Utilize esta folha de trabalho para ter a informação de instalação de que necessita para a instalação.

### Política de palavra-passe melhorada para HMC

Tem que definir uma nova palavra-passe na primeira utilização de um sistema novo com a HMC versão 9.940.0, ou posterior e após uma reposição de fábrica do sistema. Esta alteração de política ajudar a garantir que a HMC não fica numa situação em que a palavra-passe é conhecida.

Com a HMC Versão 9.940.0, e posteriores, a palavra-passe `hscroot` está expirada e tem que ser alterada antes de poder aceder às funções da HMC. Para obter mais informações sobre como alterar a palavra-passe, consulte [https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6\\_useridsandpassword.htm](https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm). No entanto, se estiver a actualizar a partir de um nível anterior da HMC ou de uma instalação funcional, não tem que alterar a palavra-passe.

### Definições de Rede

Interface da rede local: Selecciona os adaptadores disponíveis (como, por exemplo, `eth0`, `eth1`) utilizados por esta HMC para ligar a sistemas geridos, partições lógicas, assistência e suporte e utilizadores remotos. Para obter mais informações, consulte “Ligações de rede da HMC” na página 52. A conectividade a partir da HMC pode ser feita quer numa rede privada quer numa rede aberta.

#### Velocidade e Dúplex do Adaptador de Ethernet

Introduza a velocidade e o modo de dúplex pretendidos do adaptador de Ethernet. A opção de autodeteção determina qual das opções é ideal se não tiver a certeza de que velocidade e dúplex produzem resultados óptimos para o hardware. Predefinição = Autodeteção A velocidade dos suportes especifica a velocidade de um adaptador de Ethernet em modo dúplex. Selecciona Autodeteção a não ser que pretenda especificar uma velocidade de suporte fixo. Qualquer dispositivo ligado ao FSP (comutadores/HMC) terá de ser definido para o modo Auto (Velocidade) Auto (Dúplex), pois é a predefinição do FSP e não poderá ser alterada.

Tabela 10. Velocidade e Dúplex do Adaptador de Ethernet				
Características	eth0	eth1	eth2	eth3
<b>Selecione a velocidade e o modo dúplex</b>				
Velocidade dos suportes (Autodeteção, 10/100/1000 Full/Half Duplex)				

Para mais informação sobre redes privadas e abertas, consulte “Redes privadas e abertas no ambiente da HMC” na página 54.

Tabela 11. Rede Privada ou Aberta				
Características	eth0	eth1	eth2	eth3
Especifique a rede <b>Privada (Private)</b> ou <b>Aberta (Open)</b> para cada adaptador.				

O DHCP (Dynamic Host Configuration Protocol) fornece um método automatizado para configuração dinâmica de clientes. É possível especificar esta HMC como um servidor de DHCP. Se esta for a primeira ou a única HMC na rede privada, active a HMC como um servidor de DHCP. Quando activa a HMC como um

servidor de DHCP, os sistemas geridos na rede são configurados e identificados automaticamente pela HMC.

Para adaptadores de Ethernet especificados como Redes Privadas, complete a seguinte tabela:

<i>Tabela 12. Servidor DHCP</i>		
<b>Características</b>	<b>eth0</b>	<b>eth1</b>
Pretende especificar esta HMC como um servidor de DHCP? (sim/não)		
Caso seja sim, registe o intervalo de endereços de IP que pretende utilizar.		

Se estiver a utilizar a HMC 7063-CR1, tem de ligar a porta **IPMI** Ethernet a uma rede para aceder ao Controlador de Gestão de Placas de Sistema (BMC, baseboard management controller) na HMC. Para obter mais informações, consulte o tópico “Configurar a conectividade do BMC” na página 78. Preencha a seguinte tabela para a ligação BMC.

<i>Tabela 13. Ligação BMC</i>	
<b>Características</b>	<b>IPMI</b>
Pretende configurar esta ligação pelo modo DHCP? (sim/não)	
Caso não, liste os endereços estáticos especificados abaixo:	
Endereço de IP:	
Máscara de sub-rede:	
Porta de ligação:	

Para os adaptadores de Ethernet especificados como redes *abertas* (*open*), preencha as seguintes tabelas. Para obter mais informações sobre as diferentes versões de Protocolos de Internet, consulte “Configurar os tipos de rede da HMC” na página 72.

#### **Utilizar o IPv6**

Se estiver a utilizar a IPv6, entre em contacto com o administrador de rede e decida como pretende obter os endereços de IP. De seguida, preencha as seguintes tabelas:

<i>Tabela 14. IPv6 (estático)</i>				
<b>Características</b>	<b>eth0</b>	<b>eth1</b>	<b>eth2</b>	<b>eth3</b>
Está a utilizar um endereço de IP atribuído estaticamente? Se sim, grave esse endereço aqui.				

<i>Tabela 15. IPv6 (Servidor DHCP)</i>				
<b>Características</b>	<b>eth0</b>	<b>eth1</b>	<b>eth2</b>	<b>eth3</b>
Os endereços de IP estão a ser obtidos a partir de um servidor de DHCP? (Sim/Não)				

<i>Tabela 16. IPv6 (Encaminhador IPv6)</i>				
<b>Características</b>	<b>eth0</b>	<b>eth1</b>	<b>eth2</b>	<b>eth3</b>
Os endereços de IP estão a ser obtidos a partir de um encaminhador de IPv6?				

Para obter mais informações sobre a definição de endereços IPv6, consulte “Definir o endereço de IPv6” na página 79. Para obter mais informações sobre a utilização apenas de endereços IPv6, consulte “Utilizar apenas endereços IPv6” na página 80.

#### **Utilizar a IPv4**

Conclua as seguintes tabelas para adaptadores de Ethernet especificados como redes abertas através da utilização de IPv4.

<i>Tabela 17. IPv4</i>				
<b>Características</b>	<b>eth0</b>	<b>eth1</b>	<b>eth2</b>	<b>eth3</b>
Pretende obter automaticamente um endereço de IP? (sim/não)				
Caso não, liste o endereço especificado abaixo:				
Endereço de Interface de TCP/IP:				
Máscara de Rede de Interface de TCP/IP:				
Definições da Firewall:				
Deseja configurar as definições da firewall da HMC? (sim/não)				
Caso seja sim, liste as aplicações e endereços de IP que devem ser permitidos pela firewall:				

### Informações de TCP/IP

É necessária um endereço de TCP/IP exclusivo para cada nó, para o Elemento de Suporte (SE, Support Element) e para a Consola de Gestão de Hardware (HMC, Hardware Management Console). A máscara de rede atribuída é utilizada para gerar um endereço exclusivo, por predefinição, para a rede local privada. Caso os nós sejam ligados a uma rede maior com um endereço de TCP/IP administrado, será possível especificar o endereço de TCP/IP a ser utilizado. A predefinição é gerada pelo sistema.

### Definições da firewall

As definições da firewall da HMC criam uma barreira de segurança que permite ou recusa o acesso a aplicações de rede específicas na HMC. É possível especificar estas definições de controlo individualmente para cada interface de rede física, o que permite ao utilizador possuir controlo sobre as aplicações de rede da HMC que podem ser acedidas em cada rede.

Caso configure pelo menos um adaptador como um adaptador de Rede Aberta, será necessário facultar as seguintes informações adicionais para permitir à HMC aceder à rede local:

<i>Tabela 18. Adaptador de rede aberta</i>	
<b>Informações de sistema central local</b>	
Nome do sistema central da HMC:	
Nome do domínio:	
Descrição da HMC:	
<b>Informações da porta de ligação</b>	
Endereço da Porta de Ligação: (nnn.nnn.nnn.nnn)	
Dispositivo da porta de ligação:	
<b>Activação de DNS</b>	
Pretende utilizar DNS? (sim/não)	
Se “sim”, especifique a Ordem de Procura do Servidor de DNS abaixo:	
1.	
2.	
Ordem de procura do sufixo do domínio:	
1.	
2.	

### Informações de Sistema Central Local

Para identificar a Consola de Gestão de Hardware (HMC, Hardware Management Console) à rede, introduza o nome do sistema central e o nome do domínio da HMC. Excepto se estiver a utilizar apenas nomes de sistema central pequenos na rede, introduza um nome de sistema central totalmente qualificado. Exemplo de nome do domínio: nome.empresa.com

### Informações da porta de ligação

Para definir uma porta de ligação predefinida, conclua o endereço de TCP/IP a ser utilizado para pacotes de IP de encaminhamento. O endereço da porta de ligação informa cada computador ou dispositivo de rede quando deverá enviar dados caso a estação de destino não se encontre na mesma sub-rede que a origem.

### Activação de DNS

O Sistema de Nomes de Domínio (DNS, Domain Name System) é utilizado para fornecer uma convenção de nomenclatura padrão para localizar computadores baseados em IP. Ao definir os

servidores de DNS, é possível utilizar nomes do sistema central para identificar servidores e Consolas de Gestão de Hardware (HMCs, Hardware Management Consoles) em vez de endereços de IP.

#### **Ordem de Procura do Servidor de DNS**

Introduza os endereços de IP dos servidores de DNS a serem procurados para mapeamento de nomes do sistema central e endereços de IP. Esta ordem de procura está apenas disponível quando o DNS está activado.

#### **Ordem de Procura do Sufixo do Domínio**

Introduza os sufixos do domínio que está a utilizar. A HMC utiliza sufixos do domínios para anexar a nomes não qualificados para procuras de DNS. Os sufixos são procurados pela ordem em que se encontram listados. Esta ordem de procura está apenas disponível quando o DNS está activado.

### **Notificação de Correio Electrónico**

Liste as informações de contacto de correio electrónico caso pretenda receber uma notificação através de correio electrónico quando ocorrerem eventos de problemas de hardware no sistema.

<i>Tabela 19. Notificação de Correio Electrónico</i>	
<b>Características</b>	<b>Campo de entrada</b>
Endereços de correio electrónico:	
Servidor de SMTP:	
Porta:	
<b>Erros a notificar:</b>	
Apenas eventos de problemas de comunicação de retorno	
Todos os eventos de problemas	

#### **Servidor de SMTP**

Escreva o endereço de Simple Mail Transfer Protocol (SMTP) do servidor que será notificado de um evento de sistema. Um exemplo de um nome do servidor de SMTP é `relay.us.ibm.com`.

SMTP é o Protocolo utilizado para enviar correio electrónico. Quando utiliza SMTP, um cliente envia uma mensagem e comunica com o servidor de SMTP através da utilização do Protocolo SMTP.

Se não souber o endereço do SMTP do servidor ou não tiver a certeza, contacte o administrador da rede.

#### **Porta**

Escreva o número da porta do servidor para que possa ser notificado de um evento de sistema ou utilize a porta predefinida.

#### **Endereços de correio electrónico a notificar**

Introduza endereços de correio electrónico configurados para que possa ser notificado quando ocorrer um evento de sistema.

- Seleccione **Apenas eventos de problemas de comunicação de retorno (Only call-home problem events)** para receber uma notificação apenas quando ocorrem eventos que criam uma função de comunicação de retorno.
- Seleccione **Todos os eventos de problemas (All problem events)** para ser notificado quando ocorrer quaisquer eventos.

## Informações de contacto para assistência

<i>Tabela 20. Informações de contacto para assistência</i>	
<b>Características</b>	<b>Campo de entrada</b>
Nome da empresa	
Nome do administrador	
Endereço de correio electrónico	
Número de telefone	
Número de telefone alternativo	
Número de fax	
Número de telefone alternativo	
Morada	
Morada 2	
Cidade ou localidade	
Estado	
Código postal	
País ou região	
Localização da HMC (se for a mesma que o endereço do administrador, indique “mesma (same)”):	
Morada	
Morada 2	
Cidade ou localidade	
Estado	
Código postal	
País ou região	

## Autorização de assistência e conectividade

Selecione o tipo de ligação para contactar o fornecedor de serviços. Para obter uma descrição destes métodos que incluem características de segurança e requisitos de configuração, consulte “Escolher servidores de comunicação de retorno existentes para ligar para a assistência e suporte a esta HMC” na página 86.

<i>Tabela 21. Autorização de assistência e conectividade</i>	
<b>Características</b>	<b>Campo de entrada</b>
Secure Sockets Layer (SSL) através da Internet	-----
Rede privada virtual (VPN, virtual private network) através da Internet	-----

### Secure Sockets Layer (SSL) através da Internet:

Caso possua uma ligação à Internet existente a partir da HMC, será possível utilizar a mesma para chamar o fornecedor de serviços. É possível ligar directamente ao fornecedor de serviços através da utilização de Secure Sockets Layer (SSL) codificado através da utilização da ligação à Internet existente. Seleccione **Utilizar Proxy SSL (Use SSL Proxy)** caso pretenda configurar a utilização de SSL codificado através da utilização de uma ligação indirecta que utiliza um proxy SSL.

Tabela 22. SSL	
Características	Campo de entrada
Utilizar proxy SSL? (sim/não)	
Caso sim, liste as informações abaixo:	
Endereço:	
Porta:	
Autenticar com o Proxy SSL?	
Caso sim, liste as informações abaixo:	
Utilizador:	
Palavra-passe:	

### Protocolo de ligação à Internet utilizado

Para obter mais informações sobre os diferentes Protocolos de Internet, consulte [“Configurar os tipos de rede da HMC”](#) na página 72.

- \_\_\_ IPv4
- \_\_\_ IPv6
- \_\_\_ IPv4 e IPv6

### Rede Privada Virtual (VPN)

Caso possua uma ligação à Internet existente a partir da HMC, será possível utilizar a mesma para chamar o fornecedor de serviços. É possível estabelecer ligação directamente ao fornecedor de serviços pela rede privada virtual (VPN, virtual private network) através da utilização da ligação à Internet existente.

**Nota:** Caso seleccione Rede Privada Virtual (VPN, Virtual Private Network) através da Internet, não será possível seleccionar quaisquer outras opções.

### Servidores de comunicação de retorno

Decida quais as HMCs que pretende configurar como servidores de comunicação de retorno para estabelecer ligação com a assistência e suporte. Para mais informações sobre a utilização de múltiplos servidores de comunicação de retorno, consulte [“Utilizar múltiplos servidores de comunicação de retorno”](#) na página 60.

- \_\_\_ Esta HMC
- \_\_\_ Outra HMC

Caso tenha marcado **Outra HMC (Another HMC)**, liste as outras HMC que se encontram configuradas como servidores de comunicação de retorno aqui:

Tabela 23. Outras HMCs que se encontram configuradas como servidores de comunicação de retorno

**Lista de nomes do sistema central ou endereços de IP da HMC configurados como servidores de comunicação de retorno**

## Benefícios de Suportes Adicionais

### Os Meus Sistemas e a Procura Premium

Tabela 24. Os Meus Sistemas e a Procura Premium

Características	Campo de entrada
Inclua na lista o seu ID IBM	-----
Inclua na lista outros IDs IBM	-----

Para aceder a informações de suporte valiosas e personalizadas nas secções Os Meus Sistemas e Procura Premium do sítio da Web Serviços Electrónicos, os Clientes terão de registar o respectivo ID da IBM com este sistema. Se ainda não tiver um ID, pode registar-se para ter um ID IBM em: [www.ibm.com/account/profile](http://www.ibm.com/account/profile).

**Nota:** A IBM faculta funções da Web personalizadas que utilizam informações recolhidas pela aplicação do IBM Electronic Service Agent. Para utilizar estas funções, terá de se registar primeiro no sítio da Web de Registo IBM em <http://www.ibm.com/account/profile>.

Para autorizar utilizadores a utilizarem as informações do Electronic Service Agent para personalizarem as funções da Web, introduza o ID da IBM que registou no sítio da Web de Registo da IBM. Avance para <http://www.ibm.com/support/electronic> para consultar as informações de suporte valiosas disponíveis para clientes que registam um ID IBM com os respectivos sistemas.

## Configurar a HMC

Obtenha mais informações sobre como configurar as ligações de rede, a segurança, as aplicações de assistência e algumas preferências do utilizador.

Dependendo do nível de personalização que pretende aplicar à configuração da HMC, o utilizador tem várias opções para instalar a HMC de modo a corresponder às suas necessidades. O Assistente de Instalação Assistida é uma ferramenta da HMC concebida para facilitar a configuração da HMC. É possível escolher um caminho rápido através do assistente para criar rapidamente o ambiente recomendado para a HMC ou pode optar por explorar completamente as definições disponíveis à medida que o assistente o orienta. Também é possível executar os passos de configuração sem a ajuda do assistente através da Configuração da HMC através da utilização dos menus da HMC.

Antes de começar, recolha as informações de configuração necessárias para concluir os passos com êxito. Consulte [“Preparar a configuração da HMC”](#) na página 60, para obter uma lista das informações necessárias. Quando tiver terminado a preparação, certifique-se de que conclui o [“Esquema de configuração da pré-instalação para a HMC”](#) na página 62 e, em seguida, regresse a esta secção.

### Configurar a HMC utilizando o caminho rápido através do Assistente de Instalação Assistida

Na maioria dos casos, é possível configurar a HMC para funcionar de forma eficiente através da utilização de muitas das predefinições. Utilize esta lista de verificação de caminho rápido para preparar a HMC para assistência. Quando concluir estes passos, a HMC está configurada como um servidor de DHCP (Dynamic Host Configuration Protocol) numa rede privada (ligada directamente).

## Configurar a HMC através da utilização dos menus

Esta secção fornece uma lista completa de todas as tarefas de configuração da HMC, orientando-o através do processo de configuração da HMC. Opte por esta opção se preferir não utilizar o Assistente de Instalação Assistida.

Tem de reiniciar a HMC para que as definições de configuração tenham efeito, pelo que pode desejar imprimir esta lista de verificação e guardá-la enquanto configura a sua HMC.

Estas informações contêm referências a tarefas que não estão incluídas neste documento. É possível aceder ao Informações de hardware do IBM Power Systems na HMC ou na Web. Na HMC, é possível aceder ao IBM Knowledge Center a partir do canto superior direito da barra de tarefas. Na Web, é possível aceder ao IBM Knowledge Center em <https://www.ibm.com/support/knowledgecenter>.

Estas informações contêm referências a tarefas que não estão incluídas neste PDF. Poderá aceder a outros materiais de suporte consultando a secção **Recursos adicionais (Additional Resources)** na página de boas-vindas da HMC.

### Pré-requisitos

Antes de começar a configurar a HMC utilizando os menus da HMC, certifique-se de que conclui a actividade de preparação da configuração descrita no [“Preparar a configuração da HMC”](#) na página 60.

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Inicie a HMC.	<a href="#">“Iniciar a HMC”</a> na página 71
2. Defina a data e hora.	
3. Altere as palavras-passe predefinidas.	
4. Crie utilizadores adicionais e regresse a esta lista de verificação quando tiver concluído esse passo.	
5. Configure as ligações de rede.	<a href="#">“Configurar os tipos de rede da HMC”</a> na página 72
6. Para o modelo 7063-CR1 da HMC, é necessário configurar o endereço de IP do Controlador de Gestão de Placas de Sistema (BMC, baseboard management controller).	<a href="#">“Configurar a conectividade do BMC”</a> na página 78
7. Caso esteja a utilizar uma rede aberta e um endereço de IP fixo, defina as informações de identificação.	
8. Caso esteja a utilizar uma rede aberta e um endereço de IP fixo, configure uma entrada de encaminhamento como a porta de ligação predefinida.	<a href="#">“Configurar uma entrada de encaminhamento como a porta de ligação predefinida”</a> na página 81
9. Caso esteja a utilizar uma rede aberta e um endereço de IP fixo, configure os serviços do nome do domínio.	<a href="#">“Configurar serviços de nomes de domínio”</a> na página 82
10. Se estiver a utilizar um endereço de IP fixo e tiver o DNS activado, configure sufixos de domínio.	<a href="#">“Configurar sufixos de domínio”</a> na página 82
11. Configure o servidor para ligar à assistência e suporte IBM e regresse a esta lista de verificação depois de ter concluído esse passo.	<a href="#">“Configurar a consola local para comunicar falhas a assistência e suporte”</a> na página 85

*Tabela 25. Tarefas de configuração da HMC manuais e locais onde pode encontrar informações relacionadas (continuação)*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
12. Configure o Gestor de eventos para Chamadas de assistência.	<a href="#">“Configurar o Gestor de eventos para Chamadas de assistência” na página 88</a>
13. Ligue o sistema gerido a uma fonte de alimentação.	
14. Defina palavras-passe para o sistema gerido e cada uma das palavras-passe da ASMI (geral e administrador)	<a href="#">“Definir palavras-passe para o sistema gerido” na página 89</a>
15. Aceda à ASMI para definir a data e hora no sistema gerido.	
16. Inicie o sistema gerido e regresse a esta lista de verificação quando tiver concluído esse passo.	
17. Certifique-se de que tem uma partição lógica no sistema gerido.	
18. Opcional: adicione outro sistema gerido e regresse a esta lista de verificação quando tiver concluído esse passo.	
19. Opcional: se estiver a instalar um novo servidor com a HMC, configure as partições lógicas e instale o sistema operativo.	
20. Se não estiver a instalar um novo servidor neste momento, execute tarefas de pós-configuração opcionais para personalizar a sua configuração.	<a href="#">“Passos de Pós-configuração” na página 91</a>

### **Iniciar a HMC**

Pode iniciar sessão na HMC e seleccionar o idioma que pretende que seja apresentado na interface. Utilize o ID de utilizador `hscroot` e a palavra-passe `abc123` predefinidos para iniciar sessão na HMC pela primeira vez.

### **Sobre esta tarefa**

Para iniciar a HMC, execute o seguinte procedimento:

### **Procedimento**

1. Ligue a HMC premindo o botão de alimentação.
2. Se o idioma que pretende utilizar for o inglês, avance para o passo 4.  
Se a preferência quanto ao idioma for outra que não o inglês, escreva o número **2** quando lhe for solicitado que altere o locale.  
**Nota:** Se não efectuar qualquer acção, o tempo de espera deste pedido de informação termina após 30 segundos.
3. Selecciono o locale que pretende visualizar na lista da janela **Seleção de Locale** e faça clique em **OK**. O locale identifica o idioma utilizado pela interface da HMC.
4. Faça clique em **Iniciar sessão e iniciar a aplicação da Web da Consola de Gestão de Hardware (Log on and launch the Hardware Management Console web application)**.
5. Inicie sessão na HMC com as seguintes predefinições de ID de utilizador e palavra-passe:

ID: hscroot

Palavra-passe: abc123

### **HMC Enhanced**

Apresenta uma nova e melhorada interface gráfica do utilizador com as funcionalidades melhoradas do PowerVM.

### **HMC Classic**

Apresenta a interface gráfica do utilizador padrão sem as funcionalidades melhoradas do PowerVM.

**Nota:** Quando a HMC estiver a funcionar como um servidor de DHCP, a HMC utiliza a palavra-passe predefinida quando se liga ao processador de serviço pela primeira vez.

6. Prima Enter.

## ***Alterar a data e a hora***

O relógio de funcionamento a pilhas guarda a data e hora para a Consola de Gestão de Hardware (HMC). Poderá ser necessário repor a data e hora da consola se a pilha for substituída ou se transportar o sistema para um local com um fuso horário diferente. Saiba como alterar a data e hora da HMC.

## **Sobre esta tarefa**

Se alterar as informações de data e hora, as alterações não afectam os sistemas nem as partições lógicas que a HMC gere.

Para alterar a data e hora para a HMC, execute os seguintes passos:

## **Procedimento**

1. Certifique-se de que é membro de uma das seguintes funções:

- Super Administrador
- Técnico dos serviços de assistência
- Operador
- Visualizador

2. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, faça clique em **Definições da Consola**.
3. Na área da janela de conteúdos, faça clique em **Alterar data e hora (Change Date and Time)**.
4. Caso seleccione **UTC** no campo **Relógio (Clock)**, a definição de hora ajusta automaticamente para a hora de Verão no fuso horário seleccionado. Introduza a data, a hora e o fuso horário e faça clique em **OK**.

## **Resultados**

### ***Configurar os tipos de rede da HMC***

Configure a HMC para que esta consiga comunicar com o sistema gerido, partições lógicas, utilizadores remotos e assistência e suporte.

*Configurar as definições da HMC para utilizar uma rede aberta para ligar ao sistema gerido*

Configure a HMC para que esta se consiga ligar a um sistema gerido e o administrar ao utilizar uma rede aberta.

## **Antes de começar**

Para configurar as definições de rede da HMC para que esta se possa ligar ao sistema gerido ao utilizar uma rede aberta, execute o seguinte procedimento:

*Tabela 26. Configurar as definições da HMC para utilizar uma rede aberta para ligar ao sistema gerido*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Decida que interface pretende utilizar para o sistema gerido. <b>eth0</b> é o preferido.	<a href="#">“Esquema de configuração da pré-instalação para a HMC” na página 62</a>
2. Identifique as portas de Ethernet para a HMC.	<a href="#">“Identificar a porta Ethernet definida como eth0” na página 75</a>
3. Configure o adaptador de Ethernet ao executar as seguintes tarefas:	
a. Defina a velocidade dos suportes.	<a href="#">“Definir a velocidade do suporte” na página 77</a>
b. Seleccione o tipo de rede aberta.	<a href="#">“Seleccionar uma rede privada ou aberta” na página 77</a>
c. Defina os endereços estáticos.	<a href="#">“Definir o endereço de IPv6” na página 79</a>
d. Defina a firewall.	<a href="#">“Alterar as definições da firewall da HMC” na página 80</a>
e. Configure a porta de ligação predefinida.	<a href="#">“Configurar uma entrada de encaminhamento como a porta de ligação predefinida” na página 81</a>
f. Configure o DNS.	<a href="#">“Configurar serviços de nomes de domínio” na página 82</a>
4. Configure adaptadores adicionais, se existirem.	
5. Teste a ligação entre o servidor gerido e a HMC.	<a href="#">“Testar a ligação entre a HMC e o sistema gerido” na página 90</a>

*Configurar as definições da HMC para utilizar uma rede privada para ligar ao sistema gerido*

Configure a HMC para que esta se consiga ligar e administrar um sistema gerido ao utilizar uma rede privada.

## Antes de começar

Para configurar as definições de rede da HMC para que esta se consiga ligar ao sistema gerido ao utilizar uma rede privada, execute o seguinte procedimento:

*Tabela 27. Configurar as definições da HMC para utilizar uma rede privada para ligar ao sistema gerido*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Decida que interface pretende utilizar para o sistema gerido.	<a href="#">“Esquema de configuração da pré-instalação para a HMC” na página 62</a>
2. Identifique as portas de Ethernet para a HMC.	<a href="#">“Identificar a porta Ethernet definida como eth0” na página 75</a>
3. Configure a HMC como um servidor de DHCP.	<a href="#">“Configurar a HMC como um servidor de DHCP” na página 78</a>
4. Teste a ligação entre o servidor gerido e a HMC.	<a href="#">“Testar a ligação entre a HMC e o sistema gerido” na página 90</a>

Configurar as definições da HMC para utilizar uma rede aberta para ligar às partições lógicas

## Antes de começar

Para configurar as definições de rede da HMC para que esta se consiga ligar às partições lógicas ao utilizar uma rede aberta, execute o seguinte procedimento:

Tarefa	Onde encontrar informações relacionadas
1. Decida que interface pretende utilizar para o sistema gerido.	<a href="#">“Esquema de configuração da pré-instalação para a HMC” na página 62</a>
2. Identifique as portas de Ethernet para a HMC.	<a href="#">“Identificar a porta Ethernet definida como eth0” na página 75</a>
3. Configure o adaptador de Ethernet ao executar as seguintes tarefas:	
a. Defina a velocidade dos suportes.	<a href="#">“Definir a velocidade do suporte” na página 77</a>
b. Seleccione o tipo de rede aberta.	<a href="#">“Seleccionar uma rede privada ou aberta” na página 77</a>
c. Defina os endereços estáticos.	<a href="#">“Definir o endereço de IPv6” na página 79</a>
d. Defina a firewall.	<a href="#">“Alterar as definições da firewall da HMC” na página 80</a>
e. Configure a porta de ligação predefinida.	<a href="#">“Configurar uma entrada de encaminhamento como a porta de ligação predefinida” na página 81</a>
f. Configure o DNS.	<a href="#">“Configurar serviços de nomes de domínio” na página 82</a>
4. Configure adaptadores adicionais, se existirem.	
5. Teste a ligação entre o servidor gerido e a HMC.	<a href="#">“Testar a ligação entre a HMC e o sistema gerido” na página 90</a>

Configurar definições da HMC para utilizar uma rede aberta para ligar a utilizadores remotos

## Antes de começar

Para configurar as definições de rede da HMC para que esta consiga ligar a utilizadores remotos utilizando uma rede aberta, execute o seguinte procedimento:

Tarefa	Onde encontrar informações relacionadas
1. Decida que interface pretende utilizar para o sistema gerido.	<a href="#">“Esquema de configuração da pré-instalação para a HMC” na página 62</a>
2. Identifique as portas de Ethernet para a HMC.	<a href="#">“Identificar a porta Ethernet definida como eth0” na página 75</a>
3. Configure o adaptador de Ethernet ao executar as seguintes tarefas:	
a. Defina a velocidade dos suportes.	<a href="#">“Definir a velocidade do suporte” na página 77</a>

*Tabela 29. Configurar definições da HMC para utilizar uma rede aberta para ligar a utilizadores remotos (continuação)*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
b. Seleccione o tipo de rede aberta.	“ <a href="#">Seleccionar uma rede privada ou aberta</a> ” na página 77
c. Defina os endereços estáticos.	“ <a href="#">Definir o endereço de IPv6</a> ” na página 79
d. Defina a firewall.	“ <a href="#">Alterar as definições da firewall da HMC</a> ” na página 80
e. Configure a porta de ligação predefinida.	“ <a href="#">Configurar uma entrada de encaminhamento como a porta de ligação predefinida</a> ” na página 81
f. Configure o DNS.	“ <a href="#">Configurar serviços de nomes de domínio</a> ” na página 82
g. Configure sufixos.	“ <a href="#">Configurar sufixos de domínio</a> ” na página 82
4. Configure adaptadores adicionais, se existirem.	

*Configurar definições de servidor de comunicação de retorno da HMC*

## Antes de começar

Para configurar as definições de servidor de comunicação de retorno da HMC de modo a que os problemas possam ser comunicados, proceda do seguinte modo:

*Tabela 30. Configurar definições de servidor de comunicação de retorno da HMC*

<b>Tarefa</b>	<b>Onde encontrar informações relacionadas</b>
1. Certifique-se de que tem todas as informações de cliente necessárias	“ <a href="#">Esquema de configuração da pré-instalação para a HMC</a> ” na página 62
2. Configure esta HMC para comunicar falhas ou escolha um servidor de comunicação de retorno existente para comunicar falhas	“ <a href="#">Configurar a consola local para comunicar falhas a assistência e suporte</a> ” na página 85 “ <a href="#">Escolher servidores de comunicação de retorno existentes para ligar para a assistência e suporte a esta HMC</a> ” na página 86
3. Verifique se a configuração de comunicação de retorno está a funcionar	“ <a href="#">Verificar se a ligação a assistência e suporte está a funcionar</a> ” na página 87
4. Autorize utilizadores a ver os dados de sistema recolhidos	“ <a href="#">Autorizar utilizadores a ver os dados de sistema recolhidos</a> ” na página 87
5. Agende a transmissão de dados do sistema	“ <a href="#">Transmitir informações para assistência</a> ” na página 88

### *Identificar a porta Ethernet definida como eth0*

A ligação Ethernet ao servidor gerido deve ser estabelecida através da utilização da porta de Ethernet definida como eth0 na HMC.

Caso não tenha instalado quaisquer adaptadores de Ethernet adicionais nas ranhuras de PCI na HMC, então a porta de Ethernet integrada principal será sempre definida como eth0 ou eth1 na HMC, caso planeie utilizar a HMC como um servidor de DHCP para os sistemas geridos.

Caso instale adaptadores de Ethernet adicionais nas ranhuras de PCI, então a porta definida como eth0 dependerá da localização e tipo de adaptadores de Ethernet instalados.

**Nota:** As seguintes regras gerais poderão não se aplicar para todas as configurações.

A tabela seguinte descreve as regras para o posicionamento de Ethernet pelo tipo de HMC.

<b>Tipo da HMC</b>	<b>Regras de posicionamento da Ethernet</b>
HMCs instaladas em bastidor com duas portas de Ethernet integradas.	<p>A HMC suporta apenas um adaptador de Ethernet adicional.</p> <ul style="list-style-type: none"><li>• Caso seja instalado um adaptador de Ethernet adicional, então essa porta será definida como eth0. Neste caso, a porta de Ethernet integrada principal é então definida como eth1 e a porta de Ethernet integrada secundária é definida como eth2.</li><li>• Caso o adaptador de Ethernet seja um adaptador de Ethernet de duas portas, então a porta rotulada como Act/Link A será eth0. A porta rotulada como Act/link B será eth1. Neste caso, a porta de Ethernet integrada principal será então definida como eth2 e a porta de Ethernet integrada secundária será definida como eth3.</li><li>• Caso não sejam instalados quaisquer adaptadores, então a porta de Ethernet integrada principal será definida como eth0.</li></ul>
Modelos autónomos com uma única porta de Ethernet integrada.	<p>As definições dependem do tipo de adaptador de Ethernet que está instalado:</p> <ul style="list-style-type: none"><li>• Caso apenas esteja instalado um adaptador de Ethernet, então esse adaptador será definido como eth0.</li><li>• Caso o adaptador de Ethernet seja um adaptador de Ethernet de duas portas, então a porta rotulada como Act/link A será eth0. A porta rotulada como Act/link B será eth1. Neste caso, a porta de Ethernet integrada principal será então definida como eth2.</li><li>• Caso não sejam instalados quaisquer adaptadores, então a porta de Ethernet integrada será definida como eth0.</li><li>• Caso sejam instalados múltiplos adaptadores de Ethernet, consulte <a href="#">“Determinar o nome da interface para um adaptador de Ethernet”</a> na <a href="#">página 76</a>.</li></ul>

#### *Determinar o nome da interface para um adaptador de Ethernet*

Se configurar a HMC como um servidor de DHCP, esse servidor só pode operar nos conectores da placa de interface de rede (NIC, network interface card) que a HMC identificar como eth0 e eth1. Também pode necessitar de determinar a que conector de NIC terá de ligar o cabo de Ethernet. Saiba mais acerca dos conectores de NIC que a HMC identifica como eth0 e eth1.

#### **Sobre esta tarefa**

Para determinar o nome que a HMC atribuiu a um adaptador de Ethernet, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. A partir da janela **Alterar Definições de Rede (Change Network Settings)**, faça clique no separador **Adaptadores de rede local (LAN adapters)**. A seguinte entrada de exemplo demonstra que esta porta de Ethernet está identificada como eth0: Ethernet eth0 52:54:00:fa:b6:8e (<endereço de IP da HMC>).
4. Registe os resultados. Caso seja necessário visualizar ou alterar as definições do adaptador de rede local, faça clique em **Detalhes (Details)**.
5. Faça clique em **OK**.

### *Definir a velocidade do suporte*

Saiba como especificar a velocidade do suporte que inclui a velocidade e o modo de dúplex do adaptador de Ethernet.

## Antes de começar

A predefinição para as definições do adaptador da HMC é **Detecção automática (Autodetection)**. Se este adaptador estiver ligado a um comutador de LAN, é necessário corresponder às definições das portas do comutador. Para definir a velocidade de dados e de dúplex, execute os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. Faça clique no separador **Adaptadores de rede local (LAN Adapters)**.
4. Seleccione o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
5. Na secção de informações da rede local (LAN, local area network), seleccione **Detecção Automática (Autodetection)** ou a combinação adequada de velocidade do suporte e dúplex.
6. Faça clique em **OK**.

### *Seleccionar uma rede privada ou aberta*

Uma *rede de serviços privada* consiste na Consola de Gestão de Hardware (HMC) e os sistemas geridos. Uma rede de serviços privada restringe-se a consolas e aos sistemas que estas gerem e está separada da rede da empresa. Uma *rede aberta* é constituída pela rede de serviços privada e pela rede da empresa. Uma rede aberta pode conter terminais de rede, para além de consolas e sistemas geridos e pode abranger várias sub-redes e dispositivos de rede.

## Sobre esta tarefa

Para seleccionar uma rede privada ou pública, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. Faça clique no separador **Adaptadores de rede local (LAN Adapters)**.
4. Selecione o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
5. Faça clique no separador **Adaptador de rede local (LAN Adapter)**.
6. Na página de informações da rede local, selecione **Privada (Private)** ou **Aberta (Open)**.
7. Faça clique em **OK**.

### *Configurar a HMC como um servidor de DHCP*

O DHCP (Dynamic Host Configuration Protocol) fornece um método automatizado para configuração dinâmica de clientes.

Para configurar a Consola de Gestão de Hardware (HMC, Hardware Management Console) como um servidor de DHCP, conclua os seguintes passos:



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**. Abre-se a janela Personalizar Definições de Rede.
3. Selecione o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
4. Selecione **Privada (Private)** e, em seguida, selecione o tipo de rede.
5. Na secção Servidor de DHCP, selecione **Activar Servidor de DHCP (Enable DHCP Server)** para activar a HMC como um servidor de DHCP.

**Nota:** Pode configurar a HMC para ser um servidor de DHCP apenas numa rede privada. Caso utilize uma rede aberta, a opção para seleccionar **Activar DHCP (Enable DHCP)** não se encontrará disponível.

6. Introduza o intervalo de endereços do servidor de DHCP.
7. Faça clique em **OK**.

Se tiver configurado a HMC para ser um servidor de DHCP numa rede privada, tem de verificar se a rede privada DHCP da HMC está correctamente configurada. Para obter informações sobre a ligação da HMC a uma rede privada, consulte [“Seleccionar uma rede privada ou aberta”](#) na página 77.

Para obter mais informações, consulte [“A HMC como servidor de DHCP”](#) na página 55.

### *Configurar a conectividade do BMC*

Pode configurar ou visualizar as definições de rede no BMC para a consola de gestão.

**Nota:** Esta tarefa aplica-se apenas à 7063-CR1. Esta ligação é requerida para aceder ao Controlador de Gestão de Placas de Sistema (BMC, baseboard management controller) na HMC.

Para configurar a ligação BMC, conclua os seguintes passos:



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.

2. Na área da janela de conteúdo, faça clique em **Alterar as definições de rede BMC/IPMI (Change BMC/IPMI network settings)**.
3. Selecciono o modo de ligação (**DHCP** ou **Estático (Static)**).  
Se seleccionar o modo **Estático (Static)**, conclua os seguintes endereços:
  - **Endereço de IP (IP address)**
  - **Máscara de sub-rede (Subnet mask)**
  - **Porta de ligação (Gateway)**
4. Faça clique em **OK**.

Também pode configurar a ligação de rede do BMC ao utilizar a interface Petitboot bootloader. Para obter mais informações, consulte [Configurar o endereço de IP do software proprietário](#).

#### *Definir o endereço de IPv4*

Saiba como definir o endereço de IPv4 na HMC.

## Procedimento

1. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. Faça clique no separador **Adaptadores de rede local (LAN Adapters)**.
4. Selecciono o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
5. Faça clique no separador **Definições Básicas (Basic Settings)**.
6. Selecciono um endereço IPv4.
7. Se tiver optado por especificar um endereço de IP, introduza o endereço da interface de TCP/IP e a máscara de rede da interface de TCP/IP.
8. Faça clique em **OK**.

#### *Definir o endereço de IPv6*

Saiba como definir o endereço de IPv6 na HMC.

## Procedimento

1. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. Faça clique no separador **Adaptadores de rede local (LAN Adapters)**.
4. Selecciono o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
5. Faça clique no separador **Definições de IPv6 (IPv6 Settings)**.
6. Selecciono uma opção **Configuração Automática (Autoconfig)** ou adicione um endereço de IP estático.
7. Se tiver adicionado um endereço de IP, insira o endereço IPv6 e o comprimento do prefixo e faça clique em **OK**.
8. Faça clique em **OK**.

Utilizar apenas endereços IPv6

Saiba como configurar a HMC para utilizar apenas endereços IPv6.

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. Faça clique no separador **Adaptadores de rede local (LAN Adapters)**.
4. Selecione o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
5. Selecione **Sem endereço IPv4 (No IPv4 address)**.
6. Faça clique no separador **Definições de IPv6 (IPv6 Settings)**.
7. Selecione **Utilizar DHCPv6 para configurar as definições de IP** ou adicione os endereços de IP estáticos e, em seguida, faça clique em **OK**.

### Como proceder a seguir

Após fazer clique em **OK**, é necessário reiniciar a HMC para que as alterações entrem em vigor.

### **Alterar as definições da firewall da HMC**

Numa rede aberta, uma firewall é utilizada para controlar o acesso externo à rede da empresa. A HMC também tem uma firewall em cada um dos respectivos adaptadores de Ethernet. Para controlar a HMC remotamente ou fornecer acesso remoto a outros, modifique as definições de firewall do adaptador de Ethernet na HMC que está ligada à rede aberta.

### Sobre esta tarefa

Para configurar uma firewall, utilize os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**.
3. Faça clique no separador **Adaptadores de rede local (LAN Adapters)**.
4. Selecione o adaptador de rede local com o qual pretende trabalhar e faça clique em **Detalhes (Details)**.
5. Faça clique no separador **Firewall**.
6. Através da utilização de um dos seguintes métodos, é possível permitir qualquer endereço de IP através da utilização de uma aplicação específica através da firewall ou é possível especificar um ou mais endereços de IP:
  - Permitir qualquer endereço de IP através da utilização de uma aplicação específica através da firewall.
    - a. Na caixa superior, realce a aplicação.
    - b. Faça clique em **Permitir Entrada (Allow Incoming)**. A aplicação é apresentada na caixa inferior para indicar que está seleccionada.

- Especificar os endereços de IP com acesso através da firewall:
  - a. Na caixa superior, realce uma aplicação.
  - b. Faça clique em **Permitir Entrada a Endereço de IP (Allow Incoming by IP Address)**.
  - c. Na janela Sistemas Centrais Permitidos (Hosts Allowed), introduza o endereço de IP e a máscara de rede.
  - d. Faça clique em **Adicionar (Add)** e em **OK**.
- 7. Faça clique em **OK**.

*Activar o acesso da interface restrita remota*

É possível activar o acesso da interface restrita remota quando configura uma firewall.

### **Sobre esta tarefa**

Para activar o acesso da interface restrita remota, conclua os seguintes passos:

### **Procedimento**

1. Na área de navegação, faça clique em **Gestão da HMC (HMC Management)**.
2. Faça clique em **Execução do Comando Remoto (Remote Command Execution)**.
3. Selecciona **Activar execução de comando remoto utilizando a funcionalidade servssh** e depois faça clique em **OK**.

### **Como proceder a seguir**

Assim, o acesso da interface restrita remota está activado.

*Activar o acesso a Web remota*

É possível activar o acesso da Web remoto à Consola de Gestão de Hardware (HMC, Hardware Management Console).

### **Sobre esta tarefa**

Para activar o acesso da Web remoto, conclua os seguintes passos:

### **Procedimento**

1. Na área de navegação, faça clique em **Gestão da HMC (HMC Management)**.
2. Faça clique em **Operação Remota (Remote Operation)**.
3. Selecciona **Activada (Enable)** e depois faça clique em **OK**.

### **Como proceder a seguir**

Agora, o acesso da Web remota está activado.

### **Configurar uma entrada de encaminhamento como a porta de ligação predefinida**

Saiba como configurar uma entrada de encaminhamento como a porta de ligação predefinida. Esta tarefa encontra-se disponível quando utiliza uma rede aberta.

### **Antes de começar**

Para configurar uma entrada de encaminhamento como a porta de ligação predefinida, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**. Abre-se a janela Personalizar Definições de Rede.
3. Faça clique no separador **Encaminhamento (Routing)**.
4. Na secção de informações de porta de ligação predefinida, introduza o endereço da porta de ligação e o dispositivo de porta de ligação da entrada de encaminhamento que pretende para porta de ligação predefinida.
5. Faça clique em **OK**.

### **Configurar serviços de nomes de domínio**

Se pretender configurar uma rede aberta, configure serviços de nomes de domínio.

### **Sobre esta tarefa**

Se pretender configurar uma rede aberta, configure serviços de nomes de domínio. O sistema de nomes de domínio (DNS, Domain Name System) consiste num sistema de base de dados distribuída que gere os nomes dos sistemas centrais e os respectivos endereços de Protocolo Internet (IP, Internet Protocol) associados. A configuração dos serviços de nomes de domínio inclui a activação do DNS e a especificação da ordem de procura dos sufixos de domínio.

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**. Abre-se a janela Alterar Definições de Rede.
3. Faça clique no separador **Serviços de Nome (Name Services)**.
4. Seleccione **DNS activado (DNS enabled)** para activar o DNS.
5. Especifique o servidor de DNS e a ordem de pesquisa de sufixo de domínio e clique em **Adicionar (Add)**.
6. Faça clique em **OK**.

### **Configurar sufixos de domínio**

A lista de sufixos de domínio é utilizada para processar um endereço de IP que inicia com a primeira entrada na lista.

### **Sobre esta tarefa**

O sufixo de domínio é uma cadeia que é anexada a um nome de sistema central que é utilizado para ajudar a processar o respectivo endereço de IP. Por exemplo, um nome de sistema central como myname (meu nome) pode não ser resolvido. No entanto, caso a cadeia myloc.mycompany.com seja um elemento na tabela de sufixos de domínio, então será efectuada uma tentativa de processar myname.mloc.mycompany.com.

Para configurar uma entrada de sufixo de domínio, conclua os seguintes passos:

## Procedimento

1. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, faça clique em **Definições da Consola**.
2. Na área da janela de conteúdo, faça clique em **Alterar Definições de Rede (Change Network Settings)**. Abre-se a janela Personalizar Definições de Rede.
3. Faça clique no separador **Serviços de Nome (Name Services)**.
4. Introduza uma cadeia para ser utilizada como entrada de sufixo de domínio.
5. Faça clique em **Adicionar (Add)** para a adicionar à lista.

### **Configurar a HMC para utilizar autenticação remota LDAP**

Pode configurar a Consola de Gestão de Hardware (HMC, Hardware Management Console) para que esta utilize a autenticação remota LDAP (Lightweight Directory Access Protocol).

### **Antes de começar**

Quando um utilizador inicia sessão na HMC, a autenticação executada em primeiro lugar tem como base o ficheiro de palavras-passe local. Se o ficheiro de palavras-passe local não for encontrado, a HMC pode contactar um servidor de LDAP remoto para realizar a autenticação. É necessário configurar a HMC para que utilize a autenticação remota do LDAP.

**Nota:** Antes de configurar a HMC para utilizar a autenticação de LDAP, tem de certificar-se de que existe uma ligação de rede a funcionar entre a HMC e os servidores de LDAP. Para mais informações sobre como configurar ligações de rede da HMC, consulte [“Configurar os tipos de rede da HMC”](#) na página 72.

### **Sobre esta tarefa**

Para configurar a HMC para que esta utilize a autenticação LDAP, execute os seguintes passos:

## Procedimento

1. Na área de navegação, faça clique no ícone **Utilizadores e Segurança (Users and Security)**  e, em seguida, seleccione **Segurança de Sistemas e Consola (Systems and Console Security)**.
2. Na área da janela de conteúdo, seleccione **Gerir LDAP (Manage LDAP)**. Abre-se a janela Definição do Servidor de LDAP.
3. Seleccione **Activar LDAP (Enable LDAP)**.
4. Defina um servidor de LDAP para utilizar na autenticação.
5. Defina o atributo de LDAP utilizado para identificar o utilizador que está a ser autenticado. A predefinição é **ID do utilizador (uid)**, mas é possível optar pela utilização de outros atributos.
6. Defina a árvore de nome distinguido, também conhecida como base de pesquisa, para o servidor de LDAP.
7. Faça clique em **OK**.
8. Caso um utilizador pretenda utilizar autenticação de LDAP, o utilizador terá de configurar o respectivo perfil de forma a utilizar autenticação remota de LDAP em vez da autenticação local.

### **Configurar a HMC para utilizar o centro de distribuição de chaves para autenticação remota do Kerberos**

Pode configurar a HMC para utilizar o centro de distribuição de chaves (KBC) para autenticação remota do Kerberos.

## Antes de começar

Quando um utilizador inicia sessão na HMC, a autenticação primeiro efectua a verificação contra um ficheiro de palavra-passe local. Se o ficheiro de palavras-passe local não for encontrado, a HMC pode contactar um servidor Kerberos remoto para realizar a autenticação. É necessário configurar a HMC para que utilize a autenticação remota do Kerberos.

**Nota:** Antes de configurar a HMC para utilizar o centro de distribuição de chaves (KBC) para autenticação remota do Kerberos, deve certificar-se de que existe uma ligação de rede a funcionar entre a HMC e os servidores de KDC. Para mais informações sobre como configurar ligações de rede da HMC, consulte [“Configurar os tipos de rede da HMC” na página 72.](#)

## Sobre esta tarefa

Para configurar a HMC de forma a utilizar servidores de KDC para autenticação remota do Kerberos, conclua os seguintes passos:

## Procedimento

1. Active o serviço do NTP (Network Time Protocol) na HMC e defina a HMC e os servidores da HMC para sincronizarem a hora com o mesmo servidor de NTP. Para activar o serviço de NTP na HMC, conclua os seguintes passos:

- a) Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, faça clique em **Definições da Consola**.
- b) Na área da janela de conteúdo, seleccione **Alterar data e hora (Change Date and Time)**.
- c) Seleccione o separador **Configuração de NTP (NTP Configuration)**.
- d) Seleccione **Actualizar serviço do NTP nesta HMC (Enable NTP service on this HMC)**.
- e) Faça clique em **OK**.

2. Configure a HMC para que utilize a autenticação remota do Kerberos em vez da autenticação local.
3. Opcionalmente, é possível importar um ficheiro de chaves de serviço para esta HMC. Um ficheiro de chaves de serviço contém o sistema central principal que identifica a HMC ao servidor do KDC. Os ficheiros de chaves de serviço são também conhecidos por *keytabs*. Para importar um ficheiro de chaves de serviço para esta HMC, conclua os seguintes passos:

- a) Na área de navegação, faça clique no ícone **Utilizadores e Segurança (Users and Security)**  e, em seguida, seleccione **Segurança de Sistemas e Consola (Systems and Console Security)**.
- b) Na área da janela de conteúdo, seleccione **Gerir KDC (Manage KDC)**.
- c) Seleccione **Ações > Importar Chave de Serviço (Actions > Import Service Key)**. A janela para importar a chave de serviço abre-se.
- d) Escreva a localização do ficheiro da chave de serviço.
- e) Faça clique em **OK**.

4. Adicione um novo servidor do KDC a esta HMC. Para adicionar um novo servidor de KDC a esta HMC, conclua os seguintes passos:

- a) Na área de navegação, faça clique no ícone **Utilizadores e Segurança (Users and Security)**  e, em seguida, seleccione **Segurança de Sistemas e Consola (Systems and Console Security)**.
- b) Na área da janela de conteúdo, seleccione **Gerir KDC (Manage KDC)**.
- c) Seleccione **Ações > Adicionar Servidor KDC (Actions > Add KDC Server)**. A janela para importar a chave de serviço abre-se.
- d) Escreva o nicho e o nome do sistema central ou o endereço de IP do servidor do KDC.

e) Faça clique em **OK**.

### **Configurar a consola local para comunicar falhas a assistência e suporte**

Configure esta HMC de forma a poder realizar comunicação de retorno de erros através da utilização de conectividade de LAN.

*Configurar a HMC de forma a que seja possível ligar à assistência e suporte através da utilização do assistente de configuração de comunicação de retorno*

Configure a HMC de forma a que seja um servidor de comunicação de retorno através da utilização do assistente de comunicação de retorno.

### **Antes de começar**

Este procedimento descreve como configurar a HMC como um servidor de comunicação de retorno através da utilização de ligações directas (baseadas em rede local) e indirectas (SSL) à Internet.

Antes de começar esta tarefa, certifique-se de que:

- O administrador da rede verifica se a conectividade é permitida. Para obter mais informações, consulte [“Preparar a configuração da HMC”](#) na página 60.
- Caso esteja a configurar o suporte da Internet através de um servidor proxy, também será necessário possuir as seguintes informações:
  - O endereço de IP e a porta do servidor proxy
  - As informações de autenticação do proxy
- É utilizado o adaptador que é designado como **eth1** (aquele que é designado como uma rede aberta). Para obter mais informações, consulte [“Seleção de definições de rede na HMC”](#) na página 52.
- Um cabo de Ethernet liga fisicamente a HMC à rede local.

Para configurar a HMC de forma a que seja um servidor de comunicação de retorno através da utilização do assistente de comunicação de retorno, conclua os seguintes passos:

### **Procedimento**

1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)**  e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na área da janela de conteúdo, faça clique em **Assistente de configuração de Chamada Interna (Call-Home Setup Wizard)**. Irá abrir-se o Assistente Servidores de Conectividade e Chamada interna. Siga as instruções dadas no assistente para configurar comunicação de retorno.

*Configurar a consola local para comunicar falhas a assistência e suporte*

Configure esta HMC de forma a poder realizar comunicação de retorno de erros através da utilização de conectividade de LAN.

*Configurar uma HMC para contactar assistência e suporte através da utilização de Internet baseada na rede local e SSL*

Descreve como configurar uma HMC como um servidor de comunicação de retorno através da utilização de ligações directa (baseada em rede local) e indirecta (SSL) à Internet.

### **Antes de começar**

Antes de começar esta tarefa, certifique-se de que:

- O administrador da rede verifica se a conectividade é permitida. Para obter mais informações, consulte [“Preparar a configuração da HMC”](#) na página 60.

- As informações de contacto do cliente são configuradas. Verifique as informações de contacto ao aceder à interface da HMC e fazer clique em **Reparabilidade > Gestão de Assistência > Gerir Informações de Cliente (Serviceability > Service Management > Manage Customer Information)**.
- Caso esteja a configurar o suporte da Internet através de um servidor proxy, também será necessário possuir as seguintes informações:
  - O endereço de IP e a porta do servidor proxy
  - As informações de autenticação do proxy
- Precisa de ter pelo menos uma interface de rede configurada aberta. Para obter mais informações, consulte [“Redes privadas e abertas no ambiente da HMC”](#) na página 54.
- Um cabo de Ethernet liga fisicamente a HMC à rede local.

## Sobre esta tarefa

Para configurar a HMC como um servidor de comunicação de retorno através da utilização da Internet baseada em rede local e SSL, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)** e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na secção de conectividade, faça clique em **Gerir Conectividade de Transmissão (Manage Outbound Connectivity)**. A janela Consolas de servidor de comunicação de retorno (Call-Home Server Consoles) abre-se.
3. Faça clique em **Configurar (Configure)**
4. Na janela para gerir a conectividade de transmissão, marque **Activar sistema local como servidor de comunicação de retorno (Enable local system as call-home server)**.
5. Aceite o acordo.
6. Na janela Definições da Conectividade de Transmissão, seleccione a página **Internet**.
7. Marque a caixa **Permitir ligação à Internet existente para assistência (Allow an existing internet connections for service)**.
8. Se estiver a utilizar um proxy SSL, marque a caixa **Utilizar proxy SSL (Use SSL proxy)**.
9. Caso esteja a utilizar um proxy SSL, conclua o endereço e porta do proxy. Peça estas informações ao administrador de rede.
10. Se tiver marcado a opção **Utilizar proxy de SSL (Use SSL proxy)** e o proxy precisar da autenticação do ID de utilizador e palavra-passe, marque a caixa **Autenticar com o proxy de SSL (Authenticate with the SSL proxy)**. Introduza ID de utilizador e palavra-passe. Peça o ID de utilizador e palavra-passe ao administrador de rede.
11. Seleccione o **Protocolo de Internet (Protocol to Internet)** que pretende utilizar.
12. Na página **Internet**, faça clique em **Testar (Test)**.
13. Na janela Testar Internet, faça clique em **Iniciar (Start)**.
14. Verifique se o teste foi concluído com êxito.
15. Na janela Testar Internet, faça clique em **Cancelar (Cancel)**.
16. Na janela para estabelecer as definições da conectividade de transmissão, faça clique em **OK**.

*Escolher servidores de comunicação de retorno existentes para ligar para a assistência e suporte a esta HMC*

Selecione servidores de comunicação de retorno da Consola de Gestão de Hardware (HMC, Hardware Management Console) existentes reconhecidos ou identificados pela HMC para comunicar erros.

## Antes de começar

HMCs descobertas são HMCs que estão activadas como servidores de comunicação de retorno e encontram-se ou na mesma sub-rede ou gerem o mesmo sistema gerido como esta HMC.

Para seleccionar uma HMC identificada para efectuar a comunicação de retorno quando a HMC comunica erros, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)** e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na área da janela de conteúdo, faça clique em **Gerir Conectividade de Transmissão (Manage Outbound Connectivity)**. A janela Consolas de servidor de comunicação de retorno (Call-Home Server Consoles) abre-se.
3. Faça clique em **Utilizar consolas de servidor de comunicação de retorno descobertas (Use discovered call-home server consoles)**. A HMC apresenta o endereço de IP ou o nome do sistema central das HMCs configuradas para comunicação de retorno.
4. Faça clique em **OK**.

## Resultados

Pode também adicionar manualmente servidores de comunicação de retorno da HMC existentes que estiverem numa sub-rede diferente. Seleccione o endereço de IP ou nome do sistema central da HMC configurada para a comunicação de retorno e faça clique em **Adicionar (Add)** e, em seguida, faça clique em **OK**.

*Verificar se a ligação a assistência e suporte está a funcionar*

Testar relatório de problemas para verificar se a ligação a assistência e suporte está a funcionar

## Sobre esta tarefa

Para verificar se a configuração de comunicação de retorno está a funcionar, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)** e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na área da janela de conteúdo, faça clique em **Criar Evento (Create Event)**.
3. Seleccione **Testar Comunicação de Problemas Automática (Test Automatic problem Reporting)** e escreva um comentário.
4. Faça clique em **Pedir Assistência (Request Service)**. Aguarde alguns minutos para que o pedido seja enviado.
5. Na janela Gestão de Assistência, seleccione **Gerir Eventos (Manage Events)**.
6. Seleccione **Todos os problemas em aberto (All open problems)**.
7. Verifique se um evento PMH e número estão atribuídos ao número do problema que abriu.
8. Seleccione esse evento e faça clique em **Fechar (Close)**.
9. Na janela **Fechar (Close)**, escreva o seu nome e um breve comentário.

*Autorizar utilizadores a ver os dados de sistema recolhidos*

É necessário autorizar os utilizadores a ver os dados sobre os sistemas.

## Antes de começar

Antes de autorizar utilizadores a ver os dados de sistema recolhidos, precisa de obter um ID IBM. Para mais informações sobre como obter um ID IBM, consulte [“Esquema de configuração da pré-instalação para a HMC”](#) na página 62.

## Sobre esta tarefa

Para autorizar utilizadores a visualizarem dados do sistema recolhidos, conclua os seguintes passos:

## Procedimento

1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)**  e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na área da janela de conteúdo, seleccione **Autorizar utilizador (Authorize User)**.
3. Introduza o seu ID IBM.
4. Faça clique em **OK**.

### *Transmitir informações para assistência*

É possível transmitir informações para o fornecedor de assistência imediatamente ou é possível agendar o envio regular das informações.

## Antes de começar

A IBM faculta funções da Web personalizadas que utilizam informações recolhidas pelo IBM Electronic Service Agent. Para utilizar estas funções, terá de se registar primeiro no sítio da Web de Registo IBM em <http://www.ibm.com/account/profile>. Para autorizar os utilizadores a utilizarem as informações do Electronic Service Agent para personalizar as funções da Web, consulte [“Autorizar utilizadores a ver os dados de sistema recolhidos”](#) na página 87. Para mais informações sobre as vantagens de registar um ID IBM com os seus sistemas, consulte <http://www.ibm.com/support/electronic>.

**Nota:** É necessário transmitir informações ao fornecedor de assistência assim que a HMC for instalada e configurada para utilização.

## Sobre esta tarefa

Para transmitir informações de assistência, conclua os seguintes passos:

## Procedimento

1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)**  e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na área da janela de conteúdo, faça clique em **Transmitir informações de assistência (Transmit Service Information)**.
3. Conclua as tarefas na janela **Transmitir Informações de Assistência (Transmit Service Information)** e faça clique em **OK**.

### **Configurar o Gestor de eventos para Chamadas de assistência**

Obtenha mais informações sobre como configurar a tarefa Gestor de eventos para a Chamada de assistência. Através desta tarefa, pode monitorizar e aprovar os dados que estão a ser transmitidos a partir de uma HMC para a IBM.

O Gestor de Eventos para o modo de Comunicação de Retorno (activado ou desactivado) é definido através da utilização da interface de linha de comandos da HMC. A activação da tarefa Gestor de eventos para a Chamada de assistência bloqueia a HMC de executar automaticamente eventos de chamada de assistência à medida que estes vão ocorrendo. Para impedir que os sejam executados eventos de

chamada de assistência sem aprovação, todas as HCMs em execução neste ambiente têm de ter o Gestor de eventos para Chamadas de assistência activado.

Para activar ou desactivar a tarefa Gestor de eventos para a Chamada de assistência, execute o seguinte comando:

**chhmc -c emch**

**-s {enable | disable}**

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

**[--help]**

**Nota:** A activação do Gestor de Eventos para a tarefa Comunicação de Retorno retém eventos de comunicação de retorno até que os mesmos sejam aprovados para a tarefa de comunicação de retorno. Se desactivar o Gestor de eventos para a tarefa Chamada de assistência, este não desactiva automaticamente a funcionalidade de chamada de assistência. Esta configuração impede o envio de dados por parte de chamadas de assistência não pretendidas para a IBM. Seleccione a partir das seguintes opções de comandos para configurar a configuração necessária:

- Para activar o Gestor de eventos para a tarefa Chamada de assistência: **chhmc -c emch -s enable**
- Para desactivar o Gestor de eventos para a tarefa Chamada de assistência e para voltar a activar automaticamente a chamada de assistência: **chhmc -c emch -s disable --callhome enable**
- Para desactivar o Gestor de eventos para a tarefa Chamada de assistência e para não voltar a activar automaticamente a chamada de assistência: **chhmc -c emch -s disable --callhome disable**

Certifique-se de que a HMC consegue comunicar com outras HCMs implementadas neste ambiente. O Gestor de eventos para a Chamada de assistência tem uma função de ligação de teste quando uma HMC é registada.

Pode registar a HMC com o Gestor de eventos para a Chamada de assistência. Após registar a HMC, o gestor de eventos consulta a HMC registada para verificar se existem eventos a aguardar chamadas de assistência para a IBM. O Gestor de eventos mostra quais os dados que estão a ser enviados para a IBM e aprova estes eventos. Após a aprovação, o Gestor de eventos notifica a HMC registada de que esta pode avançar com a operação de chamada de assistência.

A tarefa Gestor de eventos para a Chamada de assistência pode ser executada a partir de qualquer HMC ou a partir de múltiplas HCMs. Para registar uma consola de gestão com a tarefa Gestor de eventos para a Chamada de assistência, execute os seguintes passos:

1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)**  e, em seguida, seleccione **Gestor de Eventos para Chamada de Assistência (Events Manager for Call Home)**.
2. A partir da área da janela **Gestor de Eventos para Chamada de Assistência (Events Manager for Call Home)**, faça clique em **Gerir Consolas (Manage Consoles)**.
3. A partir da janela **Gerir consolas registada (Manage Registered Consoles)**, faça clique em **Adicionar (Add Console)** para inserir as informações para registar uma consola de gestão com a tarefa Gestor de eventos para a Chamada de assistência.
4. Faça clique em **OK** para consolidar as alterações na lista da consola de gestão registada.

**Nota:** A tarefa Gestor de eventos para a Chamada de assistência pode ser utilizada com o modo de gestor de eventos desactivado. Pode também registar a HMC e ver os eventos no gestor de eventos, mas o Gestor de eventos não controla o momento em que os eventos efectuem chamadas de assistência.

### ***Definir palavras-passe para o sistema gerido***

Tem de definir palavras-passe para o servidor e para a Gestão de Sistemas Avançada (ASM, Advanced System Management). Saiba mais acerca da utilização da interface da HMC para definir estas palavras-passe.

## Antes de começar

Se tiver recebido a mensagem Authentication Pending (Autenticação Pendente), a HMC pede-lhe que defina as palavras-passe para o sistema gerido.

## Sobre esta tarefa

Se não tiver recebido a mensagem Autenticação Pendente, execute os seguintes passos para definir as palavras-passe para o sistema gerido.

*Actualizar a palavra-passe do servidor*

## Antes de começar

Para actualizar a palavra-passe do servidor, conclua os seguintes passos:

## Procedimento

1. Na área de navegação, seleccione o sistema gerido e faça clique no ícone **Utilizadores e Segurança**



**(Users and Security)** e, em seguida, seleccione **Utilizadores e Funções (Users and Roles)**.

2. Faça clique em **Alterar Palavra-passe (Change Password)**. Abre-se a janela Actualizar Palavra-passe.
3. Escreva a informação necessária e faça clique em **OK**.

*Actualizar a palavra-passe geral de Gestão de Sistemas Avançada (ASM - Advanced System Management)*

## Antes de começar

**Nota:** A palavra-passe predefinida para o ID de utilizador geral é `general` (geral) e a palavra-passe para o ID de administrador é `admin` (administrador).

Para actualizar a palavra-passe geral da ASM, conclua os seguintes passos:

## Procedimento

1. Na área de navegação HMC, seleccione o sistema gerido.
2. Na área de tarefas, faça clique em **Operações (Operations)**.
3. Faça clique em **Gestão de Sistemas Avançada (ASM - Advanced System Management)**. Abre-se a janela Iniciar a Interface de ASM.
4. Seleccione um Endereço de IP para o Processador de Serviço e clique em **OK**. A interface de ASM abre.
5. Na área da janela de boas-vindas da ASMI, especifique o ID de utilizador e a palavra-passe e faça clique em **Iniciar sessão (Log in)**.
6. Na área de navegação, expanda **Perfil de Início de Sessão (Login Profile)**.
7. Seleccione **Alterar Palavra-passe (Change Password)**.
8. Especifique as informações requeridas e faça clique em **Continuar (Continue)**.

*Repor a palavra-passe de administrador de Gestão de Sistemas Avançada (ASM - Advanced System Management)*

## Antes de começar

Para repor a palavra-passe de administrador, contacte um fornecedor de serviço autorizado.

## Testar a ligação entre a HMC e o sistema gerido

Saiba como verificar se está devidamente ligado à rede.

## Sobre esta tarefa

Para testar a conectividade de rede, é necessário ser membro de uma das seguintes funções:

- Super Administrador
- Técnico dos serviços de assistência

Para testar a ligação entre a HMC e o sistema gerido, conclua os seguintes testes:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, faça clique em **Definições da Consola**.
2. Na área de conteúdo, faça clique em **Testar Conectividade da Rede (Test Network Connectivity)**.
3. No separador Ping, escreva o nome do sistema central ou o endereço de IP de qualquer sistema ao qual pretenda estabelecer ligação. Para testar um rede aberta, indique a porta de ligação. Clique em **Ping**.

## Resultados

Caso não tenha criado quaisquer partições lógicas, não será possível contactar os endereços através do comando ping. Pode utilizar a HMC para criar partições lógicas no servidor. Para obter mais informações, consulte [Criação de partições lógicas](#).

Para saber como é que a HMC pode ser utilizada numa rede, consulte [“Ligações de rede da HMC”](#) na página 52.

Para obter mais informações sobre como configurar a HMC para estabelecer ligação a uma rede, consulte [“Configurar a HMC através da utilização dos menus”](#) na página 70.

## Passos de Pós-configuração

Após instalar e configurar a HMC, efectue uma cópia de segurança dos dados da HMC conforme necessário.

### Criar uma cópia de segurança dos dados da consola

Esta tarefa cria uma cópia de segurança (ou arquiva) os dados armazenados no disco rígido da HMC que são críticos para suportar operações da HMC.

### Antes de começar

O sistema remoto tem de ter o Network File System (NFS) ou a Secure Shell (ssh) configurada e esta rede tem de estar acessível a partir da HMC. Para executar esta tarefa, tem de encerrar e reiniciar a HMC. Utilize apenas a HMC para realizar estas tarefas.

## Sobre esta tarefa

Para efectuar a cópia de segurança da unidade de disco rígido da HMC para um sistema remoto, tem de ser membro de uma das seguintes funções:

- Super Administrador
- Operador
- Técnico dos serviços de assistência

Efectue uma cópia de segurança dos dados da HMC depois de terem sido realizadas alterações na HMC ou nas informações associadas às partições lógicas.

Os dados de HMC armazenados na unidade de disco rígido da HMC podem ser guardados numa DVD-RAM de um sistema local, num sistema remoto montado no sistema de ficheiros da HMC (como é o caso do NFS) ou enviados para um local remoto através do Protocolo de Transferência de Ficheiros (FTP).

**Nota:** Para o modelo 7063-CR1 da HMC, é possível ligar uma unidade de DVD USB externa.

Através da utilização da HMC, pode efectuar cópias de segurança de todos os dados importantes, tais como os seguintes:

- Ficheiros preferenciais do utilizador
- Informações do utilizador
- Ficheiros de configuração de plataformas da HMC
- Ficheiros de registo da HMC
- Actualizações da HMC através do Serviço Correctivo da Instalação (Install Corrective Service).

Para efectuar uma cópia de segurança do disco rígido da HMC para um sistema remoto, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Criar cópia de segurança dos dados da Consola de Gestão (Backup Management Console Data)**.
3. A partir da janela **Criar Cópia de Segurança dos Dados da Consola de Gestão**, seleccione a opção de arquivo que pretende efectuar.
4. Faça clique em **Seguinte** e, em seguida, siga as instruções adequadas, dependendo da opção que seleccionar.
5. Faça clique em **OK** para continuar com o processo de cópia de segurança.

## Actualizar, aperfeiçoar e migrar o código máquina da HMC

As actualizações e aperfeiçoamentos são publicados periodicamente para a HMC para adicionar novas funcionalidades e para melhorar as características existentes. Saiba mais sobre as diferenças entre actualizar, aperfeiçoar e migrar o código máquina da HMC. Saiba também como realizar uma actualização, um aperfeiçoamento ou uma migração de código máquina da HMC.

Quando terminar cada uma destas tarefas, a HMC é reiniciado mas as partições não.

### Actualizar o código da HMC

Aplica manutenção a um nível da HMC existente

Não requer a execução da tarefa **Guardar dados de aperfeiçoamento**

### Aperfeiçoar um código da HMC

Substitui o software da HMC por um novo nível de edição ou correcção do mesmo programa

Requer que inicie a partir dos suportes de recuperação

### Migrar código da HMC

Move dados da HMC de uma versão da HMC para outra

Uma migração é um tipo de aperfeiçoamento.

**Nota:** Para o modelo 7063-CR1 da HMC, é possível ligar uma unidade de DVD USB externa.

## Determinar a versão e a edição do código máquina da HMC

Obtenha informações sobre como visualizar a versão e a edição do código máquina da HMC.

## Sobre esta tarefa

O nível de código máquina na HMC determina as funcionalidades disponíveis, incluindo a manutenção e o aperfeiçoamento de software proprietário de servidor em simultâneo para actualizar para uma nova edição.

Para visualizar a versão e edição do código máquina da HMC, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.
3. Na nova janela, visualize e registe as informações que surgem sob o cabeçalho **Informações do Controlador Actual da HMC (Current HMC Driver Information)**, incluindo: a versão, edição, nível de manutenção, nível da compilação e versões base da HMC.

## Obter e aplicar actualizações de código máquina para a HMC com uma ligação à Internet

Saiba como obter actualizações do código máquina para a HMC, quando a HMC tiver uma ligação à Internet.

## Sobre esta tarefa

Para obter actualizações de código máquina para a HMC, conclua todos os passos.

### *Passo 1. Certifique-se de que tem uma ligação à Internet*

## Sobre esta tarefa

Para descarregar actualizações do sistema ou do sítio da Web de assistência e suporte para a HMC ou servidor, é necessário possuir uma das seguintes ligações:

- Conectividade SSL com ou sem um proxy SSL
- VPN da Internet

Para se assegurar de que tem uma ligação à Internet, execute o seguinte procedimento:

## Procedimento



1. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)** e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
2. Na área da janela de conteúdo, seleccione **Gerir Conectividade de Transmissão (Manage Outbound Connectivity)**.
3. Seleccione o separador para o tipo de conectividade de transmissão escolhido para a HMC (VPN de Internet ou conectividade SSL).

**Nota:** Se não existir uma ligação à assistência e suporte, é necessário configurar uma ligação de assistência antes de avançar neste procedimento. Para obter instruções sobre como configurar uma ligação à assistência e suporte, consulte o tópico Configurar o servidor para ligar à assistência e suporte IBM.

4. Faça clique em **Testar (Test)**.
5. Verifique se o teste foi concluído com êxito.

Se o teste não for concluído com êxito, detecte o problema de conectividade e resolva-o antes de continuar com este procedimento. Em alternativa, pode obter a actualização em DVD.

**Nota:** Para o modelo 7063-CR1 da HMC, é possível ligar uma unidade de DVD USB externa.

6. Avance para [“Passo 2. Visualizar o nível de código máquina da HMC existente”](#) na página 94.

## ***Passo 2. Visualizar o nível de código máquina da HMC existente***

### **Sobre esta tarefa**

Para visualizar o nível do código máquina existente da HMC, conclua os seguintes passos:

### **Procedimento**

1. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.
3. Na nova janela, veja e registe as informações que aparecem sob o cabeçalho Informações Actuais do Controlador da HMC, incluindo: a versão da HMC, a edição, o nível de manutenção, o nível da compilação e as versões base.
4. Avance para [“Passo 3. Visualizar os níveis do código máquina da HMC disponível”](#) na página 94.

## ***Passo 3. Visualizar os níveis do código máquina da HMC disponível***

### **Sobre esta tarefa**

Para visualizar os níveis do código máquina disponíveis da HMC, conclua os seguintes passos:

### **Procedimento**

1. Num computador ou servidor com ligação à Internet, aceda a <http://www.ibm.com/eserver/support/fixes>.
2. Seleccione a família adequada na lista Família de produtos.
3. Seleccione **Hardware Management Console** na lista de Tipo ou correcção de produtos.
4. Faça clique em **Continuar (Continue)**.  
É apresentado o sítio Consola de Gestão de Hardware (Hardware Management Console).
5. Desloque-se para baixo para o nível da versão da HMC para visualizar os níveis da HMC disponíveis.  
**Nota:** Se preferir, contacte a assistência e suporte.
6. Avance para [“Passo 4. Aplicar a actualização do código máquina da HMC”](#) na página 94.

## ***Passo 4. Aplicar a actualização do código máquina da HMC***

### **Sobre esta tarefa**

Para aplicar a actualização do código máquina da HMC, conclua os seguintes passos:

### **Procedimento**

1. Antes de instalar as actualizações do código máquina da HMC, efectue uma cópia de segurança das informações críticas da consola na HMC.  
Para obter instruções, consulte [“Criar uma cópia de segurança dos dados da consola”](#) na página 91.  
Em seguida, avance para o passo seguinte.



2. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
3. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**. Abre-se o assistente Instalar Serviço Correctivo (Install Corrective Service).
4. Siga as instruções do Assistente para instalar a actualização.
5. Encerre e reinicie a HMC para que a actualização entre em vigor.
6. Faça clique em **Iniciar sessão e iniciar a aplicação da Web da Consola de Gestão de Hardware (Log on and launch the Hardware Management Console web application)**.
7. Inicie sessão na interface da HMC.

### ***Passo 5. Verificar se a actualização do código máquina da HMC foi instalada com êxito***

#### **Sobre esta tarefa**

Para verificar se a actualização do código máquina da HMC foi correctamente instalada, conclua os seguintes passos:

#### **Procedimento**



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.
3. Na nova janela, veja e registe as informações que aparecem sob o cabeçalho Informações Actuais do Controlador da HMC, incluindo: a versão da HMC, a edição, o nível de manutenção, o nível da compilação e as versões base.
4. Verifique se a versão e a edição correspondem à actualização que instalou.
5. Se o nível de código apresentado não for o nível que instalou, execute os seguintes passos:
  - a. Seleccione a ligação de rede na HMC.
  - b. Repita a actualização do software proprietário utilizando um repositório diferente.
  - c. Se o problema persistir, contacte o nível seguinte de assistência.

### **Obter e aplicar actualizações de código máquina para a HMC utilizando um DVD ou um servidor de FTP**

Saiba como obter actualizações de código máquina para a Consola de Gestão de Hardware (HMC, Hardware Management Console) através da utilização de um DVD ou um servidor de FTP.

#### **Sobre esta tarefa**

Para obter actualizações de código máquina da HMC, conclua todos os passos.

**Nota:** Para o modelo 7063-CR1 da HMC, é possível ligar uma unidade de DVD USB externa.

### ***Passo 1. Visualizar o nível de código máquina existente da HMC***

#### **Antes de começar**

Para visualizar o nível do código máquina existente da HMC, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.
3. Na nova janela, veja e registe as informações que aparecem sob o cabeçalho Informações Actuais do Controlador da HMC, incluindo: a versão da HMC, a edição, o nível de manutenção, o nível da compilação e as versões base.
4. Avance para [“Passo 2. Visualizar os níveis do código máquina da HMC”](#) na página 96.

### ***Passo 2. Visualizar os níveis do código máquina da HMC***

#### **Antes de começar**

Para visualizar os níveis do código máquina disponíveis da HMC, conclua os seguintes passos:

#### **Sobre esta tarefa**

#### **Procedimento**

1. A partir de um computador ou de um servidor com ligação à Internet, aceda ao sítio da [Web Fix Central](#).
2. Desloque-se para baixo para o nível da versão da HMC para visualizar os níveis da HMC disponíveis.  
**Nota:** Se preferir, contacte a assistência e suporte IBM .
3. Avance para [“Passo 3. Obter actualização do código máquina da HMC”](#) na página 96.

### ***Passo 3. Obter actualização do código máquina da HMC***

#### **Antes de começar**

Para obter a actualização do código máquina da HMC, conclua os seguintes passos:

#### **Sobre esta tarefa**

Pode encomendar a actualização do código da máquina da HMC através do sítio Fix Central, contactando a assistência e suporte ou descarregando-a para um servidor de FTP.

#### **Encomendar a actualização do código máquina da HMC através do sítio da Web Fix Central**

1. A partir de um computador ou de um servidor com ligação à Internet, aceda ao sítio da [Web Fix Central](#).
2. Em Produtos suportados da HMC, seleccione o nível mais recente da HMC.
3. Desloque para baixo até à área Nomes de Ficheiros / Pacote (File names / Package) e localize a actualização que pretende encomendar.
4. Na coluna Encomendar (Order), seleccione **Ir (Go)**.
5. Faça clique em **Continuar (Continue)** para iniciar sessão com o ID da IBM.
6. Siga as instruções apresentadas no ecrã para submeter a encomenda.

#### **Descarregar a actualização do código máquina da HMC para suporte amovível**

1. A partir de um computador ou de um servidor com ligação à Internet, aceda ao sítio da [Web Fix Central](#).
2. Em Produtos suportados da HMC, seleccione o nível mais recente da HMC.

3. Desloque para baixo até à área Nomes de Ficheiros / Pacote (File names / Package) e localize a actualização que pretende descarregar.
4. Faça clique na actualização que pretende descarregar.
5. Aceite o acordo de licença e guarde a actualização no suporte amovível.

### Como proceder a seguir

Quando terminar, avance para [“Passo 4. Aplicar a actualização do código máquina da HMC”](#) na página 97.

### ***Passo 4. Aplicar a actualização do código máquina da HMC***

#### **Antes de começar**

Para aplicar a actualização do código máquina da HMC, conclua os seguintes passos:

#### **Procedimento**

1. Antes de instalar as actualizações para o código máquina da HMC, efectue uma cópia de segurança dos dados da HMC. Para obter mais informações, consulte [“Criar uma cópia de segurança dos dados da consola”](#) na página 91.
2. Se obteve ou criou a actualização em DVD-RAM, insira-o na unidade de DVD da HMC. Se obteve ou criou a actualização num dispositivo de memória USB, insira o dispositivo de memória.
3. Antes de instalar as actualizações do código máquina da HMC, efectue uma cópia de segurança das informações críticas da consola na HMC.  
Para obter instruções, consulte [“Criar uma cópia de segurança dos dados da consola”](#) na página 91. Em seguida, avance para o passo seguinte.



4. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
5. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**. Abre-se o assistente Instalar Serviço Correctivo (Install Corrective Service).
6. Siga as instruções do Assistente para instalar a actualização.
7. Encerre, reinicie e faça novamente o registo na HMC para que a actualização entre em vigor.
8. Avance para [“Passo 5. Verificar se a actualização do código máquina da HMC foi instalada com êxito”](#) na página 97.

### ***Passo 5. Verificar se a actualização do código máquina da HMC foi instalada com êxito***

#### **Antes de começar**

Para verificar se a actualização do código máquina da HMC foi instalada com êxito, conclua os seguintes passos:

#### **Procedimento**

1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.



3. Na nova janela, veja e registe as informações que aparecem sob o cabeçalho Informações Actuais do Controlador da HMC, incluindo: a versão da HMC, a edição, o nível de manutenção, o nível da compilação e as versões base.
4. Verifique se a versão e a edição correspondem à actualização que instalou.
5. Caso o nível de código apresentado não seja o nível que instalou, execute os seguintes passos:
  - a. Repita a actualização do código máquina. Se tiver criado um DVD para este procedimento, utilize um novo suporte.
  - b. Se o problema persistir, contacte o nível seguinte de assistência.

## Actualizar o software da HMC

Saiba como actualizar o software numa HMC de uma edição para a seguinte enquanto mantém os dados de configuração da HMC.

### Sobre esta tarefa

Para actualizar o código máquina numa HMC, conclua todos os passos.

**Nota:** Para os modelos da HMC 7063-CR1 e 7063-CR2, pode ligar uma unidade de DVD USB externa.

### *Passo 1. Obter a actualização*

#### Sobre esta tarefa

É possível encomendar a actualização do código máquina da HMC através do sítio da Web [Fix Central](#).

Para obter a actualização através do sítio da Web [Fix Central](#), conclua os seguintes passos:

#### Procedimento

1. A partir de um computador ou servidor com uma ligação à Internet, aceda ao sítio da Web da Consola de Gestão de Hardware em <http://www-933.ibm.com/support/fixcentral/>.
2. Faça clique em **Continuar (Continue)**.  
É apresentado o sítio Consola de Gestão de Hardware (Hardware Management Console).
3. Navegue para a versão da HMC para a qual pretende actualizar.
4. Localize a secção de encomenda e descarregamento.  
**Nota:** Caso não possua acesso à Internet, contacte a assistência e suporte da IBM para encomendar a actualização em DVD.
5. Siga as instruções apresentadas no ecrã para submeter a encomenda.
6. Quando tiver a actualização, avance para [“Passo 2. Visualizar o nível de código máquina da HMC existente”](#) na página 98.

### *Passo 2. Visualizar o nível de código máquina da HMC existente*

#### Sobre esta tarefa

Para determinar o nível existente do código máquina numa HMC, siga estes passos:

#### Procedimento

1. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, seleccione **Gestão da Consola**. Na área de navegação, faça clique em **Actualizações (Updates)**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.

3. Na nova janela, visualize e registe as informações que surgem sob o cabeçalho de informações Controlador Actual da HMC, incluindo a versão da HMC, edição, nível de manutenção, nível de compilação e versões base.
4. Avance para [“Passo 3. Efectuar cópia de segurança dos dados do perfil do sistema gerido”](#) na página 99.

### ***Passo 3. Efectuar cópia de segurança dos dados do perfil do sistema gerido***

#### **Sobre esta tarefa**

Para efectuar uma cópia de segurança dos dados do perfil do sistema gerido, conclua os seguintes passos:

#### **Procedimento**

1. Seleccione o sistema para o qual pretende guardar os dados de perfil.
2. Faça clique em **Acções (Actions) > Ver Todas as Acções (View All Actions) > Anteriores (Legacy) > Gerir Dados de Partições (Manage Partition Data) > Cópia de Segurança (Backup)**.
3. Escreva um nome de ficheiro de cópia de segurança e registe estas informações.
4. Faça clique em **OK**.
5. Repita estes passos para cada sistema.
6. Avance para [“Passo 4. Fazer cópia de segurança dos dados da HMC”](#) na página 99.

### ***Passo 4. Fazer cópia de segurança dos dados da HMC***

#### **Sobre esta tarefa**

Efectue uma cópia de segurança dos dados da HMC antes de instalar uma nova versão de software da HMC de forma a que seja possível restaurar os níveis anteriores caso ocorra um problema enquanto actualiza o software. Não utilize estes dados importantes da consola após uma actualização com êxito para uma nova versão do software da HMC.

**Nota:** Para efectuar uma cópia de segurança para suporte amovível, é necessário ter o suporte disponível.

Para efectuar uma cópia de segurança dos dados da HMC, conclua os seguintes passos:

#### **Procedimento**

1. Se pretende criar uma cópia de segurança em suporte, execute os seguintes passos para formatar o suporte:
  - a. Insira o suporte na unidade.
  - b. Na área de navegação, faça clique no ícone **Reparabilidade (Serviceability)**  e, em seguida, seleccione **Gestão de Assistência (Service Management)**.
  - c. Na área de janela de conteúdos, faça clique em **Formatar Suporte (Format Media)**.
  - d. Seleccione o tipo de suporte de dados.
  - e. Seleccione o tipo de formato.
  - f. Faça clique em **OK**.
2. Na área de navegação, faça clique no ícone **Gestão da HMC**  e, em seguida, seleccione **Gestão da Consola**.
3. Na área da janela de conteúdo, faça clique em **Criar cópia de segurança dos dados da Consola de Gestão (Backup Management Console Data)**.

É aberta a janela **Criar Cópia de Segurança dos Dados da Consola de Gestão (Backup Management Console Data)**.

4. Seleccione uma opção de arquivo.

É possível criar uma cópia de segurança para um suporte num sistema local, um sistema remoto instalado no sistema de ficheiros da HMC (por exemplo, NFS) ou enviar a cópia de segurança para um sítio remoto através da utilização do Protocolo de Transferência de Ficheiros (FTP, File Transfer Protocol).

- Para efectuar uma cópia de segurança num sistema local, seleccione **Efectuar cópia de segurança do suporte de dados no sistema local (Back up to media on local system)** e siga as instruções.
- Para efectuar uma cópia de segurança num sistema remoto instalado, seleccione **Efectuar cópia de segurança em sistema remoto instalado (Back up to mounted remote system)** e siga as instruções.
- Para efectuar uma cópia de segurança num local de FTP remoto, seleccione **Enviar cópia de segurança de dados críticos para local remoto (Send back up critical data to remote site)** e siga as instruções.

5. Avance para [“Passo 5. Registar as informações actuais da configuração da HMC”](#) na página 100.

## ***Passo 5. Registar as informações actuais da configuração da HMC***

### **Sobre esta tarefa**

Como medida preventiva, antes de efectuar a actualização para uma nova versão de software da HMC, registe as informações de configuração da HMC.

Para registar a configuração actual da HMC, conclua os seguintes passos:

### **Procedimento**

1. Seleccione um sistema gerido ou quaisquer partições que pretende para registar as informações de configuração da HMC.
2. A partir do pod do menu, seleccione **Ações (Actions) > Agendar Operações (Schedule Operations)**. São apresentadas todas as operações agendadas para o destino seleccionado.
3. Seleccione **Ordenar (Sort) > Por objecto (By Object)**.
4. Seleccione cada objecto e registe os seguintes detalhes:
  - Nome do Objecto
  - Data agendada
  - Hora da Operação (apresentada no formato de 24 horas)
  - Repetitiva (caso seja Sim, conclua os seguintes passos):
    - a. Seleccione **Visualizar (View) > Detalhes de Agendamento (Schedule Details)**.
    - b. Registe as informações de intervalo.
    - c. Feche a janela de operações agendadas.
    - d. Repita o procedimento para cada operação agendada.
5. Feche a janela **Personalizar Operações Agendadas (Customize Scheduled Operations)**.
6. Avance para [“Passo 6. Registar estado do comando remoto”](#) na página 100.

## ***Passo 6. Registar estado do comando remoto***

### **Sobre esta tarefa**

Para registar o estado do comando remoto, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Utilizadores e Segurança (Users and Security)** e, em seguida, seleccione **Segurança de Sistemas e Consola (Systems and Console Security)**.
2. Na área da janela de conteúdos, faça clique em **Activar Execução de Comandos Remotos (Enable Remote Command Execution)**.
3. Registe se a caixa de verificação **Activar a execução do comando remoto utilizando o serviço ssh (Enable remote command execution using the ssh facility)** está seleccionada.
4. Faça clique em **Cancelar (Cancel)**.
5. Avance para [“Passo 7. Guardar dados de actualização”](#) na página 101.

### **Passo 7. Guardar dados de actualização**

#### **Sobre esta tarefa**

Pode guardar a configuração actual da HMC na partição de disco designada na HMC ou no suporte de dados local. Guarde os dados da actualização apenas imediatamente antes de actualizar o software da HMC para uma nova edição. É possível restaurar as definições de configuração da HMC após actualizar.

**Nota:** Apenas é permitido um nível de dados de cópia de segurança. Sempre que guardar os dados da actualização, o nível anterior é substituído.

Para guardar os dados da actualização, conclua os seguintes passos:

## Procedimento



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Guardar dados de actualização (Save Upgrade Data)**. É aberto o assistente **Guardar Dados de Actualização (Save Upgrade Data)**.
3. Seleccione o suporte no qual pretende guardar os dados actualizados. Se optar por guardar num suporte de dados removível, insira agora o suporte. Faça clique em **Seguinte (Next)**.
4. Faça clique em **Terminar (Finish)**.
5. Aguarde que a tarefa seja concluída.  
Se a tarefa Guardar Dados de Actualização (Save Upgrade Data) falhar, contacte o nível seguinte de suporte antes de continuar.  
**Nota:** Caso ocorra uma falha ao guardar os dados de actualização, não prossiga o processo de actualização.
6. Faça clique em **OK**.
7. Avance para [“Passo 8. Actualizar o software da HMC”](#) na página 101.

### **Passo 8. Actualizar o software da HMC**

#### **Sobre esta tarefa**

Para actualizar o software da HMC, reinicie o sistema colocando o suporte amovível na unidade de DVD.

## Procedimento

1. Insira o suporte de Instalação do Produto da HMC na unidade de DVD.



2. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
3. Na área da janela de conteúdo, seleccione **Desligar ou reiniciar a Consola de Gestão (Shutdown or Restart the Management Console)**.
4. Certifique-se de que a opção **Reiniciar a HMC (Restart the HMC)** está seleccionada.
5. Faça clique em **OK**.  
A HMC é reiniciada e as informações do sistema deslocam-se na janela.
6. Seleccione **Actualizar (Upgrade)** e faça clique em **Seguinte (Next)**.
7. Escolha uma das seguintes opções:
  - Caso tenha guardado os dados da actualização durante a tarefa anterior, continue com o próximo passo.
  - Caso não tenha guardado os dados da actualização anteriormente neste procedimento, será necessário guardar os dados da actualização de imediato antes de continuar.
8. Seleccione **Actualizar a partir de suporte (Upgrade from media)** e faça clique em **Seguinte (Next)**.
9. Confirme as definições e faça clique em **Terminar (Finish)**.
10. Siga os pedidos de informação.

**Nota:**

- Se o ecrã ficar em branco, prima a barra de espaços para visualizar as informações.
  - O primeiro DVD pode demorar aproximadamente 20 minutos a ser instalado.
11. Quando for apresentado o pedido de informação de início de sessão, inicie sessão utilizando o ID de utilizador e a palavra-passe.  
A instalação do código da HMC fica concluída.
  12. Avance para [“Passo 9. Verificar se a actualização do código máquina da HMC foi instalada com êxito” na página 102.](#)

### ***Passo 9. Verificar se a actualização do código máquina da HMC foi instalada com êxito***

#### **Sobre esta tarefa**

Para verificar se a actualização da HMC foi instalada com êxito, conclua os seguintes passos:

#### **Procedimento**



1. Na área de navegação, faça clique no ícone **Gestão da HMC** e, em seguida, seleccione **Gestão da Consola**.
2. Na área da janela de conteúdo, faça clique em **Actualizar a Consola de Gestão de Hardware (Update the Hardware Management Console)**.
3. Na nova janela, visualize e registe as informações que surgem sob o cabeçalho de informações Controlador Actual da HMC, incluindo a versão da HMC, edição, nível de manutenção, nível de compilação e versões base.
4. Verifique se a versão e a edição correspondem à actualização que instalou.
5. Caso o nível de código apresentado não seja o nível que instalou, volte a tentar a tarefa de actualização através da utilização de um novo DVD. Se o problema persistir, contacte o nível seguinte de assistência.

## Actualizar a HMC a partir de uma localização remota através da utilização de imagens de actualização da rede

Saiba como actualizar o software numa HMC a partir de uma localização remota através da utilização de imagens de actualização da rede.

### Sobre esta tarefa

Saiba como actualizar o software numa HMC a partir de uma localização remota através da utilização de imagens de actualização da rede.

### Procedimento

1. A partir de um computador ou servidor com uma ligação à Internet, aceda ao [Sítio da Web de Assistência e descargas da Consola de Gestão de Hardware](http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html) (<http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html>).
2. Descarregue as imagens de rede da HMC V9 adequadas e guarde as mesmas num servidor de FTP. Não é possível descarregar estes ficheiros directamente para a HMC. Tem de descarregar os ficheiros de imagem para um servidor que aceita pedidos de FTP.
3. Certifique-se de que descarrega os seguintes ficheiros:
  - img2a
  - img3a
  - base.img
  - disk1.img
  - hmcnetworkfiles.sum
4. Guarde os dados actualizados na HMC. Execute os seguintes comandos para guardar os dados de actualização:
  - Para guardar dados em DVD e HDD, execute os seguintes comandos:  
**mount /media/cdrom**  
**saveupgdata -r diskdvd**
  - Para guardar dados na HDD, execute o seguinte comando:  
**saveupgdata -r disk**
5. Copie os ficheiros de actualização para a partição de disco passível de arranque na HMC. Execute o comando **getupgfiles** para copiar os ficheiros.  
Exemplo: **getupgfiles -h <servidor de ftp> -u <ID de utilizador> -d <directório remoto>**  
Onde,
  - **servidor de ftp** é o nome do sistema central ou endereço de IP do servidor de FTP onde descarrega as imagens de rede da HMC.
  - **ID de utilizador** é um ID de utilizador válido no servidor de FTP. Caso não especifique a palavra-passe com o argumento `--passwd`, ser-lhe-á pedida uma palavra-passe.
  - **directório remoto** é o directório no servidor de FTP onde as imagens de rede da HMC são guardadas.
6. Reinicie a HMC para actualizar o código que é copiado para a partição de disco passível de arranque. Execute o comando **chhmc -c altdiskboot -s enable --mode upgrade** para reiniciar a HMC.
7. Reinicie a HMC e inicie a actualização. Execute o comando **hmcshutdown -r -t now** para iniciar a actualização.

## Proteger a HMC

---

Saiba como melhorar a segurança da Consola de Gestão de Hardware (HMC, Hardware Management Console) baseada nos padrões de segurança empresariais.

A configuração predefinida da HMC faculta bastante segurança para a maioria dos utilizadores empresariais. Com a Consola de Gestão de Hardware (HMC, Hardware Management Console) Versão 8.4.0 ou posterior, é possível melhorar ainda mais a segurança da HMC baseada nos padrões de segurança empresariais. Para melhorar a segurança para a HMC, é necessário definir a HMC para um mínimo de segurança de Nível 1. Poderá seleccionar segurança de Nível 2 e Nível 3, dependendo do ambiente e dos requisitos de segurança empresarial.

**Nota:** Antes de alterar o nível de segurança, confirme com a equipa de conformidade de segurança empresarial.

### Segurança de Nível 1

Para proteger a HMC (segurança de nível 1), conclua os seguintes passos:

1. Altere a palavra-passe predefinida para o utilizador `hscroot` predefinido. Para obter mais informações sobre a política de palavras-passe, consulte [“Política aperfeiçoada de palavras-passe” na página 106](#).
2. Caso a HMC não pertença a um ambiente fisicamente seguro, defina a palavra-passe `grub` através da execução do seguinte comando: `chmmc -c grubpasswd -s enable --passwd <new grub password>`
3. Caso tenha configurado o Módulo de Gestão Integrada (IMM, Integrated Management Module) na HMC, defina uma palavra-passe do IMM segura.
4. Defina uma palavra-passe segura para o utilizador `admin` e utilizadores gerais em todos os servidores.
5. Actualize a HMC com as correcções de segurança publicadas mais recentes. Para obter mais informações sobre as correcções de segurança, consulte a [IBM Fix Central](#).

### Segurança de Nível 2

Caso tenha múltiplos utilizadores, conclua os seguintes passos para melhorar a segurança para a HMC:

1. Crie uma conta para cada utilizador na HMC e atribua as funções e recursos requeridos aos utilizadores. Para obter mais informações sobre as várias funções na HMC, consulte [Tarefas, funções de utilizadores, IDs e comandos associados da HMC](#).

**Nota:** Certifique-se de que atribui apenas os recursos e funções requeridos para utilizadores que são criados na HMC. Caso seja necessário, também poderá criar funções personalizadas.

2. Active a replicação de dados de utilizadores entre diferentes Consolas de Gestão de Hardware. A replicação de dados de utilizadores poderá ser executada no modo Principal-Secundário ou Par-Par. Para obter mais informações sobre a replicação de dados de utilizadores, consulte [Gerir a Replicação de Dados](#).
3. Importe um certificado assinado pela Autoridade Certificadora.

### Segurança de Nível 3

Caso tenha múltiplos administradores, conclua os seguintes passos para melhorar a segurança para a HMC:

1. Utilize autenticação centralizada como, por exemplo, LDAP (Lightweight Directory Access Protocol) ou Kerberos. Para obter mais informações sobre a configuração de LDAP, consulte [Como configurar LDAP na HMC](#).
2. Active a replicação de dados de utilizadores entre diferentes Consolas de Gestão de Hardware.
3. Certifique-se de que a HMC se encontra no [modo NIST SP 800-131A](#) de forma a que a HMC utilize apenas cifras seguras.

4. Bloqueie portas não requeridas na firewall. Para obter informações sobre as portas da HMC que podem ser utilizadas, consulte a seguinte tabela:

*Tabela 32. Porta utilizada pelo utilizador para interação com a HMC*

<b>Porta</b>	<b>Descrição</b>	<b>Tipo</b>	<b>Versão do Protocolo (Modo predefinido)</b>	<b>Versão do Protocolo (Modo NIST)</b>
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	Agente de SNMP	UDP	SNMP v3	SNMP v3
162	Desvio de SNMP	UDP	SNMP v3	SNMP v3
427	SLP	UDP	N/D	N/D
443	GUI da HMC e API REST	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (Texto simples + indexação e assinatura)	RSCT (Texto simples + indexação e assinatura)
2300	Terminal 5250 para IBM i	TCP	Texto simples	Texto simples
2301	Terminal protegido 5250 para IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (porta anterior, não funcional)	TCP	Não funcional	Não funcional
9900	FCS: Identificação HMC-HMC	UDP	FCS	FCS
9920	FCS: Comunicação HMC-HMC	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	Applet VTerm na GUI	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	API REST da HMC (porta anterior)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	Domínio de Pares RSCT	UDP	RSCT (Texto simples + indexação e assinatura)	RSCT (Texto simples + indexação e assinatura)
12348	Domínio de Pares RSCT	UDP	RSCT (Texto simples + indexação e assinatura)	RSCT (Texto simples + indexação e assinatura)

**Notas:**

- É necessário utilizar apenas SSH (porta 22), HTTPS (porta 443 e porta 12443), terminal protegido 5250 para IBM i (porta 2301) e VTerm (porta 9960) expostos a uma intranet. Todas as outras portas têm de ser utilizadas numa rede privada ou isolada. É possível utilizar uma porta Ethernet e VLAN separadas para a Monitorização e Controlo de Recursos (RMC, Resource Monitoring and Control) (porta 657), FCS (porta 9900 e porta 9920) e Domínio de Pares RSCT (porta 12347 e porta 12348).
- As portas listadas pelo comando **netstat** apenas são utilizadas para processos internos.

## Política aperfeiçoada de palavras-passe

Pode aplicar os requisitos de palavra-passe para utilizadores autenticados localmente utilizando a Consola de Gestão de Hardware (HMC). A função de política aperfeiçoada de palavras-passe permite ao administrador do sistema definir restrições de palavras-passe. A política aperfeiçoada de palavras-passe aplica-se aos sistemas nos quais está instalada uma HMC.

Os administradores do sistema podem utilizar a política aperfeiçoada de palavras-passe para definirem uma única política de palavras-passe para todos os utilizadores. A HMC fornece uma política de palavras-passe de segurança média, que pode ser activada pelos administradores do sistema para definir restrições de palavras-passe. O administrador do sistema também poderá optar por activar a política de segurança média ou uma nova política definida pelo utilizador. A política de palavras-passe de segurança média da HMC não pode ser removida do sistema. A tabela seguinte enumera os atributos da política de segurança média e os valores predefinidos.

*Tabela 33. Atributos de palavras-passe para a política de segurança média da HMC*

Atributo	Descrição	Valor predefinido
min_pwage	O número mínimo de dias para os quais uma palavra-passe tem de permanecer activa.	1
pwage	O número máximo de dias para os quais uma palavra-passe poderá permanecer activa.	180
min_length	O comprimento mínimo de uma palavra-passe.	8
hist_size	O número de palavras-passe previamente guardadas que não podem ser utilizadas.	10
warn_pwage	Quando a palavra-passe está prestes a expirar, o número de dias antes dos quais um utilizador é avisado que a palavra-passe está prestes a expirar.	7
min_digits	O número mínimo de dígitos requeridos para serem utilizados na palavra-passe.	Nenhum
min_uppercase	O número mínimo de caracteres em maiúsculas.	1
min_lowercase	O número mínimo de caracteres em minúsculas.	6
min_special_chars	O número mínimo de caracteres especiais que têm de ser utilizados na palavra-passe.	Nenhum

Considere os seguintes itens acerca da política de palavras-passe de segurança média da HMC.

- A política não se aplica aos IDs de utilizador **hscroot**, **hscpe** e **root**.
- A política afecta apenas os utilizadores autenticados localmente que são geridos pela HMC e não é possível impor a política em utilizadores LDAP ou Kerberos.
- A política de palavras-passe de segurança média da HMC ou a política definida pelo utilizador permitem que os administradores do sistema definam restrições de reutilização de palavras-passe.

- A palavra-passe de segurança média da HMC é só de leitura e os atributos da palavra-passe de segurança média da HMC não podem ser alterados. Pode criar uma nova palavra-passe definida pelo utilizador para definir a restrição da palavra-passe.

Pode utilizar os comandos seguintes para configurar a política de palavras-passe de segurança média da HMC:

#### **mkpwdpolicy**

Importa a política de palavras-passe a partir de um ficheiro que contém todos os parâmetros ou cria uma política de palavras-passe.

#### **lspwdpolicy**

Lista todos os perfis de política de palavras-passe disponíveis e procura por parâmetros específicos. Também é possível visualizar a política de palavras-passe activa actualmente.

#### **rmpwdpolicy**

Remove uma política de palavras-passe existente inactiva.

**Nota:** Não é possível remover uma política de segurança média activa e a política de palavras-passe só de leitura predefinida.

#### **chpwdpolicy**

Altera parâmetros de uma política de palavras-passe inactiva.

## **Resolver problemas comuns enquanto protege a HMC**

Saiba como resolver alguns problemas que poderá encontrar quando proteger a HMC.

### **Como proteger a ligação entre a Consola de Gestão de Hardware (HMC, Hardware Management Console) e o sistema?**

A HMC estabelece ligação ao sistema através do FSP (Flexible Service Processor). Um protocolo binário proprietário denominado protocolo NETC (Network Client) é utilizado para gerir o FSP e o hipervisor Power. A seguinte tabela lista portas utilizadas pela HMC:

*Tabela 34. Portas no FSP que são utilizadas para interagir com a HMC*

<b>Porta no FSP</b>	<b>Descrição</b>	<b>Versão do Protocolo (Modo predefinido)</b>	<b>Versão do Protocolo (Modo NIST)</b>
443	Interface de Gestão do Sistema Avançada	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). Reverte para SSLv3 para suporte de software proprietário mais antigo.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). Reverte para SSLv3 para suporte de software proprietário mais antigo.	NETC (TLS 1.2)

### **Como bloquear a HMC?**

Caso pretenda melhorar a segurança da infra-estrutura, é possível utilizar um dispositivo de Prevenção de Intrusões (IPS, Intrusion Prevention System) ou adicionar todas as Consolas de Gestão de Hardware e servidores IBM Power Systems por detrás de uma firewall. Além disso, é possível desactivar serviços de rede na HMC caso não a utilize remotamente ou caso pretenda bloquear a HMC. Para desactivar serviços de rede na HMC, conclua os seguintes passos:

1. Desactive a execução do comando remoto através da utilização da porta SSH.
2. Desactive o terminal virtual remoto (porta VTerm).

3. Desactive o [acesso da Web remota](#) (interface gráfica de utilizador da HMC e API REST).
4. Bloqueie portas na firewall através da utilização das definições de rede da HMC para cada porta Ethernet configurada.

### Como definir a HMC no modo de conformidade NIST SP 800-131A?

Com a HMC Versão 8.1.0 ou posterior, quando definir a HMC no modo de conformidade, apenas são suportadas cifras seguras listadas por [NIST SP 800-131A](#). Poderá não ser possível estabelecer ligação a servidores Power Systems mais antigos como, por exemplo, servidores POWER5 que não suporta Transport Layer Security (TLS 1.2). Para obter mais alterações sobre a alteração do modo de segurança, consulte [Modo V8R8 NIST da HMC](#).

### Como visualizar e alterar cifras utilizadas pela HMC?

Com a HMC Versão 8.1.0 ou posterior, a HMC suporta mais conjuntos de cifras seguras definidas em NIST 800-131A. As cifras que são utilizadas no modo predefinido são seguras. Para obter mais informações sobre cifras de encriptação utilizadas pela HMC, execute o comando **lshmcencr**. Caso o padrão empresarial requeira a utilização de um conjunto diferente de cifras, execute o comando **chhmcencr** para modificar as cifras de encriptação.

Para listar as cifras de encriptação utilizadas pela HMC para encriptar palavras-passe de utilizadores, execute o seguinte comando:

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

Para listar as cifras de encriptação que podem ser utilizadas actualmente pela interface da Web de utilizador de HMC e API REST, execute o seguinte comando:

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

Para listar as cifras de encriptação e algoritmo MAC que podem ser utilizados actualmente pela interface SSH da HMC, execute o seguinte comando:

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

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

### Como verificar a potência do certificado na HMC?

Os certificados de assinatura local na HMC utilizam SHA256 com encriptação RSA de 2048-bits, que é segura. Caso esteja a utilizar certificados assinados CA, certifique-se de que não está a utilizar a encriptação de 1024-bits, que é fraca. É possível utilizar os seguintes certificados para a HMC:

- É possível utilizar o certificado assinado CA para a interface de utilizador gráfica da HMC e API REST (portas 443 e 12443).
- A porta 9920 é utilizada para comunicação HMC a HMC. Não é possível substituir este certificado por um certificado próprio.

### Como escolher entre um certificado de assinatura local (predefinição) ou um certificado assinado CA?

A HMC cria automaticamente um certificado durante a instalação. No entanto, é possível criar um Pedido de Assinatura de Certificado (CSR, Certificate Signing Request) a partir da HMC e obter um novo certificado emitido por uma Autoridade Certificadora. É possível importar este certificado para a HMC. Certifique-se de que também obtém um nome de domínio para a HMC. Para obter mais detalhes sobre a gestão dos certificados na HMC, consulte [Gerir Certificados](#).

## Como auditar a HMC?

A auditoria nas Consolas de Gestão de Hardware foca-se em cifras configuradas e a actividade de utilização dos vários utilizadores da HMC. Utilize os seguintes comandos para visualizar a actividade de utilização de vários utilizadores da HMC:

Finalidade	Comando
Codificação de palavras-passe (definição global)	<code>lshmcencr -c passwd -t c</code>
Codificação de palavras-passe para cada utilizador	<code>lshmcusr -Fname:password_encryption</code>
Cifras SSH	<code>lshmcencr -c ssh -t c</code>
MAC de SSH	<code>lshmcencr -c sshmac -t c</code>
Cifras utilizadas para a interface de utilizador gráfica da HMC e API REST	<code>lshmcencr -c webui -t c</code>

Utilize os seguintes comandos para monitorizar várias informações da consola e de eventos passíveis de assistência para utilizadores na HMC:

Informações	Comando
Utilizadores da GUI	<code>lslogon -r webui -u</code>
Tarefas da GUI	<code>lslogon -r webui -t</code>
Utilizadores da CLI	<code>lslogon -r ssh -u</code>
Tarefas da CLI	<code>lslogon -r ssh -t</code>
Operações na HMC	<code>lssvcevents -t console -d &lt;number of days&gt;</code>
Operações no Sistema	<code>lssvcevents -t hardware -m &lt;managed system&gt; -d &lt;number of days&gt;</code>

**Eventos de monitorização centralizada para a HMC:** Caso possua várias Consolas de Gestão de Hardware, defina o ficheiro `rsyslog` para recolher todos os dados de utilização.

## Como corrige a IBM as vulnerabilidades de segurança da HMC?

A IBM possui um processo de resposta a incidências de segurança denominado Equipa de Resposta a Incidentes de Segurança de Produtos da IBM (PSIRT, IBM Product Security Incident Response Team). A PSIRT (IBM Product Security Incident Response Team) é uma equipa global que gere a recepção, investigação e coordenação interna de informações de vulnerabilidades de segurança relacionadas com ofertas da IBM. Os componentes de Código Aberto e da IBM que são enviados com a HMC são monitorizados e analisados de forma activa. As correcções provisórias e correcções de segurança são facultadas pela IBM para todas as edições suportadas da HMC.

## Como rastrear novas correcções provisórias na HMC?

O boletim de segurança contém informações sobre a vulnerabilidade e correcções provisórias para versões suportadas da HMC. Para rastrear correcções provisórias na HMC, é possível:

- Procurar os boletins de segurança mais recentes em [IBM Security Bulletin](#).
- Seguir [@IBMPowerSupp](#) no Twitter para obter notificações.

- Subscrever notificações de correio electrónico em [IBM Support](#).

## Perfis de segurança: Security profiles: Regulamentação de Protecção de Dados Globais (GDPR, Global Data Protection Regulation) e Padrão de Segurança de Dados de Indústria de Cartões de Pagamento (PCI-DSS, Payment Card Industry Data Security Standard)

Saiba como a Consola de Gestão de Hardware (HMC, Hardware Management Console) processa as informações de privacidade dos utilizadores.

A Consola de Gestão de Hardware (HMC, Hardware Management Console) é um dispositivo fechado que não armazenada quaisquer dados de titulares de cartões. Como tal, apenas um subconjunto de requisitos e procedimentos de avaliação de segurança da segurança das tecnologias de informação que são definidos por PCI-DSS são aplicáveis para a HMC. Apenas é possível instalar código fidedigno distribuído pela IBM na HMC. Quando qualquer vulnerabilidade é conhecida através do [processo PSIRT da IBM](#), são publicadas correcções provisórias. Os requisitos e recomendações incluem os seguintes itens:

### Consultas GDPR

<i>Tabela 37. Consultas GDPR. A tabela faculta informações sobre as questões relacionadas com GDPR.</i>	
Perguntas	Respostas
Que tipo de dados são armazenados na HMC?	A HMC armazena informações de configuração de hardware Power, virtualização PowerVM e as informações sobre as métricas de desempenho.
A HMC processa quaisquer dados pessoais?	É possível facultar informações de contacto para a função de chamada de assistência. Facultar informações de contacto para a função de chamada de assistência é opcional.
Que contas predefinidas são utilizadas para a administração do sistema da HMC?	O utilizador administrador do sistema utiliza o nome de utilizador <i>hscroot</i> .
Alguma das contas na HMC está relacionada com alguma pessoa específica?	Não.
É obrigatório facultar dados pessoais na HMC?	Não. Não é necessário facultar informações de dados pessoais. Porém, facultar estas informações é opcional.
O ficheiro de registo da HMC possui algumas informações de dados pessoais?	Não.
É possível eliminar dados pessoais completa e permanentemente?	Sim. Anule a configuração da função de chamada de assistência.

### Consultas PCI-DSS

<i>Tabela 38. Consultas PCI-DSS. A tabela faculta informações sobre as questões relacionadas com PCI-DSS.</i>	
Perguntas	Respostas
Como instalar e manter uma configuração de firewall para proteger os dados do titular do cartão?	A HMC não armazena nem acede a quaisquer dados de titulares de cartões. Porém, a HMC possui uma configuração de firewall e o utilizador poderá controlar e activar portas específicas.

*Tabela 38. Consultas PCI-DSS. A tabela faculta informações sobre as questões relacionadas com PCI-DSS. (continuação)*

<b>Perguntas</b>	<b>Respostas</b>
Posso utilizar o valor predefinido facultado pelo fornecedor para palavras-passe do sistema e outros parâmetros de segurança?	Antes de instalar um sistema na rede, altere todas as palavras-passe predefinidas do utilizador <i>hscroot</i> .
Como protege a HMC os dados armazenados do titular do cartão?	A HMC não armazena nem acede a quaisquer dados de titulares de cartões.
Como encripta a HMC os dados do titular do cartão quando os dados são transmitidos através de redes públicas abertas?	A HMC não armazena nem acede a quaisquer dados de titulares de cartões.
Como utilizar e actualizar com regularidade programas de software anti-vírus?	A HMC é um dispositivo fechado. Como tal, software malicioso não consegue contaminar a HMC.
Como desenvolver e manter sistemas e aplicações seguros?	É necessário instalar manualmente as correcções requeridas para o sistema a partir do sítio da Web da <a href="#">IBM Fix Central</a> . Apenas é possível instalar código fidedigno distribuído pela IBM na HMC.
A HMC restringe o acesso aos dados do titular do cartão?	A HMC não armazena nem acede a quaisquer dados de titulares de cartões.
Como atribuir um ID exclusivo a cada pessoa que possui acesso ao computador?	É possível implementar este requisito ao certificar-se de que não existem IDs partilhados e ao seguir as políticas de palavras-passe.
Como restringir o acesso físico aos dados do titular do cartão?	A HMC não armazena nem acede a quaisquer dados de titulares de cartões
Como rastrear e monitorizar o acesso a recursos de rede e aos dados do titular do cartão?	A HMC não armazena nem acede a quaisquer dados de titulares de cartões.
Como testa a HMC a segurança do sistema e processos?	São utilizadas ferramentas de análise para executar análises de segurança em todas as versões lançadas da HMC. As ferramentas de análise incluem: <i>Qualys, Nessus, testssl, sslscan e ASoC</i> .
Como manter uma política de segurança que inclui segurança de informações para funcionários e subcontratados?	O administrador do sistema desactiva o início de sessão remoto de utilizadores, activa o início de sessão de utilizadores conforme necessário e desactiva o início de sessão de utilizadores quando o acesso já não for requerido.

## Localizações das portas HMC

É possível encontrar localizações de portas através da utilização de códigos de localização. Utilize as ilustrações para mapear o código de localização para a posição da porta da HMC no servidor.

### **Localizações de portas da HMC do modelo 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S**

Utilize este diagrama e tabela para mapear as portas da HMC no 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S.

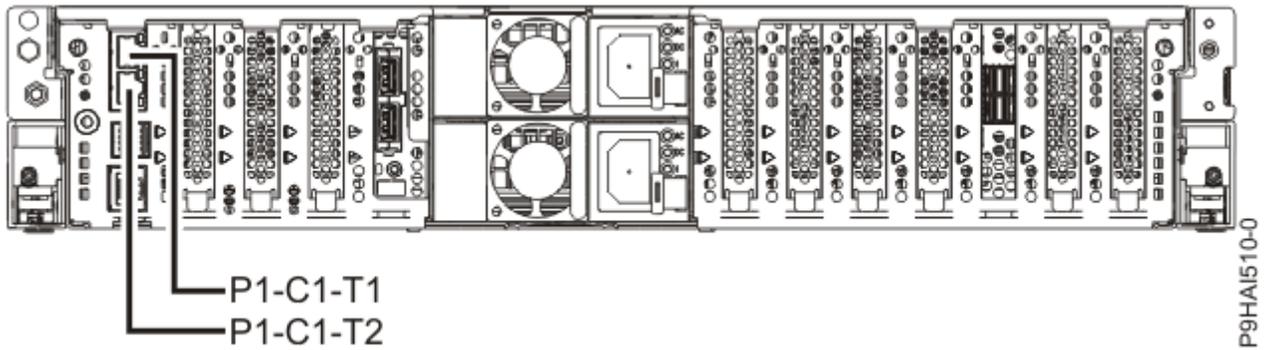


Figura 26. 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S Localizações das portas HMC

Porta	Código de localização físico	LED de identificação
Porta HMC 1	Un-P1-C1-T1	Não
Porta HMC 2	Un-P1-C1-T2	Não

Para obter mais informações sobre localizações de portas da HMC no 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H ou 9223-22S, consulte [Localização de componentes e códigos de localização](#) para 9008-22L, 9009-22A, 9009-22G, 9223-22H ou 9223-22S.

### Localizações de portas da HMC do modelo 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S

Utilize este diagrama e tabela para mapear as portas da HMC no 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S.

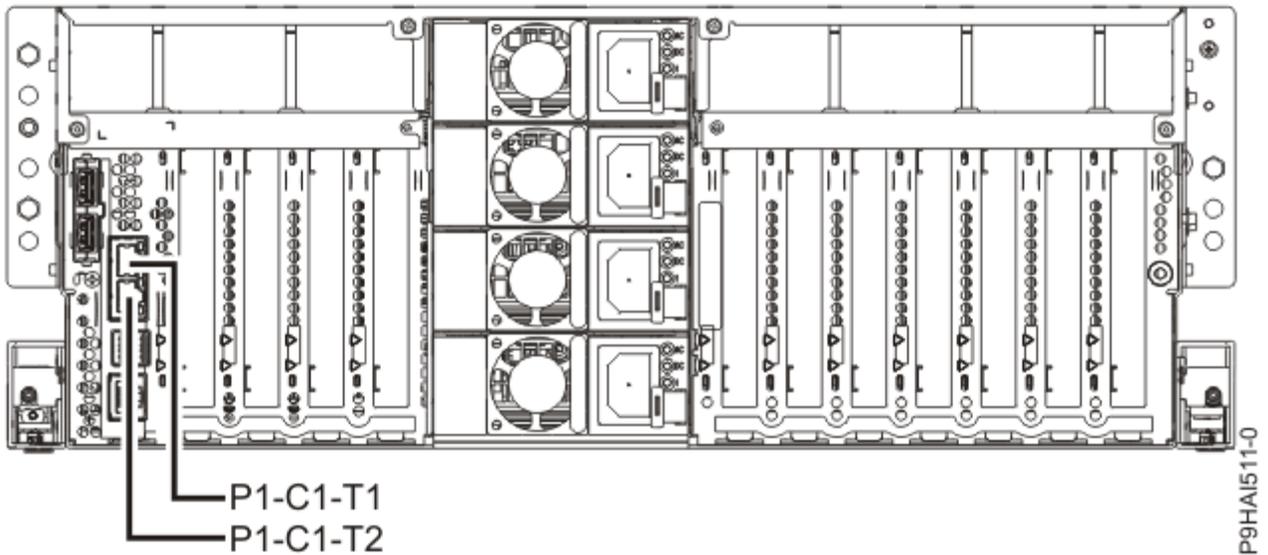


Figura 27. 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S Localizações das portas HMC

Tabela 40. 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S Localizações das portas HMC

Porta	Código de localização físico	LED de identificação
Porta HMC 1	Un-P1-C1-T1	Não
Porta HMC 2	Un-P1-C1-T2	Não

Para obter mais informações sobre localizações de portas da HMC no 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H ou 9223-42S, consulte [Localização de componentes e códigos de localização para 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H ou 9223-42S](#).

### Localizações de portas da HMC do modelo 9040-MR9

Utilize este diagrama e tabela para mapear as portas da HMC em 9040-MR9.

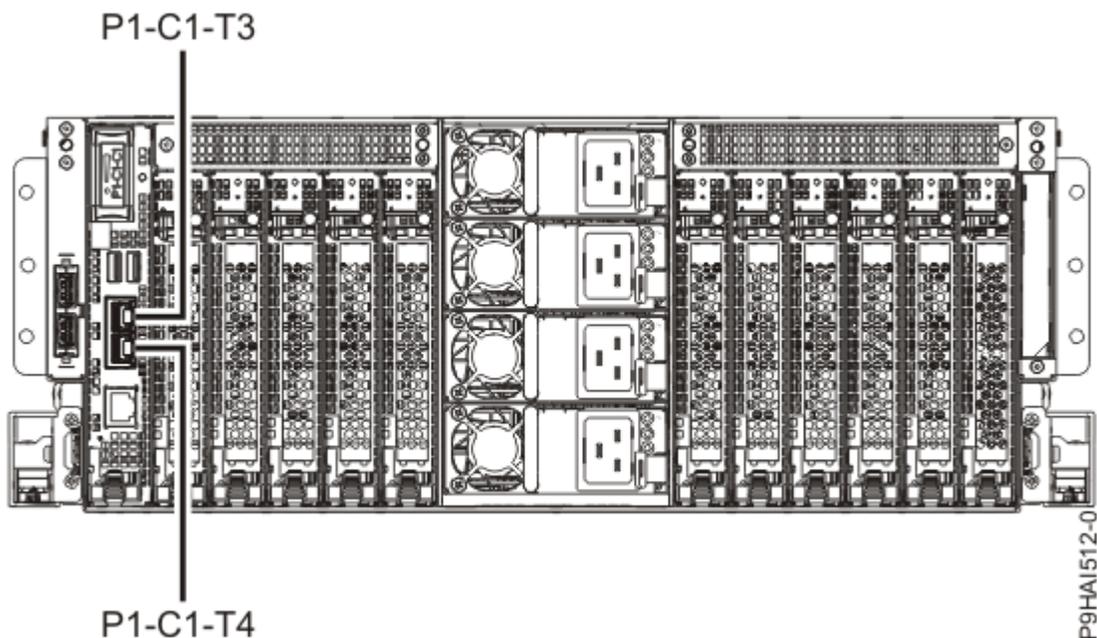


Figura 28. Localizações de portas da HMC 9040-MR9

Tabela 41. Localizações de portas da HMC 9040-MR9

Porta	Código de localização físico	LED de identificação
Porta HMC 1	Un-P1-C1-T3	Não
Porta HMC 2	Un-P1-C1-T4	Não

Para obter mais informações sobre localizações de portas da HMC no 9040-MR9, consulte [Localizações de componentes e códigos de localização](#).

### Localizações de portas da HMC do modelo 9080-M9S

Utilize este diagrama e tabela para mapear as portas da HMC em 9080-M9S.

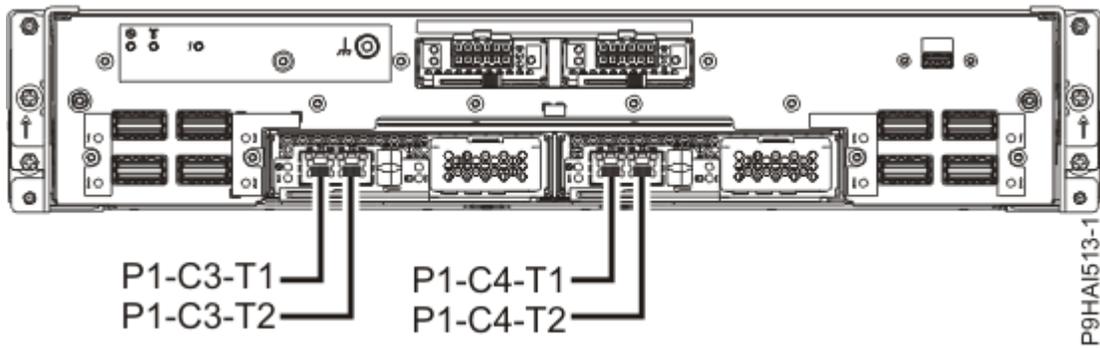


Figura 29. Localizações de portas da HMC 9080-M9S

Tabela 42. Localizações de portas da HMC 9080-M9S

Porta	Localização da porta física	LED de identificação
Placa do processador de serviço 1 - Porta da HMC 1	Un-P1-C3-T1	Não
Placa do processador de serviço 1 - Porta da HMC 2	Un-P1-C3-T2	Não
Placa do processador de serviço 2 - Porta da HMC 1	Un-P1-C4-T1	Não
Placa do processador de serviço 2 - Porta da HMC 2	Un-P1-C4-T2	Não

Para obter mais informações sobre localizações de portas da HMC no 9080-M9S, consulte [Localizações de componentes e códigos de localização](#).

---

## Avisos

Estas informações foram desenvolvidas para produtos e serviços disponibilizados nos E.U.A.

Os produtos, serviços ou funções descritos neste documento poderão não ser disponibilizados pela IBM noutros países. Consulte o seu representante IBM para obter informações sobre os produtos e serviços actualmente disponíveis na sua região. Quaisquer referências, nesta publicação, a produtos, programas ou serviços IBM não significam que apenas esses produtos, programas ou serviços IBM possam ser utilizados. Qualquer outro produto, programa ou serviço, funcionalmente equivalente, poderá ser utilizado em substituição daqueles, desde que não infrinja nenhum direito de propriedade intelectual da IBM. No entanto, é da inteira responsabilidade do utilizador avaliar e verificar o funcionamento de qualquer produto, programa ou serviço não IBM.

A IBM pode possuir patentes ou aplicações com patentes pendentes cujo assunto seja descrito no presente documento. O facto de este documento lhe ser fornecido não lhe confere qualquer direito sobre essas patentes. Caso solicite pedidos de informação sobre licenças, tais pedidos deverão ser endereçados, por escrito, para:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
EUA*

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "TAL COMO ESTÁ" (AS IS), SEM GARANTIA DE QUALQUER ESPÉCIE, EXPLÍCITA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO INFRACÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO FIM. Algumas jurisdições não permitem a exclusão de garantias, quer explícitas quer implícitas, em determinadas transacções; esta declaração pode, portanto, não se aplicar ao seu caso.

Esta publicação pode conter imprecisões técnicas ou erros de tipografia. A IBM permite-se fazer alterações periódicas às informações aqui contidas; essas alterações serão incluídas nas posteriores edições desta publicação. A IBM poderá efectuar melhorias e/ou alterações ao(s) produto(s) e/ou programa(s) descritos nesta publicação sem qualquer aviso prévio.

Quaisquer referências, nesta publicação, a sítios da Web que não sejam propriedade da IBM são fornecidas apenas para conveniência e não constituem, em caso algum, aprovação desses sítios da Web. Os materiais destes sítios da Web não fazem parte dos materiais deste produto IBM e a utilização destes sítios da Web é da inteira responsabilidade do utilizador.

A IBM pode usar ou distribuir quaisquer informações que lhe forneça, da forma que julgue apropriada, sem incorrer em nenhuma obrigação para com o utilizador.

Os exemplos de clientes e dados de desempenho mencionados no presente documento servem apenas para fins ilustrativos. Os resultados de desempenho reais podem variar dependendo de configurações e condições de funcionamento específicos.

As informações relativas a produtos não produzidos pela IBM foram obtidas junto dos fornecedores desses produtos, dos seus anúncios publicados ou de outras fontes de divulgação ao público. A IBM não testou esses produtos e não pode confirmar a exactidão do desempenho, da compatibilidade ou de quaisquer outras afirmações relacionadas com produtos não IBM. Todas as questões sobre as capacidades dos produtos não produzidos pela IBM deverão ser endereçadas aos fornecedores desses produtos.

As afirmações relativas às directivas ou tendências futuras da IBM estão sujeitas a alterações ou descontinuação sem aviso prévio, representando apenas metas e objectivos.

Todos os preços apresentados são os actuais preços de venda sugeridos pela IBM e estão sujeitos a alterações sem aviso prévio. Os preços dos concessionários podem variar.

Estas informações destinam-se apenas a planeamento. As informações estão sujeitas a alterações antes de os produtos descritos ficarem disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados em operações comerciais diárias. Para ilustrá-los o melhor possível, os exemplos incluem nomes de indivíduos, firmas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com pessoas ou empresas reais é mera coincidência.

Se estiver a consultar a versão electrónica desta publicação, é possível que as fotografias e as ilustrações a cores não estejam visíveis.

Os desenhos e especificações contidos no presente documento não podem ser reproduzidos no todo ou em parte sem consentimento por escrito da IBM.

A IBM preparou estas informações para utilização das máquinas específicas indicadas. A IBM não faz qualquer outra representação adequada a qualquer outro objectivo.

Os sistemas informáticos da IBM contêm mecanismos concebidos para reduzir a possibilidade de corrupção ou perda de dados não detectadas. No entanto, não é possível eliminar este risco. Os utilizadores que tiverem problemas de perdas de sistema não planeadas, falhas do sistema, flutuações ou cortes da alimentação, ou falhas nos componentes terão de verificar a exactidão das operações realizadas e dos dados guardados ou transmitidos pelo sistema no momento e/ou próximo do corte ou falha. Além disso, os utilizadores terão de estabelecer procedimentos que garantam a realização de uma verificação de dados independente, antes de confiar nesses dados para operações sensíveis ou críticas. Os utilizadores devem verificar periodicamente os sítios da Web de suporte da IBM para obter correcções e informações actualizadas aplicáveis ao sistema e software relacionado.

## Declaração de homologação

Este produto poderá não estar certificado no seu país para ligações, seja por que meio for, a interfaces de redes de telecomunicações públicas. Poderá ser necessária uma certificação adicional, de acordo com a lei, antes de efectuar algum destes tipos de ligação. Contacte o representante da IBM ou o revendedor, caso tenha alguma questão.

## Funções de acessibilidade para servidores IBM Power Systems

---

As funções de acessibilidade auxiliam os utilizadores que possuem alguma deficiência, tal como mobilidade restrita ou visão limitada, a utilizar o conteúdo da tecnologia de informação com êxito.

### Descrição geral

Os servidores IBM Power Systems incluem as seguintes funções principais de acessibilidade:

- Operação apenas através do teclado
- Operações que utilizam um leitor de ecrã

Os servidores IBM Power Systems utilizam o Standard W3C mais recente, [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) ([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)), para garantir a conformidade com a [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) ([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)) e com as [Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) ([www.w3.org/TR/WCAG20/](http://www.w3.org/TR/WCAG20/)). Para tirar partido das funções de acessibilidade, utilize a edição mais recente do seu leitor de ecrã e o navegador da Web mais recente suportado pelos servidores IBM Power Systems.

A documentação online de produto dos servidores IBM Power Systems no IBM Knowledge Center está preparada para as funções de acessibilidade. As funções de acessibilidade do IBM Knowledge Center são descritas no [Secção de acessibilidade da ajuda do IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility) ([www.ibm.com/support/knowledgecenter/doc/kc\\_help.html#accessibility](http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility)).

### Navegação com o teclado

Este produto utiliza teclas de navegação standard.

## Informação sobre a interface

As interfaces de utilizador dos servidores IBM Power Systems não possuem conteúdo intermitente entre 2 a 55 vezes por segundo.

A interface de utilizador da Web dos servidores IBM Power Systems assenta em folhas de estilo em cascata (CSS, cascading style sheets) para apresentar correctamente e proporcionar uma boa experiência de utilização. A aplicação fornece uma forma equivalente para utilizadores com visão limitada para utilizar as definições de apresentação do sistema, incluindo um modo de elevado contraste. Pode controlar o tamanho do tipo de letra através da utilização das definições do navegador da Web e do dispositivo.

A interface de utilizador da Web dos servidores IBM Power Systems inclui marcos de navegação WAI-ARIA, os quais pode utilizar para navegar rapidamente para áreas funcionais na aplicação.

## Software de fornecedores

Os servidores IBM Power Systems incluem algum software de fornecedores que não está coberto pelo acordo de licenciamento da IBM. A IBM não tem qualquer representação relativamente às funções de acessibilidade destes produtos. Contacte o fornecedor para obter informações sobre a acessibilidade nestes produtos.

## Informações sobre acessibilidade relacionadas

Adicionalmente ao apoio a utilizadores standard da IBM e aos sítios da Web de suporte, a IBM tem um serviço telefónico TTY para utilização por clientes com surdez ou dificuldades de audição para aceder aos serviços de vendas e suporte:

Serviço TTY  
800-IBM-3383 (800-426-3383)  
(na América do Norte)

Para obter mais informações sobre o compromisso da IBM para com a acessibilidade, Consulte [IBM Accessibility \(www.ibm.com/able\)](http://www.ibm.com/able).

## Considerações da política de privacidade

---

Os produtos de Software da IBM, incluindo o software como soluções de serviço, (“Ofertas de Software”) poderão utilizar cookies ou outras tecnologias para recolher informações de utilização de produtos, para ajudar a melhorar a experiência de utilizador final, para personalizar as interações com o utilizador final ou para outros propósitos. Na maioria dos casos não são recolhidas informações pessoais identificáveis por parte das Ofertas de Software. Algumas das Ofertas de Software podem ajudá-lo a recolher informações pessoais identificáveis. Se esta Oferta de Software utilizar cookies para recolher dados pessoais identificáveis, as informações específicas relativas à utilização que esta oferta faz dos cookies está definida mais à frente.

Dependendo das configurações implementadas, esta Oferta de Software poderá utilizar cookies de sessão que recolhem cada um dos nomes de utilizador e endereços IP do utilizador para propósitos de gestão de sessão. Estes cookies podem ser desactivados, mas a respectiva desactivação também irá eliminar a funcionalidade activada pelos mesmos.

Se as configurações implementadas para esta Oferta de Software lhe fornecerem, enquanto cliente, a capacidade para recolher informações pessoais identificáveis de utilizadores finais através de cookies e de outras tecnologias, deve procurar aconselhamento jurídico relativamente às leis aplicáveis para a recolha de dados, incluindo requisitos para aviso e consentimento.

Para obter mais informações sobre a utilização de diversas tecnologias, incluindo cookies, para estes propósitos, consulte a [Política de Privacidade da IBM em http://www.ibm.com/privacy](http://www.ibm.com/privacy) e a [Declaração de Privacidade Online da IBM em http://www.ibm.com/privacy/details/us/en/](http://www.ibm.com/privacy/details/us/en/) na secção denominada "Cookies, Web Beacons and Other Technologies".

## Marcas comerciais

---

IBM, o logótipo IBM e ibm.com são marcas comerciais ou marcas comerciais registadas da International Business Machines Corp., registadas em muitas jurisdições ao redor do mundo. Outros produtos ou nomes de serviço podem ser marcas comerciais da IBM ou de outras empresas. Está disponível uma lista actualizada das marcas comerciais da IBM na Web, em [Copyright and trademark information](#).

A marca comercial registada Linux é utilizada de acordo com uma sub-licença da Linux Foundation, o licenciado exclusivo de Linus Torvalds, proprietário da marca a nível mundial.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph e Gluster são marcas comerciais ou marcas comerciais registadas da Red Hat, Inc. ou das respectivas subsidiárias nos Estados Unidos e noutros países.

Microsoft e Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou noutros países.

Java e todas as marcas comerciais e logótipos baseados em Java são marcas comerciais ou marcas comerciais registadas da Oracle e/ou das suas empresas afiliadas.

## Avisos de emissão electrónica

---

### Informações da Classe A

As declarações seguintes da Classe A aplicam-se aos servidores IBM que contêm o processador POWER9 e respectivos componentes, a menos que seja designada como Classe B de compatibilidade electromagnética (EMC) nas informações do componente.

Ao ligar um monitor ao equipamento, tem de utilizar o cabo de monitor indicado e quaisquer dispositivos de eliminação de interferências fornecidos juntamente com o monitor.

#### **Aviso para o Canadá**

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

#### **Aviso para a Comunidade Europeia e Marrocos**

Este produto está em conformidade com os requisitos de protecção da Directiva 2014/30/EU do Conselho e do Parlamento Europeu sobre a harmonização das leis dos Estados-Membros relativas a compatibilidade electromagnética. A IBM não se responsabiliza pelo não cumprimento dos requisitos de protecção resultantes de uma modificação não recomendada do produto, incluindo a instalação de placas de opção não IBM.

Este produto pode provocar interferências se utilizado em áreas residenciais. Esta utilização deve ser evitada a menos que o utilizador tome medidas especiais para reduzir as emissões electromagnéticas para evitar interferências na recepção de emissões de rádio e televisão.

Aviso: Este equipamento está em conformidade com a Classe A de CISPR 32. Num ambiente residencial este equipamento pode causar interferências radioelétricas.

#### **Aviso para a Alemanha**

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

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

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM

übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

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

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

#### **Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten**

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

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

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

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

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

Generelle Informationen:

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

#### **Japan Electronics and Information Technology Industries Association (JEITA) Notice**

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

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類 : 6 (単相、PFC回路付)
- 換算係数 : 0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類 : 5 (3相、PFC回路付)
- 換算係数 : 0

### Japan Voluntary Control Council for Interference (VCCI) Notice

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 para a Coreia

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

### Aviso para a República Popular da 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 para a Rússia

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

## Aviso para Taiwan

警告使用者：  
此為甲類資訊技術設備，  
於居住環境中使用時，可  
能會造成射頻擾動，在此  
種情況下，使用者會被要  
求採取某些適當的對策。

### Informações de contacto da IBM Taiwan:

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 da Federal Communications Commission (FCC) dos Estados Unidos

Este equipamento foi testado e considerado como estando em conformidade com os limites para dispositivos digitais da Classe A, de acordo com a Parte 15 das normas da FCC. Os referidos limites destinam-se a facultar uma protecção razoável contra interferências prejudiciais, quando o equipamento é utilizado em ambientes comerciais. Este equipamento gera, utiliza e pode emitir energia de radiofrequência e, se não for instalado e utilizado de acordo com o manual de instruções, pode causar interferências prejudiciais nas comunicações por rádio. É provável que a utilização deste equipamento numa área residencial cause interferências prejudiciais. Nesse caso, compete ao utilizador corrigir a interferência.

Têm de ser utilizados cabos e conectores com ligação à terra devidamente isolados, de modo a respeitar os limites de emissão indicados pela FCC. Os cabos e conectores adequados estão disponíveis em concessionários autorizados da IBM. A IBM não se responsabiliza por nenhum tipo de interferência radioelétrica ou de televisão provocada pela utilização de cabos ou conectores não recomendados ou por alterações ou modificações não autorizadas a este equipamento. As alterações ou modificações não autorizadas podem anular a autorização de utilização do equipamento.

Este dispositivo está em conformidade com a Parte 15 das Normas FCC. A operação está sujeita às seguintes duas condições:  
(1) este dispositivo não pode causar interferências prejudiciais e (2) este dispositivo tem de aceitar qualquer interferência recebida, incluindo interferências que possam causar um funcionamento indesejado.

Parte Responsável:  
International Business Machines Corporation  
New Orchard Road  
Armonk, NY 10504  
Contacto apenas para informações de conformidade com a FCC: [fccinfo@us.ibm.com](mailto:fccinfo@us.ibm.com)

## Avisos da Classe B

As declarações seguintes da Classe B aplicam-se a componentes designados como Classe B de compatibilidade electromagnética (EMC) nas informações de instalação do componente.

Ao ligar um monitor ao equipamento, tem de utilizar o cabo de monitor indicado e quaisquer dispositivos de eliminação de interferências fornecidos juntamente com o monitor.

## **Aviso para o Canadá**

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

## **Aviso para a Comunidade Europeia e Marrocos**

Este produto está em conformidade com os requisitos de protecção da Directiva 2014/30/EU do Conselho e do Parlamento Europeu sobre a harmonização das leis dos Estados-Membros relativas a compatibilidade electromagnética. A IBM não se responsabiliza pelo não cumprimento dos requisitos de protecção resultantes de uma modificação não recomendada do produto, incluindo a instalação de placas de opção não IBM.

## **Aviso para a Alemanha**

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

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

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

### **Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten**

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

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

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

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

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

Generelle Informationen:

**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B**

## Japan Electronics and Information Technology Industries Association (JEITA) Notice

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

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類：6（単相、PFC回路付）
- 換算係数：0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

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

- 回路分類：5（3相、PFC回路付）
- 換算係数：0

## Japan Voluntary Control Council for Interference (VCCI) Notice

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 para Taiwan

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 da Federal Communications Commission (FCC) dos Estados Unidos

Este equipamento foi testado e considerado como estando em conformidade com os limites para dispositivos digitais da Classe B, de acordo com a Parte 15 das normas da FCC. Os referidos limites destinam-se a facultar uma protecção razoável contra interferências prejudiciais numa instalação residencial. Este equipamento gera, utiliza e pode emitir energia de radiofrequência e, se não for instalado e utilizado de acordo com as instruções, pode causar interferências prejudiciais nas comunicações por rádio. Contudo, não existe qualquer garantia de que não ocorram interferências numa instalação específica. Caso este equipamento provoque interferências prejudiciais na recepção de rádio ou televisão, que podem ser determinadas ligando e desligando o equipamento, o utilizador deve tentar corrigir a interferência efectuando uma ou mais das seguintes medidas:

- Reoriente ou mude a localização da antena receptora.
- Aumente a distância entre o equipamento e o receptor.
- Ligue o equipamento a uma tomada num circuito que não seja o circuito ao qual está ligado o receptor.
- Consulte um concessionário autorizado da IBM ou um técnico dos serviços de assistência para obter ajuda.

Têm de ser utilizados cabos e conectores com ligação à terra devidamente isolados, de modo a respeitar os limites de emissão indicados pela FCC. Os cabos e conectores adequados estão disponíveis em concessionários autorizados da IBM. A IBM não se responsabiliza por nenhum tipo de interferência radioelétrica ou de televisão provocada pela utilização de cabos ou conectores não recomendados ou por alterações ou modificações não autorizadas a este equipamento. As alterações ou modificações não autorizadas podem anular a autorização de utilização do equipamento.

Este dispositivo está em conformidade com a Parte 15 das Normas FCC. A operação está sujeita às seguintes duas condições:

(1) este dispositivo não pode causar interferências prejudiciais e (2) este dispositivo tem de aceitar qualquer interferência recebida, incluindo interferências que possam causar um funcionamento indesejado.

Parte Responsável:

International Business Machines Corporation  
New Orchard Road  
Armonk, New York 10504

Contacto apenas para informações de conformidade com a FCC: [fccinfo@us.ibm.com](mailto:fccinfo@us.ibm.com)

## Termos e condições

---

As permissões de utilização destas publicações são concedidas sujeitas aos seguintes termos e condições.

**Aplicabilidade:** Estes termos e condições são adicionais a quaisquer termos de utilização para o sítio da Web IBM.

**Utilização pessoal:** Pode reproduzir estas publicações para uso pessoal e não comercial, desde que mantenha todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas publicações, nem reproduzir, distribuir ou apresentar estas informações ou qualquer parte das mesmas fora das instalações da sua empresa, sem o expresse consentimento da IBM.

**Utilização comercial:** Pode reproduzir, distribuir e apresentar estas publicações exclusivamente no âmbito da sua empresa, desde que preserve todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas publicações, nem reproduzir, distribuir ou apresentar estas publicações ou qualquer parte das mesmas fora das instalações da empresa, sem o expresse consentimento da IBM.

**Direitos:** Salvo no expressemente concedido nesta permissão, não se concedem outras permissões, licenças ou direitos, expressas ou implícitas, relativamente às Publicações ou a informações, dados, software ou demais propriedade intelectual nela contida.

A IBM reserva-se o direito de retirar as permissões concedidas nesta publicação sempre que considerar que a utilização das publicações pode ser prejudicial aos seus interesses ou, tal como determinado pela IBM, sempre que as instruções acima referidas não estejam a ser devidamente cumpridas.

Não pode descarregar, exportar ou reexportar estas informações, excepto quando em total conformidade com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação em vigor nos Estados Unidos.

A IBM NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "TAL COMO ESTÃO" E SEM GARANTIAS DE QUALQUER ESPÉCIE, QUER EXPLÍCITAS, QUER IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRACÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.





