

Power Systems

*Instalando e Configurando o Hardware
Management Console*



Note

Antes de usar estas informações e o produto suportado por elas, leia as informações em [“Avisos de Segurança”](#) na página v, [“Avisos”](#) na página 117, no manual *IBM Systems: Avisos de Segurança*, G517-7951 e no *IBM Environmental Notices and User Guide*, Z125-5823.

Esta edição se aplica ao IBM® Hardware Management Console Versão 9, Liberação 2, Nível de manutenção 950 e a todas as liberações e modificações subsequentes, até que seja indicado o contrário em novas edições.

© Copyright International Business Machines Corporation 2018, 2021.

Índice

Avisos de Segurança.....	V
Instalando e configurando o Hardware Management Console.....	1
O que Há de Novo em Instalando e Configurando o HMC.....	1
Tarefas de Instalação e Configuração.....	2
Instalando e Configurando um Novo HMC com um Novo Servidor.....	2
Atualizando e Fazendo Upgrade do Código do HMC.....	3
Incluindo um Segundo HMC em uma Instalação Existente.....	3
Configurando o HMC.....	4
Instalando o IBM Power Systems HMC (7063-CR2) em um rack.....	4
Instalando o 7063-CR1 em um rack.....	14
Instalando o HMC 7042-CR9 em um rack.....	26
Instalando o dispositivo virtual HMC	41
Configurando o HMC.....	54
Escolhendo Configurações de Rede no HMC.....	54
Configurando o HMC.....	71
Etapas de Pós-configuração.....	92
Atualizando, Fazendo Upgrade e Migrando seu Código de Máquina do HMC.....	93
Protegendo o HMC.....	104
Política de Senha Avançada.....	106
Resolvendo problemas comuns ao proteger o HMC.....	107
Perfis de segurança: Global Data Protection Regulation (GDPR) e Padrão de Segurança de Dados do Setor de Cartão de Pagamento (PCI-DSS)	110
Locais das portas do HMC.....	112
Avisos.....	117
Recursos de acessibilidade para os servidores IBM Power Systems.....	118
Considerações sobre política de privacidade	119
Marcas Registradas.....	119
Avisos de Emissão Eletrônica.....	120
Notas de Classe A.....	120
Avisos da Classe B.....	123
Termos e Condições.....	126

Avisos de Segurança

O avisos de segurança podem estar impressos em todo este guia:

- Os avisos de **PERIGO** chamam a atenção a uma situação que é potencialmente letal ou extremamente danosa às pessoas.
- Os avisos de **CUIDADO** chamam a atenção a uma situação que é potencialmente danosa às pessoas devido a uma condição existente.
- Os avisos de **Atenção** chamam a atenção à possibilidade de danos a um programa, dispositivo, sistema ou aos dados.

Informações de Segurança de Intercâmbio Mundial

Vários países requerem que as informações de segurança contidas nas publicações do produto sejam apresentadas no idioma nacional. Se esse requisito se aplicar ao seu país, a documentação com as informações de segurança estará incluída no pacote de publicações (como em documentação impressa, em DVD ou como parte do produto) fornecido com o produto. A documentação contém as informações de segurança no idioma nacional com referências à origem em inglês dos EUA. Antes de usar uma publicação em inglês dos EUA para instalar, operar ou fazer manutenção neste produto, é necessário primeiro familiarizar-se com a documentação de informações de segurança relacionadas. Consulte também a documentação de informações de segurança sempre que você não entender claramente alguma informação de segurança nas publicações em inglês dos EUA.

Cópias de substituição ou adicionais da documentação de informações de segurança podem ser obtidas ligando para o IBM Hotline em 1-800-300-8751.

Informações de Segurança em Alemão

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

Informações de Segurança do Laser

Os servidores IBM podem utilizar placas de E/S ou recursos que são baseados em fibra ótica e que utilizam lasers ou LEDs.

Conformidade para Laser

Os servidores IBM podem ser instalados dentro ou fora de um rack de equipamento de TI.



PERIGO: Ao trabalhar no, ou próximo ao sistema, tome as seguintes precauções:

A tensão e a corrente elétrica dos cabos de alimentação, de telefone e de comunicação são perigosas. Para evitar um risco de choque elétrico: se a IBM forneceu os cabos de energia, conecte a energia a esta unidade somente com o cabo de energia fornecido pela IBM. Não utilize o cabo de alimentação fornecido pela IBM para nenhum outro produto. Não abra nem execute serviço em nenhuma montagem da fonte de alimentação. Não conecte ou desconecte nenhum cabo nem execute instalação, manutenção ou reconfiguração deste produto durante uma tempestade com raios.



- O produto pode estar equipado com vários cabos de energia. Para remover todas as voltagens de risco, desconecte todos os cabos de alimentação. Para energia de corrente alternada, desconecte todos os cabos de energia de sua fonte de energia de corrente alternada. Para racks com um painel de distribuição de energia DC (PDP), desconecte a fonte de alimentação de corrente contínua do cliente do PDP.

- Ao conectar a energia para o produto, assegure-se de que todos os cabos de energia estejam conectados corretamente. Para racks com energia de corrente alternada, conecte todos os cabos de energia a uma tomada corretamente instalada e aterrada. Certifique-se de que a tomada forneça voltagem apropriada e rotação de fases de acordo com a placa de classificação do sistema. Para racks com um painel de distribuição de energia (PDP) de corrente contínua, conecte a fonte de alimentação de corrente contínua do cliente com o PDP. Assegure-se de que a polaridade adequada seja usada ao conectar a energia e a conexão de retorno de energia de corrente contínua.
- Conecte qualquer equipamento que será conectado a este produto a tomadas com conexão física adequada.
- Quando possível, utilize apenas uma mão para conectar ou desconectar os cabos de sinais.
- Nunca ligue qualquer equipamento quando houver suspeita de fogo, água ou dano estrutural.
- Não tente ligar a energia na máquina até que todas as condições não seguras tenham sido corrigidas.
- Ao executar uma inspeção de máquina: suponha que um risco elétrico de segurança esteja presente. Faça todas as verificações de continuidade, aterramento e de cabo especificadas durante os procedimentos de instalação do subsistema para assegurar que a máquina atenda aos requisitos de segurança. Não tente alternar a energia para a máquina até que todas as possíveis condições inseguras sejam corrigidas. Antes de abrir as tampas dos dispositivos, a menos que receba instruções contrárias nos procedimentos de instalação e configuração: desconecte os cabos de energia de corrente alternada conectados, desligue os disjuntores aplicáveis localizados no painel de distribuição de energia do rack (PDP) e desconecte quaisquer sistemas de telecomunicações, redes e modems.
- Conecte e desconecte os cabos, conforme descrito a seguir, quando instalar, mover ou abrir as tampas deste produto ou de dispositivos conectados.

Para desconectar: 1) Desligue tudo (a menos que instruído de outra forma). 2) Para a energia de corrente alternada, remova os cabos de energia das tomadas. 3) Para racks com um painel de distribuição de energia DC (PDP), desligue os disjuntores localizados no PDP e remova a energia da Fonte de alimentação de corrente contínua do cliente. 4) Remova os cabos de sinal dos conectores. 5) Remova todos os cabos dos dispositivos.

Para conectar: 1) Desligue tudo (a menos que instruído de outra forma). 2) Conecte todos os cabos aos dispositivos. 3) Conecte os cabos de sinal aos conectores. 4) Para a energia de corrente alternada, conecte os cabos de energia às tomadas. 5) Para racks com um painel de distribuição de energia DC (PDP), restaure a energia da Fonte de alimentação de corrente contínua do cliente e ligue os disjuntores localizados no PDP. 6) Ligue os dispositivos.



- Bordas afiadas, cantos e juntas podem estar presentes dentro do sistema e ao redor dele. Cuidado ao manusear o equipamento para evitar cortes, arranhões e torções. (D005)

(R001 parte 1 de 2):



PERIGO: Tome as seguintes precauções ao trabalhar no, ou próximo ao, sistema do rack TI:

- Equipamento pesado – o manuseio incorreto poderá acarretar ferimentos em pessoas ou danos ao equipamento.
- Sempre abaixe os preenchimentos de nivelamento no gabinete do rack.
- Sempre instale suportes do estabilizador no gabinete do rack, se fornecidos, a menos que a opção de terremoto vá ser instalada.
- Para evitar condições de risco devido à falta de equilíbrio das cargas mecânicas, instale sempre os dispositivos mais pesados na parte inferior do gabinete do rack. Sempre instale os servidores e dispositivos opcionais começando da parte inferior do gabinete do rack.
- Os dispositivos montados em rack não devem ser utilizados como prateleira ou área de trabalho. Não coloque objetos na parte superior dos dispositivos montados no rack. Além disso, não se apoie em dispositivos montados em rack e não os use para estabilizar a posição do seu corpo (por exemplo, ao trabalhar em uma escada).



- Risco de estabilidade:
 - O rack pode tombar e causar lesão corporal grave.
 - Antes de estender o rack para a posição de instalação, leia as instruções de instalação.
 - Não coloque nenhuma carga sobre o equipamento montado em trilho deslizante colocado na posição de instalação.
 - Não deixe o equipamento montado em trilho deslizante na posição de instalação.
- Cada gabinete do rack pode ter mais de um cabo de alimentação.
 - Para racks com energia de corrente alternada, certifique-se de desconectar todos os cabos de energia do gabinete do rack quando instruído a desconectar a energia durante a manutenção.
 - Para racks com um painel de distribuição de energia DC (PDP), desligue o disjuntor que controla a energia para a unidade de sistema ou desconecte a fonte de alimentação de corrente contínua do cliente quando orientado a desconectar a energia durante a manutenção.
- Conecte todos os dispositivos instalados em um gabinete do rack aos dispositivos de alimentação instalados no mesmo gabinete. Não ligue um cabo de alimentação de um dispositivo instalado em um gabinete do rack em um dispositivo de alimentação instalado em um gabinete do rack diferente.
- Uma tomada que não esteja instalada de maneira correta pode transmitir voltagem perigosa às partes metálicas do sistema ou aos dispositivos conectados ao sistema. É responsabilidade do cliente garantir que a tomada esteja corretamente instalada e aterrada para evitar um choque elétrico. (R001 parte 1 e 2)

(R001 parte 2 de 2):



CUIDADO:

- Não instale uma unidade em um rack quando a temperatura ambiente interna do rack exceder a temperatura recomendada pelos fabricantes para todos os dispositivos montados em rack.
- Não instale a unidade em um rack onde o fluxo de ar esteja comprometido. Certifique-se de que o fluxo de ar não esteja bloqueado ou reduzido em qualquer lado, frontal ou traseiro da unidade utilizado para fluxo de ar pela unidade.
- Preste atenção na conexão do equipamento ao circuito de alimentação para que a sobrecarga dos circuitos não comprometa os fios de alimentação ou a proteção contra sobrecargas de corrente. Para fornecer a conexão de energia correta para o rack, consulte as etiquetas de classificação localizadas no equipamento no rack, para determinar o requisito de energia total do circuito de alimentação.
- *(Para gavetas deslizantes.)* Não retire nem instale nenhuma gaveta ou recurso se os suportes do estabilizador de rack não estiverem conectados ao rack ou se o rack não estiver aparafusado ao chão. Não puxe mais do que uma gaveta ao mesmo tempo. O rack poderá se tornar instável se você puxar mais de uma gaveta de cada vez.



- (Para gavetas fixas.) Esta gaveta é fixa e não deve ser retirada para manutenção, exceto se for especificado pelo fabricante. A tentativa de movimentar a gaveta parcial ou completamente do rack pode fazer com que o rack se torne instável ou com que a gaveta caia do rack. (R001 parte 2 de 2)



CUIDADO: Remover componentes das posições superiores no gabinete do rack melhorará a sua estabilidade nos deslocamentos. Siga essas diretrizes gerais sempre que realocar um gabinete de rack cheio em uma sala ou prédio.

- Reduza o peso do gabinete do rack, removendo equipamentos, começando pela parte superior do gabinete. Quando possível, restabeleça a configuração original do gabinete. Se essa configuração for desconhecida, observe as seguintes precauções:
 - Remova todos os dispositivos na posição 32U e acima.
 - Verifique se os dispositivos mais pesados estão instalados na parte inferior do gabinete do rack.
 - Assegure-se de que praticamente não haja níveis de U vazios entre os dispositivos instalados no gabinete do rack abaixo do nível 32U, a menos que a configuração recebida especificamente permita isso.
- Se o gabinete do rack que está sendo deslocado fizer parte de um conjunto de gabinetes, solte-o do conjunto.
- Se o gabinete do rack que estiver realocando foi fornecido com suportes removíveis, eles deverão ser reinstalados antes de o gabinete ser realocado.
- Examine a rota que será tomada para eliminar quaisquer riscos em potencial.
- Verifique se a rota escolhida comporta o peso do gabinete carregado. Consulte a documentação que acompanha o gabinete do rack para obter o peso de um gabinete carregado.
- Verifique se todas as aberturas de portas têm pelo menos 760 x 2083 mm (30 x 82 Pol.).
- Verifique se todos os dispositivos, prateleiras, gavetas, portas e cabos estão fixos.
- Verifique se os quatro calços de nivelamento estão na posição mais elevada.
- Verifique se não há nenhum suporte estabilizador instalado no gabinete do rack durante a movimentação.
- Não utilize rampas com mais de 10 graus de inclinação.
- Quando o gabinete do rack estiver no novo local, conclua as seguintes etapas:
 - Abaixe os quatro calços de nivelamento.
 - Instale os suportes do estabilizador no gabinete do rack ou, em um local onde ocorram terremotos, aparafuse o rack ao chão.

- Se tiver removido dispositivos do gabinete, instale-os novamente, da posição mais baixa à mais elevada.
- Se for necessária uma longa distância de deslocamento, restaure a configuração original do gabinete. Acondicione-o no material da embalagem original, ou equivalente. Diminua, também, os calços de nivelamento para levantar os rodízios para fora da paleta e parafuse o gabinete na paleta.

(R002)

(L001)



PERIGO: Níveis perigosos de voltagem, corrente ou energia estão presentes dentro de qualquer componente que tenha esta etiqueta afixada. Não abra nenhuma tampa ou barreira que contenha esta etiqueta. (L001)

(L002)

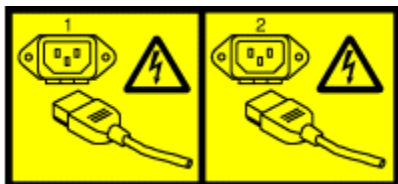


PERIGO: Os dispositivos montados em rack não devem ser utilizados como prateleira ou área de trabalho. Não coloque objetos na parte superior dos dispositivos montados no rack. Além disso, não se incline sobre dispositivos montados em rack e não os use para estabilizar seu corpo (por exemplo, ao trabalhar em uma escada). Risco de estabilidade:

- O rack pode tombar e causar lesão corporal grave.
- Antes de estender o rack para a posição de instalação, leia as instruções de instalação.
- Não coloque nenhuma carga sobre o equipamento montado em trilho deslizante colocado na posição de instalação.
- Não deixe o equipamento montado em trilho deslizante na posição de instalação.

(L002)

(L003)



ou



ou

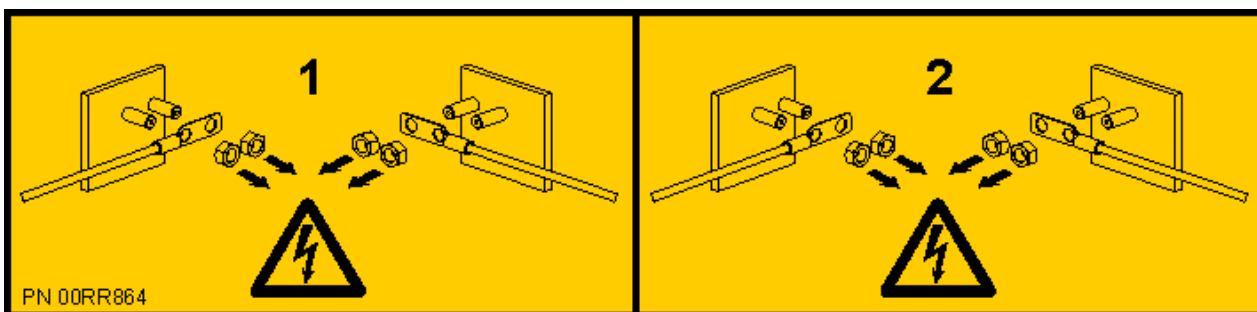


ou



ou





PERIGO: Vários cabos de alimentação. O produto deve estar equipado com vários cabos de energia de corrente alternada ou vários cabos de energia de corrente contínua. Para remover todas as voltagens perigosas, desconecte todos os cabos de energia. (L003)

(L007)



CUIDADO: Uma superfície quente próxima. (L007)

(L008)



CUIDADO: Peças móveis perigosas próximas. (L008)

Todos os lasers são certificados nos EUA de acordo com os requisitos do DHHS 21 CFR Subcapítulo J para produtos de laser classe 1. Fora dos EUA, eles são certificados como em conformidade com o IEC 60825 como produto de laser classe 1. Consulte a etiqueta em cada parte dos números de certificação do laser e as informações de aprovação.



CUIDADO: Este produto pode conter um ou mais dos seguintes dispositivos: unidade de CD-ROM, unidade de DVD-ROM, unidade de DVD-RAM ou módulo laser, que são considerados produtos a laser Classe 1. Observe as seguintes informações:

- Não remova as coberturas. Remover as coberturas do produto a laser pode resultar em exposição perigosa à radiação a laser. Não há nenhuma peça passível de manutenção dentro do dispositivo.
- A utilização de controles ou ajustes, ou a execução de procedimentos diferentes dos especificados aqui, pode resultar em exposição perigosa à radiação.

(C026)



CUIDADO: Os ambientes de processamento de dados podem conter equipamento transmitindo nos links do sistema com módulos a laser que operam em níveis de potência maiores que a Classe 1. Por essa razão, nunca olhe na extremidade de um cabo de fibra ótica ou em um receptáculo aberto. Embora a luz esteja acesa em uma extremidade e olhar dentro da outra extremidade de uma fibra ótica descontinuada para verificar a continuidade das fibras óticas não possa resultar em danos para os olhos, esse procedimento é potencialmente perigoso. Portanto, não é recomendado

verificar a continuidade das fibras óticas pela luz brilhante em uma extremidade e olhar na outra extremidade. Para verificar a continuidade de um cabo de fibra óptica, use uma fonte de luz óptica e um medidor de energia. (C027)



CUIDADO: Este produto contém um laser Classe 1M. Não olhe diretamente com instrumentos óticos. (C028)



CUIDADO: Alguns produtos a laser contém um diodo laser Classe 3A ou 3B incorporado. Observe as seguintes informações:

- Radiation a laser ao abrir.
- Não fite o feixe luminoso, não olhe diretamente com instrumentos óticos e evite a exposição direta a ele. (C030)

(C030)



CUIDADO: A bateria contém lítio. Para prevenir uma possível explosão, não queime ou aplique uma carga à bateria.

Não:

- Acione ou realize uma imersão em água
- Exponha a temperaturas superiores a 100 graus C (212 graus F)
- Conserte nem desmonte a bateria

Substitua apenas por peça autorizada pela IBM. Recicle ou descarte-a conforme instruído pelas regulamentações locais. Nos Estados Unidos, a IBM tem um sistema de coleta de baterias. Para informações, ligue 1-800-426-4333. Para obter informações adicionais, entre em contato com o seu representante IBM. (C003)



CUIDADO: Em relação à FERRAMENTA DE LEVANTAMENTO DO FORNECEDOR fornecida pela IBM:

- Operação da LIFT TOOL somente por equipe autorizada.
- A LIFT TOOL: destina-se ao uso para ajudar, levantar, instalar, remover unidades (carregar) nas elevações do rack. Ela não deve ser usada carregada no transporte sobre grandes rampas nem como uma substituição a ferramentas designadas como paleteiras e empilhadeiras e a práticas de realocação relacionadas. Quando isto não for praticável, serviços ou pessoas especialmente treinadas devem ser usados (por exemplo, montadores ou movimentadores).
- Leia e entenda completamente o conteúdo do manual do operador da FERRAMENTA DE ELEVAÇÃO antes de usá-la. A impossibilidade de ler, entender, obedecer regras de segurança e seguir instruções poderá resultar em danos em bens e/ou lesão corporal. Se houver perguntas, entre em contato com o serviço e suporte do fornecedor. Um manual em papel local deve permanecer com a máquina na área de compartimento de armazenamento fornecida. Manual de revisão mais recente disponível no website do fornecedor.
- Teste a função de freio do estabilizador antes de cada uso. Não force excessivamente a movimentação ou rolagem da FERRAMENTA DE ELEVAÇÃO com o freio do estabilizador engrenado.
- Não levante, abaixe ou deslize a plataforma de carga útil, a menos que o estabilizador (alavanca de pedal de freio) esteja totalmente acoplado. Mantenha o freio do estabilizador engrenado quando não estiver em uso ou em movimento.
- Não mova a LIFT TOOL enquanto a plataforma estiver elevada, exceto para posicionamento secundário.
- Não exceda a capacidade de carregamento classificada. Veja o GRÁFICO DE CAPACIDADE DE CARREGAMENTO com relação às cargas máximas no centro versus borda da plataforma estendida.
- Levante a carga somente se centralizada corretamente na plataforma. Não coloque mais de 200 lb (91 kg) na borda da prateleira da plataforma deslizante, considerando também o centro de massa/gravidade da carga (CoG).

- Não coloque carga no canto das plataformas, do acessório elevatório de inclinação, do calço de instalação da unidade angulada ou de qualquer outra opção de acessório. Prenda tais opções de plataformas (o acessório elevatório de inclinação, o calço, etc.) na prateleira principal ou nas forquilhas nos quatro locais (4x ou em todos os outros locais de montagem fornecidos) somente com o hardware fornecido, antes do uso. Objetos de carregamento são projetados para deslizar suavemente nas plataformas sem força apreciável, portanto, cuidado para não empurrar ou inclinar. Mantenha o acessório elevatório de inclinação [plataforma de angulação ajustável] plano em todos os momentos, exceto para o pequeno ajuste final do ângulo quando necessário.
- Não fique embaixo da carga suspensa.
- Não use em superfície regular, incline ou abaixe (rampas grandes).
- Não empilhe as cargas.
- Não opere sob a influência de drogas ou álcool.
- Não apoie a escada na FERRAMENTA DE LEVANTAMENTO (a menos que permissão específica seja fornecida para um dos procedimentos qualificados a seguir para trabalhar em elevações com essa FERRAMENTA).
- Risco de tombar. Não empurre ou apoie na carga com a plataforma levantada.
- Não use como uma plataforma ou escada de elevação da equipe. Proibido passageiros.
- Não fique em nenhuma parte da elevação. Não é uma escada.
- Não escale o mastro.
- Não opere uma máquina LIFT TOOL machine danificada ou com mau funcionamento.
- Risco de comprimir e pinçar abaixo da plataforma. Abaixar a carga somente em áreas sem pessoas e obstruções. Mantenha as mãos e pés desimpedidos durante a operação.
- Proibido o uso de Garfos. Nunca eleve ou mova a MÁQUINA DE FERRAMENTA DE ELEVAÇÃO com empilhadeira, guindaste ou guincho.
- O mastro se estende além da plataforma. Esteja ciente da altura do teto, bandejas de cabos, sprinklers, luzes e outros objetos suspensos.
- Não deixe a máquina LIFT TOOL sem assistência com uma carga elevada.
- Observe e mantenha as mãos, dedos e roupas desimpedidos quando o equipamento estiver em movimento.
- Movimente o Guincho somente com a força da mão. Se a alça do guincho não puder ser puxada facilmente com uma mão, provavelmente ele está sobrecarregado. Não continue movimentando o guincho para cima ou para baixo na plataforma. A movimentação excessiva removerá a alça e danificará o cabo. Sempre segure a alça ao abaixar e ao movimentar. Sempre se certifique de que o guincho esteja segurando a carga antes de liberar a alça do guincho.
- Um acidente com o guincho poderia causar sérios danos. Não se destina à movimentação de pessoas. Certifique-se de que algum som de clique seja ouvido conforme o equipamento estiver sendo levantado. Certifique-se de que o guincho esteja travado na posição antes de liberar a alça. Leia a página de instruções antes de operar esse guincho. Nunca permita que o guincho se movimente livremente. Andar livremente causará agrupamento de cabo irregular em torno do tambor do guincho, danificará o cabo e poderá causar sérios danos.
- Deve ser realizada manutenção correta nessa FERRAMENTA para que a Equipe de Serviço IBM a use. A IBM deve inspecionar as condições e verificar o histórico de manutenção antes da operação. A equipe reserva-se o direito de não usar a FERRAMENTA caso ela esteja inadequada. (C048)

Informações Sobre Alimentação e Cabeamento do NEBS (Network Equipment-Building System) GR-1089-CORE

Os seguintes comentários se aplicam a servidores IBM que foram projetados em conformidade com o NEBS (Network Equipment-Building System) GR-1089-CORE:

O equipamento é adequado para instalação em:

- Instalações de telecomunicações de rede
- Locais em que o NEC (National Electrical Code) se aplica

As portas de construção interna desse equipamento são adequadas para conexão somente com fiação ou cabeamento não exposto ou de construção interna. As portas de construção interna desse equipamento *não devem* ser metalicamente conectadas às interfaces que se conectam à OSP (instalação externa) ou a sua fiação. Essas interfaces foram projetadas para serem utilizadas somente como interfaces de construção interna (portas Tipo 2 ou Tipo 4, como descritas em GR-1089-CORE) e exigem isolamento do cabeamento OSP exporto. A adição de protetores primários não é uma proteção suficiente para conectar essas interfaces metalicamente à fiação OSP.

Nota: Todos os cabos Ethernet devem ser blindados e aterrados em ambas as extremidades.

O sistema alimentado por AC não exige o uso de um SPD (Surge Protection Device) externo.

O sistema alimentado por DC utiliza um design de retorno de DC isolado (DC-I). O terminal de retorno da bateria DC *não deve* ser conectado ao chassi ou aterramento do gabinete.

O sistema alimentado por DC deve ser instalado em uma rede de ligação comum (CBN), conforme descrito em GR-1089-CORE.

Instalando e configurando o Hardware Management Console

Aprenda como instalar o hardware Hardware Management Console (HMC), conectá-lo a seu sistema gerenciado e configurá-lo para uso. É possível executar essas tarefas sozinho ou entrar em contato com um provedor de serviços para executá-las para você. Talvez seja cobrada uma taxa pelo provedor de serviços para esse serviço.

O que Há de Novo em Instalando e Configurando o HMC

Leia sobre informações novas ou com mudanças significativas no tópico Instalando e configurando o HMC desde a atualização anterior da coleção de tópicos.

Abril de 2021

- Os tópicos a seguir foram incluídos:
 - [“Instalando o IBM Power Systems HMC \(7063-CR2\) em um rack”](#) na página 4
 - [“Pré-requisitos para a instalação do sistema 7063-CR2 montado em rack”](#) na página 4
 - [“Concluindo o inventário para seu sistema”](#) na página 5
 - [“Determinando e marcando o local no rack para o sistema 7063-CR2”](#) na página 5
 - [“Conectando os trilhos ajustáveis ao chassi do sistema e ao rack”](#) na página 6
 - [“Conectando os trilhos fixos ao chassi do sistema e ao rack”](#) na página 8
 - [“Instalando o sistema no rack e conectando e roteando cabos de energia”](#) na página 10
 - [“Cabeando o 7063-CR2 HMC montado em rack”](#) na página 10
 - [“Configurando o 7063-CR2 HMC”](#) na página 12

Novembro de 2020

- Atualização dos seguintes tópicos:
 - [“Tarefas de Instalação e Configuração”](#) na página 2
 - [“Instalando o HMC 7042-CR9 em um rack”](#) na página 26
 - [“Protegendo o HMC”](#) na página 104
 - [“Locais das portas do HMC”](#) na página 112

Julho de 2020

- Atualização dos seguintes tópicos:
 - [“Instalando o dispositivo virtual HMC ”](#) na página 41
 - [“Locais das portas do HMC”](#) na página 112

Outubro de 2019

- Atualização dos seguintes tópicos:
 - [“Instalando o dispositivo virtual HMC ”](#) na página 41
 - [“Protegendo o HMC”](#) na página 104

Fevereiro de 2019

- Os tópicos a seguir foram incluídos:
 - [“Protegendo o HMC” na página 104](#)
 - [“Política de Senha Avançada” na página 106](#)
 - [“Resolvendo problemas comuns ao proteger o HMC” na página 107](#)
 - [“Perfis de segurança: Global Data Protection Regulation \(GDPR\) e Padrão de Segurança de Dados do Setor de Cartão de Pagamento \(PCI-DSS\)” na página 110](#)

Agosto de 2018

- Atualização dos seguintes tópicos:
 - [“Configurando o 7063-CR1 HMC” na página 23](#)
 - [“Locais das portas do HMC” na página 112](#)

Dezembro 2017

- Informações incluídas para servidores IBM Power Systems que contêm o processador POWER9.

Tarefas de Instalação e Configuração

Saiba as tarefas que estão associadas a diferentes tarefas de instalação e configuração do HMC.

Saiba, em um alto nível, as tarefas que se deve concluir ao instalar e configurar o HMC. É possível instalar e configurar o HMC de diferentes maneiras. Localize a situação que melhor corresponda à tarefa que você deseja concluir.

Notas:

- Se você está gerenciando servidores baseados no processador POWER9, o HMC deve estar na versão 9.1.0 ou mais recente. Para obter mais informações, consulte [“Determinando sua Versão e Liberação do Código de Máquina do HMC” na página 93](#).
- O Hardware Management Console Versão 9.2.950 ou mais recente não é suportado no Tipo de máquina HMC 7042. Para obter mais informações sobre as versões do HMC para o seu HMC 7042, consulte as notas sobre a liberação do HMC que estão disponíveis no website do [Fix Central](#).

Instalando e Configurando um Novo HMC com um Novo Servidor

Saiba mais sobre as tarefas de alto nível que se deve concluir ao instalar e configurar um novo HMC com um novo servidor.

Tabela 1. Tarefas que você precisa concluir quando instala e configura um novo HMC com um novo servidor	
Tarefa	Onde localizar informações relacionadas
1. Reúna informações e conclua a planilha de Configuração de pré-instalação.	“Planilha de Configuração de Pré-instalação para o HMC” na página 64 “Preparando-se para a Configuração do HMC” na página 62
2. Desempacote o hardware.	
3. Conecte os cabos do hardware do HMC.	“Cabeando o 7063-CR1 HMC montado em rack” na página 21
4. Ligue o HMC pressionando o botão power.	

Tabela 1. Tarefas que você precisa concluir quando instala e configura um novo HMC com um novo servidor (continuação)

Tarefa	Onde localizar informações relacionadas
5. Efetue login e inicie o aplicativo da web do HMC.	
6. Acesse o assistente de configuração orientada ou use os menus do HMC para configurar o HMC.	“Configurando o HMC Usando o Atalho por meio do Assistente Guided Setup” na página 71 “Configurando o HMC usando os menus ” na página 71
7. Conecte o servidor ao HMC.	

Atualizando e Fazendo Upgrade do Código do HMC

Saiba mais sobre as tarefas de alto nível que se deve concluir ao atualizar ou fazer upgrade do código do HMC.

Se você tiver um HMC existente e desejar atualizar ou fazer upgrade do código do HMC, deverá concluir as tarefas de alto nível a seguir:

Tabela 2. Tarefas que você precisa concluir ao atualizar ou fazer upgrade do código do HMC

Tarefa	Onde localizar informações relacionadas
1. Obtenha o upgrade.	“Fazendo Upgrade de seu Software do HMC” na página 98
2. Visualize o nível de código de máquina do HMC existente.	
3. Faça backup dos dados do perfil do sistema gerenciado.	
4. Faça backup dos dados do HMC.	
5. Registre as informações de configuração do HMC atuais.	
6. Registre o status do comando remoto.	
7. Salve dados de upgrade.	
8. Faça upgrade do software do HMC.	
9. Verifique se o upgrade do código de máquina do HMC foi instalado com sucesso	

Incluindo um Segundo HMC em uma Instalação Existente

Saiba mais sobre as tarefas de alto nível que se deve concluir quando você inclui um segundo HMC em seu sistema gerenciado.

Se você tiver um HMC e um sistema gerenciado existentes e desejar incluir um segundo HMC nessa configuração, conclua as etapas a seguir:

Tabela 3. Tarefas que você precisa concluir quando inclui um segundo HMC em uma instalação existente

Tarefa	Onde localizar informações relacionadas
1. Assegure-se de que o hardware do HMC suporte o código do HMC Versão 7.	
2. Reúna informações e conclua a planilha de Configuração de pré-instalação.	“Planilha de Configuração de Pré-instalação para o HMC” na página 64

Tabela 3. Tarefas que você precisa concluir quando inclui um segundo HMC em uma instalação existente (continuação)

Tarefa	Onde localizar informações relacionadas
3. Desempacote o hardware.	
4. Conecte os cabos do hardware do HMC.	“Cabeando o 7063-CR1 HMC montado em rack” na página 21
5. Ligue o HMC pressionando o botão power.	
6. Efetue login no HMC.	
7. Os níveis de código do HMC devem corresponder. Altere o código em um dos HMCs para corresponder ao código no outro.	“Determinando sua Versão e Liberação do Código de Máquina do HMC” na página 93 “Fazendo Upgrade de seu Software do HMC” na página 98
8. Acesse o assistente de configuração orientada ou use os menus do HMC para configurar o HMC.	“Configurando o HMC usando os menus ” na página 71
9. Configure este HMC para serviço usando o assistente de Configuração de call home.	“Configurando o HMC para que ele possa se conectar ao serviço e suporte usando o assistente de configuração de call home” na página 86
10. Conecte o servidor ao HMC.	

Configurando o HMC

Você deve configurar o hardware do HMC antes de configurar o software do HMC. Aprenda mais sobre como configurar um HMC de desk-side ou um HMC montado em rack.

Instalando o IBM Power Systems HMC (7063-CR2) em um rack

Aprenda como instalar o IBM Power Systems HMC (7063-CR2) em um rack.

É possível visualizar a documentação de instalação on-line ou imprimir a versão PDF das mesmas informações. Para visualizar ou imprimir a versão em PDF, veja [Instalando e configurando o Hardware Management Console](#).

Pré-requisitos para a instalação do sistema 7063-CR2 montado em rack

Use as informações para entender os pré-requisitos que são necessários para instalar o sistema.

Sobre Esta Tarefa



CUIDADO: Esta peça ou unidade é pesada, mas tem um peso inferior a 18 kg (39,7 lb). Cuidado ao levantar, remover ou instalar a peça ou unidade. (C008)

Você pode precisar ler os documentos a seguir antes de iniciar a instalação do servidor:

- A versão mais recente deste documento é mantida on-line. Consulte [Instalando o 7063-CR2 em um rack](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 planejar a instalação de seu servidor, consulte [Planejamento de site e hardware](#).

Procedimento

1. Assegure-se de ter os seguintes itens antes de iniciar a instalação:

- Chave de fenda Phillips tamanho 2
- Chave de fenda comum
- Chave de fenda T25
- Estilete
- Pulseira de descarga eletrostática (ESD)
- Rack com uma unidade (1U) da Associação das Indústrias Eletrônicas (EIA) de espaço.

Notas:

- Se você não tiver um rack que esteja instalado, instale o rack. Para obter instruções, consulte [Racks e recursos de rack \(http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm\)](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).
- As classificações de fonte de alimentação são de 100 a 127 V AC, 9 A (x2), 200 a 240 V AC, 4,5 A (x2); 50 ou 60 hertz.

2. Continue com [“Concluindo o inventário para seu sistema”](#) na página 5.

Concluindo o inventário para seu sistema

Use estas informações para concluir o inventário para seu sistema.

Procedimento

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

Nota:

As informações de seu pedido estão incluídas com o produto. É possível também obter informações do pedido com o representante de marketing ou com o Parceiro de Negócios IBM.

Se houver peças incorretas, ausentes ou danificadas, consulte qualquer um dos seguintes recursos:

- Seu revendedor IBM.
- Linha de informação automatizada de manufatura IBM Rochester em 1-800-300-8751 (apenas Estados Unidos).
- O website [Directory of worldwide contacts \(http://www.ibm.com/planetwide\)](http://www.ibm.com/planetwide). Selecione o seu local para visualizar as informações de contato de serviço e suporte.

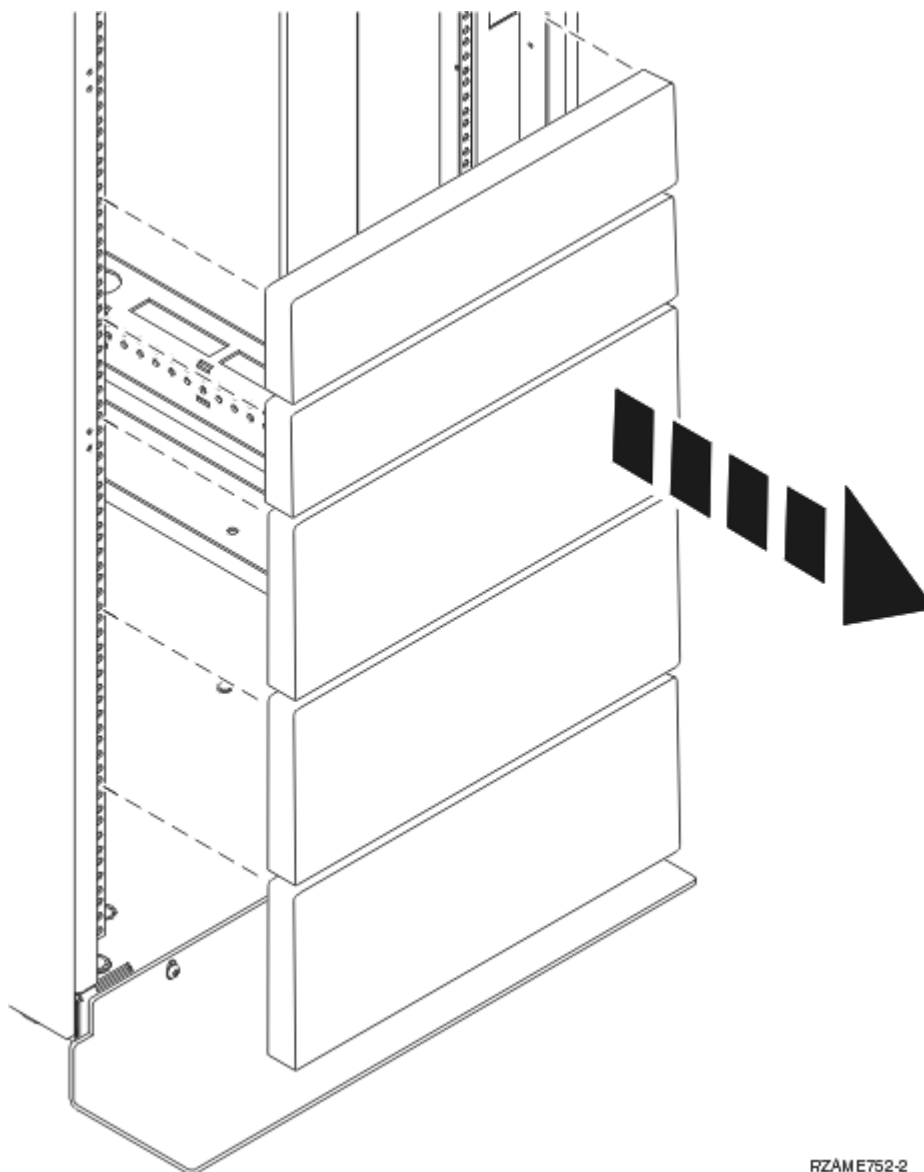
4. Continue com [“Determinando e marcando o local no rack para o sistema 7063-CR2”](#) na página 5.

Determinando e marcando o local no rack para o sistema 7063-CR2

É necessário determinar onde instalar a unidade de sistema no rack.

Procedimento

1. Leia os [Avisos de segurança do rack \(http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm\)](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Determine onde colocar a unidade de sistema no rack. Conforme você planejar a instalação da unidade de sistema em um rack, considere as informações a seguir:
 - Organize as unidades maiores e mais pesadas na parte inferior do rack.
 - Planeje instalar as unidades de sistema na parte mais baixa do rack primeiro.
 - Registre os locais da Aliança das Indústrias Eletrônicas (EIA) em seu plano.
3. Se necessário, remova os painéis de preenchimento para permitir acesso à parte interna do gabinete do rack em que planeja colocar a unidade, conforme mostrado na [Figura 1 na página 6](#).



RZAME752-2

Figura 1. Removendo os painéis do preenchimento

4. Determine onde colocar o sistema no rack. Anote o local de EIA.
5. De frente para o rack e trabalhando do lado direito, utilize fita, um marcador ou lápis para marcar o orifício inferior de cada unidade EIA.
6. Repita a etapa “5” na [página 6](#) para os buracos correspondentes localizados no lado esquerdo do rack.
7. Acesse para a parte traseira do rack.
8. No lado direito, localize a unidade EIA que corresponde à unidade EIA inferior marcada na parte frontal do rack.
9. Marque a unidade EIA inferior.
10. Marque os orifícios correspondentes no lado esquerdo do rack.
11. Continue com o “Conectando os trilhos ajustáveis ao chassi do sistema e ao rack” na [página 6](#) para anexar os trilhos ajustáveis ou continue com o “Conectando os trilhos fixos ao chassi do sistema e ao rack” na [página 8](#) para anexar os trilhos fixos.

Conectando os trilhos ajustáveis ao chassi do sistema e ao rack

Deve-se instalar os trilhos no chassi e no rack. Use este procedimento para executar esta tarefa.

Sobre Esta Tarefa



Atenção: Para evitar falha dos trilhos e potencial dano a si mesmo e à unidade, certifique-se de que você tenha os trilhos e encaixes corretos para seu rack. Se o rack tiver orifícios do flange de suporte quadrados ou orifícios do flange de suporte rosqueados, assegure-se de que os trilhos e os encaixes correspondam aos orifícios do flange de suporte que são usados no rack. Não instale hardware incompatível usando arruelas ou espaçadores. Se você não tiver os trilhos e ajustes corretos para seu rack, entre em contato com seu revendedor da IBM.

Nota: As unidades EIA 1 em racks são medidas em incrementos verticais de 44,45 milímetros (1,75 pol.) cada uma. Cada incremento de 44,45 milímetros (1,75 pol.) é chamado de “EIA”. Em alguns países, o mesmo incremento pode ser referido como um “U”.

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

Assegure-se de ter as peças necessárias para instalar os trilhos. As peças a seguir estão incluídas no kit de trilho:

- 4 - Parafusos Philips de 6,35 milímetros (0,25 pol.).
- 2 - Montagens de trilho de suporte de rack e deslizante
- 2 - Suportes deslizantes do HMC
- 10 - Presilhas de encaixe para orifícios de montagem de EIA quadrados
- 10 - Presilhas de encaixe para orifícios de montagem de EIA redondos
- 10 - Parafusos de flange hexadecimal M5

Procedimento

1. Remova as peças do trilho da embalagem e coloque-as em uma superfície de trabalho.
2. Identifique o espaço 1U no rack do HMC.
3. Para conectar os suportes deslizantes ao HMC, execute as tarefas a seguir:
 - a. Identifique o suporte deslizante direito.
 - b. Alinhe os furos no suporte deslizante direito com os pinos de suporte deslizante localizados no lado direito do HMC. Assegure-se de que todos os pinos estejam alinhados com os furos de suporte.
 - c. Empurre o suporte deslizante do HMC em direção ao lado da parte traseira do HMC até que ele esteja totalmente travado na posição.
 - d. Prenda o suporte deslizante direito no lado direito da estação de trabalho do HMC instalando dois parafusos Philips de 6,35 milímetros (0,25 pol.) nos orifícios do parafuso.
 - e. Repita as etapas “3.a” na página 7 - “3.d” na página 7 para instalar o suporte deslizante esquerdo no lado esquerdo da estação de trabalho do HMC.
4. Vá para a frente do rack.
 - a. No lado esquerdo, instale três presilhas de encaixe nos três furos na borda frontal do rack no slot 1U que é designado para o HMC.

Nota: O kit de trilho inclui presilhas de encaixe para orifícios do rack quadrados e redondos. Assegure-se de usar presilhas de encaixe apropriadas que combinem com os orifícios no rack.
 - b. Repita a etapa “4.a” na página 7 no lado direito do rack.
5. Mova para a parte traseira do rack.
 - a. No lado esquerdo, instale duas presilhas de encaixe nos furos superiores e inferiores na borda frontal do rack no slot 1U que é designado para o HMC.

Nota: O furo do meio deve permanecer vazio.
 - b. Repita a etapa “5.a” na página 7 no lado direito do rack.
6. Para instalar os trilhos deslizantes do HMC no rack, execute as etapas a seguir:

- a. Meça a profundidade do rack. A profundidade deve estar entre 558,8 milímetros (22 pol.) e 863,6 milímetros (34 pol.).
- b. Coloque os trilhos deslizantes do HMC em uma superfície plana e localize os parafusos pré-instalados.

Nota: Os trilhos deslizantes têm quatro orifícios do parafuso.

- c. Solte os parafusos pré-instalados nos trilhos deslizantes o suficiente para que os trilhos possam ser movidos para dentro e para fora facilmente.
- d. Com base na profundidade do rack medido na etapa [“6.a” na página 8](#), deve-se ajustar os parafusos nos trilhos.
 - i) Se a profundidade do rack estiver entre 558,8 milímetros (22 pol.) e 698,5 milímetros (27,5 pol.), fixe os parafusos no primeiro e no terceiro furos.
 - ii) Se a profundidade do rack estiver entre 698,5 milímetros (27,5 pol.) e 863,6 milímetros (34 pol.), fixe os parafusos no segundo e no quarto furos.

Notas:

- O primeiro furo é sempre o furo mais próximo da extremidade do trilho deslizante. O terceiro e o quarto furos estão localizados próximos uns dos outros.
- Certifique-se de que os parafusos estejam soltos o suficiente para que o comprimento do trilho deslizante possa ser levemente ajustado enquanto ele estiver sendo instalado no rack.

7. Na frente do rack, instale os trilhos deslizantes do HMC no rack executando as etapas a seguir:

- a. Localize a montagem de trilho deslizante esquerdo.
- b. Oriente a montagem de trilho para que a extremidade com o orifício do parafuso mais próximo (o primeiro furo) entre no rack primeiro. Assegure-se de que os cabeçotes do parafuso estejam voltados para o interior do rack. O slot aberto da montagem de trilho está mais próximo da frente do rack.
- c. No lado esquerdo do rack, conecte o flange na extremidade do trilho deslizante na borda frontal do rack usando dois parafusos M5, deixando o furo do meio aberto. Assegure-se de que a montagem de trilho seja deixada levemente solta na frente do rack para permitir que o HMC seja inserido.

8. Na parte traseira do rack, no lado direito, puxe a extremidade livre do trilho deslizante em direção à parte traseira e prenda o flange do trilho deslizante no rack usando dois parafusos M5, deixando o orifício do parafuso do meio aberto.

9. Repita a etapa [“7” na página 8](#) e a etapa [“8” na página 8](#) para instalar a montagem de trilho deslizante direito no lado direito do rack.

10. Na frente do rack, instale a estação de trabalho do HMC no rack executando as etapas a seguir:

- a. Mantendo o nível da estação de trabalho do HMC, insira os suportes deslizantes nos trilhos deslizantes do HMC que você instalou na etapa anterior. Empurre o HMC para a frente até que os flanges na frente do HMC estejam nivelados com os orifícios do parafuso abertos na frente do rack.
- b. Conecte o HMC ao lado esquerdo da estrutura usando um parafuso M5. Repita esta etapa no lado direito do rack.

11. Continue com [“Instalando o sistema no rack e conectando e roteando cabos de energia” na página 10](#).

Conectando os trilhos fixos ao chassi do sistema e ao rack

Deve-se instalar os trilhos no chassi e no rack. Use este procedimento para executar esta tarefa.

Sobre Esta Tarefa



Atenção: Para evitar falha dos trilhos e potencial dano a si mesmo e à unidade, certifique-se de que você tenha os trilhos e encaixes corretos para seu rack. Se o rack tiver orifícios do flange de

suporte quadrados ou orifícios do flange de suporte rosqueados, assegure-se de que os trilhos e os encaixes correspondam aos orifícios do flange de suporte que são usados no rack. Não instale hardware incompatível usando arruelas ou espaçadores. Se você não tiver os trilhos e ajustes corretos para seu rack, entre em contato com seu revendedor da IBM.

Nota: A unidade EIA 1 em racks é medida em incrementos verticais de 44,45 milímetros (1,75 pol.) cada uma. Cada incremento de 44,45 milímetros (1,75 pol.) é chamado de “EIA”. Em alguns países, o mesmo incremento pode ser referido como um “U”.

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

Assegure-se de ter as peças necessárias para instalar os trilhos. As peças a seguir estão incluídas no kit de trilho:

- 4 - Parafusos Philips de 6,35 milímetros (0,25 pol.).
- 2 - Trilhos internos
- 2 - Trilhos de suporte do HMC
- 2 - Presilhas de encaixe para orifícios de montagem de EIA quadrados
- 2 - Presilhas de encaixe para orifícios de montagem de EIA redondos
- 8 - Parafusos de flange hexadecimal M5

Procedimento

1. Remova as peças do trilho da embalagem e coloque-as em uma superfície de trabalho.
2. Identifique o espaço 1U no rack do HMC.
3. Para conectar os trilhos internos ao HMC, execute as tarefas a seguir:
 - a. Identifique o trilho interno direito.
 - b. Alinhe os furos no trilho interno direito com os pinos do trilho interno localizados no lado direito do HMC. Assegure-se de que todos os pinos estejam alinhados com os furos de trilho interno
 - c. Empurre o trilho interno do HMC em direção ao lado frontal do HMC até que ele esteja totalmente travado na posição.
 - d. Prenda o trilho interno direito no lado direito da estação de trabalho do HMC instalando dois parafusos Philips de 6,35 milímetros (0,25 pol.) nos orifícios do parafuso.
 - e. Repita as etapas 3.a - “3.d” na [página 9](#) para instalar o trilho interno esquerdo no lado esquerdo da estação de trabalho do HMC.
4. Mude para a parte frontal do rack. No lado esquerdo, instale uma presilha de encaixe no furo na borda frontal do rack no slot 1U que é designado para o HMC.

Nota: O kit de trilho inclui presilhas de encaixe para orifícios do rack quadrados e redondos. Assegure-se de usar presilhas de encaixe apropriadas que combinem com os orifícios no rack.

5. Mova para a parte traseira do rack. No lado esquerdo, instale uma presilha de encaixe no furo do meio na borda frontal do rack no slot 1U, que é designado para o HMC.
6. Na frente do rack, instale os trilhos de suporte do HMC no rack executando as etapas a seguir:
 - a. Alinhe os pinos dos trilhos de suporte acima e abaixo da presilha de encaixe que você instalou na etapa anterior.
 - b. No lado direito do rack, conecte o flange na extremidade do trilho de suporte até a borda frontal do rack usando dois parafusos M5 nos orifícios do parafuso superiores e inferiores, deixando o orifício do parafuso do meio aberto. Assegure-se de que a montagem de trilho seja deixada levemente solta na frente do rack para permitir que o HMC seja inserido.
7. Na parte traseira do rack, no lado direito, puxe a extremidade livre do trilho de suporte em direção à parte traseira e prenda o flange do trilho de suporte ao rack usando dois parafusos M5, deixando o orifício do parafuso do meio aberto.
8. Repita a etapa “6” na [página 9](#) e a etapa “7” na [página 9](#) para instalar a montagem de trilho de suporte no lado esquerdo do rack.

9. Na frente do rack, instale a estação de trabalho do HMC no rack executando as etapas a seguir:
 - a. Mantendo o nível da estação de trabalho do HMC, insira os trilhos internos nos trilhos de suporte do HMC que você instalou na etapa anterior. Empurre o HMC para a frente até que os flanges na frente do HMC estejam nivelados com os orifícios do parafuso abertos na frente do rack.
 - b. Conecte o HMC ao lado esquerdo da estrutura usando um parafuso M5. Repita esta etapa no lado direito do rack.

Nota: Se estiverem presentes, remova os suportes da remessa laranja que estão conectados à parte traseira do sistema e reinstale o parafuso de volta.

10. Continue com [“Instalando o sistema no rack e conectando e roteando cabos de energia”](#) na página 10.

Instalando o sistema no rack e conectando e roteando cabos de energia

Instale o sistema nos trilhos e conecte e roteie os cabos de energia.

Sobre Esta Tarefa



CUIDADO: Esta peça ou unidade é pesada, mas tem um peso inferior a 18 kg (39,7 lb). Cuidado ao levantar, remover ou instalar a peça ou unidade. (C008)

Procedimento

1. Remova o filme protetor plástico da parte superior do chassi do sistema.
2. Conecte os cabos de energia às fontes de alimentação.

Nota: Não conecte a outra extremidade do cabo de energia à fonte de alimentação agora.

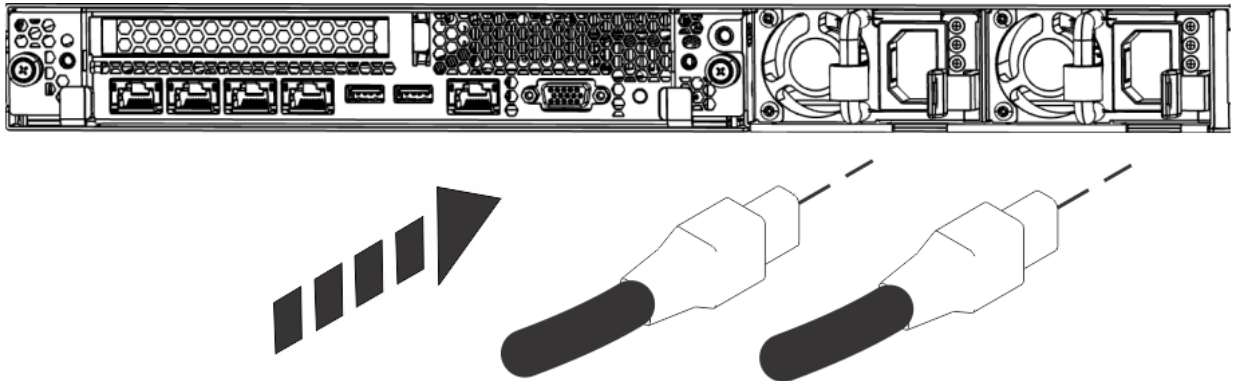


Figura 2. Conectando os cabos de energia às fontes de alimentação

3. Aperte as fitas de velcro para prender os cabos de energia.
4. Continue com [“Cabeando o 7063-CR2 HMC montado em rack”](#) na página 10.

Cabeando o 7063-CR2 HMC montado em rack

Aprenda como instalar fisicamente seu HMC (Hardware Management Console) montado em rack.

Procedimento

1. Assegure-se de que o HMC esteja instalado em um rack e os cabos de energia estejam conectados às fontes de alimentação. Para obter informações adicionais, consulte [“Instalando o sistema no rack e conectando e roteando cabos de energia”](#) na página 10. Após instalar o HMC em um rack, continue na próxima etapa.
2. Conecte o teclado, monitor e mouse.

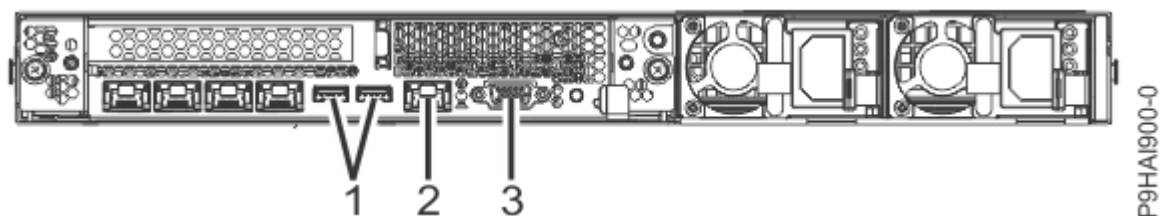


Figura 3. Portas traseiras

Tabela 4. Portas de entrada e de saída	
Identificador	Descrição
1	USB 2.0 usado para teclado e mouse
2	Intelligent Platform Management Interface (IPMI) Ethernet
3	Video Graphics Array (VGA) que é usado para o monitor. Somente a configuração 1024 x 768 a 60 Hz VGA é suportada. Somente um cabo de até três metros é suportado.

Nota: O sistema tem duas portas USB frontais que podem ser usadas.

3. Conecte a porta Ethernet Intelligent Platform Management Interface (IPMI) a uma rede.

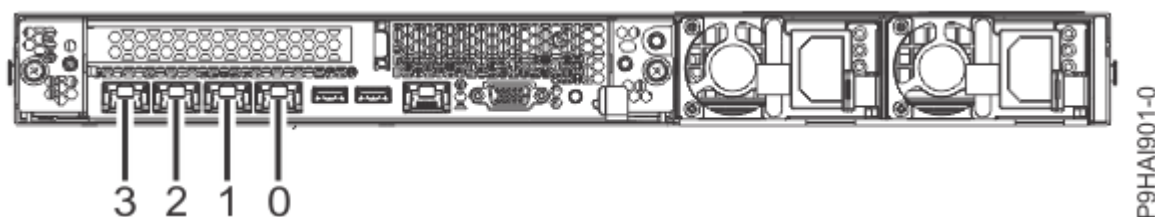


Figura 4. Portas Ethernet

Tabela 5. Portas Ethernet	
Identificador	Descrição
0	Conexão de rede compartilhada do Ethernet Intelligent Peripheral Management Interface (IPMI) e do HMC
1, 2 e 3	Conexão de rede do HMC

Nota: Essa conexão é necessária para acessar o Baseboard Management Controller (BMC) no HMC. O acesso ao BMC é necessário para tarefas de serviço e para manter o firmware HMC. Para obter mais informações, consulte “Tipos de Conexões de Rede do HMC” na página 55.

Aviso: Este produto não pode ser certificado em seu país para conexão, por qualquer meio, com as interfaces das redes de telecomunicações públicas. Certificação adicional pode ser requerida por lei antes desse tipo de conexão. Entre em contato com a IBM para obter mais informações.

4. Conecte o cabo Ethernet que está destinado para a conexão ao sistema ou sistemas gerenciados.

Notas:

- Se você estiver usando uma conexão compartilhada para IPMI e HMC, um único cabo para a porta 0 na Figura 2 poderá satisfazer ambos os requisitos para IPMI e HMC.

- Para aprender mais sobre as conexões de rede do HMC, consulte [“Conexões de Rede do HMC”](#) na página 54.
5. Se o sistema gerenciado já estiver instalado, será possível verificar se a conexão do cabo Ethernet está ativa observando as luzes verdes de status nas portas Ethernet do HMC e do sistema gerenciado à medida que a instalação progride.
 6. Conecte os cabos de energia do sistema e os cabos de energia de quaisquer outros dispositivos conectados à fonte de alimentação de corrente alternada (AC).
 7. Verifique o status de energia usando os LEDs da fonte de alimentação como indicadores. Para obter mais informações, consulte [LEDs no sistema 7063-CR2](#) LEDs no sistema 7063-CR2.
 8. Pressione o botão power para iniciar o sistema. A luz indicadora de funcionamento para de piscar e permanece acesa, indicando que a energia do sistema está ligada.

Resultados

Depois, é necessário instalar e configurar o software HMC. Continue com [“Configurando o 7063-CR2 HMC”](#) na página 12.

Configurando o 7063-CR2 HMC

Aprenda como instalar e configurar o HMC (Hardware Management Console).

Verifique a versão do HMC que é enviada com seu HMC. Para descobrir como visualizar a versão e a liberação do código de máquina do HMC, consulte [Verificar a versão do HMC que é enviada com o seu HMC](#). É possível fazer download da versão mais recente do HMC que estiver disponível no [website Fix Central](#). Use a mídia removível (como um DVD ou USB) para criar um arquivo ISO inicializável de um pacote HMC (imagem ISO).

Nota: A tabela a seguir descreve as informações de login predefinidas (padrão) para as interfaces do HMC e BMC.

Tabela 6.			
Console ou interface	ID Padrão	Senha Padrão	Descrição
BMC (OpenBMC)	root	0penBmc	O ID do usuário raiz e a senha são usados para efetuar login no BMC pela primeira vez.
HMC	hscroot	abc123	O ID de usuário hscroot e a senha são utilizados para efetuar login no HMC pela primeira vez. Eles fazem distinção entre maiúsculas e minúsculas e só podem ser utilizados por um membro com a função de superadministrador.
HMC	root	passw0rd	O ID do usuário root e a senha são utilizados pelo fornecedor de serviços para executar procedimentos de manutenção. Eles não podem ser utilizados para efetuar login no HMC.

Nota: As seguintes instalações são mostradas como exemplos.

Instalando o HMC usando unidade flash USB

Para instalar o HMC usando a unidade flash USB, conclua as etapas a seguir para os sistemas Linux®:

Nota: Para obter exemplos em diferentes sistemas operacionais, consulte:

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

1. Faça download da versão do HMC que você deseja no website [Fix Central](#).
2. Execute o comando a seguir: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (em que **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 estiver conectada.

3. Insira a unidade USB e ligue o sistema.

Nota: A unidade USB deve ser de pelo menos 8 GB. Algumas unidades USB podem ser muito grandes para se ajustarem de forma adequada na porta USB na parte traseira do sistema. Teste o ajuste de sua unidade USB antes de continuar.

4. Quando o menu Petitboot for exibido, selecione a opção **Instalar o Hardware Management Console** que está localizada em **USB**.

Instalando o HMC usando mídia virtual do BMC

Para instalar o HMC usando mídia virtual do BMC, conclua as etapas a seguir:

1. Abra um navegador da web suportado. Na barra de endereço, insira o endereço IP do BMC com o qual você deseja se conectar. Por exemplo, é possível usar o formato `https://<BMC IP>` na barra de endereço do navegador da web.
2. Na janela **Logon do OpenBMC**, insira o endereço do **Host** do BMC e o **Nome do usuário** e **Senha** designados a você.

Nota: O ID de usuário padrão é `root` e a senha raiz é `OpenBmc`.

Se você estiver usando o nível de firmware OP940.01 ou mais recente, a senha raiz será expirada por padrão. Deve-se mudar a senha padrão antes de acessar o BMC. Para obter mais informações sobre a mudança da senha padrão expirada, consulte [Configurando a senha](#).

Se você esqueceu a sua senha, será possível executar uma reconfiguração de fábrica do sistema para restaurar a senha padrão. Para reconfigurar o sistema, consulte [Executando uma reconfiguração de fábrica](#).

3. Clique em **Efetuar Login**.
4. Selecione **Controle do servidor**.
5. Selecione **Mídia virtual**.
6. Clique em **Escolher arquivo**.
7. Localize a ISO de mídia de Recuperação do HMC e clique em **Abrir**.
8. Dê um clique em **Iniciar**.
9. Ligue o sistema.
10. Quando o menu Petitboot for exibido, selecione a opção **Instalar o Hardware Management Console** que está localizada em **USB**.

Instalando o HMC usando uma unidade de DVD conectada ao USB externo

Para instalar o HMC usando uma unidade de DVD conectada ao USB externo, conclua as etapas a seguir:

1. Faça download da versão de recuperação do HMC que você deseja por meio do website do [Fix Central](#).
2. Grave a imagem do DVD de recuperação do HMC em uma mídia DVD-R DL como uma imagem.
3. Desligue o HMC.
4. Conecte a unidade de DVD USB externa ao HMC e insira o DVD de recuperação do HMC.

Nota: Pode ser necessário conectar a unidade de DVD USB a uma fonte de alimentação externa ou usar um cabo USB Y para se conectar a uma porta USB adicional para fornecer energia suficiente para a unidade de DVD.

5. Ligue o HMC.

Nota: O monitor de exibição pode não mostrar sinal durante a inicialização. O processo pode levar 2 ou 3 minutos antes de o monitor de exibição mostrar qualquer status.

6. Quando o carregador de inicialização do Petitboot for iniciado, navegue para parar a inicialização automática.

Nota: Um tempo limite de 10 segundos é cumprido. Se nenhuma ação for tomada dentro de 10 segundos, o sistema tentará inicializar da unidade de disco rígido.

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

Nota: Esse processo pode levar até um minuto.

8. Selecione a opção **Instalar o Hardware Management Console** que está localizada em **CD/DVD**.

Instalando o 7063-CR1 em um rack

Saiba como instalar o 7063-CR1 HMC (Hardware Management Console) em um rack.

É possível visualizar a documentação de instalação on-line ou imprimir a versão PDF das mesmas informações. Para visualizar ou imprimir a versão em PDF, veja [Instalando e configurando o Hardware Management Console](#).

Pré-requisitos para a instalação do sistema 7063-CR1 montado em rack

Use as informações para entender os pré-requisitos que são necessários para instalar o sistema.

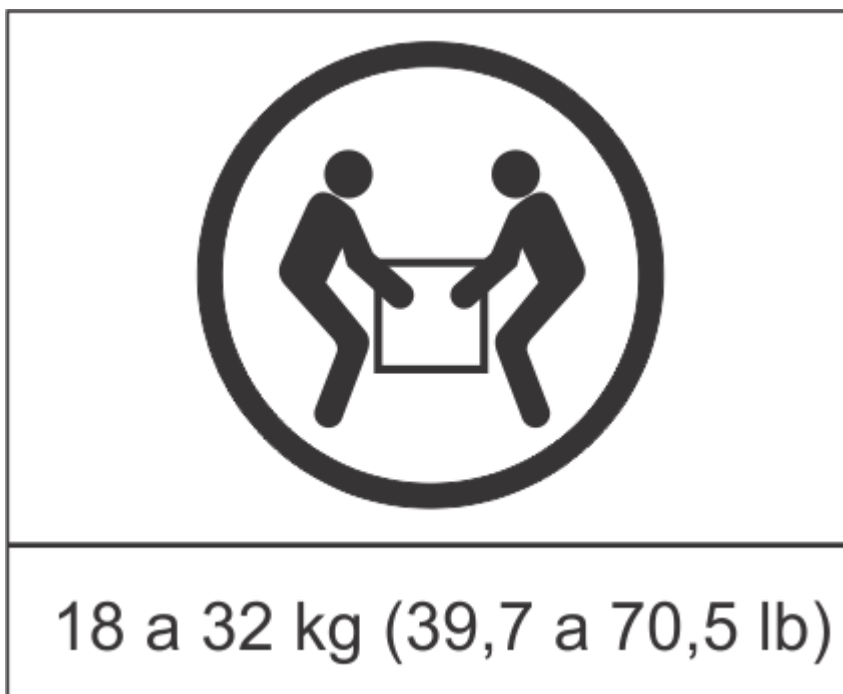
Sobre Esta Tarefa



CUIDADO:

ou

ou



O peso desta peça ou unidade está entre 18 e 32 kg (39,7 e 70,5 lb). Levantá-la de forma segura envolve duas pessoas. (C009)

Você pode precisar ler os documentos a seguir antes de iniciar a instalação do servidor:

- A versão mais recente deste documento é mantida on-line, consulte [Instalando o 7063-CR1 em um rack](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 planejar a instalação de seu servidor, consulte [Planejamento de site e hardware](#).

Procedimento

Assegure-se de ter os seguintes itens antes de iniciar a instalação:

- Chave de fenda Phillips tamanho 2
- Chave de fenda comum
- Estilete
- Pulseira de descarga eletrostática (ESD)
- Rack com uma unidade (1U) da Associação das Indústrias Eletrônicas (EIA) de espaço.

Nota: Se você não tiver um rack que esteja instalado, instale o rack. Para obter instruções, consulte [Racks e recursos de rack](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).

Concluindo o inventário para seu sistema

Use estas informações para concluir o inventário para seu sistema.

Procedimento

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

Nota:

As informações de seu pedido estão incluídas com o produto. É possível também obter informações do pedido com o representante de marketing ou com o Parceiro de Negócios IBM.

Se houver peças incorretas, ausentes ou danificadas, consulte qualquer um dos seguintes recursos:

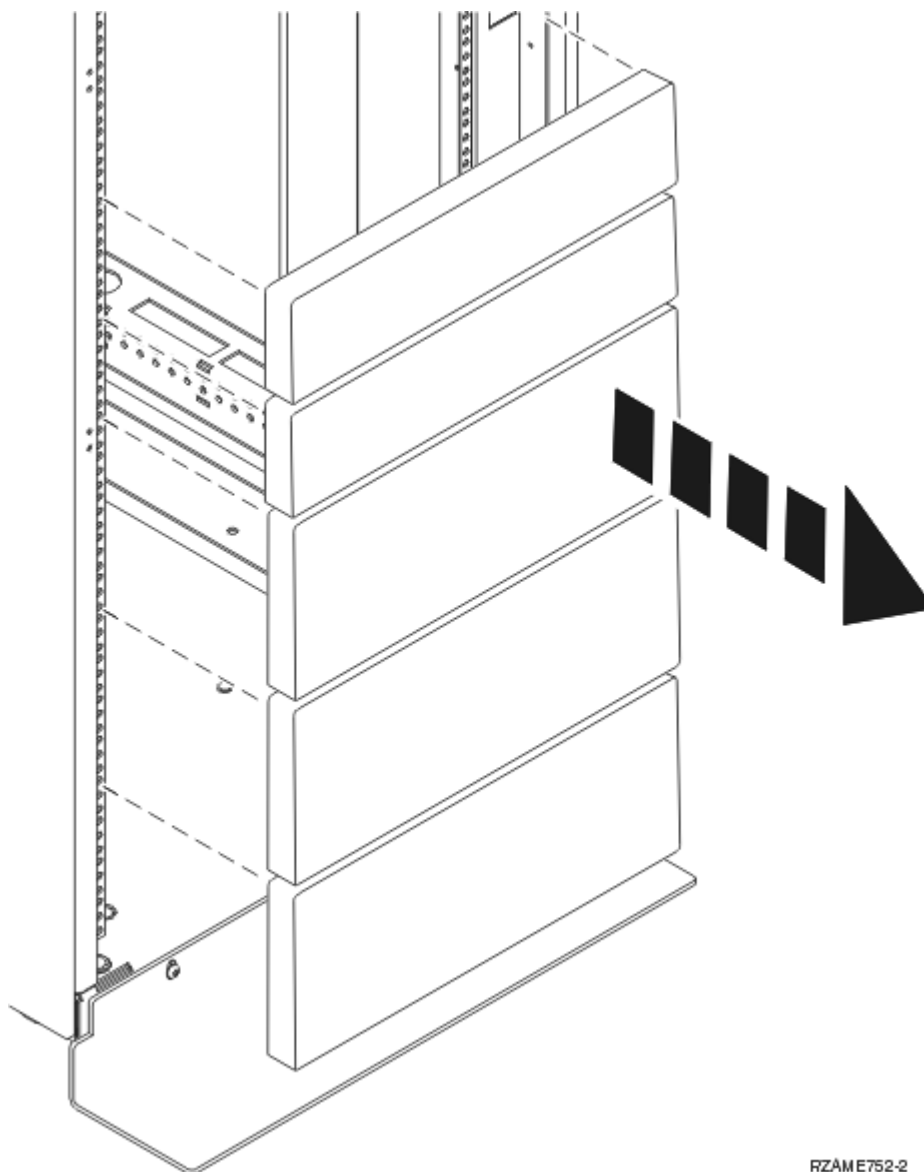
- Seu revendedor IBM.
- Linha de informação automatizada de manufatura IBM Rochester em 1-800-300-8751 (apenas Estados Unidos).
- O [website Directory of worldwide contacts](http://www.ibm.com/planetwide) (<http://www.ibm.com/planetwide>). Selecione o seu local para visualizar as informações de contato de serviço e suporte.

Determinando e marcando o local no rack para o sistema 7063-CR1

Você poderá precisar determinar onde instalar a unidade de sistema no rack.

Procedimento

1. Leia os Avisos de segurança do rack (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Determine onde colocar a unidade de sistema no rack. Conforme você planejar a instalação da unidade de sistema em um rack, considere as informações a seguir:
 - Organize as unidades maiores e mais pesadas na parte inferior do rack.
 - Planeje instalar as unidades de sistema na parte mais baixa do rack primeiro.
 - Registre os locais da Aliança das Indústrias Eletrônicas (EIA) em seu plano.
3. Se necessário, remova os painéis de preenchimento para permitir acesso à parte interna do gabinete do rack em que planeja colocar a unidade, conforme mostrado na [Figura 5 na página 17](#).



RZAME752-2

Figura 5. Removendo os painéis do preenchimento

4. Determine o local adequado para colocar o sistema no rack. Anote o local de EIA.
5. De frente para o rack e trabalhando do lado direito, utilize fita, um marcador ou lápis para marcar o orifício inferior de cada unidade EIA.
6. Repita a etapa “5” na [página 17](#) para os buracos correspondentes localizados no lado esquerdo do rack.
7. Acesse para a parte traseira do rack.
8. No lado direito, localize a unidade EIA que corresponde à unidade EIA inferior marcada na parte frontal do rack.
9. Marque a unidade EIA inferior.
10. Marque os orifícios correspondentes no lado esquerdo do rack.

Conectando os trilhos fixos ao chassi do sistema e ao rack

Deve-se instalar os trilhos no chassi e no rack. Use este procedimento para executar esta tarefa.

Sobre Esta Tarefa



Atenção: Para evitar falha dos trilhos e potencial dano a si mesmo e à unidade, certifique-se de que você tenha os trilhos e encaixes corretos para seu rack. Se o rack tiver orifícios do flange de suporte quadrados ou orifícios do flange de suporte rosqueados, assegure-se de que os trilhos e os encaixes correspondam aos orifícios do flange de suporte que são usados no rack. Não instale hardware incompatível usando arruelas ou espaçadores. Se você não tiver os trilhos e ajustes corretos para seu rack, entre em contato com seu revendedor da IBM.

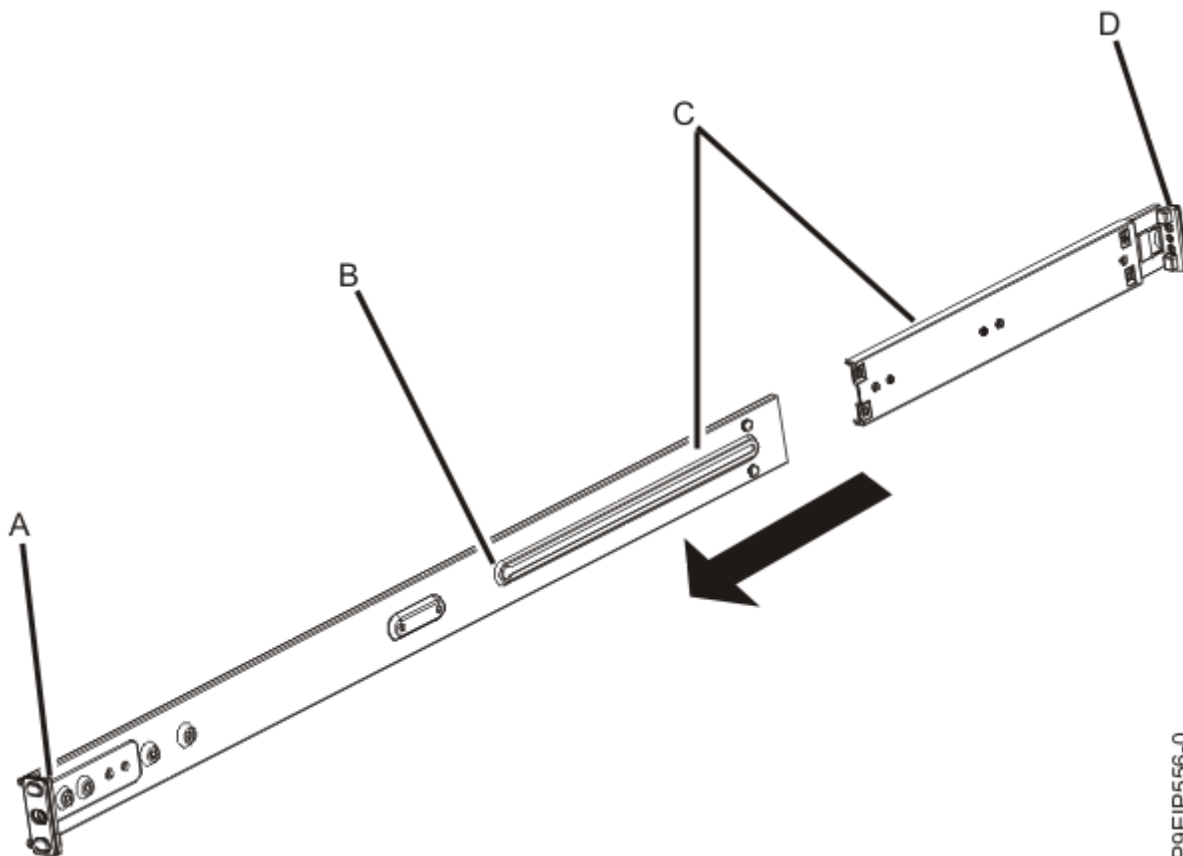
Nota: O sistema requer 1 unidade de rack EIA (1U) de espaço.

Assegure-se de ter as peças necessárias para instalar os trilhos. As peças a seguir estão incluídas no kit de trilho:

- Parafusos do trilho deslizante, usados para conectar as duas partes de cada trilho deslizante
- Parafusos do trilho deslizante, usados para fixar os trilhos ao rack
- Trilhos
- Dez parafusos 32 x 0,635 cm (0,25 polegadas) usados para conectar os trilhos ao chassi do sistema

Procedimento

1. Remova as peças do trilho da embalagem e coloque-as em uma superfície de trabalho.
2. Substitua os pinos quadrados do trilho do rack (A) e (D) pelos pinos redondos do trilho do rack.
3. Conecte as duas partes de cada trilho deslizante do rack. Para conectar as duas partes do trilho deslizante do rack, execute as tarefas a seguir:
 - a. Identifique as duas partes do trilho deslizante esquerdo do rack. Alinhe as peças curtas e longas (C). Verifique se os pinos do trilho do rack estão apontando para a mesma direção (A) e (D).



- b. A menor parte do trilho deslizante do rack tem um pino de metal. Insira o pino no orifício na peça mais longa do trilho deslizante do rack (B). Deslize a parte mais curta do trilho do rack na parte mais longa do trilho do rack.

- c. Alinhe os orifícios nas duas peças dos trilhos deslizantes do rack. Usando uma chave de fenda Phillips, conecte as duas peças apertando ligeiramente os dois parafusos roscados do trilho através dos furos no trilho deslizante do rack.

Nota: Não aperte os parafusos do trilho deslizante do rack.

- d. Repita essas etapas para o trilho deslizante direito.
4. Instale os trilhos deslizantes do rack no rack.
- a. Mude para a parte frontal do rack.
 - b. Selecione o trilho deslizante esquerdo do rack e localize a unidade EIA que você marcou anteriormente. Cada trilho deslizante também é marcado com **Traseiro**, para designar a parte traseira do rack. Segure a parte dianteira do trilho deslizante do rack.
 - c. Estenda o trilho da parte frontal do rack para a parte traseira do rack e alinhe os pinos do trilho deslizante do rack com os orifícios no flange do rack que você marcou anteriormente.
 - d. Empurre os pinos do trilho do rack no flange do rack traseiro até a trava do trilho do rack traseiro se encaixar no lugar.
 - e. Puxe a frente do trilho do rack em direção à parte frontal do flange do trilho do rack. Alinhe os pinos do trilho deslizante com os orifícios no flange do trilho e puxe-os até a trava do trilho se encaixar no lugar.
 - f. Usando uma chave de fenda, aperte os parafusos do trilho que você instalou na etapa [2](#).
- Nota:** Você pode precisar de 2U de espaço para acessar e apertar os parafusos do trilho.
- g. Repita as etapas [4a](#) a [4f](#) para o trilho deslizante direito.

Instalando o sistema no rack e conectando e roteando cabos de energia

Instale o sistema nos trilhos e conecte e roteie os cabos de energia.

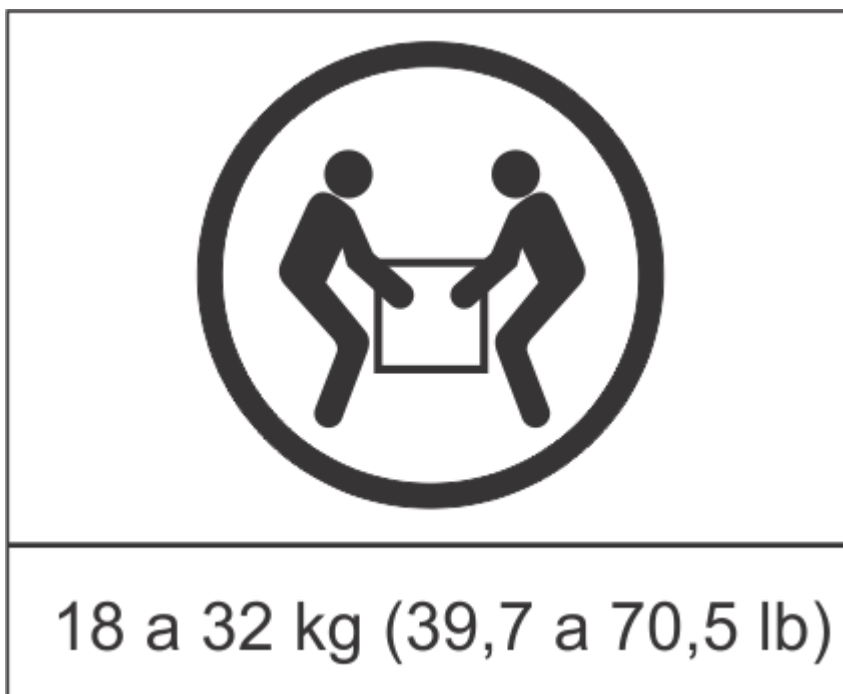
Sobre Esta Tarefa



CUIDADO:

ou

ou



O peso desta peça ou unidade está entre 18 e 32 kg (39,7 e 70,5 lb). Levantá-la de forma segura envolve duas pessoas. (C009)

Procedimento

1. Remova o filme protetor plástico da parte superior do chassi do sistema.
2. Vá para a frente do rack.
3. Usando duas pessoas, uma em cada lado do sistema, erga o sistema e alinhe os trilhos do chassi do sistema em cada lado do chassi com os trilhos deslizantes do rack.
4. Empurre o sistema para a parte traseira do rack.
5. Prenda o sistema ao rack apertando um parafuso com arruela nas alças em cada lado do chassi do sistema.

Nota: Deve-se usar arruelas com os parafusos. Deslize uma arruela em cada um dos dois parafusos mais longos (1,5 cm (0,59 pol.)) que está incluída com o kit de trilho. Aperte o parafuso com a arruela pelos lados direito e esquerdo do sistema na frente.

6. Conecte os cabos de energia às fontes de alimentação.

Nota: Não conecte a outra extremidade do cabo de energia à fonte de alimentação agora.

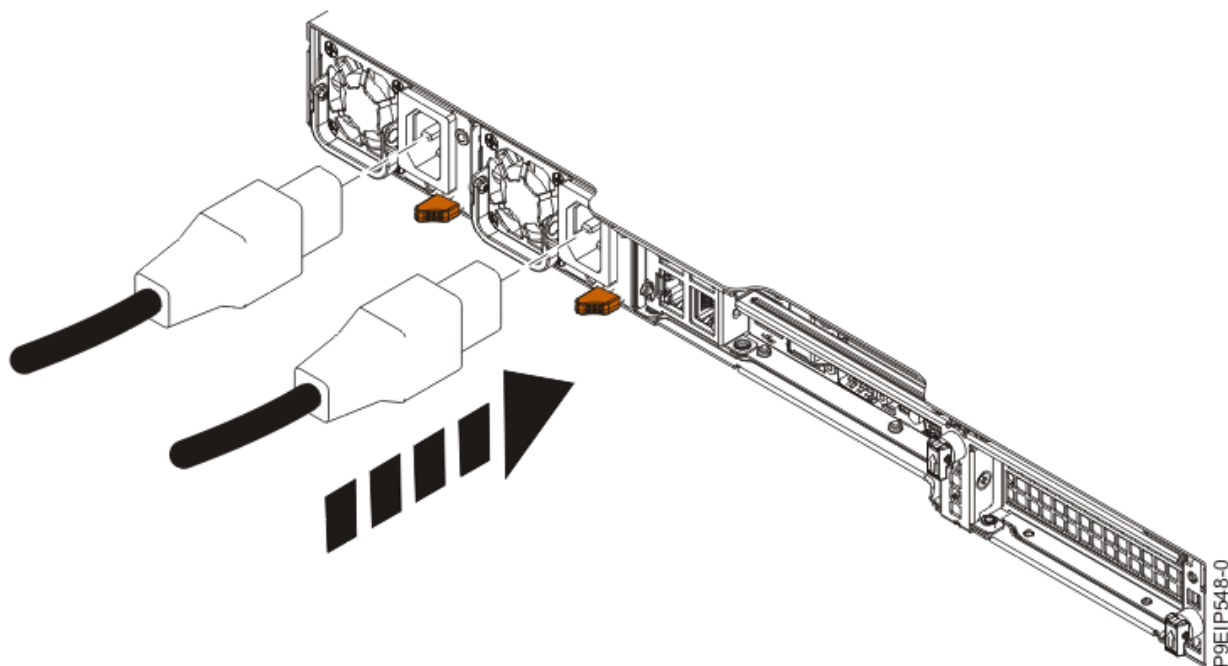


Figura 6. Conectando os cabos de energia às fontes de alimentação

7. Continue com [“Cabeando o 7063-CR1 HMC montado em rack”](#) na página 21.

Cabeando o 7063-CR1 HMC montado em rack

Aprenda como instalar fisicamente seu HMC (Hardware Management Console) montado em rack.

Procedimento

1. Assegure-se de que o HMC esteja instalado em um rack e os cabos de energia estejam conectados às fontes de alimentação. Para obter mais informações, consulte [“Instalando o sistema no rack e conectando e roteando cabos de energia”](#) na página 19. Após instalar o HMC em um rack, continue na próxima etapa.

Nota: Se um plugue estiver cobrindo uma porta que você precisa usar na parte traseira do sistema, remova e descarte-o. As tampas da porta asseguram que você seja lembrado de que deve reconfigurar a senha do Administrador em seu sistema gerenciado no IPL inicial do sistema.

2. Conecte o teclado, monitor e mouse.

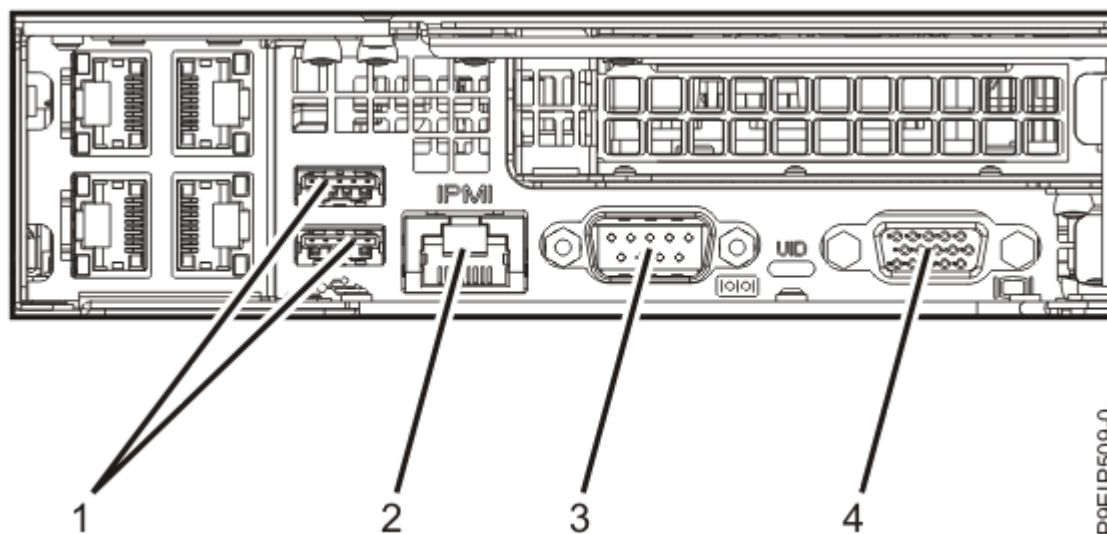


Figura 7. Portas traseiras

Tabela 7. Portas de entrada e de saída	
Identificador	Descrição
1	USB 2.0 usado para teclado e mouse
2	Intelligent Platform Management Interface (IPMI) Ethernet
3	IPMI serial
4	Video Graphics Array (VGA) que é usado para o monitor. Somente a configuração 1024 x 768 a 60 Hz VGA é suportada. Somente um cabo de até três metros é suportado.

Nota: O sistema tem duas portas USB frontais que podem ser usadas. A porta serial frontal é não funcional.

3. Conecte o cabo Ethernet que está destinado para a conexão ao sistema ou sistemas gerenciados.

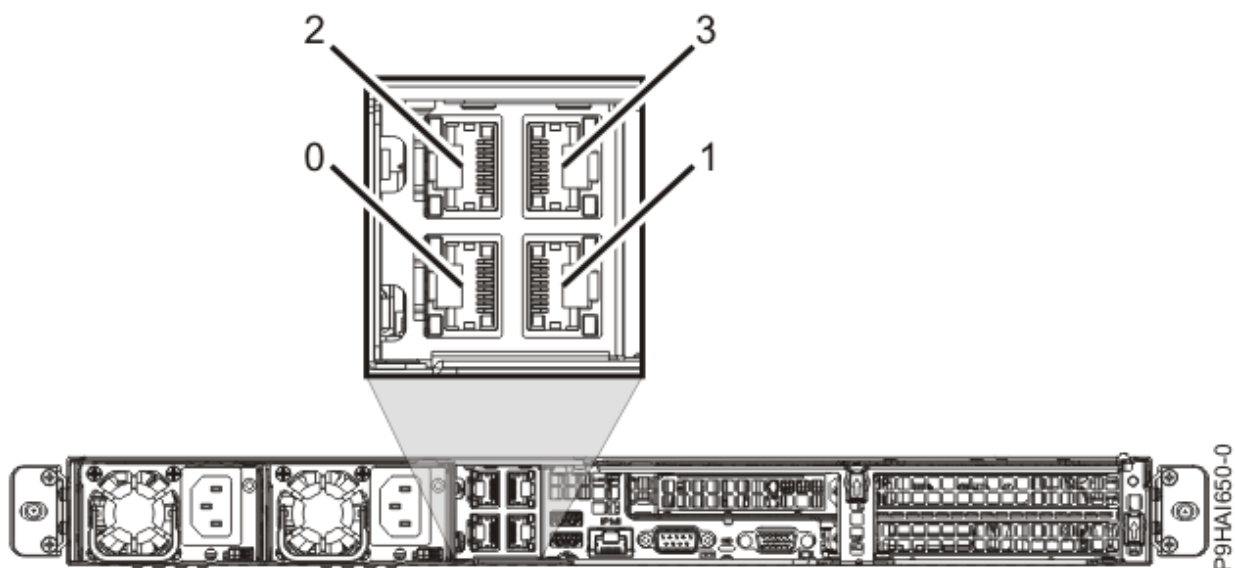


Figura 8. Portas Ethernet

Nota: Para aprender mais sobre as conexões de rede do HMC, consulte [“Conexões de Rede do HMC”](#) na página 54.

4. Se o sistema gerenciado já estiver instalado, será possível verificar se a conexão do cabo Ethernet está ativa observando as luzes verdes de status nas portas Ethernet do HMC e do sistema gerenciado à medida que a instalação progride.
5. Conecte a porta Ethernet Intelligent Platform Management Interface (IPMI) a uma rede.

Nota: Essa conexão é necessária para acessar o Baseboard Management Controller (BMC) no HMC. O acesso ao BMC é necessário para tarefas de serviço e para manter o firmware HMC. Para obter mais informações, consulte [“Tipos de Conexões de Rede do HMC”](#) na página 55.

6. Conecte os cabos de energia do sistema e os cabos de energia de quaisquer outros dispositivos conectados à fonte de alimentação de corrente alternada (AC).
7. Verifique o status de energia usando os LEDs da fonte de alimentação como indicadores. Para obter mais informações, consulte [LEDs no sistema 7063-CR1](#) LEDs no sistema 7063-CR1.

Resultados

Depois, é necessário instalar e configurar o software HMC. Continue com [“Configurando o 7063-CR1 HMC”](#) na página 23.

Configurando o 7063-CR1 HMC

Aprenda como instalar e configurar o HMC (Hardware Management Console).

Verifique a versão do HMC que é enviada com seu HMC. É possível fazer download da versão mais recente do HMC que estiver disponível no website [Fix Central](#). Use a mídia removível (como um DVD ou USB) para criar um arquivo ISO inicializável de um pacote HMC (imagem ISO).

Nota: A tabela a seguir descreve as informações de login predefinidas (padrão) para as interfaces do HMC e BMC.

Tabela 8.			
Console ou interface	ID Padrão	Senha Padrão	Descrição
BMC	ADMIN	ADMIN	O ID do usuário e senha ADMIN são usados para efetuar login no BMC pela primeira vez.
HMC	hscroot	abc123	O ID de usuário hscroot e a senha são utilizados para efetuar login no HMC pela primeira vez. Eles fazem distinção entre maiúsculas e minúsculas e só podem ser utilizados por um membro com a função de superadministrador.
HMC	root	passw0rd	O ID do usuário root e a senha são utilizados pelo fornecedor de serviços para executar procedimentos de manutenção. Eles não podem ser utilizados para efetuar login no HMC.

Nota: As seguintes instalações são mostradas como exemplos.

Instalando o HMC usando unidade flash USB

Para instalar o HMC usando a unidade flash USB, conclua as etapas a seguir para os sistemas Linux:

Nota: Para obter exemplos em diferentes sistemas operacionais, consulte:

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

1. Faça download da versão do HMC que você deseja no website [Fix Central](#).
2. Execute o comando a seguir: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (em que **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 estiver conectada.

3. Insira a unidade USB e ligue o sistema.

Nota: A unidade USB deve ser de pelo menos 4 GB. Algumas unidades USB podem ser muito grandes para se ajustarem de forma adequada na porta USB na parte traseira do sistema. Teste o ajuste de sua unidade USB antes de continuar.

4. Quando o menu Petitboot for exibido, selecione a opção **Instalar o Hardware Management Console** que está localizada em **USB**.

Instalando o HMC usando uma mídia remota do visualizador do console

Para instalar o HMC usando uma mídia remota do visualizador do console, conclua as etapas a seguir:

1. Efetue login na interface da web do BMC (<http://<bmc-ip>>).
2. Selecione **Controle remoto**.
3. Selecione **Redirecionamento de console**.
4. Clique em **Ativar console**.
5. No Java™ iKVM Viewer, selecione **Mídia virtual > Armazenamento virtual**.
6. Em **Tipo de unidade lógica**, selecione **Arquivo ISO**.
7. Clique em **Abrir imagem** e localize o arquivo ISO em seu sistema.
8. Pressione **Plugin** para montar o arquivo ISO.
9. Ligue o sistema.
10. Quando o menu Petitboot for exibido, selecione a opção **Instalar o Hardware Management Console** que está localizada em **CD/DVD**.

Instalando o HMC usando uma unidade de DVD conectada ao USB externo

Para instalar o HMC usando uma unidade de DVD conectada ao USB externo, conclua as etapas a seguir:

1. Faça download da versão de recuperação do HMC que você deseja por meio do website do [Fix Central](#).
2. Queime a imagem do DVD de recuperação do HMC em uma mídia de DVD-R como uma imagem. Como alternativa, é possível pedir a mídia de recuperação em DVD.
3. Desligue o HMC.
4. Conecte a unidade de DVD USB externa ao HMC e insira o DVD de recuperação do HMC.

Nota: Pode ser necessário conectar a unidade de DVD USB a uma fonte de alimentação externa ou usar um cabo USB Y para se conectar a uma porta USB adicional para fornecer energia suficiente para a unidade de DVD.

5. Ligue o HMC.

Nota: O monitor de exibição pode não mostrar sinal durante a inicialização. O processo pode levar 2 ou 3 minutos antes de o monitor de exibição mostrar qualquer status.

6. Quando o carregador de inicialização do Petitboot for iniciado, navegue para parar a inicialização automática.

Nota: Um tempo limite de 10 segundos é cumprido. Se nenhuma ação for tomada dentro de 10 segundos, o sistema tentará inicializar da unidade de disco rígido.

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

Nota: Esse processo pode levar até um minuto.

8. Selecione a opção **Instalar o Hardware Management Console** que está localizada em **CD/DVD**.

Instalando o HMC usando uma mídia remota que é hospedada por um servidor de arquivos SMB

Para instalar o HMC usando uma mídia remota que seja hospedada pelo servidor de arquivos Bloco de Mensagens do Servidor (SMB), conclua as etapas a seguir:

1. Copie o arquivo ISO de recuperação para um host de compartilhamento em seu servidor de arquivos compatível com SMB.

Nota: O Bloco de Mensagens do Servidor versão 3 (SMBv3) não é suportado.

2. Efetue login na interface da web do BMC (<http://<bmc-ip>>).
3. Selecione **Mídia virtual**.
4. Selecione **Imagem do CD-ROM**.
5. Complete as informações a seguir:

Host de compartilhamento

O IP do host do SMB. Se você estiver usando o nome do host, assegure-se de que o DNS (sistema do nome de domínio) no BMC esteja configurado corretamente.

Caminho para a imagem

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

Usuário (opcional)

O nome do usuário que é usado para efetuar login no host SMB.

Senha (opcional)

A senha para o usuário.

6. Clique em **Save**.
7. Clique em **Montar**.
8. Agora o Dispositivo 1 mostra a mensagem a seguir: **Há um arquivo ISO montado**.

Nota: Se a mensagem não aparecer, verifique novamente as informações e repita as etapas [6](#) a [8](#).

9. Ligue o sistema.
10. Quando o menu Petitboot for exibido, selecione a opção **Instalar o Hardware Management Console** que está localizada em **CD/DVD**.

Opcional: atualize o nível de firmware do HMC usando o Memory Key USB incluído

Nota: Se sua configuração incluiu uma atualização de firmware do HMC em um Memory Key USB, conclua as etapas a seguir para atualizar o nível de firmware do HMC.

Para atualizar o nível de firmware do HMC usando o Memory Key USB incluído, conclua as etapas a seguir:

1. Insira a unidade de Memory Key USB na porta USB na parte traseira do sistema.
2. Ligue o sistema e efetue logon no HMC.



3. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Gerenciamento de console**.
4. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
5. Siga as instruções na tela no assistente Instalar o serviço corretivo do HMC.

Em seguida, é necessário configurar seu software HMC. Para obter instruções, consulte [“Configurando o HMC” na página 54](#).

Conceitos relacionados

[Configure a conectividade do BMC](#)

É possível configurar ou visualizar as configurações de rede no BMC para o console de gerenciamento.

Instalando o HMC 7042-CR9 em um rack

Aprenda a instalar o Hardware Management Console (HMC) 7042-CR9 em um rack.

Antes de Iniciar

Nota:

O Hardware Management Console Versão 9.2.950 ou mais recente não é suportado no HMC 7042-CR9. Para obter mais informações sobre as versões do HMC para o seu HMC 7042-CR9, consulte as notas sobre a liberação do HMC que estão disponíveis no website do [Fix Central](#).

Conclua um inventário das peças. As ilustrações a seguir mostram os itens necessários para instalar o servidor no gabinete do rack. Se os itens estiverem ausentes ou danificados, entre em contato com o local da compra.

Conteúdo da caixa do Suporte para organização de cabos

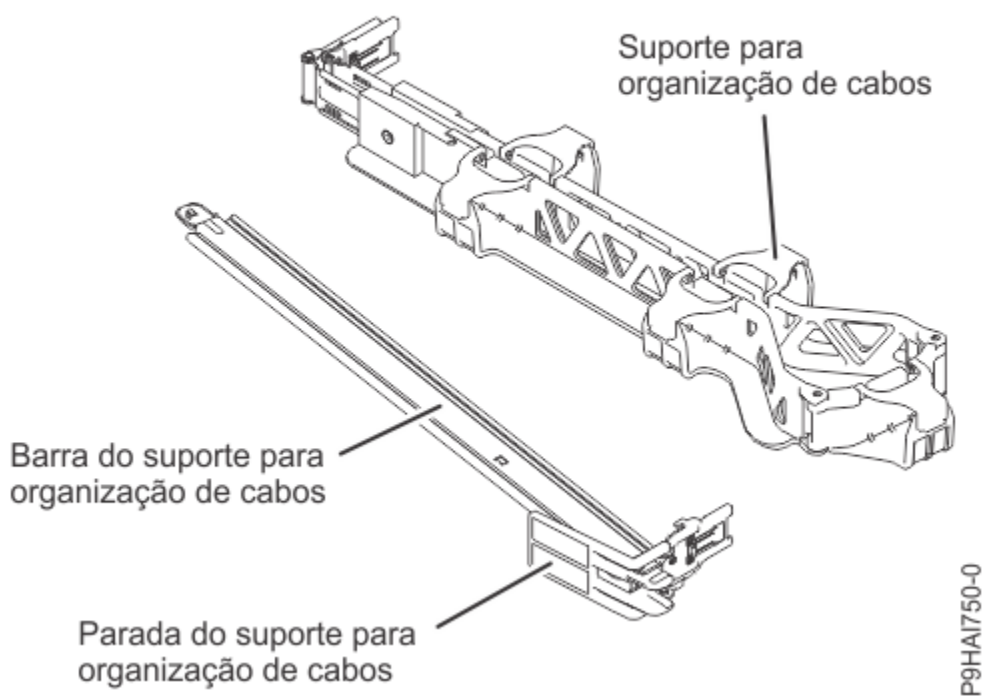


Figura 9. Conteúdo da caixa do suporte para organização de cabos

Conteúdo da caixa de trilhos

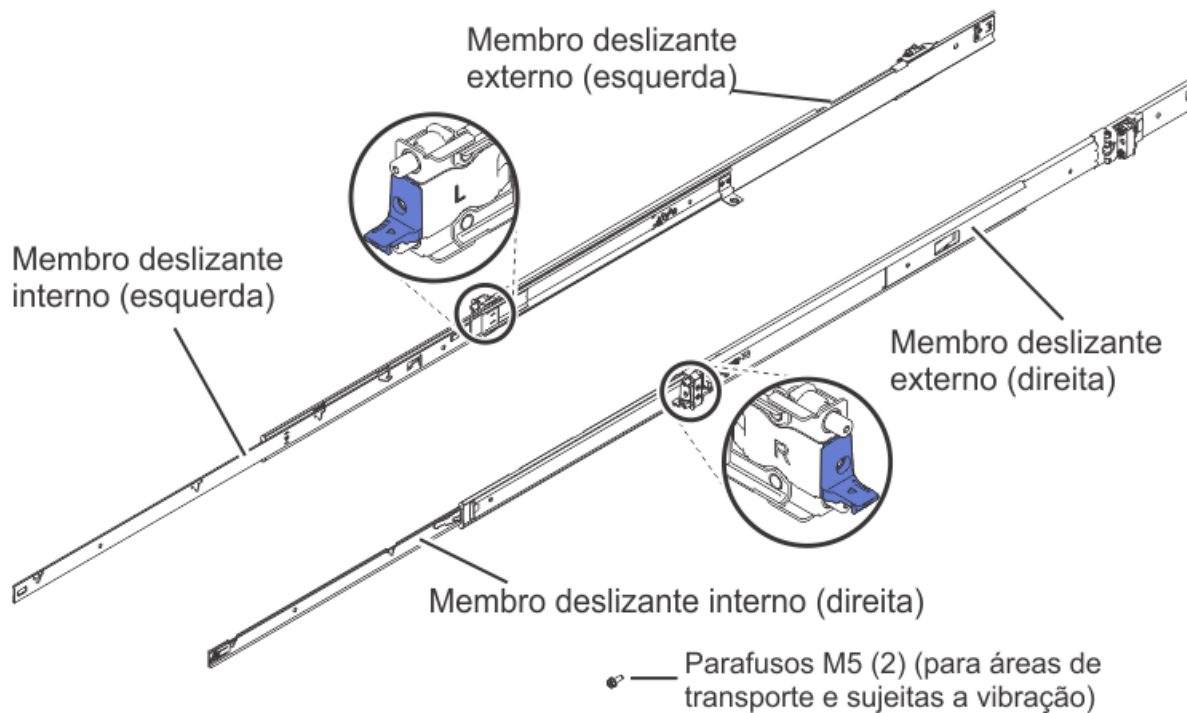


Figura 10. Conteúdo da caixa de trilhos

Nota: Você precisa da caixa de trilhos deslizantes e da caixa do suporte para organização de cabos para esta instalação.

Sobre Esta Tarefa

Para instalar um HMC 7042-CR9 em um rack, conclua as etapas a seguir:

Procedimento

1. Selecione um espaço disponível (dependendo do servidor que você está instalando) no rack para instalar o servidor.

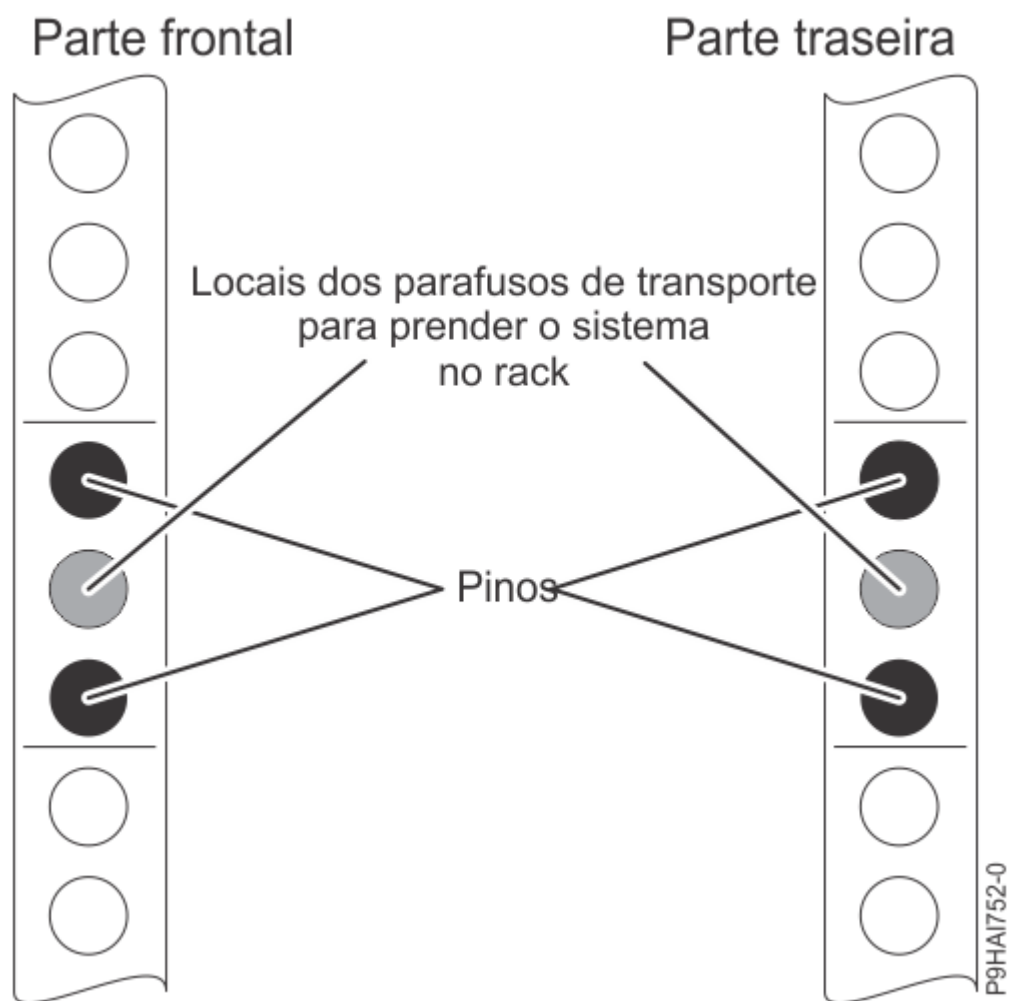


Figura 11. Identificando um espaço do rack

Nota: Você precisa de uma unidade (1 U) de espaço e os trilhos deslizantes são instalados na unidade (U) inferior dessa unidade de espaço.

2. Estenda o membro deslizante externo por toda a parte traseira até ouvir um clique audível. O suporte de montagem do rack traseiro agora é girado para a posição destravada.

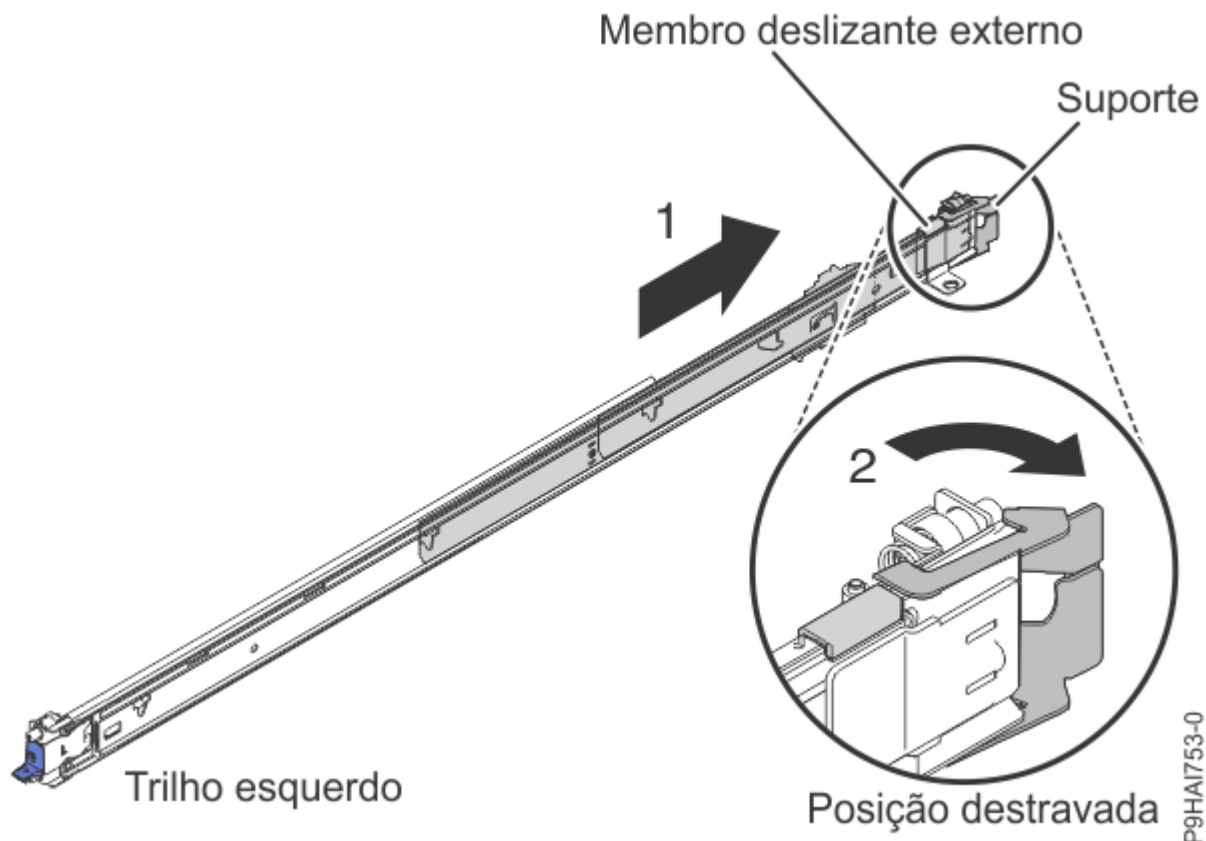


Figura 12. Trilho deslizante e o membro deslizante externo

Nota: Cada trilho deslizante é marcado como **R (direito)** ou **L (esquerdo)** em suas extremidades.

3. Alinhe a extremidade traseira do membro deslizante externo com relação aos furos na parte traseira do rack. Alinhe os pinos e empurre a corrediça para dentro de modo que os pinos entrem nos furos. Os dois pinos deslizantes passam pelos orifícios superior e inferior do frange EIA. Empurre o trilho na direção da parte traseira do rack até que o suporte de montagem traseiro do rack trave no lugar.

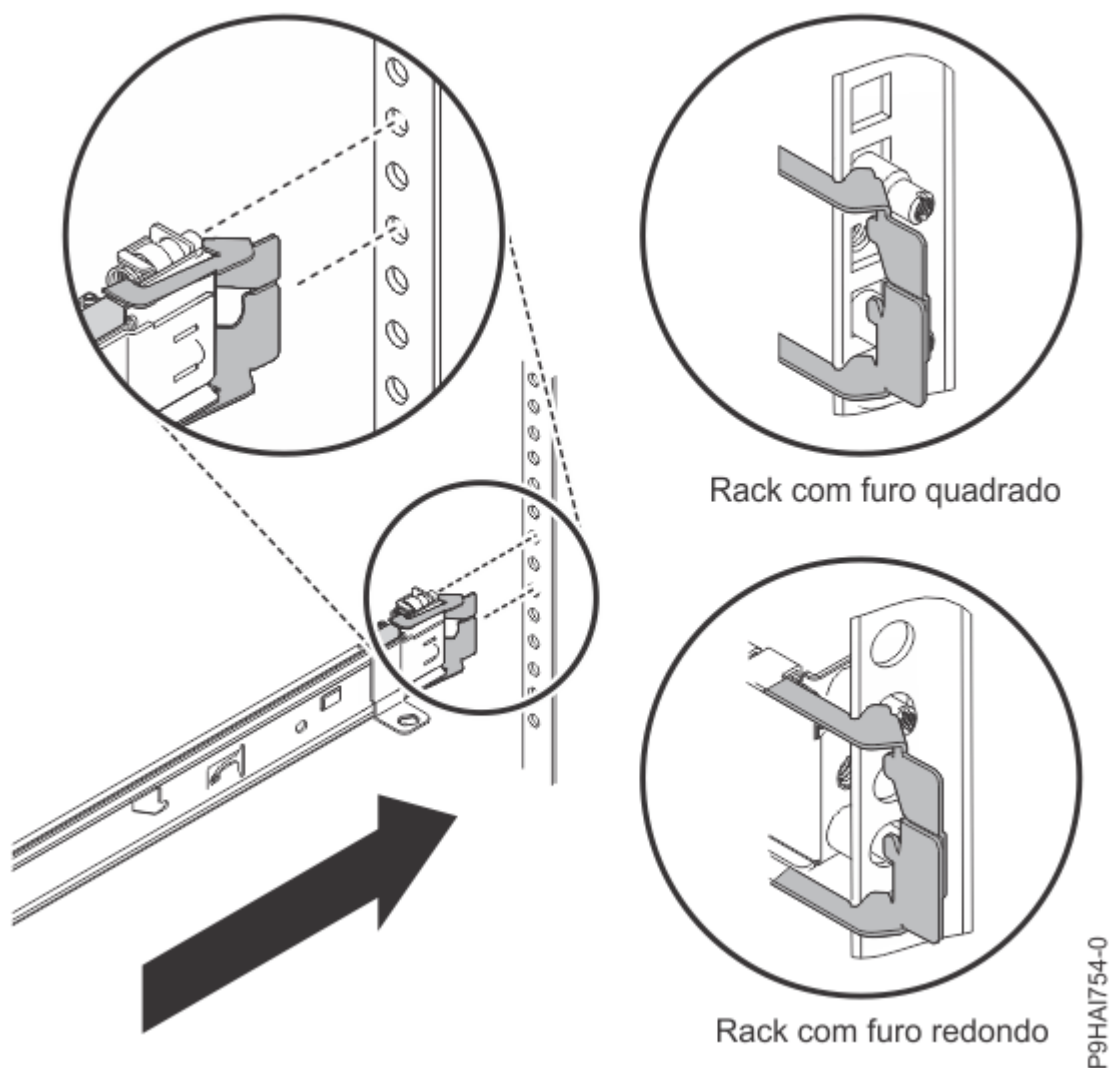


Figura 13. Alinhar os Pinos com os Orifícios na Parte Traseira do Rack

4. Gire a trava frontal para a posição aberta e alinhe a extremidade frontal do membro de slide externo com relação aos furos na frente do rack. Alinhe os pinos com os furos nos flanges EIA e puxe o slide para a frente para que os pinos se projetem através dos furos. Bloqueie a frente do slide permitindo que a trava frontal gire para a posição fechada. Repita as etapas 2- 4 para o outro membro deslizante externo.

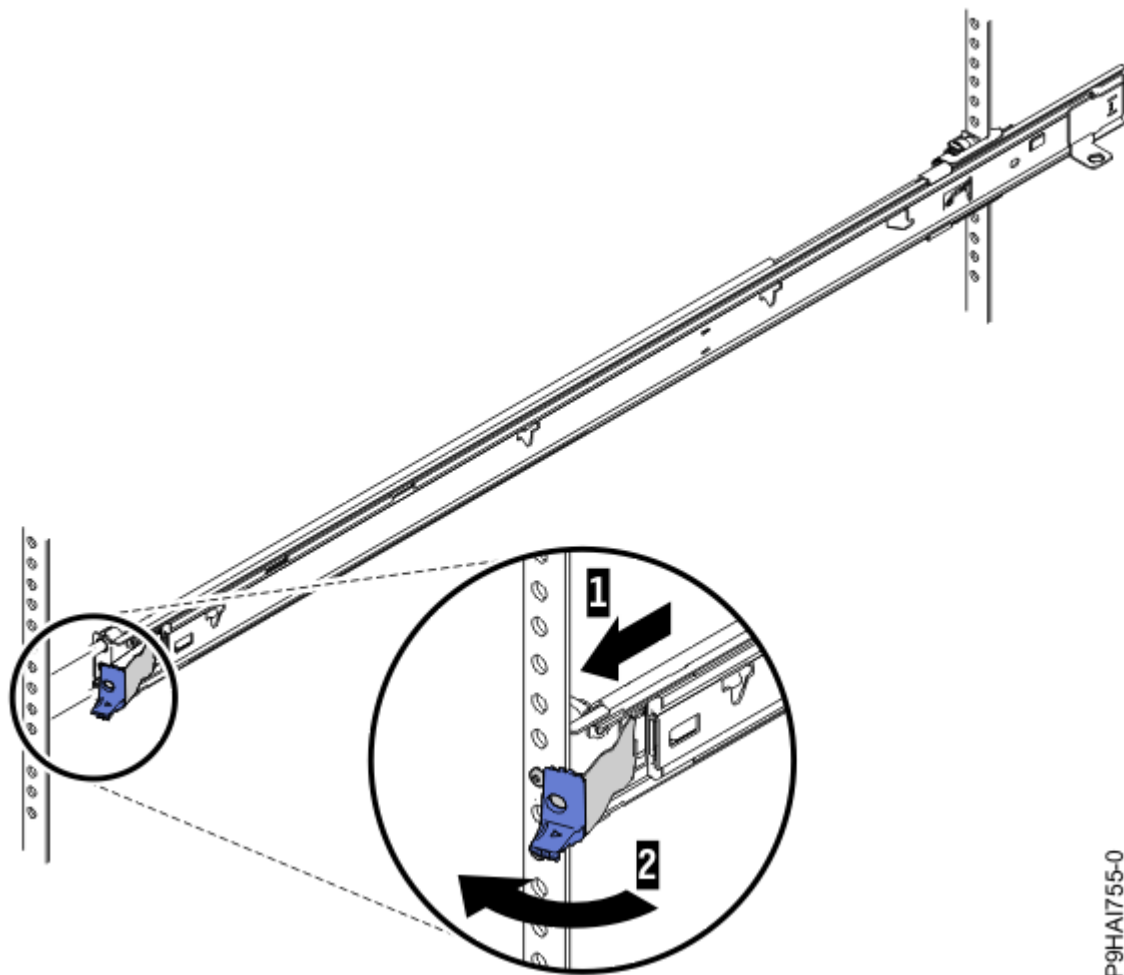


Figura 14. Trava do trilho deslizante frontal

5. Pressione as travas de liberação **(1)**. Quando você mover o gabinete do rack ou se instalar o gabinete do rack em uma área sujeita a vibração, aperte os parafusos M5 fixos **(2)** na parte da frente do servidor.

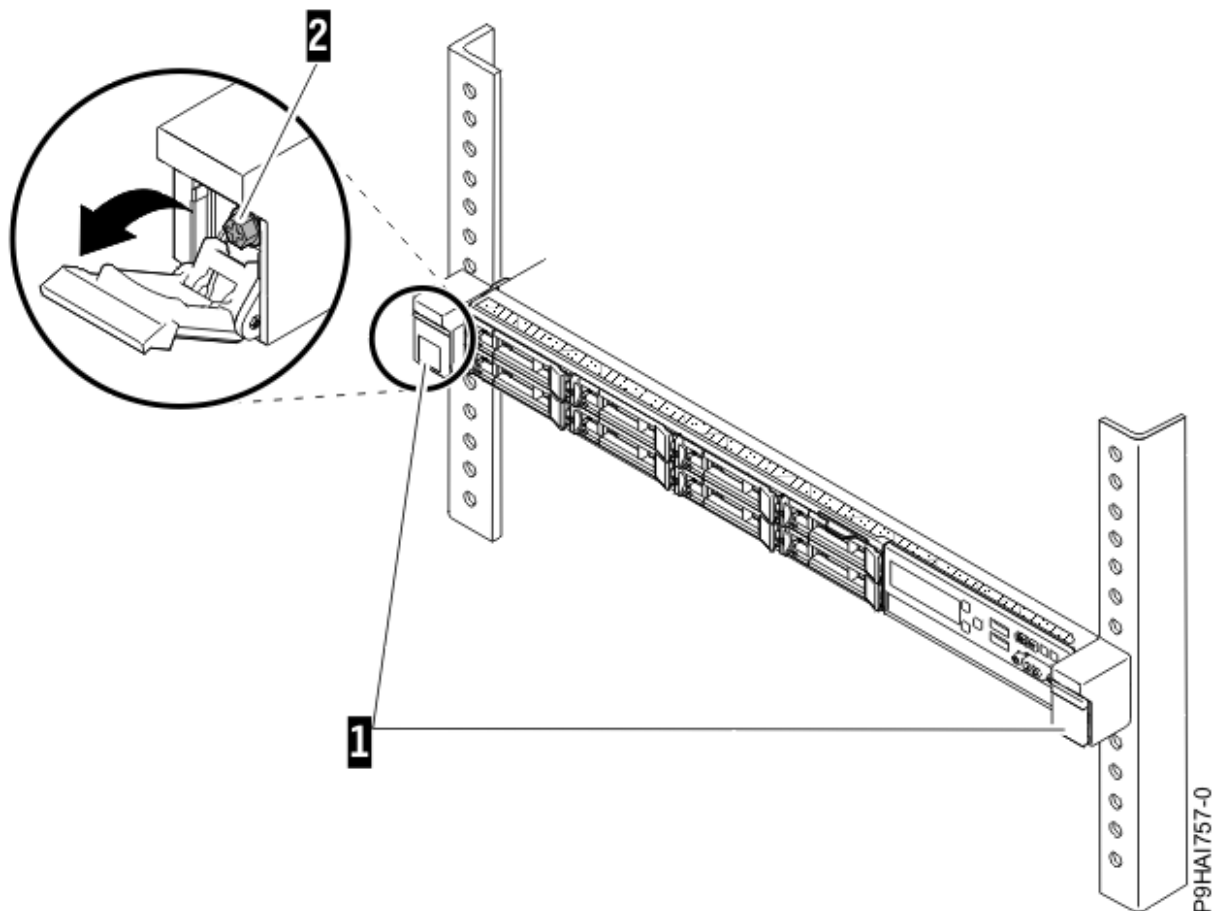


Figura 15. Trilho Frontal e Pinos do Rack

6. Puxe os trilhos deslizantes para frente **(1)** até que eles façam um clique duas vezes no lugar. Erga cuidadosamente o servidor e o incline na posição sobre os trilhos deslizantes, de modo que as cabeças dos pregos traseiros **(2)** no servidor se alinhem com os slots traseiros nos trilhos deslizantes. Baixe o servidor até que as cabeças dos pregos traseiros deslizem para os dois slots traseiros e, em seguida, abaixe lentamente a frente do servidor **(3)** até que as outras cabeças dos pregos entrem nos outros slots dos trilhos deslizantes. Assegure-se de que as travas frontais cubram a cabeça do prego frontal, de modo que o sistema fique preso nos trilhos deslizantes.

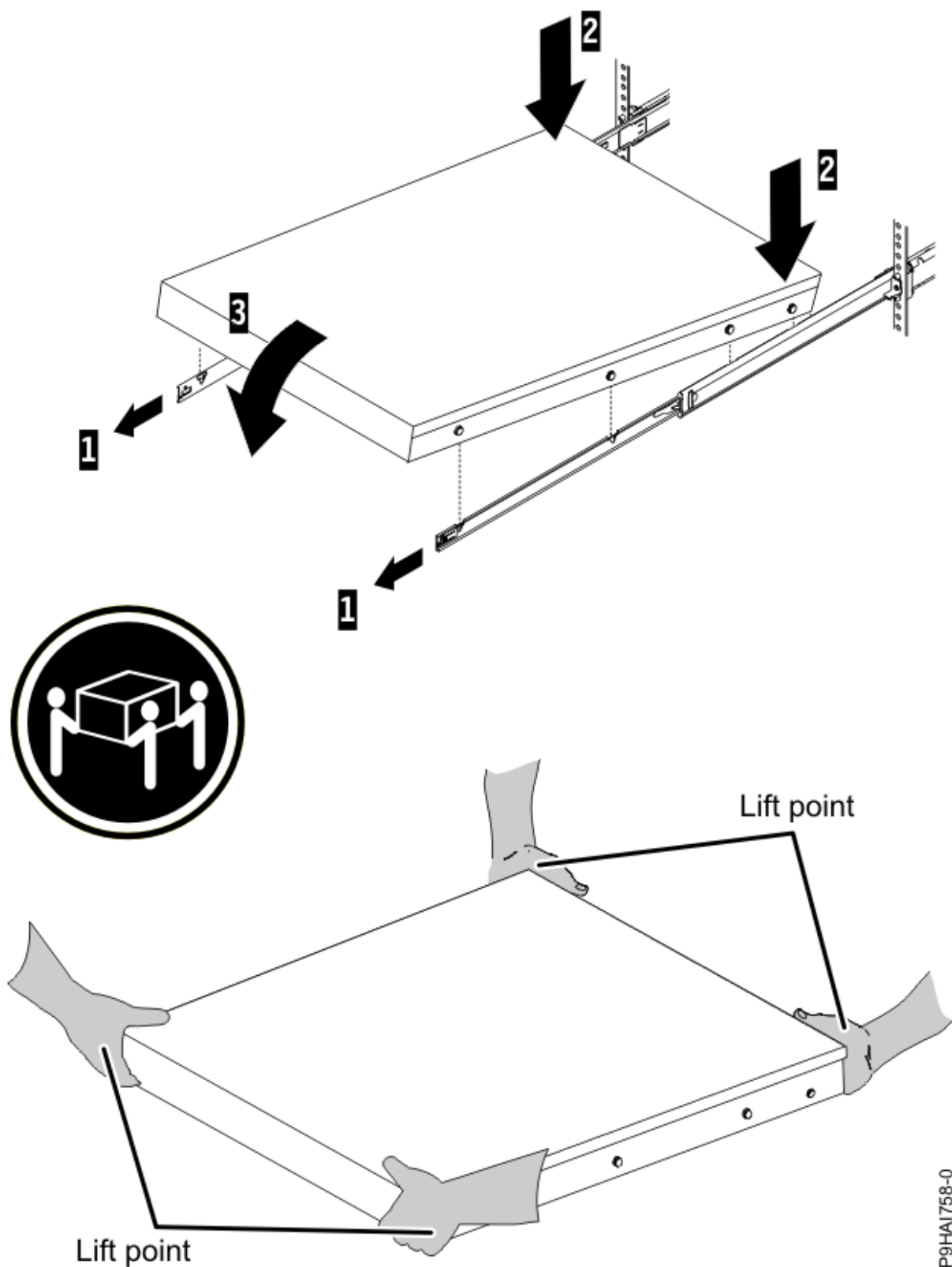


Figura 16. Deslize os trilhos estendidos, as cabeças dos pregos do servidor alinhadas com os slots no trilho e pontos de levantamento

Nota: Use práticas seguras ao erguer. Se você estiver instalando um servidor de 1 U, assegure-se de que tenha duas pessoas para erguer o servidor. Suas mãos devem estar posicionadas conforme ilustrado em [Figura 16 na página 33](#).

7. Erga as alavancas de travamento **(1)** nos trilhos deslizantes e empurre completamente o servidor **(2)** em direção ao rack até que ele se encaixe no lugar.

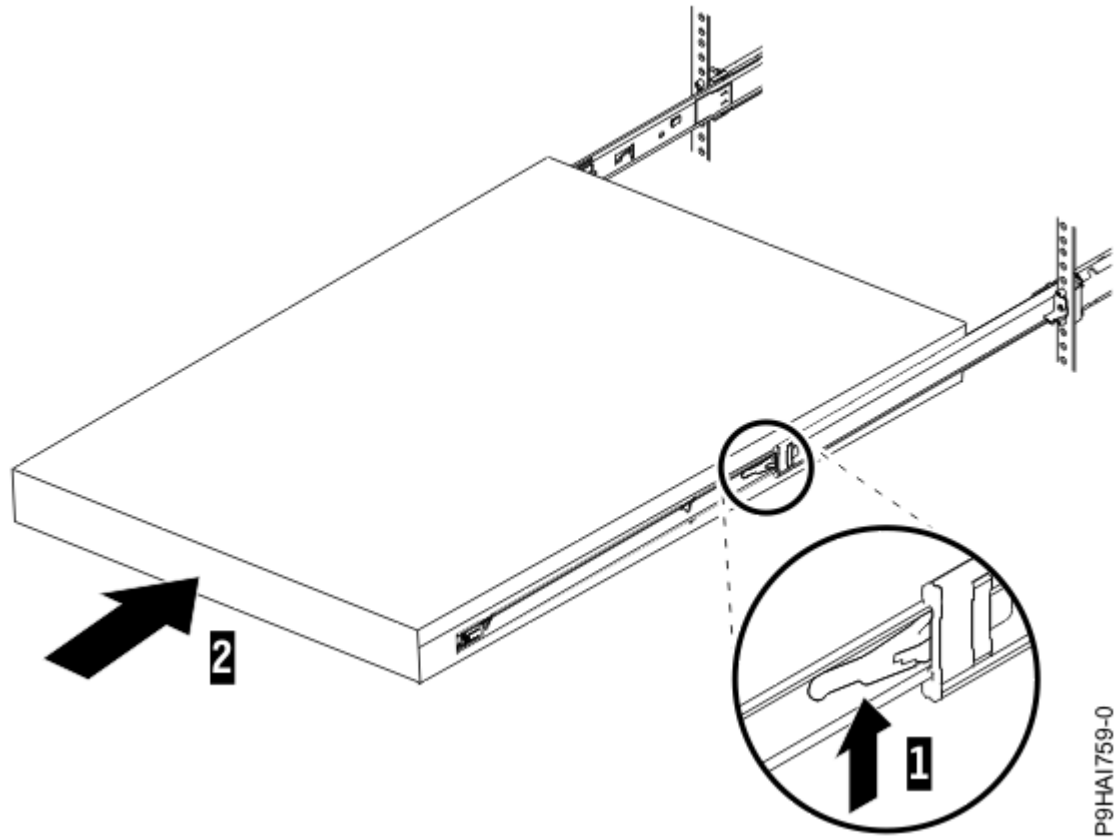


Figura 17. Travas de Liberação e Servidor

8. O suporte para organização de cabos pode ser instalado em qualquer um dos lados do servidor. A [Figura 18 na página 35](#) mostra o suporte sendo instalado no lado esquerdo. É melhor instalar o suporte para organização de cabos para que ele se articule no lado oposto ao das fontes de alimentação a fim de dar acesso a elas. Para instalar o suporte para organização de cabos no lado direito, siga as instruções e instale o hardware no lado oposto. Coloque o pino **(1)** no slot horizontal na parte traseira dos trilhos deslizantes. Em seguida, gire a outra extremidade da barra **(2)** na direção do rack.

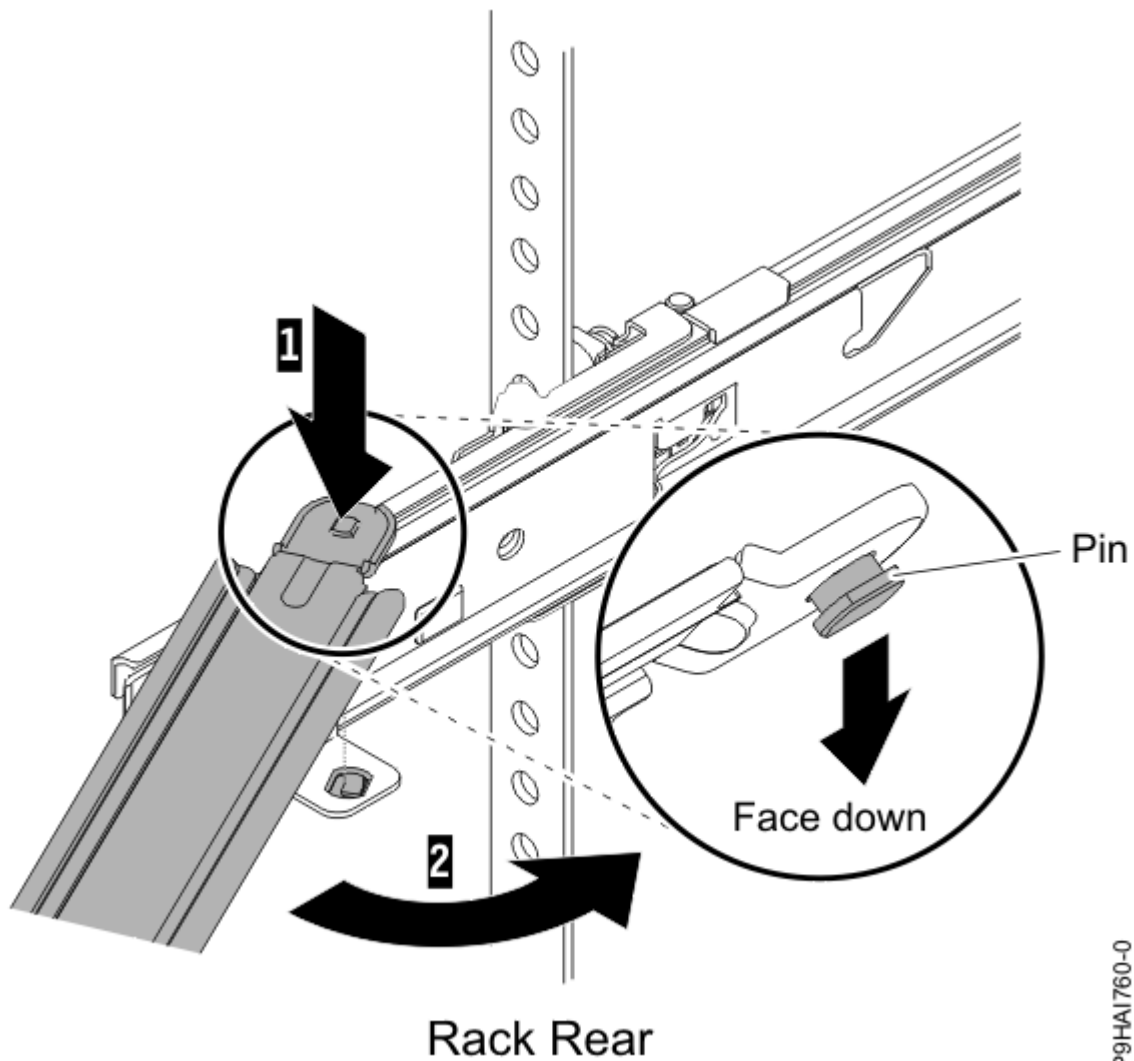


Figura 18. Conexão do Suporte para Organização

Nota: A barra do suporte para organização de cabos deve ficar em cima da guia deslizante para funcionar corretamente.

9. Instale a alça de parada para organização de cabos (com a letra maiúscula **O**) na extremidade não conectada do braço de suporte. Assegure-se de que o braço de suporte esteja instalado com segurança.

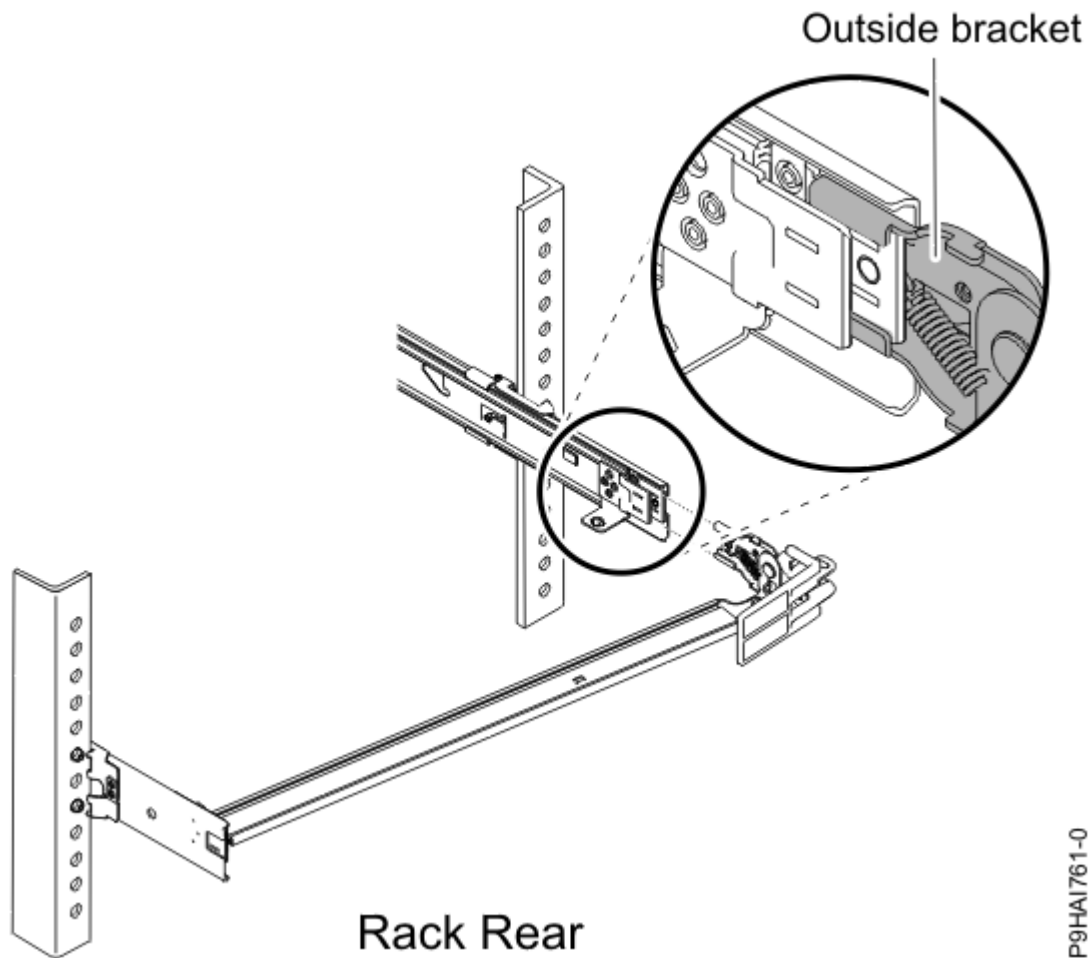
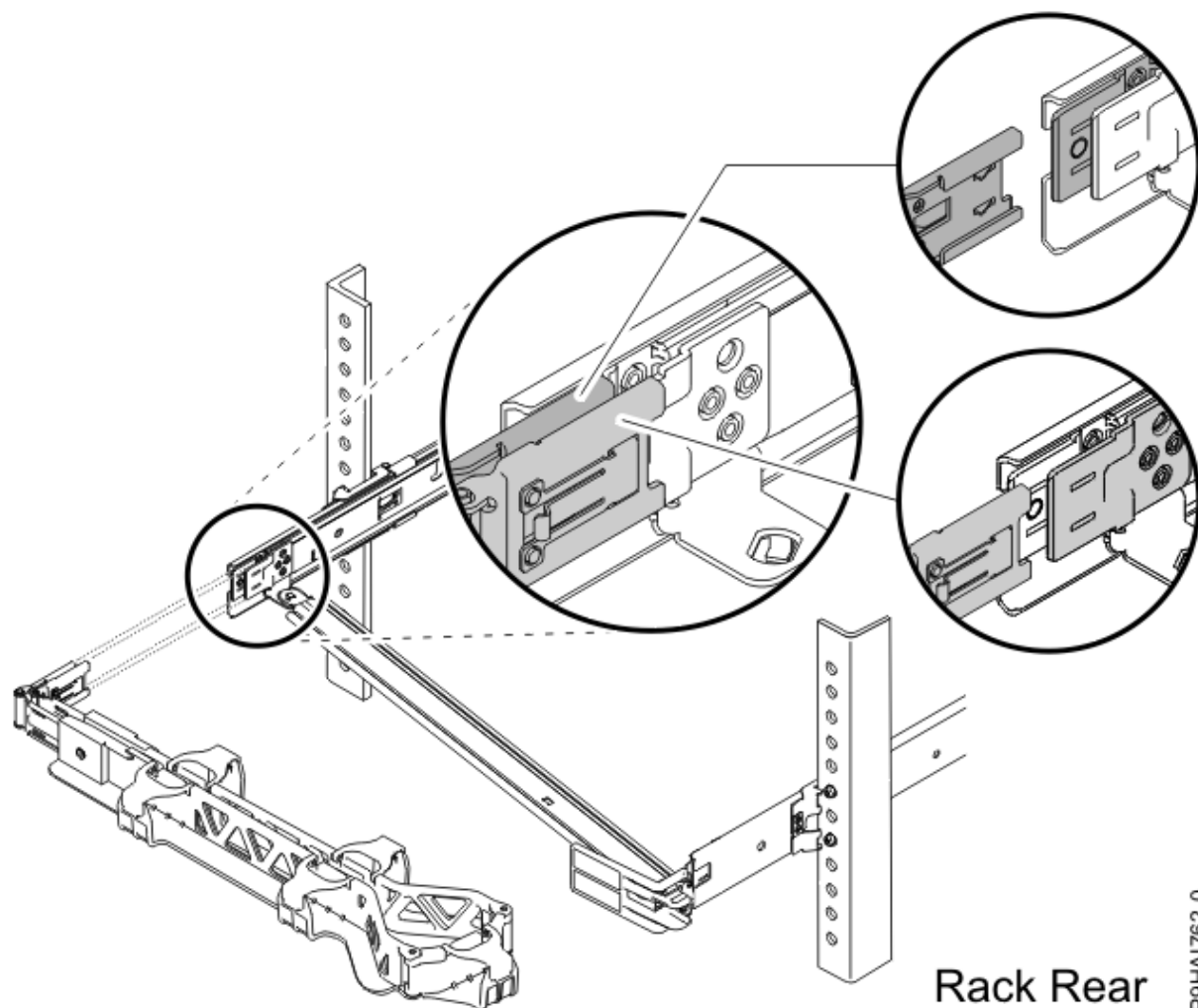


Figura 19. Conectando a alça de parada ao trilho deslizante

Nota: A letra maiúscula **O** está marcada nos pinos do suporte para organização de cabos para identificar os pinos externos.

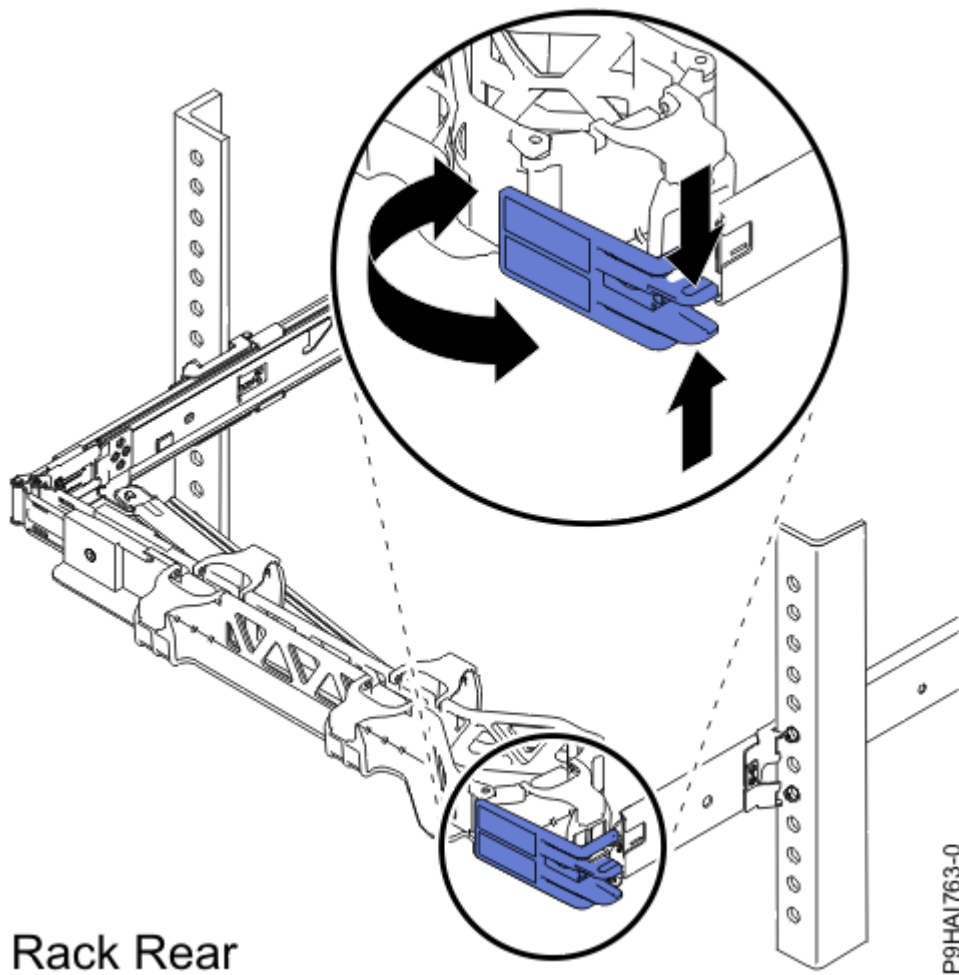
10. Posicione o suporte para organização de cabos no braço de suporte. Deslize as guias do suporte para organização de cabos na direção dos slots internos e externos do trilho deslizante. Empurre as guias até elas se encaixem.



P9HAI762-0

Figura 20. Conexão do Suporte para Organização de Cabos

11. Para facilitar girar o suporte para organização de cabos para dentro e para fora do braço de suporte para organização de cabos, é possível abrir a alça de parada empurrando as guias para cima e para baixo do suporte.



Rack Rear

Figura 21. Alça de parada do suporte para organização de cabos

12. Conecte os cabos de energia e outros cabos na parte traseira do servidor (incluindo cabos do teclado, do monitor e do mouse, se necessário). Roteie os cabos e os cabos de energia no suporte para organização de cabos e prenda-os com abraçadeiras ou com fitas de velcro.

Nota: O local das fitas de cabos pode ser ligeiramente diferente em sistemas diferentes. Use as fitas de cabos fornecidas na parte traseira do sistema para prender os cabos e evitar que eles cedam.

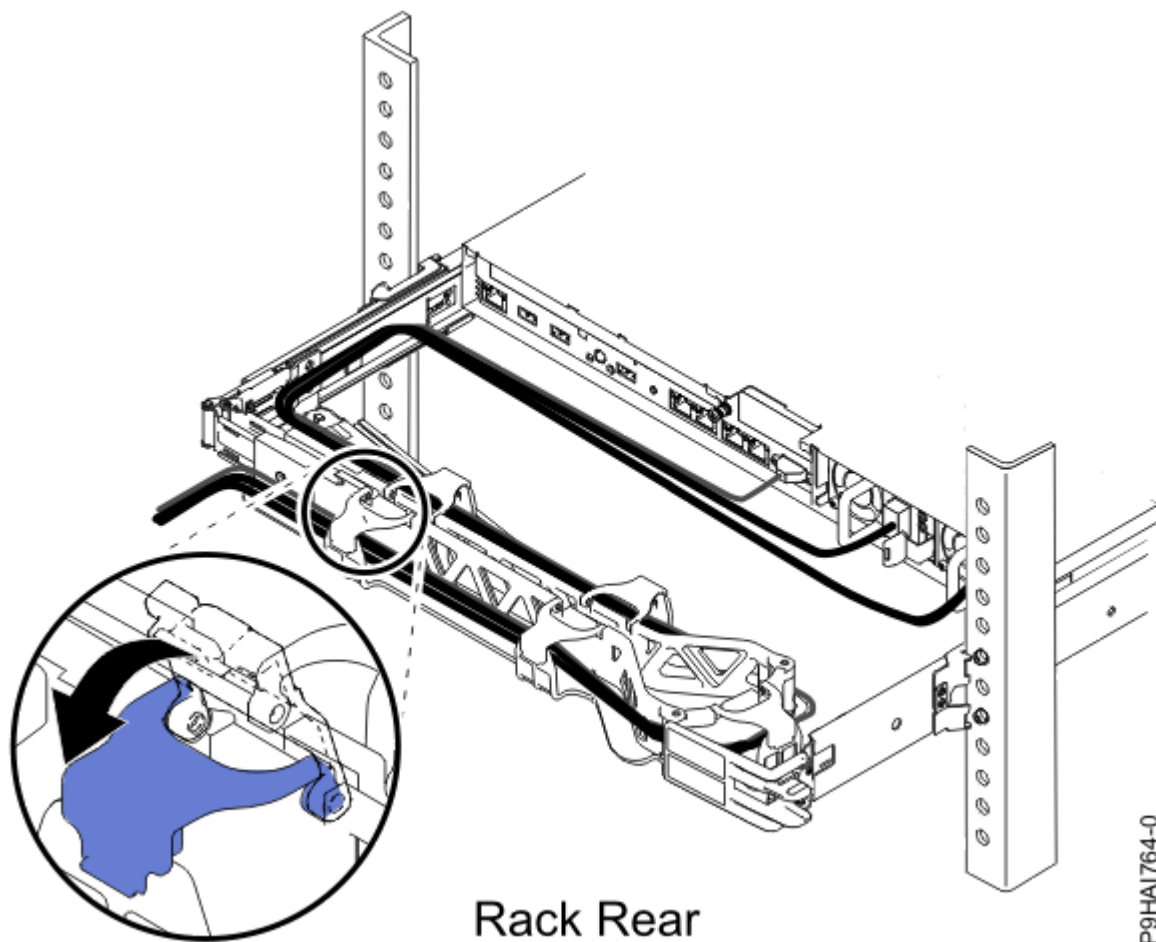


Figura 22. Conectando o cabo de energia e roteando o cabo

13. Os cabos devem ser presos com a tira para cabo para a movimentação adequada do suporte para organização de cabos.

Nota: Assegure-se de que os cabos não cedam abaixo do espaço de U, para que não toquem nos sistemas inferiores. Permita folga em todos os cabos para evitar tensão nos cabos, conforme o suporte para organização de cabos se move.

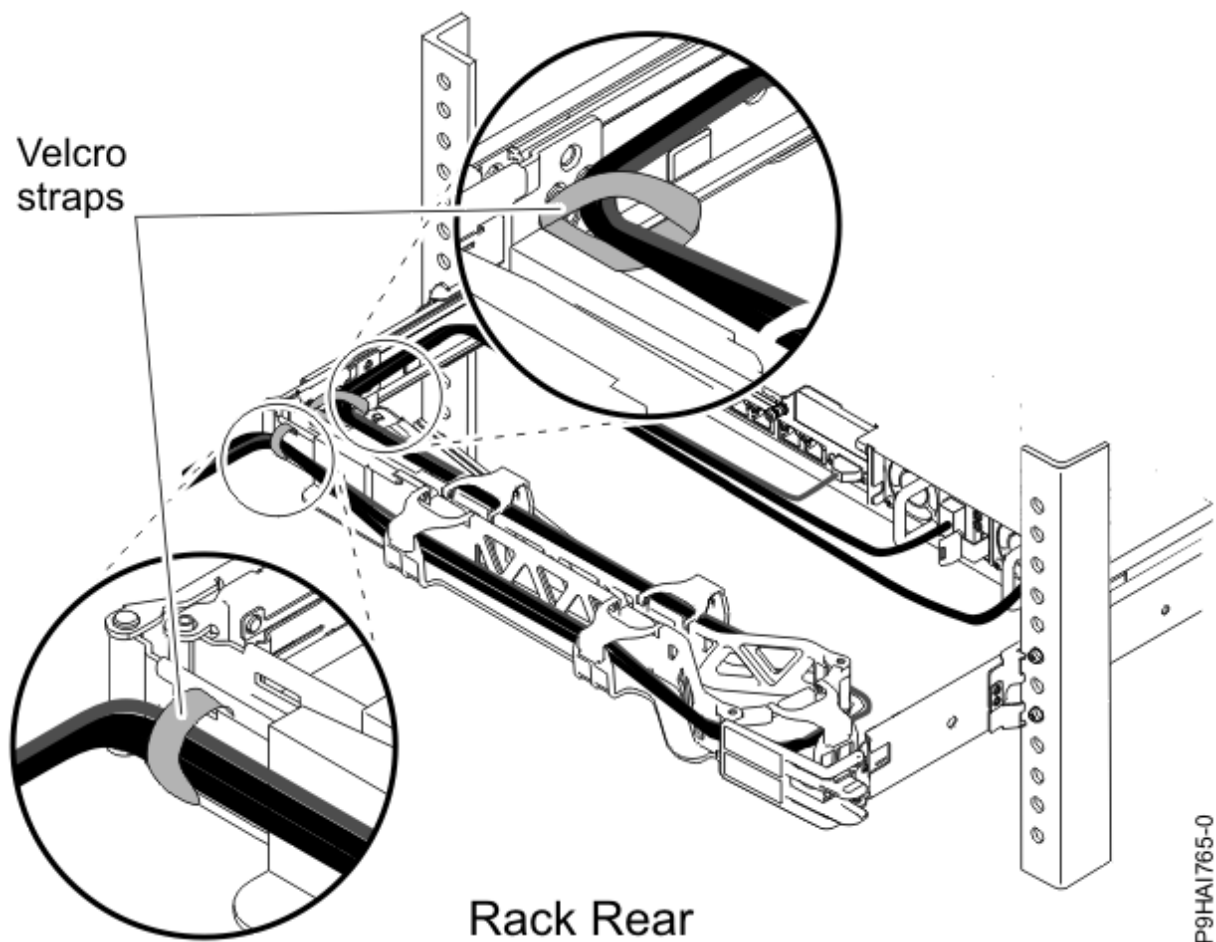


Figura 23. Fita de velcro

14. Se você estiver enviando o rack com o sistema instalado ou estiver em uma área sujeita à vibração, insira os parafusos M5 na parte traseira dos slides. Use uma abraçadeira para prender a extremidade solta do suporte para organização de cabos no rack, se necessário.

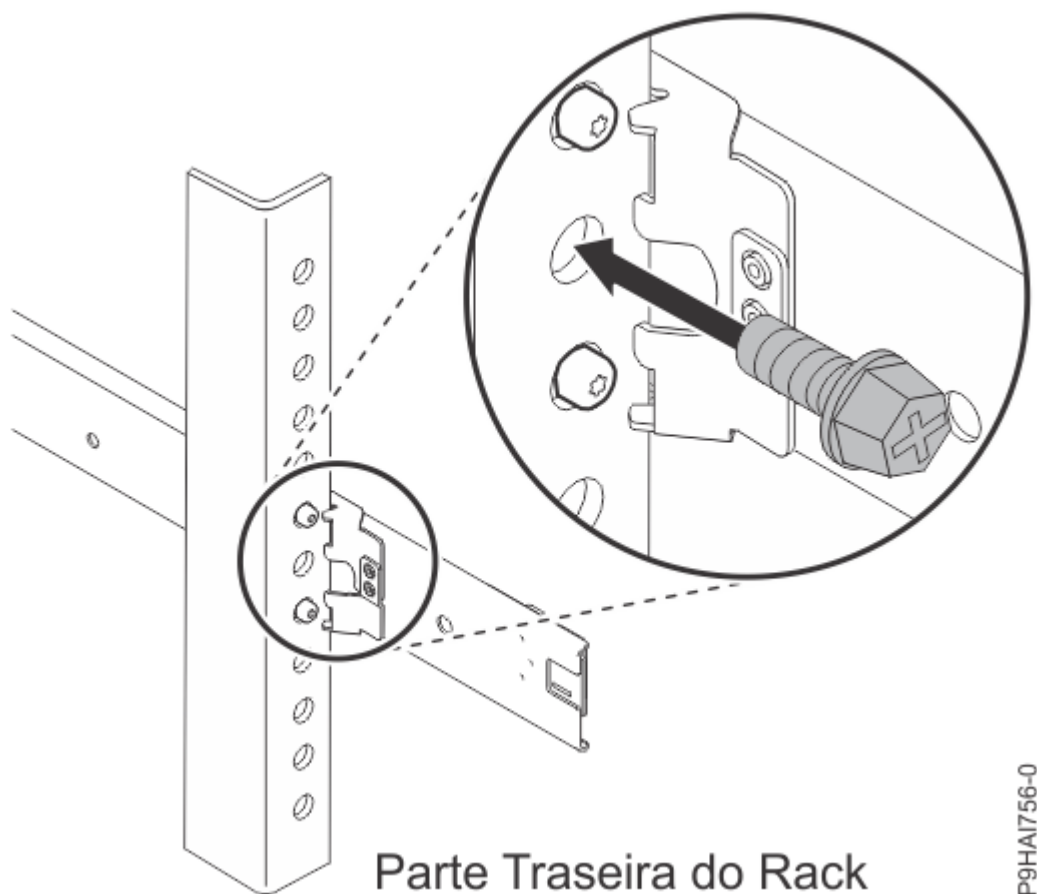


Figura 24. Protegendo o servidor para remessa

Instalando o dispositivo virtual HMC

Aprenda a instalar o dispositivo virtual Hardware Management Console (HMC).

O dispositivo virtual HMC pode ser instalado em sua infraestrutura virtualizada existente x86 ou POWER. O dispositivo virtual HMC suporta os hypervisors de virtualização x86 a seguir:

- Máquina virtual baseada em Kernel (KVM)
- Xen
- VMware

O dispositivo virtual HMC suporta os hypervisors de virtualização do POWER a seguir:

- PowerVM

Requisitos mínimos para executar o dispositivo virtual HMC:

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

Notas:

- O processador nos sistemas que hospedam o dispositivo virtual HMC deve ser um processador ativado por virtualização de hardware AMD-V ou Intel VT-x.
- Os DVDs do dispositivo virtual HMC que você recebe não são inicializáveis. Deve-se montar a mídia primeiro e, em seguida, copiar o arquivo .tgz a partir da mídia. O método para montar o DVD poderá variar dependendo do sistema operacional que você usar.

- A sintaxe de comando que é usada nos exemplos a seguir poderá variar dependendo do sistema operacional que você usar.
- O hypervisor de virtualização do PowerVM requer 160 GB de espaço em disco. No entanto, 500 GB de memória são recomendados.
- O processador PowerVM requer pelo menos 1,0 unidade de processamento e quatro processadores virtuais compartilhados no modo de compartilhamento limitado. Não é recomendado usar processadores dedicados. O processador PowerVM também requer 16 GB de memória.

Informações relacionadas

[Imagens de instalação de rede e instruções de instalação do HMC V8](#)

Instalando o dispositivo virtual HMC em x86

Saiba como instalar o dispositivo virtual Hardware Management Console (HMC) em um ambiente x86.

Instalando o dispositivo virtual HMC usando o hypervisor KVM

Aprenda a instalar o dispositivo virtual Hardware Management Console (HMC) usando o hypervisor da máquina virtual baseada em kernel (KVM).

Para instalar o dispositivo virtual HMC no KVM, conclua as etapas a seguir:

Nota: O seguinte usa a interface da linha de comandos e requer autoridade de usuário raiz. A sintaxe de comando pode variar dependendo do sistema operacional.

1. Verifique se pacotes de virtualização são instalados em sistemas com o Red Hat Enterprise Linux (RHEL) versão 7.0 ou mais recente.
2. Faça download do arquivo `<KVM vHMC installation filename>.tar.gz` para o sistema host.
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 imagens do disco virtual, execute o comando a seguir: `tar -zxvf <KVM vHMC installation filename>.tgz`

Nota: Nesse comando, especifique o caminho completo do seu arquivo .tar do dispositivo virtual HMC.

6. Um arquivo **domain.xml** é fornecido no arquivo `<KVM vHMC installation filename>.tar.gz` file. Conclua as etapas a seguir:
 - a. Edite o arquivo **domain.xml** e verifique se o caminho para seus discos está correto. Esse arquivo contém a sequência **DISK_PATH**.
 - b. Certifique-se de que `virtio` é usado para o valor do barramento do seu dispositivo de disco.
 - c. É possível escolher ter um nome diferente para sua VM. O nome padrão no arquivo **domain.xml** é **vHMC**.
 - d. Verifique se o endereço do Controle de Acesso à Mídia (MAC) está configurado no arquivo **domain.xml**. O arquivo contém a sequência **MAC_ADDRESS**.
- Nota:** Remova essa linha se desejar que um endereço MAC seja gerado automaticamente para você.
- e. Verifique se suas pontes correspondem aos seus dispositivos Ethernet. O arquivo **domain.xml** padrão especifica uma Ethernet.
 - f. Se você estiver usando o Mecanismo de ativação, substitua **AEDISK** pelo nome da imagem do disco virtual do Mecanismo de ativação. Caso contrário, remova o elemento de disco.

7. Para definir a VM, execute o comando a seguir: `virsh define <domain>.xml`.
8. Para verificar se o HMC virtual foi incluído na lista de VMs definidas, execute o comando a seguir: `virsh list --all`.
9. Para iniciar a VM, execute o seguinte comando: `virsh start vHMC`.

10. Para determinar o número de exibição do Virtual Network Computing (VNC) do seu console, execute o seguinte comando: `virsh vncdisplay vHMC`.
 11. Para conectar ao seu console com um visualizador VNC, execute o seguinte comando: `vncviewer HOSTNAME:ID` (em que ID é o número de exibição, por exemplo 0).
- Nota:** Se requerer acesso remoto, deve-se descartar ou configurar seu firewall para permitir acesso à porta 5900.

Instalando o dispositivo virtual HMC usando o hypervisor Xen

Saiba como instalar o dispositivo virtual Hardware Management Console (HMC) usando o hypervisor Xen. O dispositivo virtual HMC suporta o Xen versão 4.2 ou mais recente.

Para instalar o dispositivo virtual HMC usando o hypervisor Xen, conclua as etapas a seguir:

Nota: As etapas a seguir usam a interface da linha de comandos e requerem autoridade de usuário raiz. A sintaxe de comando pode variar dependendo do sistema operacional.

1. Verifique se pacotes de virtualizações são instalados em sistemas com Red Hat Enterprise Linux (RHEL) versão 6.4 ou mais recente.
2. Faça download do arquivo `<XEN vHMC installation filename>.tar.gz` para o sistema host.
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 do disco virtual, execute o comando a seguir: `tar -zxvf <XEN vHMC installation filename>.tgz`

Nota: Nesse comando, especifique o caminho completo do seu arquivo .tar do dispositivo virtual HMC.

6. Um arquivo **vhmc.cfg** é fornecido no arquivo `<nome do arquivo de instalação do XEN vHMC>.tar.gz`. Abra o arquivo **vhmc.cfg** em um editor de texto e edite os valores a seguir:
 - a. Mude o nome do HMC virtual (opcional): edite o arquivo **vhmc.cfg** e verifique se o caminho para os seus discos está correto. Esse arquivo contém a sequência **DISK_PATH**.
 - b. Substitua **DISK_PATH** pelo caminho para `disk1.img`:

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

- c. Substitua **adaptador Ethernet** e inclua o endereço de Controle de Acesso à Mídia (opcional):

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

Endereço de Controle de Acesso à Mídia opcional:

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

Nota: Quando o HMC virtual é reinicializado, o hypervisor Xen automaticamente gera novamente um endereço de Controle de Acesso à Mídia. Incluir o endereço de Controle de Acesso à Mídia opcional resolve esse problema.

- d. Substitua **FLOPPYPATH** (se você estiver usando o Mecanismo de ativação):

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

7. Para criar e iniciar a VM, execute o comando a seguir: `xl create vHMC.cfg`.
8. Para verificar se a VM foi incluída na lista de máquinas virtuais definidas, execute o comando a seguir: `xl list`.
9. Para acessar o console local da VM, execute o comando a seguir: `vncviewer localhost 0`.

Instalando o dispositivo virtual HMC usando o VMware ESXi

Aprenda a instalar o dispositivo virtual Hardware Management Console (HMC) usando o VMware ESXi.

É possível instalar o dispositivo virtual HMC no VMware ESXi usando a interface gráfica com o usuário no cliente vSphere para implementar o modelo Open Virtualization Format (OVF).

Nota: É possível instalar o dispositivo virtual HMC no VMware ESXi versão 6.0 ou mais recente.

Para instalar o dispositivo virtual HMC em um VMware ESXi usando o cliente vSphere, conclua as etapas a seguir:

Nota: A sintaxe de comando pode variar dependendo do sistema operacional.

1. Obtenha o archive Tar: <nome do arquivo de instalação do VMware vHMC>.tgz.
2. Use o comando `tar` para extrair o arquivo OVA do archive Tar.
3. Inicie o cliente vSphere e efetue login no host ESXi.
4. A partir do menu **Arquivo**, selecione **Implementar modelo OVF**.
5. Clique em **Procurar** e selecione o arquivo OVA.
6. Clique em **Next**.
7. Após a implementação ser concluída, clique em **Fechar** e selecione o ícone dispositivo virtual HMC para ligar o dispositivo virtual HMC.

Instalando o dispositivo virtual HMC no POWER

Aprenda como instalar o dispositivo virtual Hardware Management Console (HMC) em um ambiente POWER virtualizado.

Instalando o dispositivo virtual HMC no PowerVM (partição lógica)

Saiba como instalar o dispositivo virtual Hardware Management Console (HMC) em um ambiente do PowerVM.

O dispositivo virtual HMC suporta os servidores POWER9 no nível de firmware FW910 ou mais recente. Para obter mais informações, consulte Distribuições Linux suportadas para POWER8 e POWER9 Linux em sistemas Power (<https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm>).

Notes:

1. Não é possível gerenciar o servidor que hospeda o dispositivo virtual HMC.
2. Não é possível gerenciar o servidor que hospeda outro dispositivo virtual HMC que está gerenciando o servidor que hospeda esse dispositivo virtual HMC.

Por exemplo, dispositivo virtual HMC A está em execução no servidor A e dispositivo virtual HMC B está em execução no servidor B. dispositivo virtual HMC A não pode gerenciar o servidor B e dispositivo virtual HMC B não pode gerenciar o servidor A ao mesmo tempo. Um dos dispositivo virtual HMC pode gerenciar o outro servidor, mas ambos os dispositivo virtual HMC não podem gerenciar um ao outro ao mesmo tempo.

Criar imagem de instalação automatizada do HMC (opcional)

É possível criar uma imagem de instalação automatizada do HMC que instale automaticamente o dispositivo virtual HMC sem solicitar pelo assistente de **Instalação do HMC**.

Nota: O dispositivo virtual HMC no PowerVM não fornece suporte do adaptador gráfico para adaptadores que estão designados à partição. É possível usar um navegador da web suportado para se conectar ao HMC para obter o suporte da interface com o usuário.

Para criar uma imagem de instalação automatizada do HMC, conclua as etapas a seguir:

1. Crie dois diretórios executando os comandos a seguir: `mkdir -p oldiso` e `mkdir -p newiso`.
2. Monte a imagem de instalação do HMC no diretório **oldiso** executando o comando a seguir: `sudo mount -o loop <image_path> oldiso`.

3. Copie os conteúdos do diretório **oldiso** no diretório **newiso** executando o comando a seguir: `cp -r oldiso/* newiso`.
4. Edite o arquivo Grub para a instalação automática executando o comando a seguir: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Torne o arquivo Grub somente leitura executando o comando a seguir: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Crie um novo ISO de instalação do HMC executando o comando a seguir: `mkisofs -o <new_iso_name> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso (em que ISO label deve ser HMC-<hmc version release number>, por exemplo HMC-8.0.870.0)`.

Nota: Para obter mais informações sobre como configurar o Mecanismo de ativação e o arquivo de configuração, veja [“Usando o Mecanismo de ativação para o dispositivo virtual HMC”](#) na página 48.

Configuração do volume lógico

Para configurar o volume lógico, conclua as etapas a seguir:

1. Selecione um sistema gerenciado.
2. No pod do menu, selecione **Ações do sistema > PowerVM > Armazenamento virtual**.
3. Selecione **Gerenciar VIOS do sistema > Ação > Gerenciar armazenamento virtual**.
4. Selecione a guia **Discos virtuais**.
5. Clique em **Criar disco virtual** e insira as informações a seguir:
 - **Nome do disco virtual:** o nome do disco virtual.
 - **Nome do conjunto de armazenamentos:** o nome do conjunto de armazenamentos.
 - **Tamanho do disco virtual:** o tamanho do disco virtual.
 - **Partição designada:** o nome da partição lógica.

Nota: Um mínimo de 160 GB de espaço em disco é necessário (500 GB de espaço em disco é recomendado).

Configuração de mídia de instalação - criar biblioteca de mídia

Para criar uma biblioteca de mídia, conclua as etapas a seguir:

1. Selecione um sistema gerenciado.
2. No pod do menu, selecione **Ações do sistema > PowerVM > Armazenamento virtual**.
3. Selecione **Gerenciar VIOS do sistema > Ação > Gerenciar armazenamento virtual**.
4. Selecione a guia **Dispositivos Óticos**.
5. Clique em **Criar biblioteca** e insira as informações a seguir:
 - **Conjunto de armazenamentos:** o nome do conjunto de armazenamentos.
 - **Tamanho da biblioteca de mídia:** o tamanho da biblioteca de mídia.
6. Clicar em **OK**.

Configuração de mídia de instalação - fazer upload de mídia para o VIOS

Para fazer upload de mídia para o Virtual I/O Server (VIOS), conclua as etapas a seguir:

1. Efetue login no VIOS.
2. No modo raiz do VIOS, execute o comando a seguir: `oem_setup_env`.
3. Para permitir conexão NFS, execute o comando a seguir: `nfso -o nfs_use_reserved_ports=1`.

4. Para montar o NFS na pasta do VIOS local, execute o comando a seguir: `mount <server_ip>:/ Mountpoint <local_folder>`.
5. Para verificar se a montagem NFS inclui seu ISO de instalação do HMC e a imagem de configuração do Mecanismo de ativação (opcional), execute o comando a seguir: `ls`.

Configuração de mídia de instalação - vincular mídia à biblioteca de mídia

Para vincular a mídia à biblioteca de mídia, conclua as etapas a seguir:

1. Navegue de volta para **Gerenciar VIOS do sistema > Ação > Gerenciar armazenamento virtual** e selecione a guia **Dispositivos óticos**.
2. Na seção **Mídia ótica virtual**, selecione **Incluir mídia** no menu **Ações**.
3. Na janela **Incluir mídia virtual**, selecione **Incluir arquivo existente do sistema de arquivos VIOS** e insira as informações a seguir:
 - **Nome da mídia:** o nome da mídia (por exemplo, HMCInstall ou AEDrive).
 - **Nome do arquivo de mídia ótica:** o nome do arquivo do arquivo ISO de instalação (por exemplo, 01234567-ppc64ie.iso).
4. Clicar em **OK**.
5. Se você criou uma imagem de configuração do Mecanismo de ativação, repita as etapas 3 - 4 para incluir a imagem de configuração do Mecanismo de ativação. Caso contrário, continue com a etapa 6.
6. Verifique se a mídia ótica foi transferida por upload para a biblioteca de mídia, verificando se o nome da mídia é mostrado na lista **Mídia ótica virtual** disponível.

Configuração de partição lógica

Para configurar a partição lógica, conclua as etapas a seguir:

1. Selecione um sistema gerenciado.
2. No pod do menu, selecione **Ações do sistema > Partições > Partições**.
3. Clique em **Criar partição** e insira as informações a seguir:
 - **Nome da partição:** o nome da partição.
 - **ID da partição:** o ID da partição.
 - **Tipo de partição:** selecione o sistema operacional (**AIX/Linux** ou **IBM i**).
4. Clicar em **OK**.
5. Aloque o número de processadores e a quantia de memória para a partição.

Nota: No mínimo, quatro processadores virtuais e 8 GB de memória são necessários.
6. No pod do menu, selecione **Ações da partição > E/S virtual > Redes virtuais**.
7. Clique em **Conectar rede virtual** e selecione a caixa de seleção **Mostrar e anexar novos adaptadores Ethernet virtuais**. Na tabela, selecione os adaptadores de rede virtuais que você deseja anexar à partição lógica.

Nota: Um máximo de quatro adaptadores de rede virtual é permitido.
8. No pod do menu, selecione **Ações da partição > E/S virtual > Armazenamento virtual**.
9. Na guia **Dispositivo ótico virtual**, clique em **Incluir dispositivo ótico virtual**.
10. Insira o **Nome do dispositivo** (por exemplo, HMCInstall ou AEDrive) e selecione o Virtual I/O Server desejado na tabela.

Nota: A instalação do AEDrive é opcional.
11. Clicar em **OK**.
12. Verifique se os dispositivos óticos virtuais que você incluiu na etapa 10 estão agora listados na tabela.

13. No menu **Ação**, clique em **Carregar**.
14. Selecione o arquivo de mídia para designar à partição lógica e clique em **OK**.
15. Verifique se os dispositivos óticos virtuais que você carregou da etapa [13](#) estão agora listados na tabela.

Iniciando o dispositivo virtual HMC

Nota: Quando instalar o dispositivo virtual HMC em uma partição usando o arquivo de imagem ISO do HMC, você não terá acesso do console gráfico local à interface com o usuário da web.

Para iniciar o dispositivo virtual HMC no PowerVM, conclua as etapas a seguir:

1. Selecione a partição gerenciada.
2. Abra uma conexão ativa com a partição lógica selecionando **Ações > Console > Abrir janela do terminal**.
3. Ative a partição lógica, selecionando **Ações > Ativar**.
4. Selecione **Ativar (normal)** e **Configuração atual**.
5. Clique em **Concluir**.
6. Alterne para a janela do terminal.
7. No menu **Inicializar**, selecione **1 = Menu SMS**.
8. No menu **Principal**, selecione **5 = Selecionar opções de inicialização**.
9. No menu **Inicialização múltipla**, selecione **1 = Selecionar dispositivo de instalação/inicialização**.
10. No menu **Selecionar tipo de dispositivo**, selecione **5 = Listar todos os dispositivos**.
11. Selecione o dispositivo HMCInstall com base na localização de dispositivo.
12. Selecione **2. Normal Mode Boot**.
13. Selecione **1. Sim** para confirmar.
14. Siga as instruções na tela do assistente de **Instalação do HMC**.

Nota: Ignore esta etapa se você usou uma imagem de instalação automatizada do HMC.

15. Após a instalação ser concluída e o sistema ser iniciado, será necessário selecionar um idioma na caixa de diálogo **seleção de idioma**.
16. Aceite o contrato de licença.

Nota: Assegure-se de que o controlador de comando esteja pronto para aceitar comandos antes de executar qualquer comando. Por exemplo, executando o comando **lshmc -V** até que ele seja bem-sucedido.

17. Efetue login como hscroot e use o comando **chhmc** para configurar a rede.

O exemplo a seguir mostra a sequência de comandos **chhmc** que podem ser usados para configurar a rede e ativar o Shell Seguro (SSH) e acesso remoto à web no 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 ser configurado.
- **hmc ip address** é o endereço IP do seu HMC.
- **hmc network mask** é a máscara de rede do seu HMC.
- **hmc hostname** é o nome do host do seu HMC.
- **hmc domain name** é o nome de domínio do seu HMC.

- **gateway ip** é o endereço IP do gateway em sua rede.
- **name server** é o endereço do servidor de nomes da sua rede.
- **domain search** é o nome dos domínios nos quais você deseja que o HMC procure.
- Para permitir o acesso em todos os endereços IP, use **-a 0.0.0.0 -nm 0** no lugar de **endereço IP**.

Nota: Quando você usar múltiplos adaptadores Ethernet virtuais, execute o comando **cat /etc/sysconfig/network-scripts/ifcfg-ethX** no dispositivo virtual HMC em cada interface. Compare o endereço de controle de acesso à mídia (MAC) com o que o HMC mostra na visualização do adaptador da rede virtual da partição. É possível clicar em **Visualizar configurações do adaptador Ethernet virtual** para obter mais informações sobre os adaptadores Ethernet virtuais. Esta etapa ajuda a determinar a interface correta a ser usada.

18. Reinicie o sistema.

Usando o Mecanismo de ativação para o dispositivo virtual HMC

Aprenda a usar o Mecanismo de ativação para o dispositivo virtual Hardware Management Console (HMC).

Mecanismo de ativação é uma estrutura que permite que vários componentes em uma máquina virtual sejam configurados durante a inicialização do sistema. Para usar o Mecanismo de ativação, é necessário definir um perfil de configuração XML para permitir que o dispositivo virtual HMC esteja em um estado pronto para gerenciar no primeiro início. Para obter mais informações sobre como configurar o perfil de configuração XML, consulte [“Definindo o perfil de configuração para o Mecanismo de Ativação”](#) na página 49. O arquivo de configuração pode ser usado para configurar as seguintes opções:

- Configurar o teclado padrão (EUA)
- Código padrão de idioma padrão (EUA)
- Desativar configuração do teclado
- Desativar configuração de exibição
- Contrato de licença e Contrato do código de máquina
- Desabilitar assistente de configuração
- Desabilitar assistente de call home
- Configure até quatro Placas da interface de rede
- Defina configurações de firewall para cada interface
- Configurar interface de rede como Servidor DHCP IPv4
- Configurar interface aberta e privada
- Configurar dispositivo de interface de gateway padrão

Nota: O número de adaptadores Ethernet que está definido no arquivo de configuração **vHMC-Conf.xml** deve estar correlacionado aos adaptadores de rede definidos no arquivo de configuração **domain.xml**, **vHMC.cfg** ou **VMWare**.

O Mecanismo de ativação requer um disco virtual que contenha uma configuração XML. É possível editar o arquivo **user_data** com um editor de texto e usar o guia de configuração XML que é mostrado no exemplo a seguir.

Para criar uma imagem de disco ISO virtual com a configuração de Mecanismo de ativação em um ambiente Linux, conclua as etapas a seguir:

1. Crie um diretório:

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

2. Copie o arquivo **user_data** editado no diretório:

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

3. Crie uma imagem de disco virtual com a configuração de Mecanismo de ativação:

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

Definindo o perfil de configuração para o Mecanismo de Ativação

Aprenda como definir o arquivo de configuração do Mecanismo de Ativação usando identificações XML.

Arquivo de Configuração

Use o exemplo a seguir do arquivo de configuração para aprender sobre as tags 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>
```

Identificações XML para o arquivo de configuração

As identificações XML são usadas no arquivo de configuração do Mecanismo de Ativação para configurar valores específicos para vários atributos. É possível configurar manualmente esses valores no arquivo de configuração do Mecanismo de Ativação. Use a tabela a seguir para ver uma descrição de cada tag e seus valores permitidos:

Tabela 9. tags XML			
Rótulos	Descrição	Valores aceitáveis	Notes
ConfigurationVersion	Elemento necessário que define a versão de configuração a ser usada.	2.0	

Tabela 9. tags XML (continuação)			
Rótulos	Descrição	Valores aceitáveis	Notes
LicenseAgreement	Elemento necessário que exibe o contrato de licença do dispositivo virtual HMC.		
AcceptLicense	Elemento necessário para aceitar o contrato de licença do dispositivo virtual HMC.	• Sim: aceita o contrato de licença do HMC. • Não: solicita ao usuário para aceitar o contrato de licença do HMC	Se um valor inválido for inserido, o Mecanismo de ativação usará a configuração padrão de Não .
Código do Idioma	Elemento necessário para definir as configurações do código de idioma.	en_US.UTF-8	Se um valor inválido for inserido, o Mecanismo de ativação usará a configuração padrão de US .
SetupWizard	Elemento necessário para ativar ou desativar o assistente de Configuração do HMC .	• Sim: exibe o assistente de Configuração do HMC. • Não: desativa a exibição do assistente de Configuração do HMC.	Se um valor inválido for inserido, o Mecanismo de ativação usará a configuração padrão de Sim .
SetupCallHomeWizard	Elemento necessário para ativar ou desativar o assistente de Call home do HMC .	• Sim: exibe o assistente de Call home do HMC. • Não: desativa a exibição do assistente de Call home do HMC.	Se um valor inválido for inserido, o Mecanismo de ativação usará a configuração padrão de Sim .
SetupKeyboard	Elemento necessário para definir a configuração do teclado.	• Sim: solicita ao usuário a configuração do teclado. • Não: aceita a configuração do teclado padrão (EUA).	Se um valor inválido for inserido, o Mecanismo de ativação usará a configuração padrão de Sim .
SetupDisplay	Elemento necessário para ativar ou desativar a configuração de exibição.	• Sim: solicita o usuário a configuração de exibição. • Não: aceita a configuração de exibição padrão.	Se um valor inválido for inserido, o Mecanismo de ativação usará a configuração padrão de Sim .

Tabela 9. tags XML (continuação)

Rótulos	Descrição	Valores aceitáveis	Notes
Ethernet	Elemento necessário que contém valores para as configurações do adaptador Ethernet. Um máximo de quatro adaptadores Ethernet pode ser configurado.	Ativar: • Sim: configurar esse adaptador. • Não: não configurar esse adaptador. DefaultGatewayDevice: • Sim: configurar esse adaptador como o adaptador de rede principal. • Não: não configurar esse adaptador como o adaptador de rede principal. PrivateInterface: • Sim: configurar esse adaptador como uma interface privada. Sim é necessário para configurar a interface como um Servidor DHCP IPv4. • Não: não configurar esse adaptador como uma interface privada. Não é necessário para configurar a interface como tipo estático IPv4.	O Mecanismo de ativação executará a configuração padrão se quaisquer valores inválidos forem inseridos na seção do adaptador Ethernet ou se múltiplos Dispositivos de gateway padrão forem definidos. Elementos opcionais podem ser omitidos da configuração. Pelo menos uma configuração de IPv4 ou IPv6 é necessária. Se você não especificar uma configuração de IP, o Mecanismo de ativação usará a configuração padrão.
Nome do Host	Elemento opcional para definir o nome do host da rede.	Qualquer sequência de nomes de hosts válidos.	Se o elemento não for definido, o Mecanismo de ativação usará o valor HostName do host local padrão.
Domain	Elemento opcional para definir o domínio de rede.	Qualquer valor de domínio válido (por exemplo, example.us.com).	Se o elemento não for definido, o Mecanismo de ativação usará o valor padrão Domínio vazio.
DNSServers	Elemento opcional para definir os servidores DNS de rede.	É aceitável ter um valor de Servidor DNS ou até três endereços IPv4 ou IPv6 válidos que são separados por uma vírgula. • Exemplo 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • Exemplo 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • 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	Se o elemento não for definido, o Mecanismo de ativação usará o valor padrão DNSServers vazio.

Tabela 9. tags XML (continuação)

Rótulos	Descrição	Valores aceitáveis	Notes
IP4Config	Elemento opcional para estabelecer as definições de configuração de IPv4.	IPType: elemento Necessário para definir o tipo de configuração de IPv4. • Estático: configure esse adaptador usando a configuração estática. • DHCP: configure esse adaptador usando a configuração DHCP. • DHCPServer: configurar esse adaptador como servidor DHCP IPv4 (requer PrivateInterface para ser configurado para Sim). IPAddress: elemento opcional que será necessário somente se Estático ou DHCPServer for selecionado. • Configuração estática: qualquer valor de endereço IPv4 válido. • DHCPServer Configuration: qualquer IP do servidor DHCP dentro do intervalo de IP. Máscara de rede: elemento opcional que será necessário somente se a configuração Estático for selecionada. • Qualquer valor de máscara de rede IPv4 válido. Gateway: elemento opcional que será necessário somente se a configuração Estático for selecionada. • Qualquer valor de máscara de rede IPv4 válido.	
IP6Config	Elemento opcional para estabelecer as definições de configuração de IPv6.	IPType: elemento necessário para definir o tipo de configuração de IPv6. • Estático: configure esse adaptador usando a configuração estática. • DHCP: configure esse adaptador usando a configuração DHCP. IPAddress: é aceitável ter o formato IPv6 longo ou curto e o prefixo IPv6 longo ou curto. • Exemplo 1: IPv6: 2001:4860:4860:0000:0000:0000:8888 • Exemplo 2: IPv6: 2001:4860:4860::8888 • Exemplo 3: IPv6: 2001:4860:4860::8888/128 Se nenhum prefixo for especificado, o Mecanismo de ativação usará a configuração padrão de prefixo /64. Gateway: • Qualquer valor de endereço IPv6 válido.	

Tabela 9. tags XML (continuação)

Rótulos	Descrição	Valores aceitáveis	Notes
Firewall	Elemento opcional para definir as configurações de firewall.	PEGASUS: • Ativado: permite que as portas do PEGASUS sejam abertas. • Desativado: desativa as portas do PEGASUS. RPD: • Ativado: permite que as portas do RMC sejam abertas. • Desativado: Desativa as portas do RMC. FCS: • Ativado: permite que as portas do FCS sejam abertas. • Desativado: desativa as portas do FCS. I5250: • Ativado: permite que as portas do 5250 sejam abertas. • Desativado: desativa as portas do 5250. PING: • Ativado: permite que a porta de Ping seja aberta. • Desativado: desativa a porta de Ping. L2TP: • Ativado: permite que as portas do L2TP sejam abertas. • Desativado: desativa as portas do L2TP. SLP: • Ativado: permite que as portas do SLP sejam abertas. • Desativado: desativa as portas do SLP. RSCT: • Ativado: permite que as portas do RSCT sejam abertas. • Desativado: desativa as portas do RSCT. SECUREREMOTEACCESS: • Ativado: permite que as portas de acesso remoto seguro sejam abertas. • Desativado: desativa as portas de acesso remoto seguro. SSH: • Ativado: permite que a porta do SSH seja aberta. • Desativado: desativa a porta do SSH.	

Tabela 9. tags XML (continuação)			
Rótulos	Descrição	Valores aceitáveis	Notes
Firewall	Elemento opcional para definir as configurações de firewall.	NTP: • Ativado: permite que as portas do NTP sejam abertas. • Desativado: desativa as portas do NTP. SNMPTraps: • Ativado: permite que as portas de traps SNMP sejam abertas. • Desativado: desativa as portas de traps SNMP. SNMPAgents: • Ativado: permite que as portas de agentes do SNMP sejam abertas. • Desativado: desativa as portas de agentes do SNMP.	
NTPServers	A tag NTPServers é necessária se você deseja configurar até cinco servidores NTP dentro de um dispositivo virtual HMC.	NTPServers: aceita <ntpparam ntpserver="server" ntpversion="version"/> ntpparam: • ntpserver: aceita quaisquer valores válidos de IPv4 ou IPv6 e nomes de hosts válidos. • ntpversion: aceita o valor numérico 1-4 Amostra: <pre> <NTPServers> <ntpparam ntpserver= "test.austin.ibm.com" ntpversion="2"/> <ntpparam ntpserver="192.168.34.1" ntpversion="4"/> <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/> </NTPServers> </pre>	

Configurando o HMC

Aprenda como configurar suas conexões de rede, configurar seu HMC, concluir as etapas de pós-configuração e fazer upgrade e atualizar seu HMC.

Escolhendo Configurações de Rede no HMC

Aprenda sobre as configurações de rede que podem ser usadas no Hardware Management Console (HMC).

Conexões de Rede do HMC

Aprenda como o Hardware Management Console HMC pode ser usado em uma rede.

É possível usar tipos diferentes de conexões de rede para conectar o HMC a sistemas gerenciados. Para obter mais informações sobre como configurar o HMC para se conectar a uma rede, consulte

“Configurando o HMC” na página 71. Para obter mais informações sobre como usar o HMC em uma rede, veja as informações a seguir:

Tipos de Conexões de Rede do HMC

Saiba como usar o gerenciamento remoto e as funções de serviço do HMC usando sua rede.

O HMC suporta os tipos de comunicações lógicas a seguir:

HMC para sistema gerenciado

Usado para executar a maioria das funções de gerenciamento de hardware em que o HMC emite solicitações de função de controle por meio do processador de serviços do sistema gerenciado. A conexão entre o HMC e o processador de serviços é às vezes referida como *rede de serviço*. Essa conexão é necessária para gerenciamento de sistemas gerenciado.

HMC para partição lógica

Usado para coletar informações relacionadas à plataforma (eventos de erro de hardware, inventário de hardware) dos sistemas operacionais que estão executando em partições lógicas, bem como coordenar determinadas atividades da plataforma (dynamic LPAR, reparo simultâneo) com esses sistemas operacionais. Se você desejar usar recursos de notificação de serviço e erro, deverá criar esta conexão.

HMC para o BMC

Nota: A conexão do Baseboard Management Controller (BMC) é aplicável apenas ao HMC modelo 7063-CR1.

Usado para executar tarefas de serviço e de manutenção. A conexão do BMC é usada para carregar e manter o firmware no sistema HMC. Essa conexão é necessária para obter o acesso ao BMC no HMC.

HMC para usuários remotos

Fornece aos usuários remotos o acesso a funções do HMC. Os usuários remotos podem acessar o HMC das maneiras a seguir:

- Usando o navegador da web para acessar todas as funções da GUI do HMC remotamente.
- Usando o Secure Socket Shell (SSH) para acessar as funções da linha de comandos do HMC remotamente.
- Usando um servidor de terminal virtual para obter acesso remoto aos consoles de partição lógica virtual.

HMC para serviço e suporte

Usado para transmitir dados, como relatórios de erro de hardware, dados do inventário e atualizações de microcódigo, para e a partir de seu provedor de serviços. É possível usar esse caminho de comunicações para fazer chamadas de serviço automáticas.

O HMC pode suportar até quatro interfaces físicas Ethernet separadas, dependendo do modelo. A versão independente do HMC suporta apenas três interfaces do HMC, usando um adaptador Ethernet integrado e até dois adaptadores de plug-in. Use cada uma dessas interfaces das maneiras a seguir:

- Uma interface de rede pode ser usada exclusivamente para comunicações do HMC-para-sistema gerenciado, o que significa que apenas o HMC e os processadores de serviços dos sistemas gerenciados estariam nessa rede. Uma ou mais interfaces de rede podem ser usadas exclusivamente para comunicações do HMC-para-sistema gerenciado, o que significa que apenas o HMC e os processadores de serviços dos sistemas gerenciados estão nessa rede. Mesmo que as interfaces de rede nos processadores de serviços sejam criptografadas para o Protocolo Secure Sockets Layer (SSL) e protegidas por senha, ter uma rede dedicada separada pode fornecer um nível mais alto de segurança para essas interfaces.
- Uma interface de rede aberta seria normalmente usada para a conexão de rede entre o HMC e as partições lógicas nos sistemas gerenciados, para as comunicações do HMC-para-partição lógica. Também é possível usar essa interface de rede aberta para gerenciar o HMC remotamente.
- Opcionalmente, é possível usar uma terceira interface para conectar a partições lógicas e gerenciar o HMC remotamente. Essa interface também pode ser usada como uma conexão do HMC separada para diferentes grupos de partições lógicas. Por exemplo, você pode ter uma LAN administrativa que esteja

separada da LAN na qual todas as transações de negócios usuais estão em execução. Os administradores remotos podem acessar o HMC e outras unidades gerenciadas usando esse método. Às vezes, as partições lógicas estão em domínios de segurança de rede diferentes, talvez atrás de um firewall, e pode ser desejado ter conexões de rede do HMC diferentes em cada um desses dois domínios.

Requisitos do Navegador da Web para HMC

O Hardware Management Console (HMC) versão 9.1.0 é suportado 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.

Se seu navegador estiver configurado para usar um proxy de Internet, um endereço IP local deverá ser incluído na lista de exceções. Consulte seu administrador da rede para obter mais informações sobre a lista de exceções. Se ainda for necessário usar o proxy para chegar ao HMC, ative Usar HTTP 1.1 por meio de conexões proxy sob a guia Avançado em sua janela Opções de Internet.

Os cookies de sessão devem ser ativados para que o ASMI trabalhe quando conectado remotamente ao HMC. O código de proxy asm salva as informações da sessão e as utiliza. Siga as etapas para ativar os cookies de sessão.

Ativando cookies de sessão no Internet Explorer.

1. Selecione Ferramentas e clique em Opções da Internet
2. Selecione Privacidade e clique em Avançado
3. Assegure-se de que Sempre permitir cookies por sessão esteja marcado. Se não, selecione Ignorar manipulação automática de cookies e selecione Sempre permitir cookies por sessão.
4. Selecione Avisar sob Cookies Primários e Cookies Secundários
5. Clique em OK.

Ativando cookies de sessão no Firefox.

1. Selecione Ferramentas e clique em Opções
2. Clique em Cookies
3. Selecione Permitir que os sites configurem cookies.
4. Selecione Exceções e inclua HMC.
5. Clique em OK.

Redes Privas e Abertas no Ambiente do HMC

O Hardware Management Console (HMC) pode ser configurado para usar redes abertas e privadas. As redes privadas permitem o uso de um intervalo selecionado de endereços IP não roteáveis. Uma rede *pública* ou "aberta" descreve uma conexão de rede entre o HMC para quaisquer partições e para outros sistemas em sua rede regular.

Redes Privadas

Os únicos dispositivos na rede privada do HMC são o próprio HMC e cada um dos sistemas gerenciados aos quais esse HMC está conectado. O HMC é conectado ao Processador de Serviços Flexível (FSP) de cada sistema gerenciado.

Na maioria dos sistemas, o FSP fornece duas portas Ethernet que são rotuladas como **HMC1** e **HMC2**. É possível conectar até dois HMCs.

Alguns sistemas possuem uma opção FSP dual. Nesta situação, o segundo FSP age como um backup redundante. Os requisitos de configuração básica para um sistema com dois FSPs são essencialmente os mesmos que para um sistema sem um segundo FSP. O HMC deve ser conectado a cada FSP, portanto mais hardware de rede é necessário (por exemplo, um comutador ou hub de LAN) quando há mais de um FSP ou múltiplos sistemas gerenciados.

Nota: Cada porta FSP no sistema gerenciado deve ser conectado a apenas um HMC.

Redes Públicas

A rede aberta pode ser conectada a um firewall ou roteador para conectar-se à Internet. Conectar-se à Internet permite que o HMC use call home quando quaisquer erros de hardware precisam ser relatados.

O próprio HMC fornece seu próprio firewall em cada uma de suas interfaces de rede. Um firewall básico é configurado automaticamente ao executar o assistente Guided Setup do HMC, mas você customiza suas configurações de firewall após a instalação e configuração iniciais do HMC.

HMC como um Servidor DHCP

É possível usar o Hardware Management Console (HMC) como um servidor Protocolo de Configuração de Host Dinâmico (DHCP).

Se você deseja configurar a primeira interface de rede como uma rede privada, será possível selecionar a partir de um intervalo de endereços IP do servidor DHCP para designar a seus clientes. As variações de endereços selecionáveis incluem segmentos das variações de endereços IP não roteáveis padrão.

Além desses intervalos padrão, um intervalo especial de endereços IP é reservado para endereços IP. Esse intervalo especial pode ser usado para evitar conflitos nos casos em que as redes abertas conectadas ao HMC estão usando uma das variações de endereços não roteáveis. Com base no intervalo selecionado, a interface de rede do HMC na rede privada é designada automaticamente ao primeiro endereço IP desse intervalo e os processadores de serviços são designados a endereços do restante do intervalo.

O servidor DHCP no HMC usa a alocação automática, o que significa que cada interface Ethernet do processador de serviços exclusivo é redesignada ao mesmo endereço IP toda vez que ela é iniciada. Cada interface Ethernet tem um identificador exclusivo que é baseado em um endereço de Controle de Acesso à Mídia (MAC) integrado, que permite que o servidor DHCP redesigne os mesmos parâmetros de IP. É possível configurar as portas HMC **eth0** e **eth1** para servir endereços DHCP. É possível configurar as portas HMC **eth0** e **eth1** para servir endereços DHCP.

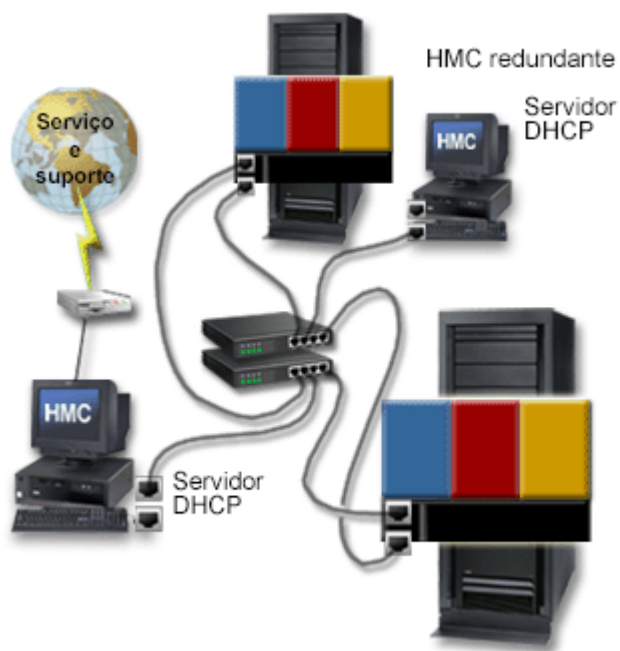
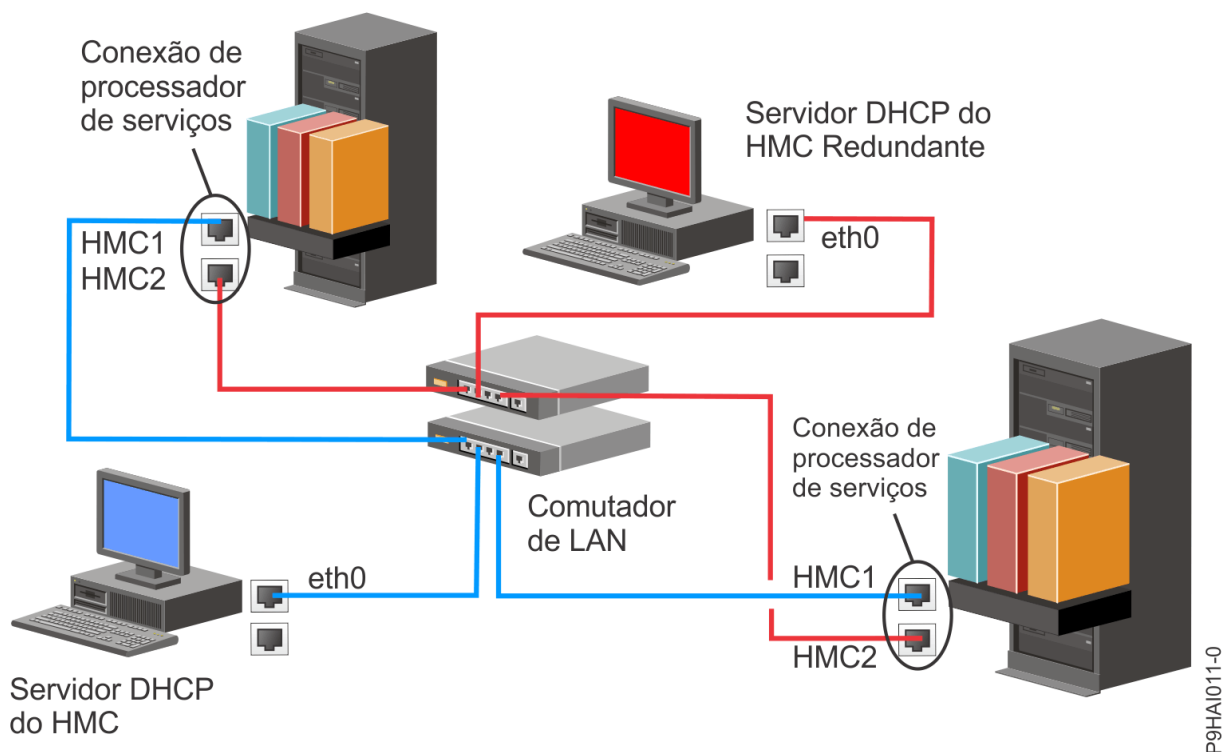


Figura 25. Rede Privada com um HMC como um Servidor DHCP

Nota: Se você estiver usando IPv6, o processo de descoberta deverá ser feito manualmente. Para IPv6, a descoberta automática não está disponível.

Para obter mais informações sobre como configurar o HMC como um servidor DHCP, consulte [“Configurando o HMC como um servidor DHCP”](#) na página 80.

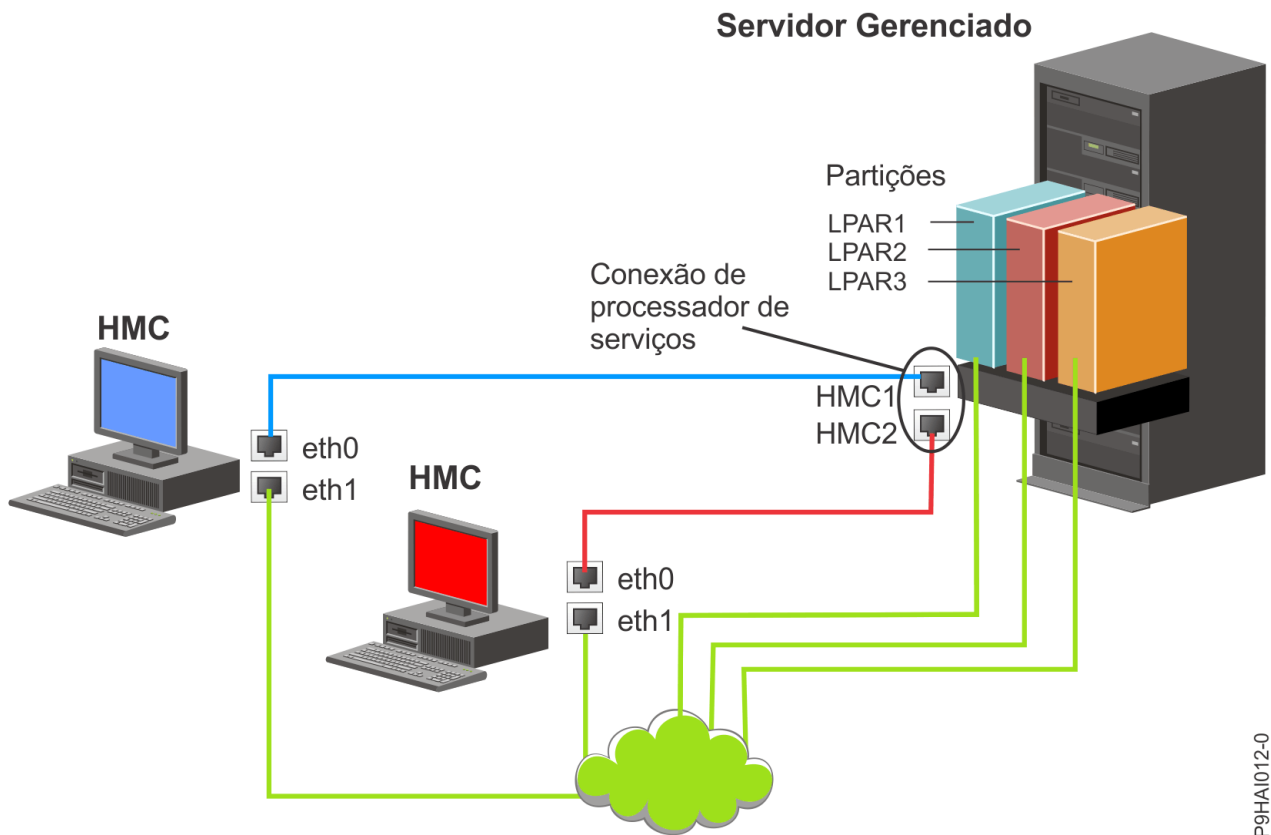


Esta figura mostra um ambiente HMC redundante com dois sistemas gerenciados. O primeiro HMC é conectado à primeira porta em cada FSP e o HMC redundante é conectado à segunda porta em cada HMC. Cada HMC é configurado como um servidor DHCP, usando um intervalo diferente de endereços IP. As conexões estão em redes privadas separadas. Como tal, é importante assegurar que nenhuma porta FSP seja conectada a mais de um HMC.

A porta FSP de cada sistema gerenciado que é conectada a um HMC requer um endereço IP exclusivo. Para assegurar que cada FSP tenha um endereço IP exclusivo, use o recurso do servidor DHCP integrado do HMC. Quando o FSP detecta o link de rede ativa, ele emite uma solicitação de transmissão para localizar um servidor DHCP. Quando configurado corretamente, o HMC responde a essa solicitação alocando um de um intervalo selecionado de endereços.

Se você tiver vários FSPs, deverá ter seu próprio comutador ou hub LAN do HMC para a rede privada FSP. Alternativamente, esse segmento privado pode existir como várias portas em uma *virtual LAN* (VLAN) em um comutador gerenciado maior. Caso você tenha múltiplas VLANs privadas, deve-se assegurar que elas estejam isoladas e sem qualquer tráfego de cruzamento.

Se você tiver mais de um HMC, também deverá conectar cada HMC às partições lógicas, e umas às outras, na mesma rede aberta.



Esta figura mostra dois HMCs conectados a um único servidor gerenciado na rede privada e a três partições lógicas na rede pública. É possível ter um adaptador Ethernet adicional para que o HMC tenha três interfaces de rede. É possível usar essa terceira rede como uma rede de gerenciamento ou conectá-la ao Servidor de Gerenciamento CSM (Cluster Systems Manager).

Decidindo qual Método de Conectividade Usar para o Servidor de Call Home

Aprenda mais sobre as opções de conectividade que você tem ao usar o servidor de call home.

É possível configurar o Hardware Management Console (HMC) para enviar informações relacionadas ao serviço de hardware à IBM usando uma conexão de Internet baseada em LAN ou uma conexão discada por meio de um modem.

Você tem duas opções de comunicação ao configurar a conexão de Internet baseada em LAN. A primeira opção é usar o Secure Sockets Layer (SSL) padrão. A comunicação de SSL pode ser ativada para conectar-se à Internet por meio de seu servidor proxy. A conectividade SSL tem mais probabilidade de ser compatível com as diretrizes de segurança corporativa.

Nota: Se a sua conexão de interface de rede aberta usa somente o Protocolo da Internet versão 6 (IPv6), não é possível usar a VPN da Internet para se conectar ao suporte. Para obter mais informações sobre os protocolos que são usados, consulte [“Escolhendo um Protocolo da Internet”](#) na página 61.

As vantagens de usar uma conexão de Internet podem incluir:

- Velocidade de transmissão mais rápida
- Despesa reduzida do cliente (por exemplo, o custo de uma linha de telefone analógica dedicada)
- Maior confiabilidade

As características de segurança a seguir estão em vigor, independentemente do método de conectividade escolhido:

- As solicitações de Remote Support Facility são sempre iniciadas do HMC para a IBM. Uma conexão de entrada nunca é iniciada a partir do IBM Service Support System.

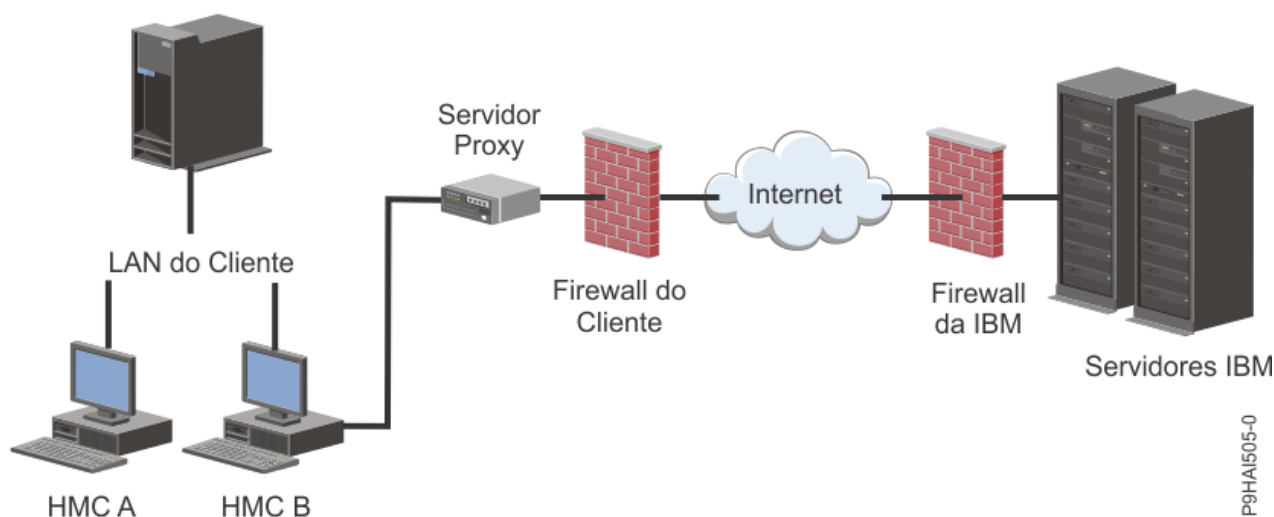
- Todos os dados transferidos entre o HMC e o IBM Service Support System são criptografados usando uma criptografia de alto grau. Dependendo do método de conectividade escolhido, eles são criptografados usando SSL ou IPSec Encapsulating Security Payload (ESP).
- Quando você inicializa a conexão criptografada, o HMC autentica o destino alvo como o IBM Service Support System.

Os dados enviados ao IBM Service Support System consistem unicamente de informações sobre problemas de hardware e configuração. Nenhum dado do aplicativo ou do cliente é transmitido à IBM.

Usando uma conexão de Internet indireta com um servidor proxy

Se sua instalação requer que o HMC esteja em uma rede privada, você pode ser capaz de se conectar indiretamente à Internet usando um proxy SSL, que pode encaminhar solicitações para a Internet. Uma das outras potenciais vantagens de usar um proxy SSL é que o proxy pode suportar os recursos de criação de log e auditoria.

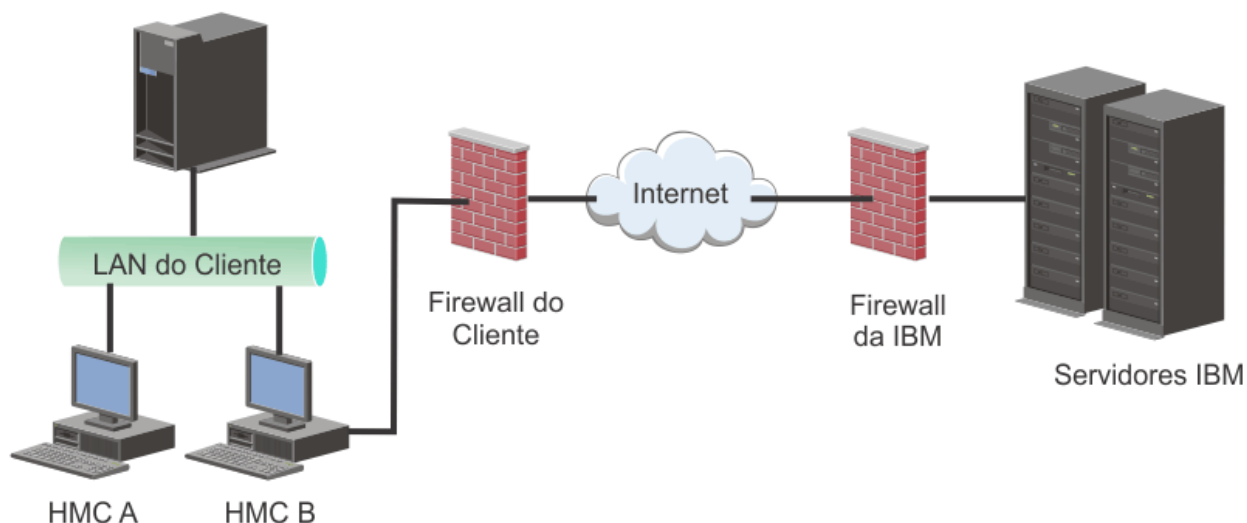
Para encaminhar soquetes SSL, o servidor proxy deve suportar as funções básicas de cabeçalho do proxy (conforme descrito no RFC 2616) e o método CONNECT. Opcionalmente, a autenticação básica de proxy (RFC 2617) pode ser configurada para que o HMC seja autenticado antes de tentar encaminhar soquetes por meio do servidor proxy.



Para que o HMC se comunique com êxito, o servidor proxy do cliente deve permitir conexões com a porta 443. É possível configurar seu servidor proxy para limitar os endereços IP específicos aos quais o HMC pode se conectar. Consulte [“Listas de Endereços SSL da Internet”](#) na página 61 para obter uma lista de endereços IP.

Usando uma conexão SSL de Internet direta

Se o seu HMC pode ser conectado à Internet e o firewall externo puder ser configurado para permitir que pacotes TCP estabelecidos transmitam a saída para os destinos descritos em [“Listas de Endereços SSL da Internet”](#) na página 61, é possível usar uma conexão de Internet direta.



P9HAI504-0

Usando SSL de Internet para se conectar ao suporte remoto

Todas as comunicações são manipuladas por meio de soquetes TCP que são iniciados pelo Hardware Management Console (HMC) e usam um SSL de alto grau para criptografar os dados que são transmitidos. Os endereços TCP/IP de destino são publicados (consulte [“Listas de Endereços SSL da Internet”](#) na página 61) para que firewalls externos possam ser configurados para permitir essas conexões.

Nota: A porta HTTPS padrão 443 é usada para todas as comunicações.

O HMC pode ser ativado para se conectar diretamente à Internet ou para se conectar indiretamente de um servidor proxy que é fornecido pelo cliente. A decisão sobre qual abordagem é melhor para sua instalação depende dos requisitos de segurança e rede de sua empresa. O HMC (diretamente ou por meio do proxy SSL) usa os endereços a seguir quando é configurado para usar conectividade SSL da Internet.

Escolhendo um Protocolo da Internet

Determine a versão do endereço IP que é usada quando o Hardware Management Console (HMC) se conecta ao seu provedor de serviços.

A maioria dos usuários usam o Internet Protocol Version 4 (IPv4) para se conectar a um provedor de serviços. Os endereços IPv4 aparecem no formato que representa os 4 bytes do endereço IPv4, que é separado por pontos (por exemplo, 9.60.12.123) para acessar a Internet. Também é possível usar o Internet Protocol Version 6 (IPv6) para se conectar a um provedor de serviços. O IPv6 é geralmente usado por administradores de rede para assegurar espaço de endereço exclusivo. Se você não tiver certeza do protocolo da Internet usado por sua instalação, entre em contato com seu administrador da rede. Para obter mais informações sobre como usar cada versão, consulte [“Configurando o Endereço IPv4”](#) na página 80 e [“Configurando o Endereço IPv6”](#) na página 81.

Listas de Endereços SSL da Internet

Saiba os endereços que o Hardware Management Console (HMC) usa quando o HMC está usando conectividade SSL da Internet.

O HMC usa os endereços IPv4 a seguir para entrar em contato com o serviço e suporte IBM quando ele está configurado para usar conectividade SSL da Internet.

Os endereços IPv4 a seguir 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 IPv4 a seguir são para as Américas:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Os endereços IPv4 a seguir são para todos os locais diferentes das Américas:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Nota: Ao configurar um firewall para permitir que um HMC se conecte a esses servidores, somente os endereços IP específicos para a região geográfica são necessários.

O HMC usa os endereços IPv6 a seguir para entrar em contato com o serviço e suporte IBM quando ele está configurado para usar conectividade SSL da Internet:

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

Usando Vários Servidores de Call Home

Aprenda o que você precisa saber quando decidir usar mais de um servidor de call home.

Para evitar um ponto único de falha, configure o Hardware Management Console (HMC) para usar múltiplos servidores de call home. O primeiro servidor de call home disponível tenta manipular cada evento de serviço. Se a conexão ou transmissão falhar com esse servidor de call home, a solicitação de serviço será tentada novamente usando os outros servidores de call home disponíveis até que um seja bem-sucedido ou todos os servidores sejam tentados.

O HMC conectado é identificado pela análise de problemas como o console primário de análise para um determinado sistema gerenciado que relata o problema. Esse console primário também replicará o relatório de problemas para qualquer HMC secundário. Esse HMC deve ser reconhecido na rede pelo HMC primário. Um HMC secundário é reconhecido pelo HMC primário como um servidor de call home adicional quando:

- O HMC primário está configurado para usar servidores de call home "descobertos" e o servidor de call home está na mesma sub-rede que o HMC primário ou ele gerencia o mesmo sistema.
- O servidor de call home é incluído manualmente na lista de consoles de servidores de call home disponíveis para conectividade de saída.

Preparando-se para a Configuração do HMC

Aprenda sobre as definições de configuração necessárias que você precisa saber antes de iniciar as etapas de configuração.

Para configurar o HMC, deve-se entender os conceitos relacionados, tomar decisões e preparar informações.

Saiba as informações que você precisa para conectar o HMC aos locais a seguir:

- Processadores de serviços em seus sistemas gerenciados
- Partições lógicas nesses sistemas gerenciados

- Estações de trabalho remotas
- Serviço IBM para implementar funções de “call home”

Para preparar a configuração do HMC, conclua as seguintes etapas:

1. Obtenha e instale o nível mais recente da versão do código do HMC que você deseja instalar.
2. Determine o local físico do HMC em relação aos servidores que ele gerencia. Se o HMC estiver a mais de 25 pés de seu sistema gerenciado, você deverá fornecer acesso ao navegador da Web para o HMC a partir da localização do sistema gerenciado para que a equipe de serviços possa acessar o HMC.
3. Identifique os servidores que o HMC gerencia.
4. Determine se você usa uma rede privada ou aberta para gerenciar servidores. Se você decidir usar uma rede privada, use DHCP, a menos que esteja usando uma configuração do Cluster Systems Management (CSM). O CSM não suporta IPv6. Para acessar o CSM, você deve ter duas redes. Para obter mais informações sobre o CSM, consulte a documentação que foi fornecida com esse recurso. Para obter mais informações sobre redes privadas e abertas, consulte [“Selecionando uma Rede Privada ou Aberta”](#) na página 79.
5. Se você usa uma rede aberta para gerenciar um FSP, deve-se configurar o endereço do FSP manualmente por meio dos menus da Advanced System Management Interface. Uma rede privada não roteável é recomendada.
6. Se tiver dois HMCs, designe um HMC primário e um secundário. O HMC primário precisa estar fisicamente mais perto do sistema e deve ser o HMC que está configurado para call home.
7. Determine as configurações de rede que você precisa para conectar o HMC a estações de trabalho remotas, partições lógicas e dispositivos de rede.
8. Defina como o HMC usa o call home. As opções de call home incluem uma conexão de Internet Secure Sockets Layer (SSL) somente de saída, um modem ou uma conexão de Rede Privada Virtual (VPN).
9. Determine os usuários do HMC que você cria e suas senhas, além de quais funções devem ser atribuídas a eles. Deve-se designar uma senha aos usuários **hscroot** e **hscpe**.
10. Documente as informações de contato da empresa a seguir que são necessárias quando você configura o call home:
 - Nome da Empresa
 - Contato do Administrador
 - Endereço de email
 - Números de Telefone
 - Números de Fax
 - O endereço do local físico do HMC
11. Se você planeja usar e-mail para notificar os operadores ou administradores dos sistemas quando informações são enviadas para o Serviço IBM por meio de call home, identifique o servidor de Protocolo Simples de Transporte de Correio (SMTP) e os endereços de e-mail usados.
12. Você deve definir as senhas a seguir:
 - A senha de acesso que é usada para autenticar o HMC para o FSP.
 - A senha de ASMI que é usada para o usuário **administrador**.
 - A senha de ASMI que é usada para o usuário **geral**.

Crie as senhas quando se conectar do HMC a um novo servidor pela primeira vez. Se o HMC for um HMC redundante ou um segundo HMC, obtenha a senha do usuário do HMC e prepare-se para inseri-la quando se conectar pela primeira vez ao FSP do servidor gerenciado.

Quando você concluir estas etapas de preparação, conclua a [“Planilha de Configuração de Pré-instalação para o HMC”](#) na página 64.

Planilha de Configuração de Pré-instalação para o HMC

Use esta planilha para deixar as informações de instalação necessárias prontas para a instalação.

Política de senha aprimorada para HMC

Deve-se configurar uma nova senha no primeiro uso para sistemas recém-fabricados com o HMC versão 9.940.0, ou mais recente, e após uma reconfiguração de fábrica do sistema. Essa mudança de política ajuda a impedir que o HMC não seja deixado em um estado com uma senha conhecida.

Com o HMC Versão 9.940.0, e mais recente, a senha do hscroot é expirada e deve ser alterada antes que você possa acessar as funções do HMC. Para obter mais informações sobre como mudar a senha, consulte https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm. No entanto, se você estiver fazendo upgrade de um nível do HMC ou de uma instalação operacional anterior, não será necessário mudar a senha.

Configurações de Rede

Interface de LAN: escolha os adaptadores disponíveis (como eth0, eth1) que são usados por esse HMC para conectar-se a sistemas gerenciados, partições lógicas, serviço e suporte e usuários remotos. Para obter informações adicionais, consulte “Conexões de Rede do HMC” na página 54. A conectividade do HMC pode ser em uma rede privada ou aberta.

Velocidade e duplex do adaptador Ethernet

Insira a velocidade desejada do adaptador Ethernet e o modo duplex. A opção de detecção automática determina qual opção é ideal se você não tiver certeza de qual velocidade e duplex produziram resultados para seu hardware. A velocidade Default = Autodetection Media especifica a velocidade no modo duplex do adaptador Ethernet. Selecione Detecção automática a menos que você precisa especificar uma velocidade de mídia fixa. Qualquer dispositivo conectado ao FSP (comutadores/HMC) deve ser configurado para o modo Automático (velocidade)/Automático (duplex), uma vez que é a configuração padrão do FSP e não pode ser mudada.

Tabela 10. Velocidade e duplex do adaptador Ethernet				
Característica	eth0	eth1	eth2	eth3
Selecione a velocidade e o modo duplex				
Velocidade da mídia (Detecção automática, 10/100/1000 Full/Half Duplex)				

Para obter mais informações sobre redes privadas e abertas, consulte “Redes Privas e Abertas no Ambiente do HMC” na página 56.

Tabela 11. Rede privada ou aberta				
Característica	eth0	eth1	eth2	eth3
Especifique rede Privada ou Aberta para cada adaptador.				

O Protocolo de Configuração de Host Dinâmico (DHCP) fornece um método automatizado para configuração dinâmica do cliente. É possível especificar este HMC como um servidor DHCP. Se este for o primeiro ou o único HMC na rede privada, ative o HMC como um servidor DHCP. Quando você ativa o HMC como um servidor DHCP, os sistemas gerenciados na rede são configurados e descobertos automaticamente pelo HMC.

Para adaptadores Ethernet especificados como redes privadas, complete a tabela a seguir:

Tabela 12. Servidor DHCP		
Características	eth0	eth1
Deseja especificar este HMC como um servidor DHCP? (sim/não)		
Se sim, registre o intervalo de endereço IP que você deseja usar		

Se você está usando o 7063-CR1 HMC, deve-se conectar a porta Ethernet **IPMI** a uma rede para acessar o Baseboard Management Controller (BMC) no HMC. Para obter mais informações, consulte [“Configure a conectividade do BMC” na página 80](#). Preencha a tabela a seguir para sua conexão do BMC.

Tabela 13. Conexão do BMC	
Características	IPMI
Deseja configurar essa conexão por meio do modo DHCP? (sim/não)	
Se não, liste os endereços estáticos especificados abaixo:	
Endereço IP:	
Máscara de Sub-rede:	
Gateway:	

Para adaptadores Ethernet especificados como redes *abertas*, complete as tabelas a seguir. Para obter mais informações sobre as diferentes versões de Internet Protocol, consulte [“Configurando os Tipos de Rede do HMC” na página 74](#).

Usando IPv6

Se você estiver usando IPv6, converse com seu administrador da rede e decida como deseja obter endereços IP. Em seguida, complete as tabelas a seguir:

Tabela 14. IPv6 (estático)				
Característica	eth0	eth1	eth2	eth3
Você está usando um endereço IP estaticamente designado? Se sim, registre o endereço aqui.				

Tabela 15. IPv6 (servidor DHCP)				
Característica	eth0	eth1	eth2	eth3
Você está obtendo endereços IP de um servidor DHCP? (Sim/Não)				

Tabela 16. IPv6 (roteador IPv6)				
Característica	eth0	eth1	eth2	eth3
Você está obtendo endereços IP de um roteador IPv6?				

Para obter mais informações sobre como configurar endereços IPv6, consulte “Configurando o Endereço IPv6” na página 81. Para obter mais informações sobre como usar apenas endereços IPv6, consulte “Usando Apenas Endereços IPv6” na página 81.

Usando IPv4

Conclua as tabelas a seguir para adaptadores Ethernet que são especificados como redes abertas usando IPv4.

Tabela 17. IPv4				
Características	eth0	eth1	eth2	eth3
Deseja obter um endereço IP automaticamente? (sim/não)				
Se não, liste o endereço especificado abaixo:				
Endereço da Interface TCP/IP:				
Máscara de Rede da Interface TCP/IP:				
Configurações de Firewall:				
Deseja configurar as definições de firewall do HMC? (sim/não)				
Se sim, liste os aplicativos e endereços IP que devem ser permitidos por meio do firewall:				

Informações TCP/IP

Um endereço TCP/IP exclusivo é necessário para cada nó, tanto para Elemento de Suporte (SE) como para Hardware Management Console (HMC). A máscara de rede designada é usada para gerar um endereço exclusivo, por padrão, para a LAN privada local. Se os nós estão conectados a uma rede maior com um endereço TCP/IP administrado, é possível especificar o endereço TCP/IP a ser usado. O padrão é gerado pelo sistema.

Configurações de Firewall

As configurações de firewall do HMC criam uma barreira de segurança que permite ou nega acesso a aplicativos de rede específicos no HMC. É possível especificar essas configurações de controle individualmente para cada interface de rede física, permitindo que você controle quais aplicativos de rede do HMC podem ser acessados em cada rede.

Se você configura pelo menos um adaptador como um adaptador de rede Aberta, deve-se fornecer as informações adicionais a seguir para permitir que o HMC acesse a LAN:

Tabela 18. Adaptador de rede aberta

Informações do host local	
Nome do host do HMC:	
Nome de domínio:	
Descrição do HMC:	
Informação do Gateway	
Endereço do gateway: (nnn.nnn.nnn.nnn)	
Dispositivo de gateway:	
Ativação de DNS	
Deseja usar o DNS? (sim/não)	
Se “sim”, especifique a Ordem de Procura de Servidores do Sistema de Nomes de Domínio:	
1.	
2.	
Ordem de procura de sufixos de domínio:	
1.	
2.	

Informações do host local

Para identificar o Hardware Management Console (HMC) na rede insira o nome do host e nome de domínio do HMC. A menos que você esteja usando apenas nomes abreviados de host em sua rede, insira um nome completo de host. Exemplo de nome de domínio: nome.suaempresa.com

Informações do gateway

Para definir um gateway padrão, conclua o endereço TCP/IP a ser usado para rotear pacotes de IP. O endereço do gateway informa a cada computador ou dispositivo de rede quando enviar dados se a estação de destino não está na mesma sub-rede que a origem.

Ativação de DNS

O Sistema de Nomes de Domínio (DNS) é usado para fornecer uma convenção de nomenclatura padrão para localizar computadores baseados em IP. Definindo servidores DNS, é possível usar nomes de hosts para identificar servidores e Hardware Management Consoles (HMCs) em vez de endereços IP.

Ordem de Procura de Servidores do Sistema de Nomes de Domínio

Insira os endereços IP dos servidores do Sistema de Nomes de Domínio a serem procurados para mapear os nomes de hosts e endereços IP. Esta ordem de procura está disponível apenas quando o DNS está ativado.

Ordem de Procura de Sufixos de Domínio

Insira os sufixos de domínio que você está usando. O HMC usa sufixos de domínio para anexar a nomes não qualificados para procuras de DNS. Os sufixos são procurados na ordem em que são listados. Esta ordem de procura está disponível apenas quando o DNS está ativado.

Notificação por E-mail

Liste as informações de contato de e-mail se você desejar ser notificado por e-mail quando eventos de problemas de hardware ocorrerem em seu sistema.

Tabela 19. Notificação por E-mail	
Características	Campo de Entrada
Endereços de E-mail:	
Servidor SMTP:	
Porta:	
Erros a serem notificados:	
Apenas eventos de problemas de call home	
Todos os eventos de problemas	

Servidor SMTP

Digite o endereço de Protocolo Simples de Transporte de Correio (SMTP) do servidor a ser notificado de um evento do sistema. Um exemplo de nome de servidor SMTP é `relay.us.ibm.com`.

SMTP é o Protocolo usado para enviar e-mail. Ao usar SMTP, um cliente envia uma mensagem e se comunica com o servidor SMTP usando o Protocolo SMTP.

Se você não souber o endereço SMTP de seu servidor ou não tiver certeza, entre em contato com seu administrador da rede.

Porta

Digite o número da porta do servidor a ser notificado de um evento do sistema ou use a porta padrão.

Endereços de e-mail a serem notificados

Insira os endereços de e-mail configurados a serem notificados quando um evento do sistema ocorrer.

- Selecione **Somente eventos de problemas de call home** para receber notificação somente quando ocorrerem eventos que criam uma função de call home.
- Selecione **Todos os eventos de problema** para receber notificação quando quaisquer eventos ocorrerem.

Informações de contato de serviço

Tabela 20. Informações de contato de serviço	
Características	Campo de Entrada
Nome da Empresa	
Nome do administrador	
Endereço de e-mail	
Número do telefone	
Número do telefone alternativo	
Número do fax	
Número do telefone alternativo	
Endereço	
Endereço 2	
Cidade ou localidade	
Estado	

Tabela 20. Informações de contato de serviço (continuação)	
Características	Campo de Entrada
Código de endereçamento postal	
País ou região	
Local do HMC (se mesmo que o endereço do administrador acima, especifique “same”):	
Endereço	
Endereço 2	
Cidade ou localidade	
Estado	
Código de endereçamento postal	
País ou região	

Autorização e Conectividade de Serviço

Selecione o tipo de conexão para entrar em contato com seu provedor de serviços. Para obter uma descrição desses métodos que incluem características de segurança e requisitos de configuração, veja [“Escolhendo Servidores de Call Home Existentes para Conectar ao Serviço e Suporte para este HMC”](#) na página 87.

Tabela 21. Autorização e Conectividade de Serviço	
Características	Campo de Entrada
Secure Sockets Layer (SSL) por meio da Internet	-----
Rede privada virtual (VPN) por meio da Internet	-----

Secure Sockets Layer (SSL) por meio da Internet:

Se você tiver uma conexão de Internet existente de seu HMC, será possível usá-la para chamar seu provedor de serviços. É possível conectar-se diretamente ao provedor de serviços usando Secure Sockets Layer (SSL) criptografado, usando a conexão de Internet existente. Selecione **Usar proxy SSL** se você deseja configurar o uso de SSL criptografado usando uma conexão indireta que usa um Proxy SSL.

Tabela 22. SSL	
Características	Campo de Entrada
Usar proxy SSL? (sim/não)	
Se sim, liste as informações abaixo:	
Endereço:	
Porta:	
Autenticar com o Proxy SSL?	
Se sim, liste as informações abaixo:	
Usuário:	

Tabela 22. SSL (continuação)	
Características	Campo de Entrada
Senha:	

Protocolo de conexão de Internet usado

Para obter mais informações sobre os diferentes protocolos da Internet, veja [“Configurando os Tipos de Rede do HMC”](#) na página 74.

- ___ IPv4
- ___ IPv6
- ___ IPv4 e IPv6

Rede Privada Virtual (VPN)

Se você tiver uma conexão de Internet existente de seu HMC, será possível usá-la para chamar seu provedor de serviços. É possível conectar-se diretamente ao seu provedor de serviços por rede privada virtual (VPN) usando a conexão de Internet existente.

Nota: Caso selecione Rede Privada Virtual (VPN) por meio da Internet, não será possível selecionar nenhuma outra opção.

Servidores de Call Home

Determine quais HMCs você deseja configurar para conectar ao serviço e suporte como servidores de call home. Para obter mais informações sobre como usar vários servidores de call home, consulte [“Usando Vários Servidores de Call Home”](#) na página 62.

- ___ Este HMC
- ___ Outro HMC

Se você marcou **Outro HMC**, liste os outros HMCs que estão configurados como servidores de call home aqui:

Tabela 23. Outros HMCs que estão configurados como servidores de call home	
Lista de nomes de hosts ou endereços IP do HMC que estão configurados como servidores de call home	

Benefícios do suporte adicional

My Systems and Premium Search

Tabela 24. My Systems and Premium Search	
Características	Campo de Entrada
Liste seu ID IBM	_____
Liste quaisquer IDs IBM adicionais	_____

Para acessar informações de suporte customizadas e de valor nas seções Meus sistemas e Procura premium do website de Serviços Eletrônicos, os clientes devem registrar seu IBMid com este sistema. Se você ainda não tiver, será possível registrar um ID IBM em: www.ibm.com/account/profile.

Nota: A IBM fornece funções da web personalizadas que usam informações que são coletadas pelo aplicativo IBM Electronic Service Agent. Para usar essas funções, você deve primeiro registrar-se no website de Registro IBM em <http://www.ibm.com/account/profile>.

Para autorizar os usuários a usar as informações do Electronic Service Agent para personalizar as funções da web, insira o IBMid que você registrou no website de Registro IBM. Acesse <http://www.ibm.com/support/electronic> para ver as informações de suporte de valor disponíveis para os clientes que registrarem um ID IBM com seus sistemas.

Configurando o HMC

Aprenda a configurar conexões de rede, segurança, aplicativos de serviço e algumas preferências do usuário.

Dependendo do nível de customização que você pretende aplicar à sua configuração do HMC, há várias opções para configurar o HMC de modo a adequar às suas necessidades. O Assistente de Configuração Orientada é uma ferramenta no HMC projetada para facilitar a configuração do HMC. É possível escolher um atalho por meio do assistente para criar rapidamente o ambiente do HMC recomendado, ou escolher explorar completamente as configurações disponíveis pelas quais o assistente guiará você. Também é possível executar as etapas de configuração sem o auxílio do assistente [Configurando o HMC usando os menus do HMC](#).

Antes de iniciar, reúna as informações de configuração necessárias para concluir as etapas com êxito. Consulte [“Preparando-se para a Configuração do HMC”](#) na página 62 para obter uma lista das informações necessárias. Quando concluir a preparação, assegure-se de concluir a [“Planilha de Configuração de Pré-instalação para o HMC”](#) na página 64 e, em seguida, retorne a esta seção.

Configurando o HMC Usando o Atalho por meio do Assistente Guided Setup

Na maioria dos casos, o HMC pode ser configurado para operar eficazmente usando muitas das configurações padrão. Use esta lista de verificação de atalho para preparar o HMC para o serviço. Ao concluir estas etapas, o HMC é configurado como um servidor Protocolo de Configuração de Host Dinâmico (DHCP) em uma rede privada (conectada diretamente).

Configurando o HMC usando os menus

Esta seção fornece uma lista completa de todas as tarefas de configuração do HMC, guiando você pelo processo de configuração do HMC. Escolha esta opção se você preferir não usar o Assistente de Configuração Orientada.

Você deve reiniciar o HMC para que as definições de configuração entrem em vigor, portanto, você talvez queira imprimir esta lista de verificação e mantê-la junto ao configurar o HMC.

Estas informações contêm referências a tarefas que não estão incluídas neste documento. É possível acessar as Informações de Hardware do IBM Power Systems no HMC ou na web. No HMC, o IBM Knowledge Center pode ser acessado no canto superior direito da barra de tarefas. Na web, o IBM Knowledge Center pode ser acessado em <https://www.ibm.com/support/knowledgecenter>.

Estas informações contêm referências a tarefas que não estão incluídas neste PDF. É possível acessar materiais de suporte adicionais consultando a seção **Additional Resources** na página HMC Welcome.

Pré-requisitos

Antes de começar a configurar o HMC usando os menus do HMC, certifique-se de concluir a atividade de preparação de configuração descrita em [“Preparando-se para a Configuração do HMC”](#) na página 62.

Tabela 25. Tarefas de Configuração Manual do HMC e Onde Localizar Informações Relacionadas	
Tarefa	Onde localizar informações relacionadas
1. Inicie o HMC.	“Iniciando o HMC” na página 73
2. Configure a data e hora.	

Tabela 25. Tarefas de Configuração Manual do HMC e Onde Localizar Informações Relacionadas (continuação)

Tarefa	Onde localizar informações relacionadas
3. Altere as senhas predefinidas.	
4. Crie usuários adicionais e retorne a esta lista de verificação após a conclusão dessa etapa.	
5. Configure conexões de rede.	“Configurando os Tipos de Rede do HMC” na página 74
6. Para o HMC modelo 7063-CR1, deve-se configurar o endereço IP do Baseboard Management Controller (BMC).	“Configure a conectividade do BMC” na página 80
7. Se você estiver usando uma rede aberta e um endereço IP fixo, configure informações de identificação.	
8. Se você estiver usando uma rede aberta e um endereço IP fixo, configure uma entrada de roteamento como o gateway padrão.	“Configurando uma Entrada de Roteamento como o Gateway Padrão” na página 83
9. Se você estiver usando uma rede aberta e um endereço IP fixo, configure os serviços de nome de domínio.	“Configurando Serviços de Nomes de Domínio” na página 83
10. Se você estiver usando um endereço IP fixo e tiver o DNS ativado, configure sufixos de domínio.	“Configurando Sufixos de Domínio” na página 84
11. Configure o servidor para conectar ao serviço e suporte IBM e retorne a esta lista de verificação após a conclusão dessa etapa.	“Configurando o Console Local para Relatar Erros para o Serviço e Suporte” na página 86
12. Configure o Gerenciador de eventos como Call home.	“Configurando o Gerenciador de eventos para Call home” na página 89
13. Conecte o sistema gerenciado a uma fonte de alimentação.	
14. Configure as senhas para o sistema gerenciado e cada uma das senhas da ASMI (geral e administrativa)	“Configurando Senhas para o Sistema Gerenciado” na página 90
15. Acesse a ASMI para configurar a data e hora no sistema gerenciado.	
16. Inicie o sistema gerenciado e retorne a esta lista de verificação após a conclusão dessa etapa.	
17. Assegure-se de que você tenha uma partição lógica no sistema gerenciado.	
18. Opcional: inclua um outro sistema gerenciado e retorne a esta lista de verificação após a conclusão dessa etapa.	
19. Opcional: Se você estiver instalando um novo servidor com o HMC, configure as partições lógicas e instale o sistema operacional.	

Tabela 25. Tarefas de Configuração Manual do HMC e Onde Localizar Informações Relacionadas (continuação)

Tarefa	Onde localizar informações relacionadas
20. Se você não estiver instalando um novo servidor no momento, execute tarefas de pós-configuração opcionais para customizar ainda mais sua configuração.	“Etapas de Pós-configuração” na página 92

Iniciando o HMC

É possível efetuar login no HMC e escolher qual idioma você deseja que seja exibido na interface. Use o ID do Usuário padrão `hscroot` e a senha `abc123` para efetuar login no HMC pela primeira vez.

Sobre Esta Tarefa

Para iniciar o HMC, execute o procedimento a seguir:

Procedimento

1. Ligue o HMC pressionando o botão de energia.
2. Se inglês for sua preferência de idioma, continue com a etapa 4.
Se sua preferência de idioma for um idioma diferente do inglês, digite o número **2** quando solicitado para alterar o código de idioma.
Nota: Esse prompt atingirá o tempo limite em 30 segundos se você não agir.
3. Selecione o código de idioma que você deseja exibir na lista da janela **Seleção de código de idioma** e clique em **OK**. O código de idioma identifica o idioma que a interface do HMC usa.
4. Clique em **Log on and launch the Hardware Management Console web application**.
5. Efetue login no HMC com o ID de usuário e a senha padrão a seguir:

ID: `hscroot`

Senha: `abc123`

HMC Aprimorado

Exibe a GUI aprimorada mais recente com os recursos aprimorados do PowerVM.

HMC Clássico

Exibe a GUI padrão sem os recursos aprimorados do PowerVM.

Nota: Quando o HMC estiver funcionando como um servidor DHCP, o HMC usará a senha padrão ao conectar ao processador de serviço pela primeira vez.

6. Pressione Enter.

Alterando a Data e Hora

O relógio operado por bateria mantém a data e hora para o Hardware Management Console (HMC). Pode ser necessário reconfigurar a data e hora do console se a bateria for substituída, ou se você mover fisicamente seu sistema para um fuso horário diferente. Aprenda como alterar a data e hora para o HMC.

Sobre Esta Tarefa

Se você alterar as informações de data e hora, a mudança não afetará os sistemas e partições lógicas que o HMC gerencia.

Para alterar a data e hora do HMC, conclua as etapas a seguir:

Procedimento

1. Assegure-se de que você seja um membro de uma das funções a seguir:

- Superadministrador
- Representante de Serviço
- Operador
- Visualizador



2. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Configurações do console**.
3. Na área de conteúdo, clique em **Change Date and Time**.
4. Se você selecionar **UTC** no campo **Relógio**, a configuração de horário se ajustará automaticamente para o horário de verão no fuso horário selecionado. Insira a data, o horário e o fuso horário e clique em **OK**.

Resultados

Configurando os Tipos de Rede do HMC

Configure seu HMC de modo que ele possa se comunicar com o sistema gerenciado, as partições lógicas, os usuários remotos e o serviço e suporte.

Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar ao Sistema Gerenciado

Configure o HMC de modo que ele possa se conectar e gerenciar um sistema gerenciado usando uma rede aberta.

Antes de Iniciar

Para configurar as definições de rede do HMC para que ele possa se conectar ao sistema gerenciado usando uma rede aberta, faça o seguinte:

Tabela 26. Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar ao Sistema Gerenciado	
Tarefa	Onde localizar informações relacionadas
1. Decida qual interface você deseja usar para seu sistema gerenciado. eth0 é preferencial.	“Planilha de Configuração de Pré-instalação para o HMC” na página 64
2. Identifique as portas Ethernet para seu HMC.	“Identificando a porta Ethernet que está definida como eth0” na página 77
3. Configure o adaptador Ethernet executando as tarefas a seguir:	
a. Configure a velocidade de mídia.	“Configurando a Velocidade de Mídia” na página 79
b. Selecione o tipo de rede aberta.	“Selecionando uma Rede Privada ou Aberta” na página 79
c. Configure endereços estáticos.	“Configurando o Endereço IPv6” na página 81
d. Configure o firewall.	“Alterando as Configurações de Firewall do HMC” na página 82
e. Configure o gateway padrão.	“Configurando uma Entrada de Roteamento como o Gateway Padrão” na página 83
f. Configure o DNS.	“Configurando Serviços de Nomes de Domínio” na página 83

Tabela 26. Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar ao Sistema Gerenciado (continuação)

Tarefa	Onde localizar informações relacionadas
4. Configure adaptadores adicionais, se você os tiver.	
5. Teste a conexão entre o servidor gerenciado e o HMC.	“Testando a conexão entre o HMC e o sistema gerenciado” na página 91

Configurando as Definições do HMC para Usar uma Rede Privada para Conectar ao Sistema Gerenciado
Configure o HMC de modo que ele possa se conectar e gerenciar um sistema gerenciado usando uma rede privada.

Antes de Iniciar

Para configurar as definições de rede do HMC para que ele possa se conectar ao sistema gerenciado usando uma rede privada, faça o seguinte:

Tabela 27. Configurando as Definições do HMC para Usar uma Rede Privada para Conectar ao Sistema Gerenciado

Tarefa	Onde localizar informações relacionadas
1. Decida qual interface você deseja usar para seu sistema gerenciado.	“Planilha de Configuração de Pré-instalação para o HMC” na página 64
2. Identifique as portas Ethernet para seu HMC.	“Identificando a porta Ethernet que está definida como eth0” na página 77
3. Configure o HMC como um servidor DHCP.	“Configurando o HMC como um servidor DHCP” na página 80
4. Teste a conexão entre o servidor gerenciado e o HMC.	“Testando a conexão entre o HMC e o sistema gerenciado” na página 91

Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar a Partições Lógicas

Antes de Iniciar

Para configurar as definições de rede do HMC para que ele possa se conectar a partições lógicas usando uma rede aberta, faça o seguinte:

Tabela 28. Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar a Partições Lógicas

Tarefa	Onde localizar informações relacionadas
1. Decida qual interface você deseja usar para seu sistema gerenciado.	“Planilha de Configuração de Pré-instalação para o HMC” na página 64
2. Identifique as portas Ethernet para seu HMC.	“Identificando a porta Ethernet que está definida como eth0” na página 77
3. Configure o adaptador Ethernet executando as tarefas a seguir:	
a. Configure a velocidade de mídia.	“Configurando a Velocidade de Mídia” na página 79
b. Selecione o tipo de rede aberta.	“Selecionando uma Rede Privada ou Aberta” na página 79

Tabela 28. Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar a Partições Lógicas (continuação)

Tarefa	Onde localizar informações relacionadas
c. Configure endereços estáticos.	“Configurando o Endereço IPv6” na página 81
d. Configure o firewall.	“Alterando as Configurações de Firewall do HMC” na página 82
e. Configure o gateway padrão.	“Configurando uma Entrada de Roteamento como o Gateway Padrão” na página 83
f. Configure o DNS.	“Configurando Serviços de Nomes de Domínio” na página 83
4. Configure adaptadores adicionais, se você os tiver.	
5. Teste a conexão entre o servidor gerenciado e o HMC.	“Testando a conexão entre o HMC e o sistema gerenciado” na página 91

Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar a Usuários Remotos

Antes de Iniciar

Para configurar as definições de rede do HMC para que ele possa se conectar a usuários remotos usando uma rede aberta, faça o seguinte:

Tabela 29. Configurando as Definições do HMC para Usar uma Rede Aberta para Conectar a Usuários Remotos

Tarefa	Onde localizar informações relacionadas
1. Decida qual interface você deseja usar para seu sistema gerenciado.	“Planilha de Configuração de Pré-instalação para o HMC” na página 64
2. Identifique as portas Ethernet para seu HMC.	“Identificando a porta Ethernet que está definida como eth0” na página 77
3. Configure o adaptador Ethernet executando as tarefas a seguir:	
a. Configure a velocidade de mídia.	“Configurando a Velocidade de Mídia” na página 79
b. Selecione o tipo de rede aberta.	“Selecionando uma Rede Privada ou Aberta” na página 79
c. Configure endereços estáticos.	“Configurando o Endereço IPv6” na página 81
d. Configure o firewall.	“Alterando as Configurações de Firewall do HMC” na página 82
e. Configure o gateway padrão.	“Configurando uma Entrada de Roteamento como o Gateway Padrão” na página 83
f. Configure o DNS.	“Configurando Serviços de Nomes de Domínio” na página 83
g. Configure sufixos.	“Configurando Sufixos de Domínio” na página 84
4. Configure adaptadores adicionais, se você os tiver.	

Antes de Iniciar

Para configurar as definições do servidor de call home do HMC para que problemas possam ser relatados, faça o seguinte:

Tabela 30. Configurando as Definições do Servidor de Call Home do HMC	
Tarefa	Onde localizar informações relacionadas
1. Certifique-se de que você tenha todas as informações do cliente necessárias	“Planilha de Configuração de Pré-instalação para o HMC” na página 64
2. Configure este HMC para relatar erros ou escolha um servidor de call home existente para relatar erros	“Configurando o Console Local para Relatar Erros para o Serviço e Suporte” na página 86 “Escolhendo Servidores de Call Home Existentes para Conectar ao Serviço e Suporte para este HMC” na página 87
3. Verifique se sua configuração de call home está funcionando	“Verificando se sua Conexão com o Serviço e Suporte Está Funcionando” na página 88
4. Autorizar os usuários a visualizar dados do sistema coletados	“Autorizando os Usuários a Visualizar Dados do Sistema Coletados” na página 88
5. Planejar a transmissão de dados do sistema	“Transmitindo Informações do Serviço” na página 89

Identificando a porta Ethernet que está definida como eth0

Sua conexão Ethernet com o servidor gerenciado deve ser feita usando a porta Ethernet que está definida como eth0 em seu HMC.

Se você não instalou quaisquer adaptadores Ethernet adicionais nos slots PCI em seu HMC, a porta Ethernet integrada primária será sempre definida como eth0 ou eth1 no HMC, se pretender usar o HMC como um servidor DHCP para seus sistemas gerenciados.

Se você instalar adaptadores Ethernet adicionais nos slots PCI, a porta que for definida como eth0 dependerá do local e tipo de adaptadores Ethernet que estão instalados.

Nota: As regras gerais a seguir podem não se aplicar a todas as configurações.

A tabela a seguir descreve as regras para colocação de Ethernet por tipo de HMC.

Tabela 31. Tipos de HMC e Regras Associadas para Colocação de Ethernet

Tipo de HMC	Regras para colocação de Ethernet
HMCs montados em rack com duas portas Ethernet integradas.	O HMC suporta somente um adaptador Ethernet adicional. • Se um adaptador Ethernet adicional for instalado, essa porta será definida como eth0. Nesse caso, a porta Ethernet integrada primária será definida como eth1 e a porta Ethernet integrada secundária será definida como eth2. • Se o adaptador Ethernet for um adaptador Ethernet de porta dual, a porta rotulada como Act/Link A será eth0. A porta rotulada como Act/link B é eth1. Nesse caso, a porta Ethernet integrada primária será definida como eth2 e a porta Ethernet integrada secundária como eth3. • Se nenhum adaptador for instalado, a porta Ethernet integrada primária será definida como eth0.
Os modelos independentes com uma única porta Ethernet integrada.	As definições dependem do tipo de adaptador Ethernet que é instalado: • Se somente um adaptador Ethernet for instalado, esse adaptador será definido como eth0. • Se o adaptador Ethernet for um adaptador Ethernet de porta dual, a porta rotulada como Act/link A será eth0. A porta rotulada como Act/link B seria eth1. Nesse caso, a porta Ethernet integrada primária será definida como eth2. • Se nenhum adaptador for instalado, a porta Ethernet integrada será definida como eth0. • Se múltiplos adaptadores Ethernet forem instalados, veja “Determinando o Nome da Interface para um Adaptador Ethernet” na página 78.

Determinando o Nome da Interface para um Adaptador Ethernet

Se você configurar o HMC como um servidor DHCP, esse servidor poderá operar apenas nos conectores de placa da interface de rede (NIC) que o HMC identifica como eth0 e eth1. Talvez também seja necessário determinar a qual conector NIC o cabo Ethernet precisa ser conectado. Aprenda mais sobre como determinar quais conectores NIC o HMC identifica como eth0 e eth1.

Sobre Esta Tarefa

Para determinar o nome que o HMC designou a um adaptador Ethernet, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Mudar configurações de rede**.

3. Na janela **Mudar configurações de rede**, clique na guia **Adaptadores LAN**. A entrada de exemplo a seguir mostra que essa porta Ethernet é identificada como eth0: Ethernet eth0 52:54:00:fa:b6:8e (<endereço IP do HMC>).
4. Registre seus resultados. Se você precisar visualizar ou mudar as configurações do adaptador LAN, clique em **Detalhes**.
5. Clique em **OK**.

Configurando a Velocidade de Mídia

Aprenda como especificar a velocidade de mídia que inclui a velocidade e o modo duplex do adaptador Ethernet.

Antes de Iniciar

O padrão para as configurações do adaptador do HMC é **Autodetection**. Se esse adaptador estiver conectado a um comutador de LAN, você deverá corresponder a configurações da porta do comutador. Para configurar a velocidade de mídia e o duplex, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**.
3. Clique na guia **LAN Adapters**.
4. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
5. Na seção de informações da rede local (LAN), selecione **Deteção automática** ou a combinação apropriada de velocidade de mídia e duplex.
6. Clique em **OK**.

Selecionando uma Rede Privada ou Aberta

Um *rede de serviço particular* consiste no Hardware Management Console (HMC) e os sistemas gerenciados. Uma rede de serviço privada é restrita a consoles e aos sistemas que eles gerenciam e é separada de sua rede da empresa. Uma *rede aberta* consiste em sua rede de serviço privada e sua rede da empresa. Uma rede aberta pode conter terminais de rede, além de consoles e sistemas gerenciados, e pode abranger várias sub-redes e dispositivos de rede.

Sobre Esta Tarefa

Para selecionar uma rede privada ou pública, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**.
3. Clique na guia **LAN Adapters**.
4. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
5. Clique na guia **Adaptador de LAN**.
6. Na página de informações de rede local, selecione **Privada** ou **Aberta**.
7. Clique em **OK**.

Configurando o HMC como um servidor DHCP

O Protocolo de Configuração de Host Dinâmico (DHCP) fornece um método automatizado para configuração dinâmica do cliente.

Para configurar o Hardware Management Console (HMC) como um servidor DHCP, conclua as etapas a seguir:



1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**. A janela Customize Network Settings é aberta.
3. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
4. Selecione **Private** e, em seguida, selecione o tipo de rede.
5. Na seção DHCP Server, selecione **Enable DHCP Server** para ativar o HMC como um servidor DHCP.
Nota: É possível configurar o HMC para ser um servidor DHCP apenas em uma rede privada. Se você usa uma rede aberta, a opção para selecionar **Ativar DHCP** não está disponível.
6. Insira a variação de endereços do servidor DHCP.
7. Clique em **OK**.

Se você configurou o HMC para ser um servidor DHCP em uma rede privada, deverá verificar se a rede privada DHCP do HMC está configurada corretamente. Para obter informações sobre conectar o HMC a uma rede privada, consulte [“Selecionando uma Rede Privada ou Aberta”](#) na página 79.

Para obter mais informações, consulte [“HMC como um Servidor DHCP”](#) na página 57.

Configure a conectividade do BMC

É possível configurar ou visualizar as configurações de rede no BMC para o console de gerenciamento.

Nota: Essa tarefa se aplica somente ao 7063-CR1. Essa conexão é necessária para acessar o Baseboard Management Controller (BMC) no HMC.

Para configurar a conexão do BMC, conclua as etapas a seguir:



1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Mudar configurações de rede do BMC/IPMI**.
3. Selecione o modo de conexão (**DHCP** ou **Estático**).

Se você selecionar o modo **Estático**, preencha os endereços a seguir:

- **Endereço IP**
- **Máscara de sub-rede**
- **Gateway**

4. Clique em **OK**.

Também é possível configurar a conexão de rede do BMC usando o carregador de inicialização do Petitboot. Para obter mais informações, consulte [Configurando o endereço IP do firmware](#).

Configurando o Endereço IPv4

Aprenda a configurar seu endereço IPv4 no HMC.

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**.
3. Clique na guia **LAN Adapters**.
4. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
5. Clique na guia **Basic Settings**.
6. Selecione um endereço IPv4.
7. Se você selecionou para especificar um endereço IP, insira o endereço da interface TCP/IP e a máscara de rede da interface TCP/IP.
8. Clique em **OK**.

Configurando o Endereço IPv6

Aprenda a configurar seu endereço IPv6 no HMC.

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**.
3. Clique na guia **LAN Adapters**.
4. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
5. Clique na guia **IPv6 Settings**.
6. Selecione uma opção **Configuração automática** ou inclua um endereço IP estático.
7. Se você incluiu um endereço IP, insira o endereço IPv6 e o comprimento do prefixo e clique em **OK**.
8. Clique em **OK**.

Usando Apenas Endereços IPv6

Aprenda como configurar o HMC para que use apenas endereços IPv6.

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**.
3. Clique na guia **LAN Adapters**.
4. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
5. Selecione **No IPv4 address**.
6. Clique na guia **IPv6 Settings**.
7. Selecione **Usar DHCPv6 para definir configurações de IP** ou inclua endereços IP estáticos, em seguida, clique em **OK**.

O que Fazer Depois

Depois de clicar em **OK**, deve-se reiniciar o HMC para que essas mudanças entrem em vigor.

Alterando as Configurações de Firewall do HMC

Em uma rede aberta, um firewall é usado para controlar o acesso externo para sua rede da empresa. O HMC também possui um firewall de cada um de seus adaptadores Ethernet. Para controlar o HMC remotamente ou fornecer acesso remoto a outros, modifique as configurações de firewall do adaptador Ethernet no HMC que está conectado à sua rede aberta.

Sobre Esta Tarefa

Para configurar um firewall, use as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**.
3. Clique na guia **LAN Adapters**.
4. Selecione o adaptador LAN com o qual você deseja trabalhar e clique em **Details**.
5. Clique na guia **Firewall**.
6. Usando um dos métodos a seguir, é possível permitir qualquer endereço IP usando um aplicativo específico por meio do firewall ou especificar um ou mais endereços IP:
 - Permita qualquer endereço IP usando um aplicativo específico por meio do firewall:
 - a. Na caixa superior, destaque o aplicativo.
 - b. Clique em **Allow Incoming**. O aplicativo é exibido na caixa inferior para indicar que ele está selecionado.
 - Especifique quais endereços IP permitir por meio do firewall:
 - a. Na caixa superior, destaque um aplicativo.
 - b. Clique em **Allow Incoming by IP Address**.
 - c. Na janela Hosts Allowed, insira o endereço IP e a máscara de rede.
 - d. Clique em **Add** e clique em **OK**.
7. Clique em **OK**.

Ativando o Acesso ao Shell Restrito remoto

É possível ativar o acesso ao shell restrito remoto quando você configura um firewall.

Sobre Esta Tarefa

Para ativar o acesso ao shell restrito remoto, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique em **HMC Management**.
2. Clique em **Remote Command Execution**.
3. Selecione **Enable remote command execution using the ssh facility** e, em seguida, clique em **OK**.

O que Fazer Depois

Agora, o acesso ao shell restrito remoto está ativado.

Ativando o acesso remoto à web

É possível ativar o acesso remoto à web para seu Hardware Management Console (HMC).

Sobre Esta Tarefa

Para ativar o acesso remoto à web, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique em **HMC Management**.
2. Clique em **Remote Operation**.
3. Selecione **Enable** e, em seguida, clique em **OK**.

O que Fazer Depois

Agora o acesso remoto à web está ativado.

Configurando uma Entrada de Roteamento como o Gateway Padrão

Aprenda como configurar uma entrada de roteamento como o gateway padrão. Esta tarefa está disponível quando você está usando uma rede aberta.

Antes de Iniciar

Para configurar uma entrada de roteamento como o gateway padrão, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**. A janela Customize Network Settings é aberta.
3. Clique na guia **Routing**.
4. Na seção Default gateway information, insira o endereço do gateway e o dispositivo de gateway da entrada de roteamento que você deseja configurar como o gateway padrão.
5. Clique em **OK**.

Configurando Serviços de Nomes de Domínio

Se você planeja configurar uma rede aberta, configure os serviços de nomes de domínio.

Sobre Esta Tarefa

Se você planeja configurar uma rede aberta, configure os serviços de nomes de domínio. O Sistema de Nomes de Domínio (DNS) é um sistema de banco de dados distribuído para gerenciar nomes de hosts e seus endereços Internet Protocol (IP) associados. Configurar serviços de nomes de domínio inclui ativar o DNS e especificar a ordem de procura de sufixos de domínio.

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**. A janela Change Network Settings é aberta.
3. Clique na guia **Name Services**.
4. Selecione **DNS ativado** para ativar o DNS.
5. Especifique o servidor DNS e a ordem de procura de sufixos de domínio e clique em **Add**.
6. Clique em **OK**.

Configurando Sufixos de Domínio

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

Sobre Esta Tarefa

O sufixo de domínio é uma sequência anexada a um nome do host que é usada para ajudar a resolver seu endereço IP. Por exemplo, um nome de host myname pode não ser resolvido. Entretanto, se a sequência myloc.mycompany.com for um elemento na tabela de sufixos de domínios, uma tentativa será feita para resolver myname.mloc.mycompany.com.

Para configurar uma entrada de sufixo do domínio, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Alterar configurações de rede**. A janela Customize Network Settings é aberta.
3. Clique na guia **Name Services**.
4. Insira uma sequência a ser usada como uma entrada de sufixo de domínio.
5. Clique em **Add** para incluí-la na lista.

Configurando o HMC para que Use a Autenticação Remota LDAP

É possível configurar o Hardware Management Console (HMC) para que use autenticação remota LDAP (Lightweight Directory Access Protocol).

Antes de Iniciar

Quando um usuário efetua login no HMC, a autenticação é executada primeiro com relação a um arquivo de senha local. Se um arquivo de senha local não for localizado, o HMC poderá contatar um servidor LDAP remoto para autenticação. Você deve configurar o HMC para que ele use a autenticação remota LDAP.

Nota: Antes de configurar o HMC para que ele utilize a autenticação LDAP, você deve se certificar de que há uma conexão de rede funcional entre o HMC e os servidores LDAP. Para obter mais informações sobre como configurar conexões de rede do HMC, consulte [“Configurando os Tipos de Rede do HMC”](#) na página 74.

Sobre Esta Tarefa

Para configurar seu HMC para usar autenticação LDAP, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Usuários e segurança**  e, em seguida, selecione **Segurança de sistemas e do console**.
2. Na área de janela de conteúdo, selecione **Gerenciar LDAP**. A janela LDAP Server Definition é aberta.
3. Selecione **Enable LDAP**.
4. Defina um servidor LDAP para utilizar para autenticação.
5. Defina o atributo LDAP que é usado para identificar o usuário que está sendo autenticado. O padrão é **uid**, mas é possível usar seus próprios atributos.
6. Defina a árvore de nomes distintos, também conhecida como base de procura, para o servidor LDAP.
7. Clique em **OK**.

8. Se um usuário desejar usar autenticação LDAP, o usuário deve configurar seu perfil para que ele use a autenticação remota LDAP em vez de autenticação local.

Configurando o HMC para que Use os Servidores do Centro de Distribuição de Chaves para Autenticação Remota do Kerberos

É possível configurar o HMC para que use os servidores do Centro de Distribuição de Chaves (KDC) para autenticação remota do Kerberos.

Antes de Iniciar

Quando um usuário efetua login no HMC, a autenticação é verificada primeiro com relação a um arquivo de senha local. Se um arquivo de senha local não for localizado, o HMC poderá contatar um servidor Kerberos remoto para autenticação. Você deve configurar o HMC para que ele use a autenticação remota do Kerberos.

Nota: Antes de configurar o HMC para que use servidores KDC para autenticação remota do Kerberos, você deve assegurar que exista uma conexão de rede funcional entre o HMC e os servidores KDC. Para obter mais informações sobre como configurar conexões de rede do HMC, consulte [“Configurando os Tipos de Rede do HMC”](#) na página 74.

Sobre Esta Tarefa

Para configurar o HMC para que ele use servidores KDC para autenticação remota do Kerberos, conclua as etapas a seguir:

Procedimento

1. Ative o serviço Network Time Protocol (NTP) no HMC e configure o HMC e os servidores KDC para sincronizar o horário com o mesmo servidor NTP. Para ativar o serviço NTP no HMC, conclua as etapas a seguir:
 - a) Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Configurações do console**.
 - b) Na área de janela de conteúdo, selecione **Alterar data e hora**.
 - c) Selecione a guia **NTP Configuration**.
 - d) Selecione **Enable NTP service on this HMC**.
 - e) Clique em **OK**.
2. Configure o perfil do usuário do HMC remoto para que use a autenticação remota do Kerberos em vez de autenticação local.
3. Opcionalmente, é possível importar um arquivo de chave de serviço para esse HMC. O arquivo de chave de serviço contém o host principal que identifica o HMC para o servidor KDC. Os arquivos de chave de serviço também são conhecidos como *keytabs*. Para importar um arquivo de chave de serviço para esse HMC, conclua as etapas a seguir:

- a) Na área de navegação, clique no ícone **Usuários e segurança**  e, em seguida, selecione **Segurança de sistemas e do console**.
 - b) Na área de janela de conteúdo, selecione **Gerenciar KDC**.
 - c) Selecione **Ações > Importar chave de serviço**. A janela Import Service Key é aberta.
 - d) Digite o local do arquivo de chave de serviço.
 - e) Clique em **OK**.
4. Inclua um novo servidor KDC neste HMC. Para incluir um novo servidor KDC nesse HMC, conclua as etapas a seguir:



- a) Na área de navegação, clique no ícone **Usuários e segurança** e, em seguida, selecione **Segurança de sistemas e do console**.
- b) Na área de janela de conteúdo, selecione **Gerenciar KDC**.
- c) Selecione **Ações > Incluir servidor KDC**. A janela Import Service Key é aberta.
- d) Digite a região e o nome do host ou endereço IP do servidor KDC.
- e) Clique em **OK**.

Configurando o Console Local para Relatar Erros para o Serviço e Suporte

Configure este HMC para que ele possa efetuar um call home de erros usando a conectividade de LAN.

Configurando o HMC para que ele possa se conectar ao serviço e suporte usando o assistente de configuração de call home

Configure o HMC para que ele seja um servidor de call home usando o assistente de call home.

Antes de Iniciar

Este procedimento descreve como configurar o HMC como um servidor de call home usando conexões diretas (baseadas em LAN) e indiretas (SSL) com a Internet.

Antes de iniciar esta tarefa, assegure-se de que:

- O administrador da rede verifica se a conectividade é permitida. Para obter mais informações, consulte [“Preparando-se para a Configuração do HMC”](#) na página 62.
- Se você está configurando o suporte de Internet por meio de um servidor proxy, deve-se também ter as informações a seguir:
 - O endereço IP e porta do servidor proxy
 - As informações sobre autenticação do proxy
- O adaptador que está designado como **eth1** (aquele designado como uma rede aberta) é usado. Para obter mais informações, consulte [“Escolhendo Configurações de Rede no HMC”](#) na página 54.
- Um cabo Ethernet conecta fisicamente o HMC à LAN.

Para configurar o HMC para que ele seja um servidor de call home usando o assistente de call home, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Capacidade de manutenção** e, em seguida, selecione **Gerenciamento de serviço**.
2. Na área de janela de conteúdo, clique em **Assistente de configuração de call home**. O assistente Conectividade e Servidores de Call-Home é aberta. Siga as instruções no assistente para configurar o recurso de call-home.

Configurando o Console Local para Relatar Erros para o Serviço e Suporte

Configure este HMC para que ele possa efetuar um call home de erros usando a conectividade de LAN.

Configurando um HMC para contatar o serviço e suporte usando Internet baseada em LAN e SSL

Descreve como configurar o HMC como um servidor de call home usando conexões diretas (baseadas em LAN) e indiretas (SSL) com a Internet.

Antes de Iniciar

Antes de iniciar esta tarefa, assegure-se de que:

- O administrador da rede verifica se a conectividade é permitida. Para obter mais informações, consulte [“Preparando-se para a Configuração do HMC”](#) na página 62.
- As informações de contato do cliente sejam configuradas. Verifique as informações de contato acessando a interface do HMC e clicando em **Capacidade de manutenção > Gerenciamento de serviço > Gerenciar informações do cliente**.
- Se você está configurando o suporte de Internet por meio de um servidor proxy, deve-se também ter as informações a seguir:
 - O endereço IP e porta do servidor proxy
 - As informações sobre autenticação do proxy
- É necessário ter pelo menos uma interface de rede aberta configurada. Para obter mais informações, consulte [“Redes Privas e Abertas no Ambiente do HMC”](#) na página 56.
- Um cabo Ethernet conecta fisicamente o HMC à LAN.

Sobre Esta Tarefa

Para configurar o HMC como um servidor de call home usando Internet baseada em LAN e SSL, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Capacidade de manutenção** e, em seguida, selecione **Gerenciamento de serviço**.
2. Na seção Connectivity, clique em **Manage Outbound Connectivity**. A janela Call-home Server Consoles é aberta.
3. Clique em **Configure**.
4. Na janela Outbound Connectivity Settings, marque **Enable local system as call-home server**.
5. Aceite o contrato.
6. Na janela Outbound Connectivity Settings, selecione a página **Internet**.
7. Marque a caixa **Allow an existing internet connections for service**.
8. Se você estiver usando um proxy SSL, marque a caixa **Use SSL proxy**.
9. Se você estiver usando um proxy SSL, conclua o endereço e porta do proxy. Obtenha essas informações com o administrador da rede.
10. Se você marcou **Use SSL proxy** e o proxy requer autenticação de ID do usuário e senha, marque a caixa **Authenticate with the SSL proxy**. Digite o ID do usuário e a senha. Obtenha o ID do usuário e a senha com o administrador da rede.
11. Selecione o **Protocol to Internet** que você deseja usar.
12. Na página **Internet**, clique em **Test**.
13. Na janela Testar Internet, clique em **Iniciar**.
14. Verifique se o teste é concluído com êxito.
15. Na janela Testar Internet, clique em **Cancelar**.
16. Na janela Outbound Connectivity Settings, clique em **OK**.

Escolhendo Servidores de Call Home Existentes para Conectar ao Serviço e Suporte para este HMC
Escolha os servidores de call home existentes do Hardware Management Console (HMC) que são reconhecidos ou descobertos pelo HMC para relatar erros.

Antes de Iniciar

Os HMCs descobertos são HMCs que estão ativados como servidores de call home e estão na mesma sub-rede ou gerenciam o mesmo sistema gerenciado que este HMC.

Para escolher um HMC descoberto para call home quando o HMC relata erros, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Capacidade de manutenção** e, em seguida, selecione **Gerenciamento de serviço**.
2. Na área de janela de conteúdo, clique em **Gerenciar conectividade de saída**. A janela Call-Home Server Consoles é aberta.
3. Clique em **Usar consoles dos servidores de call home descobertos**. O HMC exibe o endereço IP ou nome do host dos HMCs configurados para call home.
4. Clique em **OK**.

Resultados

Também é possível incluir manualmente servidores de call home do HMC existentes que estão em uma sub-rede diferente. Selecione o endereço IP ou nome do host do HMC que está configurado para call home e clique em **Incluir** e, em seguida, clique em **OK**.

Verificando se sua Conexão com o Serviço e Suporte Está Funcionando

Teste o relatório de problemas para assegurar que a conexão com o serviço e suporte esteja funcionando.

Sobre Esta Tarefa

Para verificar se sua configuração de call home está funcionando, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Capacidade de manutenção** e, em seguida, selecione **Gerenciamento de serviço**.
2. Na área de janela de conteúdo, clique em **Criar evento**.
3. Selecione **Testar relatório de problemas automático** e digite um comentário.
4. Clique em **Request Service**. Aguarde alguns minutos para que a solicitação seja enviada.
5. Na janela Service Management, selecione **Manage Events**.
6. Selecione **All open problems**.
7. Verifique se há um evento e um número do PMH estão designados ao problema aberto.
8. Selecione esse evento e clique em **Fechar**.
9. Na janela **Fechar**, digite seu nome e um breve comentário.

Autorizando os Usuários a Visualizar Dados do Sistema Coletados

Você deve autorizar os usuários a visualizar dados sobre seus sistemas.

Antes de Iniciar

Antes de autorizar os usuários a visualizar dados do sistema coletados, você deve obter um ID IBM. Para obter mais informações sobre como obter um ID IBM, consulte [“Planilha de Configuração de Pré-instalação para o HMC” na página 64](#).

Sobre Esta Tarefa

Para autorizar os usuários a visualizarem dados do sistema coletados, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Capacidade de manutenção Gerenciamento de serviço**.
2. Na área de janela de conteúdo, selecione **Autorizar usuário**.
3. Insira seu ID IBM.
4. Clique em **OK**.

Transmitindo Informações do Serviço

É possível transmitir informações para seu provedor de serviços imediatamente ou planejar as informações para serem enviadas regularmente.

Antes de Iniciar

A IBM fornece funções da web personalizadas que usam informações coletadas pelo IBM Electronic Service Agent. Para usar essas funções, você deve primeiro registrar-se no website de Registro IBM em <http://www.ibm.com/account/profile>. Para autorizar os usuários a usar as informações do Electronic Service Agent para personalizar as funções da web, veja “Autorizando os Usuários a Visualizar Dados do Sistema Coletados” na página 88. Para obter mais informações sobre os benefícios de registrar um ID IBM com seus sistemas, consulte <http://www.ibm.com/support/electronic>.

Nota: Deve-se transmitir as informações do provedor de serviços assim que o HMC é instalado e configurado para uso.

Sobre Esta Tarefa

Para transmitir informações de serviço, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Capacidade de manutenção Gerenciamento de serviço**.
2. Na área de janela de conteúdo, selecione **Transmitir informações de serviço**.
3. Conclua as tarefas na janela **Transmitir informações de serviço** e clique em **OK**.

Configurando o Gerenciador de eventos para Call home

Aprenda a configurar a tarefa Gerenciador de eventos para Call home. É possível monitorar e aprovar quaisquer dados que estejam sendo transmitidos de um HMC para a IBM por meio desta tarefa.

O modo Gerenciador de eventos para call home (ativado ou desativado) é configurado usando a interface da linha de comandos do HMC. Ativar a tarefa Gerenciador de eventos para Call home bloqueia o HMC de eventos Call home automaticamente na medida em que eles ocorrem. Para evitar eventos nos quais a ação de call home é executada sem aprovação, todos os HMCs em execução neste ambiente devem ter o Gerenciador de eventos para Call home ativado.

Para ativar ou desativar a tarefa Gerenciador de eventos para Call home, execute o comando a seguir:

```
chhmc -c emch
```

```
-s {enable | disable}
```

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

```
[--help]
```

Nota: Ativar a tarefa Gerenciador de eventos para call home retém os eventos de call home até que eles sejam aprovados para a tarefa de call home. Se você desativar a tarefa Gerenciador de eventos para call home, isso não ativa automaticamente o recurso call home. Essa configuração evita qualquer ação de call

home de dados não intencional para a IBM. Escolha as opções de comando a seguir para configurar a configuração necessária:

- Para ativar a tarefa Gerenciador de eventos para call home: **chhmc -c emch -s enable**
- Para desativar a tarefa Gerenciador de eventos para call home e para reativar call home automático: **chhmc -c emch -s disable --callhome enable**
- Para desativar a tarefa Gerenciador de eventos para call home e não reativar call home automático: **chhmc -c emch -s disable --callhome disable**

Assegure-se de que o HMC possa se comunicar com outros HMCs implementados neste ambiente. O Gerenciador de eventos para Call home possui uma função de conexão de teste quando um HMC é registrado.

É possível registrar o HMC com o Gerenciador de eventos para Call home. Depois de registrar o HMC, o gerenciador de eventos consulta o HMC registrado para quaisquer eventos que estejam aguardando a ação de call home para a IBM. O Gerenciador de eventos mostra quais dados estão sendo retornados à IBM e aprova esses eventos. Após a aprovação, o Gerenciador de eventos notifica o HMC registrado de que ele pode continuar com a operação de call home.

A tarefa Gerenciador de eventos para Call home pode ser executada de qualquer HMC ou de vários HMCs. Para registrar um console de gerenciamento com a tarefa Gerenciador de eventos para Call home, conclua as etapas a seguir:



1. Na área de navegação, clique no ícone **Capacidade de manutenção** e, em seguida, selecione **Gerenciador de eventos para Call home**.
2. Na área de janela **Gerenciador de eventos para call home**, clique em **Gerenciar consoles**.
3. Na janela **Gerenciar consoles registrados**, clique em **Incluir console** para inserir informações para registrar um console de gerenciamento com a tarefa Gerenciador de eventos para Call home.
4. Clique em **OK** para confirmar as mudanças na lista de consoles de gerenciamento registrados.

Nota: O Gerenciador de eventos para Call home pode ser usado com o modo de gerenciador de eventos desativado. É possível ainda registrar o HMC e visualizar eventos no gerenciador de eventos, mas o Gerenciador de eventos não controla quando a ação de call home é executada.

Configurando Senhas para o Sistema Gerenciado

Você deve configurar senhas para o servidor e o Advanced System Management (ASM). Leia mais sobre como usar a interface do HMC para configurar essas senhas.

Antes de Iniciar

Se você recebeu a mensagem Authentication Pending, o HMC solicitará para configurar as senhas para o sistema gerenciado.

Sobre Esta Tarefa

Se você não recebeu a mensagem Authentication Pending, conclua as etapas a seguir para configurar as senhas para o sistema gerenciado.

Atualizando sua Senha do Servidor

Antes de Iniciar

Para atualizar sua senha do servidor, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, selecione o sistema gerenciado e clique no ícone **Usuários e segurança** e, em seguida, selecione **Usuários e funções**.
2. Clique em **Change Password**. A janela Update Password é aberta.
3. Digite as informações necessárias e clique em **OK**.



Atualizando sua Senha Geral do Advanced System Management (ASM)

Antes de Iniciar

Nota: A senha padrão para o ID do usuário geral é `general` e a senha padrão para o ID de administrador é `admin`.

Para atualizar sua senha geral do ASM, conclua as etapas a seguir:

Procedimento

1. Na área de navegação do HMC, selecione o sistema gerenciado.
2. Na área Tasks, clique em **Operations**.
3. Clique em **Advanced System Management (ASM)**. A janela Launch ASM Interface é aberta.
4. Selecione um Service Processor IP Address e clique em **OK**. A interface do ASM é aberta.
5. Na área de janela ASMI Welcome, especifique o seu ID de usuário e senha, e clique em **Log In**.
6. Na área de navegação, expanda **Login Profile**.
7. Selecione **Change Password**.
8. Especifique as informações necessárias e clique em **Continue**.

Reconfigurando a Senha do Administrador do Advanced System Management (ASM)

Antes de Iniciar

Para reconfigurar a senha do administrador, entre em contato com um provedor de serviços autorizado.

Testando a conexão entre o HMC e o sistema gerenciado

Aprenda como verificar se você está conectado de forma adequada à rede.

Sobre Esta Tarefa

Para testar a conectividade de rede, deve-se ser um membro de uma das funções a seguir:

- Superadministrador
- Representante de Serviço

Para testar a conexão entre o HMC e o sistema gerenciado, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Configurações do console**.
2. Na área de janela de conteúdo, clique em **Testar conectividade de rede**.
3. Na guia Ping, digite o nome do host ou endereço IP de qualquer sistema ao qual você deseja se conectar. Para testar uma rede aberta, digite o gateway. Clique em **Ping**.



Resultados

Se você não criou nenhuma partição lógica, não é possível executar ping dos endereços. É possível usar o HMC para criar partições lógicas em seu servidor. Para obter mais informações, consulte [Particionamento lógico](#).

Para entender como o HMC pode ser usado em uma rede, consulte [“Conexões de Rede do HMC” na página 54](#).

Para obter mais informações sobre como configurar o HMC para se conectar a uma rede, consulte [“Configurando o HMC usando os menus” na página 71](#).

Etapas de Pós-configuração

Depois de instalar e configurar o HMC, faça backup dos dados do HMC conforme necessário.

Fazendo backup de dados do console de gerenciamento

Esta tarefa faz backup (ou arquiva) dos dados armazenados em seu disco rígido HMC e que são críticos para suportar operações HMC.

Antes de Iniciar

Seu sistema remoto deve ter o Network File System (NFS) ou o shell seguro (ssh) configurado e essa rede deve ser acessível a partir do HMC. Para concluir esta tarefa, você deve encerrar e reinicializar o HMC. Use apenas o HMC para executar estas tarefas.

Sobre Esta Tarefa

Para fazer o backup da unidade de disco rígido do HMC em um sistema remoto, você deve ser um membro de uma das funções a seguir:

- Superadministrador
- Operador
- Representante de Serviço

Faça backup dos dados do HMC após realizar alterações no HMC ou nas informações associadas às partições lógicas.

Os dados HMC armazenados na unidade de disco rígido HMC podem ser salvos em um DVD-RAM no sistema local, em um sistema remoto montado no sistema de arquivos HMC (como o NFS), ou enviado a um site remoto utilizando FTP (Protocolo de Transferência de Arquivos).

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

Utilizando o HMC, você pode fazer backup de todos os dados importantes, como os seguintes:

- Arquivos de preferências do usuário
- Informações do usuário
- Arquivos de configuração da plataforma HMC
- Arquivos de log HMC
- Atualizações HMC através do Install Corrective Service.

Para fazer backup do disco rígido do HMC em um sistema remoto, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento do console**.

2. Na área de janela de conteúdo, clique em **Fazer backup dos dados do console de gerenciamento**.
3. Na janela **Fazer backup dos dados do console de gerenciamento**, selecione a opção de archive que você deseja executar.
4. Clique em **Next**, e então siga as instruções apropriadas, dependendo da opção que você fez.
5. Clique em **OK** para continuar com o processo de backup.

Atualizando, Fazendo Upgrade e Migrando seu Código de Máquina do HMC

As atualizações e os upgrades são liberados periodicamente para o HMC para incluir nova funcionalidade e para melhorar os recursos existentes. Aprenda mais sobre as diferenças entre atualizar, fazer upgrade e migrar seu código de máquina do HMC. Aprenda também como executar uma atualização, upgrade ou migração do código de máquina do HMC.

Quando você conclui cada uma destas tarefas, o HMC reinicializa mas as partições não.

Atualizando código do HMC

Aplica manutenção a um nível existente do HMC

Não requer a execução da tarefa **Salvar Dados de Upgrade**

Fazendo upgrade de código do HMC

Substitui o software do HMC por uma nova liberação ou nível de correção do mesmo programa

Requer a reinicialização a partir da mídia de recuperação

Migrando código do HMC

Move dados do HMC de uma versão do HMC para outra

Uma migração é um tipo de upgrade.

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

Determinando sua Versão e Liberação do Código de Máquina do HMC

Descubra como visualizar a versão e liberação do código de máquina do HMC.

Sobre Esta Tarefa

O nível de código de máquina no HMC determina os recursos disponíveis, incluindo a manutenção simultânea de firmware do servidor e aprimoramentos para upgrade para uma nova liberação.

Para visualizar a versão e liberação de código de máquina do HMC, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título **Informações atuais do driver HMC**, incluindo: versão, liberação, nível de manutenção, nível de construção e versões base do HMC.

Obtendo e Aplicando Atualizações de Código de Máquina para o HMC com uma Conexão de Internet

Aprenda como obter atualizações de código de máquina para o HMC quando ele possui uma conexão de Internet.

Sobre Esta Tarefa

Para obter atualizações de código de máquina do HMC, conclua todas as etapas.

Etapas 1. Assegurar que Você Tenha uma Conexão de Internet

Sobre Esta Tarefa

Para fazer download de atualizações do sistema de serviço e suporte ou do website para seu HMC ou servidor, deve-se ter uma das conexões a seguir:

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

Para assegurar que você tenha uma conexão de Internet, faça o seguinte:

Procedimento

1. Na área de navegação, clique no ícone **Capacidade de manutenção**  e, em seguida, selecione **Gerenciamento de serviço**.
2. Na área de janela de conteúdo, clique em **Gerenciar conectividade de saída**.
3. Selecione a guia para o tipo de conectividade de saída que você escolheu para seu HMC (conectividade VPN ou SSL da Internet).

Nota: Se a conexão para o serviço e suporte não existir, configure a conexão do serviço antes de continuar com este procedimento. Para obter instruções sobre como configurar uma conexão para o serviço e suporte, consulte Configurando seu Servidor para Conectar ao Serviço e Suporte IBM.

4. Clique em **Testar**.
5. Verifique se o teste é concluído com êxito.

Se o teste não for bem-sucedido, solucione o problema de conectividade e corrija o problema antes de continuar com este procedimento. Como alternativa, é possível obter a atualização no DVD.

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

6. Continue com [“Etapas 2. Visualizar o Nível de Código de Máquina do HMC Existente”](#) na página 94.

Etapas 2. Visualizar o Nível de Código de Máquina do HMC Existente

Sobre Esta Tarefa

Para visualizar o nível de código de máquina do HMC existente, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título Informações do driver atual do HMC, incluindo: versão, liberação, nível de manutenção, nível de construção e versões base do HMC.
4. Continue com [“Etapas 3. Visualizar os Níveis de Código de Máquina do HMC Disponíveis”](#) na página 95.

Etapa 3. Visualizar os Níveis de Código de Máquina do HMC Disponíveis

Sobre Esta Tarefa

Para visualizar os níveis de código de máquina do HMC disponíveis, conclua as etapas a seguir:

Procedimento

1. A partir de um computador ou servidor com uma conexão da Internet, acesse <http://www.ibm.com/eserver/support/fixes>.
2. Selecione a família apropriada na lista de família de produtos.
3. Selecione **Hardware Management Console** na lista de produtos ou tipos de correção.
4. Clique em **Continuar**.
O site do Hardware Management Console é exibido.
5. Role para baixo até o seu nível de Versão do HMC para visualizar os níveis do HMC disponíveis.
Nota: Se você preferir, é possível entrar em contato com o serviço e suporte.
6. Continue com “[Etapa 4. Aplicar a Atualização de Código de Máquina do HMC](#)” na página 95.

Etapa 4. Aplicar a Atualização de Código de Máquina do HMC

Sobre Esta Tarefa

Para aplicar a atualização de código de máquina do HMC, conclua as etapas a seguir:

Procedimento

1. Antes de instalar atualizações para o código de máquina do HMC, faça backup das informações críticas do console em seu HMC.
Para obter instruções, consulte “[Fazendo backup de dados do console de gerenciamento](#)” na página 92. Em seguida, continue com a próxima etapa.
2. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**.
3. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**. O Install Corrective Service Wizard é aberto.
4. Siga as instruções no assistente para instalar a atualização.
5. Encerre e, em seguida, reinicie o HMC para que a atualização entre em vigor.
6. Clique em **Log on and launch the Hardware Management Console web application**.
7. Efetue login na interface do HMC.

Etapa 5. Verificar se a Atualização do Código de Máquina do HMC Foi Instalada com Sucesso

Sobre Esta Tarefa

Para verificar se a atualização de código de máquina do HMC foi instalada corretamente, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Gerenciamento de console**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título Informações do driver atual do HMC, incluindo: versão, liberação, nível de manutenção, nível de construção e versões base do HMC.
4. Verifique se a versão e a liberação correspondem à atualização que você instalou.
5. Se o nível de código exibido não for o nível que você instalou, execute as etapas a seguir:
 - a. Selecione a conexão de rede no HMC.
 - b. Tente novamente a atualização de firmware usando um repositório diferente.
 - c. Se o problema persistir, entre em contato com seu próximo nível de suporte.

Obtendo e Aplicando Atualizações de Código de Máquina para o HMC Usando o DVD ou um Servidor FTP

Aprenda como obter atualizações de código de máquina para o Hardware Management Console (HMC) usando DVD ou um servidor FTP.

Sobre Esta Tarefa

Para obter atualizações de código de máquina do HMC, conclua todas as etapas.

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

Etapas 1. Visualizar o Nível de Código de Máquina do HMC Existente

Antes de Iniciar

Para visualizar o nível de código de máquina do HMC existente, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Gerenciamento de console**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título Informações do driver atual do HMC, incluindo: versão, liberação, nível de manutenção, nível de construção e versões base do HMC.
4. Continue com [“Etapas 2. Visualizar os Níveis de Código de Máquina do HMC Disponíveis” na página 96.](#)

Etapas 2. Visualizar os Níveis de Código de Máquina do HMC Disponíveis

Antes de Iniciar

Para visualizar os níveis de código de máquina do HMC disponíveis, conclua as etapas a seguir:

Sobre Esta Tarefa

Procedimento

1. Em um computador ou servidor com uma conexão de Internet, acesse o website [Fix Central](#).
2. Role para baixo até o seu nível de Versão do HMC para visualizar os níveis do HMC disponíveis.

Nota: Se você preferir, é possível entrar em contato com o serviço e suporte IBM.

3. Continue com [“Etapa 3. Obter a Atualização de Código de Máquina do HMC”](#) na página 97.

Etapa 3. Obter a Atualização de Código de Máquina do HMC

Antes de Iniciar

Para obter a atualização de código de máquina do HMC, conclua as etapas a seguir:

Sobre Esta Tarefa

É possível pedir a atualização de código de máquina do HMC por meio do website do Fix Central, entrar em contato com o serviço e suporte ou fazer download dela em um servidor FTP.

Pedindo a atualização de código de máquina do HMC por meio do website Fix Central

1. Em um computador ou servidor com uma conexão de Internet, acesse o website [Fix Central](#).
2. Em Supported HMC products, selecione o nível do HMC mais recente.
3. Role para baixo até a área Nomes de arquivos/Pacote e localize a atualização que você deseja pedir.
4. Na coluna Order, selecione **Go**.
5. Clique em **Continue** para efetuar sign in com seu ID IBM.
6. Siga os prompts na tela para enviar seu pedido.

Fazendo o download da atualização de código de máquina do HMC em mídia removível

1. Em um computador ou servidor com uma conexão de Internet, acesse o website [Fix Central](#).
2. Em Supported HMC products, selecione o nível do HMC mais recente.
3. Role para baixo até a área Nomes de arquivos/Pacote e localize a atualização que você deseja fazer download.
4. Clique na atualização que você deseja fazer download.
5. Aceite o contrato de licença e salve a atualização em sua mídia removível.

O que Fazer Depois

Quando concluir, continue com [“Etapa 4. Aplicar a Atualização de Código de Máquina do HMC”](#) na página 97.

Etapa 4. Aplicar a Atualização de Código de Máquina do HMC

Antes de Iniciar

Para aplicar a atualização de código de máquina do HMC, conclua as etapas a seguir:

Procedimento

1. Antes de instalar atualizações para o código de máquina do HMC, faça backup dos dados do HMC. Para obter informações adicionais, consulte [“Fazendo backup de dados do console de gerenciamento”](#) na página 92.
2. Se você obteve ou criou a atualização no DVD-RAM, insira-a na unidade de DVD no HMC. Se você obteve ou criou a atualização em um dispositivo de memória USB, insira o dispositivo de memória.

3. Antes de instalar atualizações para o código de máquina do HMC, faça backup das informações críticas do console em seu HMC.

Para obter instruções, consulte [“Fazendo backup de dados do console de gerenciamento”](#) na página 92. Em seguida, continue com a próxima etapa.



4. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Gerenciamento de console**.
5. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**. O Install Corrective Service Wizard é aberto.
6. Siga as instruções no assistente para instalar a atualização.
7. Encerre, reinicie e efetue login novamente no HMC para que a atualização entre em vigor.
8. Continue com [“Etapa 5. Verificar se a Atualização do Código de Máquina do HMC Foi Instalada com Sucesso”](#) na página 98.

Etapa 5. Verificar se a Atualização do Código de Máquina do HMC Foi Instalada com Sucesso

Antes de Iniciar

Para verificar se a atualização de código de máquina do HMC foi instalada com êxito, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Gerenciamento de console**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título Informações do driver atual do HMC, incluindo: versão, liberação, nível de manutenção, nível de construção e versões base do HMC.
4. Verifique se a versão e a liberação correspondem à atualização que você instalou.
5. Se o nível de código que é exibido não for o nível que você instalou, execute as seguintes etapas:
 - a. Tente novamente a atualização de código de máquina. Se você criou um DVD para este procedimento, use uma nova mídia.
 - b. Se o problema persistir, entre em contato com seu próximo nível de suporte.

Fazendo Upgrade de seu Software do HMC

Aprenda como fazer upgrade do software em um HMC de uma liberação para a outra enquanto mantém seus dados de configuração do HMC.

Sobre Esta Tarefa

Para fazer upgrade do código de máquina em um HMC, conclua todas as etapas.

Nota: Para o 7063-CR1 e o 7063-CR2, dos modelos do HMC, é possível conectar uma unidade de DVD de USB externa.

Etapa 1. Obter o Upgrade

Sobre Esta Tarefa

É possível pedir o upgrade de código de máquina do HMC por meio do website [Fix Central](#).

Para obter o upgrade por meio do website [Fix Central](#), conclua as etapas a seguir:

Procedimento

1. Em um computador ou servidor com uma conexão de Internet, acesse o website do Hardware Management Console em <http://www-933.ibm.com/support/fixcentral/>.
2. Clique em **Continuar**.
O site do Hardware Management Console é exibido.
3. Navegue para a versão do HMC para a qual você deseja fazer o upgrade.
4. Localize a seção de download e pedidos.

Nota: Se você não tiver acesso à Internet, entre em contato com o serviço e suporte IBM para pedir o upgrade em DVD.

5. Siga os prompts na tela para enviar seu pedido.
6. Depois que você tiver o upgrade, continue com [“Etapa 2. Visualizar o Nível de Código de Máquina do HMC Existente”](#) na página 99.

Etapa 2. Visualizar o Nível de Código de Máquina do HMC Existente

Sobre Esta Tarefa

Para determinar o nível existente de código de máquina em um HMC, siga estas etapas:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**. Na área de navegação, clique em **Updates**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título Informações atuais do driver HMC, incluindo a versão, liberação, nível de manutenção, nível de construção e versões base do HMC.
4. Continue com [“Etapa 3. Fazer Backup dos Dados do Perfil do Sistema Gerenciado”](#) na página 99.

Etapa 3. Fazer Backup dos Dados do Perfil do Sistema Gerenciado

Sobre Esta Tarefa

Para fazer backup dos dados do perfil do sistema gerenciado, conclua as etapas a seguir:

Procedimento

1. Selecione o sistema em que deseja salvar os dados do perfil.
2. Clique em **Ações > Visualizar todas as ações > Anterior > Gerenciar dados de partição > Backup**.
3. Digite um nome de arquivo de backup e registre essas informações.
4. Clicar em **OK**.
5. Repita essas etapas para cada sistema.
6. Continue com [“Etapa 4. Fazer Backup dos Dados do HMC”](#) na página 100.

Etapa 4. Fazer Backup dos Dados do HMC

Sobre Esta Tarefa

Faça backup de dados do HMC antes de instalar uma nova versão do software do HMC para que níveis anteriores possam ser restaurados no evento de um problema ao fazer upgrade do software. Não use esses dados críticos do console após um upgrade bem-sucedido para uma nova versão do software do HMC.

Nota: Para fazer backup em mídia removível, é necessário ter essa mídia disponível.

Para fazer backup dos dados do HMC, conclua as etapas a seguir:

Procedimento

1. Se você planeja fazer backup em mídia, execute as etapas a seguir para formatar a mídia:

- a. Insira a mídia na unidade.

- b. Na área de navegação, clique no ícone **Capacidade de manutenção**  e, em seguida, selecione **Gerenciamento de serviço**.

- c. Na área de janela de conteúdo, clique em **Formatar mídia**.

- d. Selecione o tipo de mídia.

- e. Selecione o tipo de formato.

- f. Clicar em **OK**.

2. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**.

3. Na área de janela de conteúdo, clique em **Fazer backup dos dados do console de gerenciamento**.

A janela **Fazer backup dos dados do console de gerenciamento** é aberta.

4. Selecione uma opção de archive.

É possível fazer backup em mídia em um sistema local, em um sistema remoto montado no sistema de arquivos do HMC (por exemplo, NFS) ou enviar o backup para um site remoto usando o Protocolo de Transferência de Arquivos (FTP).

- Para fazer backup em um sistema local, escolha **Back up to media on local system** e siga as instruções.
- Para fazer backup em um sistema remoto montado, escolha **Back up to mounted remote system** e siga as instruções.
- Para fazer backup em um site FTP remoto, escolha **Send back up critical data to remote site** e siga as instruções.

5. Continue com [“Etapa 5. Registrar as Informações de Configuração do HMC Atuais” na página 100.](#)

Etapa 5. Registrar as Informações de Configuração do HMC Atuais

Sobre Esta Tarefa

Antes de fazer upgrade para uma nova versão do software do HMC, como uma medida de precaução, registre as informações de configuração do HMC.

Para registrar a configuração do HMC atual, conclua as etapas a seguir:

Procedimento

1. Selecione um sistema gerenciado ou qualquer partição em que você deseja registrar as informações de configuração do HMC.
2. No pod do menu, selecione **Ações > Planejar operações**.
Todas as operações planejadas para o destino que você selecionou são exibidas.
3. Selecione **Sort > By Object**.
4. Selecione cada objeto e registre os detalhes a seguir:
 - Nome do Objeto
 - Data de planejamento
 - Horário da Operação (exibido no formato 24 horas)
 - Repetitivo (se Sim, conclua as etapas a seguir):
 - a. Selecione **View > Schedule Details**.
 - b. Registre as informações do intervalo.
 - c. Feche a janela de operações planejadas.
 - d. Repita para cada operação planejada.
5. Feche a janela **Customizar operações planejadas**.
6. Continue com [“Etapa 6. Registrar o Status do Comando Remoto”](#) na página 101.

Etapa 6. Registrar o Status do Comando Remoto

Sobre Esta Tarefa

Para registrar o status do comando remoto, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Usuários e segurança**  e, em seguida, selecione **Segurança de sistemas e do console**.
2. Na área de janela de conteúdo, clique em **Ativar execução de comando remoto**.
3. Registre se a caixa de seleção **Enable remote command execution using the ssh facility** está selecionada.
4. Clique em **Cancel**.
5. Continue com [“Etapa 7. Salvar Dados de Upgrade”](#) na página 101.

Etapa 7. Salvar Dados de Upgrade

Sobre Esta Tarefa

É possível salvar a configuração do HMC atual em uma partição de disco designada no HMC ou na mídia local. Salve os dados de upgrade somente imediatamente antes de fazer upgrade do software do HMC para uma nova liberação. É possível restaurar as definições de configuração do HMC após o upgrade.

Nota: Somente um nível de dados de backup é permitido. Cada vez que você salva dados de upgrade, o nível anterior é sobrescrito.

Para salvar dados de upgrade, conclua as etapas a seguir:

Procedimento

1. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**.
 2. Na área de janela de conteúdo, clique em **Salvar dados de upgrade**. O assistente **Salvar dados de upgrade** é aberto.
 3. Selecione a mídia na qual você deseja salvar os dados de upgrade. Se você escolher salvar em mídia removível, insira a mídia agora. Clique em **Next**.
 4. Clique em **Concluir**.
 5. Aguarde a tarefa ser concluída.
Se a tarefa Salvar Dados de Upgrade falhar, entre em contato com seu próximo nível de suporte antes de continuar.
- Nota:** Se a tarefa salvar dados de upgrade falhar, não continue o processo de upgrade.
6. Clicar em **OK**.
 7. Continue com [“Etapa 8. Fazer Upgrade do Software do HMC”](#) na página 102.

Etapa 8. Fazer Upgrade do Software do HMC

Sobre Esta Tarefa

Para fazer upgrade do software do HMC, reinicie o sistema com a mídia removível na unidade de DVD.

Procedimento

1. Insira a mídia de Instalação do Produto HMC na unidade de DVD.
 2. Na área de navegação, clique no ícone **Gerenciamento do HMC**  e, em seguida, selecione **Gerenciamento de console**.
 3. Na área de janela de conteúdo, selecione **Encerrar ou reiniciar o console de gerenciamento**.
 4. Assegure-se de que **Restart the HMC** esteja selecionado.
 5. Clicar em **OK**.
O HMC reinicia e as informações do sistema rolam na janela.
 6. Selecione **Upgrade** e clique em **Next**.
 7. Escolha dentre as opções a seguir:
 - Se você salvou os dados de upgrade durante a tarefa anterior, continue com a próxima etapa.
 - Se você não salvou os dados de upgrade anteriormente neste procedimento, deve-se salvar os dados de upgrade agora antes de continuar.
 8. Selecione **Upgrade from media** e clique em **Next**.
 9. Confirme as configurações e clique em **Finish**.
 10. Siga os avisos.
- Nota:**
- Se a tela ficar em branco, pressione a barra de espaço para visualizar as informações.
 - O primeiro DVD pode levar aproximadamente 20 minutos para instalação.
11. No prompt de login, efetue login usando seu ID do usuário e senha.
A instalação do código do HMC está concluída.
 12. Continue com [“Etapa 9. Verificar se o Upgrade do Código de Máquina do HMC Foi Instalado com Sucesso”](#) na página 103.

Etapla 9. Verificar se o Upgrade do Código de Máquina do HMC Foi Instalado com Sucesso

Sobre Esta Tarefa

Para verificar se o upgrade do HMC foi instalado com êxito, conclua as etapas a seguir:

Procedimento



1. Na área de navegação, clique no ícone **Gerenciamento do HMC** e, em seguida, selecione **Gerenciamento de console**.
2. Na área de janela de conteúdo, clique em **Atualizar o Hardware Management Console**.
3. Na nova janela, visualize e registre as informações que aparecem sob o título Informações atuais do driver HMC, incluindo a versão, liberação, nível de manutenção, nível de construção e versões base do HMC.
4. Verifique se a versão e a liberação correspondem à atualização que você instalou.
5. Se o nível de código exibido não for o nível que você instalou, tente novamente a tarefa de upgrade usando um novo DVD. Se o problema persistir, entre em contato com seu próximo nível de suporte.

Fazendo upgrade do HMC do local remoto usando imagens de upgrade de rede

Aprenda como fazer upgrade do software em um HMC de um local remoto usando imagens de upgrade de rede.

Sobre Esta Tarefa

Aprenda como fazer upgrade do software em um HMC de um local remoto usando imagens de upgrade de rede.

Procedimento

1. De um computador ou servidor com uma conexão de Internet, acesse o website de suporte e downloads do Hardware Management Console (<http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html>).
2. Faça download das imagens de rede apropriadas do HMC V9 e salve-as em um servidor FTP. Não é possível fazer o download desses arquivos diretamente para o HMC. Você deve fazer o download dos arquivos de imagem em um servidor que aceite solicitações FTP.
3. Assegure-se em fazer o download dos seguintes arquivos:
 - img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. Salve os dados do upgrade no HMC. Execute os comandos a seguir para salvar os dados de upgrade:
 - Para salvar os dados em DVD e HDD, execute os comandos a seguir:
mount /media/cdrom
saveupgdata -r diskdvd
 - Para salvar os dados no HDD, execute o comando a seguir:
saveupgdata -r disk

5. Copie os arquivos de upgrade para a partição de disco inicializável no HMC. Execute o comando **getupgfiles** para copiar os arquivos

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

Em que,

- **ftp server** é o nome do host ou endereço IP do servidor FTP no qual você faz download das imagens de rede do HMC.
 - **user id** é um ID do usuário válido no servidor FTP. Se não especificar a senha com o argumento **--passwd**, você será solicitado uma senha.
 - **remote directory** é o diretório no seu servidor FTP onde as imagens de rede do HMC estão salvas.
6. Reinicie o HMC para fazer upgrade do código que é copiado para a partição de disco inicializável. Execute o **chhmc -c altdiskboot -s enable -- mode upgrade** para reiniciar o HMC.
 7. Reinicie o HMC e inicie o upgrade. Execute o comando **hmcshutdown -r -t now** para começar o upgrade.

Protegendo o HMC

Aprenda como aprimorar a segurança de seu Hardware Management Console (HMC) que é baseada nos padrões de segurança corporativa.

A configuração padrão do HMC fornece ampla segurança para a maioria dos usuários corporativos. Com o Hardware Management Console (HMC) Versão 8.4.0, ou mais recente, é possível aprimorar ainda mais a segurança do HMC que é baseada em seus padrões de segurança corporativa. Para aprimorar a segurança para o HMC, deve-se configurar o HMC para um nível mínimo de segurança 1. É possível escolher a segurança de Nível 2 e Nível 3 dependendo do seu ambiente e dos requisitos de segurança corporativa.

Nota: Antes de mudar o nível de segurança, verifique com sua equipe de conformidade de segurança corporativa.

Segurança de Nível 1

Para proteger o HMC (segurança nível 1), conclua as etapas a seguir:

1. Mude a senha predefinida para o usuário **hscroot**. Para obter mais informações sobre a política de senha, consulte [“Política de Senha Avançada”](#) na página 106.
2. Se o HMC não pertencer a um ambiente seguro fisicamente, configure a senha **grub** executando o comando a seguir: **chhmc -c grubpasswd -s enable --passwd <new grub password>**
3. Se você tiver configurado o Módulo de gerenciamento integrado (IMM) no HMC, configure uma senha IMM forte.
4. Configure uma senha forte para o usuário **admin** e usuários gerais em todos os servidores.
5. Atualize o HMC com as correções de segurança liberadas mais recentes. Para obter mais informações sobre correções de segurança, consulte [IBM Fix Central](#).

Segurança Nível 2

Se você tiver múltiplos usuários, conclua as etapas a seguir para aprimorar a segurança para o HMC:

1. crie uma conta para cada usuário no HMC e designe as funções e recursos necessários aos usuários. Para obter mais informações sobre as várias funções no HMC, consulte [Tarefas do HMC, funções do usuário, IDs e comandos associados](#).

Nota: Assegure-se de designar apenas os recursos e funções necessários para usuários que são criados no HMC. Se necessário, também é possível criar funções customizadas.

2. Ative a replicação de dados do usuário entre diferentes Hardware Management Consoles. A replicação de dados do usuário pode ser executada no modo Mestre-escravo ou no modo Peer-Peer. Para obter mais informações sobre replicação de dados do usuário, consulte [Gerenciar replicação de dados](#).

3. Importe um certificado que seja assinado pela Autoridade de certificação.

Segurança Nível 3

Se você tiver múltiplos Hardware Management Consoles e administradores do sistema, conclua as etapas a seguir para aprimorar a segurança para o HMC:

1. Use a autenticação centralizada, como o Lightweight Directory Access Protocol (LDAP) ou Kerberos. Para obter mais informações sobre configurar o LDAP, consulte [Como configurar o LDAP no HMC](#).
2. Ative a replicação de dados do usuário entre diferentes Hardware Management Consoles.
3. Assegure-se de que o HMC esteja no [modo NIST SP 800-131A](#) para que o HMC use somente cifras fortes.
4. Bloqueie portas que não sejam necessárias no firewall. Para obter informações sobre as portas do HMC que possam ser usadas, consulte a tabela a seguir:

Tabela 32. Porta usada pelo usuário para interação com o HMC				
Porta	Descrição	Tipo	Versão do protocolo (modo padrão)	Versão do protocolo (modo NIST)
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	Agente SNMP	UDP	SNMP v3	SNMP v3
162	Trap de SNMP	UDP	SNMP v3	SNMP v3
427	SLP	UDP	Não disponível	Não disponível
443	GUI e API de REST do HMC	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (texto sem formatação + hash e sinal)	RSCT (texto sem formatação + hash e sinal)
2300	Terminal 5250 para IBM i	TCP	Texto corrido	Texto corrido
2301	Terminal seguro 5250 para IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (porta anterior, não funcional)	TCP	Não funcional	Não funcional
9900	FCS: descoberta de HMC-HMC	UDP	FCS	FCS
9920	FCS: comunicação de 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 de REST do HMC (porta anterior)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)

Tabela 32. Porta usada pelo usuário para interação com o HMC (continuação)				
Porta	Descrição	Tipo	Versão do protocolo (modo padrão)	Versão do protocolo (modo NIST)
12347	Domínio do mesmo nível RSCT	UDP	RSCT (texto sem formatação + hash e sinal)	RSCT (texto sem formatação + hash e sinal)
12348	Domínio do mesmo nível RSCT	UDP	RSCT (texto sem formatação + hash e sinal)	RSCT (texto sem formatação + hash e sinal)

Notas:

- Deve-se usar somente SSH (porta 22), HTTPS (porta 443 e porta 12443), terminal seguro 5250 para IBM i (porta 2301) e VTerm (porta 9960) que são expostos a uma intranet. Todas as outras portas devem ser usadas em uma rede privada ou isolada. É possível usar uma porta Ethernet separada e VLAN para o Resource Monitoring and Control (RMC) (porta 657), FCS (porta 9900 e porta 9920) e Domínio do mesmo nível RSCT (porta 12347 e porta 12348).
- As portas listadas no comando **netstat** são usadas apenas para processos internos.

Política de Senha Avançada

É possível forçar os requisitos de senha para usuários localmente autenticados usando o Hardware Management Console (HMC). A função de política de senha avançada permite que o administrador do sistema configure as restrições de senha. A política de senha aprimorada se aplica aos sistemas nos quais um HMC está instalado.

Os administradores do sistema podem usar a política de senha aprimorada para definir uma única política de senha para todos os usuários. O HMC fornece uma política de senha de segurança média, que pode ser ativada pelos administradores do sistema para configurar as restrições da senha. O administrador do sistema também pode escolher ativar a política de segurança média ou uma nova política definida pelo usuário. A política da senha de segurança média do HMC não pode ser removida do sistema. A tabela a seguir lista os atributos da política de segurança média e os valores padrão.

Tabela 33. Atributos de Senha para a Política da Senha de Segurança Média HMC		
Atributo	Descrição	Valor padrão
min_pwage	O número mínimo de dias para os quais uma senha deve permanecer ativa.	1
pwage	O número máximo de dias para os quais uma senha pode permanecer ativa.	180
min_length	O comprimento mínimo de uma senha.	8
hist_size	O número de senhas salvas anteriormente que não podem ser reusadas.	10
warn_pwage	Quando a senha está prestes a expirar, o número de dias antes dos quais um usuário é avisado de que a senha está prestes a expirar.	7
min_digits	O número mínimo de dígitos que são necessários para serem usados na senha.	None
min_uppercase	O número mínimo de caracteres maiúsculos.	1
min_lowercase	O número mínimo de caracteres minúsculos.	6

Tabela 33. Atributos de Senha para a Política da Senha de Segurança Média HMC (continuação)		
Atributo	Descrição	Valor padrão
min_special_chars	O número mínimo de caracteres especiais que devem ser usados na senha.	None

Considere os itens a seguir sobre a política de senha de segurança média do HMC:

- A política não se aplica aos IDs de usuário **hscroot**, **hscpe** e **root**.
- A política afeta somente os usuários autenticados localmente que são gerenciados pelo HMC e a política não pode ser forçada no LDAP ou usuários Kerberos.
- A política de senha de segurança média do HMC ou a política definida pelo usuário permite que os administradores do sistema configurem restrições de reutilização de senha.
- A senha de segurança média do HMC é apenas para leitura e os atributos da senha de segurança média do HMC não podem ser alterados. É possível criar uma nova senha definida pelo usuário para configurar a restrição da senha.

É possível usar os seguintes comandos para configurar a política da senha de segurança média do HMC:

mkpwdpolicy

Importa a política de senha de um arquivo, que contém todos os parâmetros ou cria uma política de senha.

lspwdpolicy

Lista todos os perfis de política de senha disponíveis e procura parâmetros específicos. Também é possível visualizar a política de senha que está ativa atualmente.

rmpwdpolicy

Remove uma política de senha inativa existente.

Nota: Não é possível remover uma política de segurança média ativa e a política de senha somente leitura padrão.

chpwdpolicy

Muda parâmetros de uma política de senha inativa.

Resolvendo problemas comuns ao proteger o HMC

Aprenda a resolver alguns problemas que você pode encontrar ao proteger o HMC.

Como proteger a conexão entre o Hardware Management Console (HMC) e o sistema?

O HMC se conecta ao sistema por meio do Processador de serviços flexível (FSP). Um protocolo binário proprietário chamado Network Client (NETC) é usado para gerenciar o FSP e o hypervisor Power. A tabela a seguir lista as portas que são usadas pelo HMC:

Tabela 34. Portas no FSP que são usadas para interagir com o HMC			
Porta no FSP	Descrição	Versão do protocolo (modo padrão)	Versão do protocolo (modo NIST)
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). Recorre ao SSLv3 para suporte de firmware mais antigo.	NETC (TLS 1.2)

Tabela 34. Portas no FSP que são usadas para interagir com o HMC (continuação)

Porta no FSP	Descrição	Versão do protocolo (modo padrão)	Versão do protocolo (modo NIST)
30001	VTerm	NETC (TLS 1.2). Recorre ao SSLv3 para suporte de firmware mais antigo.	NETC (TLS 1.2)

Como bloquear o HMC?

Se desejar aprimorar a segurança para sua infraestrutura, será possível usar um dispositivo do Sistema de prevenção de intrusão (IPS) ou incluir todos os Hardware Management Consoles e servidores IBM Power Systems atrás de um firewall. Além disso, é possível desativar serviços de rede no HMC se você não os usa remotamente ou se deseja bloquear o HMC. Para desativar serviços de rede no HMC, conclua as etapas a seguir:

1. Desative a [execução de comando remoto](#) usando a porta SSH.
2. Desative o [terminal virtual remoto](#) (porta VTerm).
3. Desative o [acesso à web remoto](#) (interface com o usuário HMC e API de REST).
4. Bloqueie portas no firewall usando as configurações de rede do HMC para cada porta Ethernet configurada.

Como configurar o HMC no modo de conformidade NIST SP 800-131A?

Com o HMC Versão 8.1.0, ou mais recente, quando você configura o HMC no modo de conformidade, apenas cifras fortes listadas pelo NIST SP 800-131A são suportadas. Talvez você não possa se conectar a servidores Power Systems mais antigos, como servidores POWER5 que não suportam a Segurança da Camada de Transporte (TLS 1.2). Para obter mais informações sobre mudar o modo de segurança, consulte [Modo HMC V8R8 NIST](#).

Como visualizar e mudar cifras que são usadas pelo HMC?

Com o HMC Versão 8.1.0, ou mais recente, o HMC suporta conjuntos de cifras mais seguros que são definidos no NIST 800-131A. As cifras que são usadas no modo padrão são fortes. Para obter mais informações sobre cifras de criptografia que são usadas pelo HMC, execute o comando **lshmcencr**. Se seus padrões corporativos requererem o uso de um conjunto de cifras diferente, execute o comando **chhmcencr** para modificar as cifras de criptografia.

Para listar as cifras de criptografia que são usadas pelo HMC para criptografar a senha de usuário, execute o comando a seguir:

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

Para listar as cifras de criptografia que podem ser usadas atualmente pela interface com o usuário da web do HMC e a API de REST, execute o comando a seguir:

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

Para listar as cifras de criptografia e o algoritmo MAC que pode ser usado atualmente pela interface SSH do HMC, execute o comando a seguir:

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

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

Como verificar a intensidade do certificado no HMC?

Os certificados autoassinados no HMC usam SHA256 com criptografia RSA de 2.048 bits, o que é forte. Se você estiver usando certificados assinados por CA, assegure-se de que não esteja usando a criptografia de 1.024 bits, que é fraca. Os certificados a seguir podem ser usados para o HMC:

- O certificado assinado por CA pode ser usado para a interface gráfica com o usuário do HMC e a API de REST (portas 443 e 12443).
- A porta 9920 é usada para comunicação HMC com HMC. Não é possível substituir esse certificado pelo seu próprio certificado.

Como escolher entre um certificado autoassinado (padrão) ou um certificado assinado por CA?

O HMC gera automaticamente um certificado durante a instalação. Entretanto, é possível gerar uma Solicitação de assinatura de certificado (CSR) do HMC e obter um novo certificado que é emitido por uma autoridade de certificação. É possível importar esse certificado no HMC. Assegure-se de também obter um nome de domínio para o HMC. Para obter mais detalhes sobre gerenciar os certificados no HMC, consulte [Gerenciar certificados](#).

Como auditar o HMC?

A auditoria nos Hardware Management Consoles foca nas cifras configuradas e na atividade de uso de vários usuários do HMC. Use os comandos a seguir para visualizar a atividade de uso de vários usuários do HMC:

Tabela 35. Cifras que são usadas pelo HMC	
Finalidade	Comando
Criptografia de senha (configuração global)	<code>lshmcencr -c passwd -t c</code>
Criptografia de senha para cada usuário	<code>lshmcusr -Fname:password_encryption</code>
Cifras SSH	<code>lshmcencr -c ssh -t c</code>
MAC SSH	<code>lshmcencr -c sshmac -t c</code>
Cifra que é usada para a interface gráfica com o usuário do HMC e a API de REST	<code>lshmcencr -c webui -t c</code>

Use os comandos a seguir para monitorar várias informações de console e eventos que permitem manutenção para usos no HMC:

Tabela 36. Comandos para visualizar os usuários com login efetuado e informações de console ou eventos que permitem manutenção no HMC	
Informações	Comando
Usuários da GUI	<code>lslogon -r webui -u</code>
Tarefas da GUI	<code>lslogon -r webui -t</code>
Usuários da CLI	<code>lslogon -r ssh -u</code>
Tarefas da CLI	<code>lslogon -r ssh -t</code>
Operações no HMC	<code>lssvcevents -t console -d <number of days></code>
Operações no sistema	<code>lssvcevents -t hardware -m <managed system> -d <number of days></code>

Eventos de monitoramento centralizados para o HMC: se você tiver muitos Hardware Management Consoles, configure o arquivo `rsyslog` para coletar todos os dados de uso.

Como o IBM corrige as vulnerabilidades de segurança do HMC?

A IBM tem um processo de resposta de incidentes de segurança chamado IBM Product Security Incident Response Team (PSIRT). A IBM Product Security Incident Response Team (PSIRT) é uma equipe global que gerencia o recebimento, a investigação e a coordenação interna de informações de vulnerabilidades de segurança relacionadas a ofertas da IBM. Os componentes de software livre e da IBM que são enviados com o HMC são monitorados e analisados ativamente. Correções temporárias e correções de segurança são fornecidas pela IBM para todas as liberações suportadas do HMC.

Como rastrear novas correções temporárias no HMC?

O boletim de segurança contém informações sobre a vulnerabilidade e as correções temporárias para versões suportadas do HMC. Para rastrear correções temporárias no HMC, é possível:

- Procurar os boletins de segurança mais recentes no [IBM Security Bulletin](#).
- Siga [@IBMPowerSupp](#) no Twitter para obter notificações.
- Assine notificações por e-mail no [Suporte IBM](#).

Perfis de segurança: Global Data Protection Regulation (GDPR) e Padrão de Segurança de Dados do Setor de Cartão de Pagamento (PCI-DSS)

Aprenda como o Hardware Management Console (HMC) trata as informações de privacidade dos usuários.

O Hardware Management Console (HMC) é um dispositivo fechado que não armazena nenhum dado do dono do cartão. Portanto, apenas um subconjunto de requisitos e procedimentos de avaliação de segurança de TI que são definidos por PCI-DSS são aplicáveis para o HMC. Apenas o código confiável que é distribuído pela IBM pode ser instalado no HMC. Quando qualquer vulnerabilidade é conhecida por meio do [processo IBM PSIRT](#), correções temporárias são publicadas. Os requisitos e recomendações incluem os itens a seguir:

Consultas GDPR

Tabela 37. Consultas GDPR . A tabela fornece informações sobre as perguntas relacionadas ao GDPR.	
Perguntas	Respostas
Que tipo de dados são armazenados no HMC?	O HMC armazena informações de configuração do hardware Power, virtualização de PowerVM e as informações de métricas de desempenho.
O HMC processa algum dado pessoal?	É possível fornecer informações de contato para a função call home. Fornecer informações de contato para a função call home é opcional.
Quais contas predefinidas são usadas para administração do sistema do HMC?	O usuário administrador do sistema usa o nome do usuário <code>hscroot</code> .
Alguma das contas no HMC está relacionada a uma pessoa específica?	No.
É obrigatório fornecer dados pessoais no HMC?	Não. Você não precisa fornecer informações de dados pessoais. Entretanto, fornecer essas informações é opcional.
O arquivo de log do HMC tem alguma informação de dados pessoais?	No.

Tabela 37. Consultas GDPR . A tabela fornece informações sobre as perguntas relacionadas ao GDPR. (continuação)

Perguntas	Respostas
É possível excluir dados pessoais completa e permanentemente?	Sim. Desconfigure a função call home.

Consultas PCI-DSS

Tabela 38. Consultas PCI-DSS . A tabela fornece informações sobre as perguntas relacionadas a PCI-DSS

Perguntas	Respostas
Como instalar e manter uma configuração de firewall para proteger os dados do titular do cartão?	O HMC não armazena nem acessa nenhum dado do titular do cartão. Entretanto, o HMC tem uma configuração de firewall e o usuário pode controlar e ativar portas específicas.
Posso usar o valor padrão fornecido pelo fornecedor para senhas do sistema e outros parâmetros de segurança?	Antes de instalar um sistema na rede, mude todas as senhas predefinidas do usuário <i>hscroot</i> .
Como o HMC protege os dados armazenados do titular do cartão?	O HMC não armazena nem acessa nenhum dado do titular do cartão.
Como o HMC criptografa os dados do titular do cartão quando os dados são transmitidos em redes públicas abertas?	O HMC não armazena nem acessa nenhum dado do titular do cartão.
Como usar e atualizar regularmente programas de software antivírus?	O HMC é um dispositivo fechado. Portanto, o malware não pode infectar o HMC.
Como desenvolver e manter sistemas e aplicativos seguros?	Deve-se instalar as correções necessárias em seu sistema manualmente por meio do website IBM Fix Central . Apenas código confiável distribuído pela IBM pode ser instalado no HMC.
O HMC restringe acesso aos dados do dono do cartão?	O HMC não armazena nem acessa nenhum dado do titular do cartão.
Como designar um ID exclusivo a cada pessoa que tem acesso ao computador?	É possível implementar este requisito assegurando que não haja IDs compartilhados e seguindo as políticas de senha.
Como restringir o acesso físico aos dados do titular do cartão?	O HMC não armazena nem acessa nenhum dado do titular do cartão
Como rastrear e monitorar o acesso a recursos de rede e aos dados do dono do cartão?	O HMC não armazena nem acessa nenhum dado do titular do cartão.
Como o HMC testa a segurança do sistema e processos?	As ferramentas de varredura são usadas para executar varreduras de segurança em todas as versões liberadas do HMC. As ferramentas de varredura incluem: <i>Qualys</i> , <i>Nessus</i> , <i>testssl</i> , <i>ssllscan</i> e <i>ASoC</i> .
Como manter uma política de segurança que inclua segurança de informações para funcionários e contratados?	O administrador do sistema desativa o login do usuário remoto, ativa o login do usuário com base na necessidade e desativa o login do usuário quando o acesso não é mais necessário.

Locais das portas do HMC

É possível localizar os locais das portas usando códigos dos locais. Use as ilustrações dos locais das portas do HMC para mapear um código do local para a posição da porta do HMC no servidor.

Locais da porta do modelo 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S HMC

Use este diagrama e esta tabela para mapear as portas do HMC no 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S.

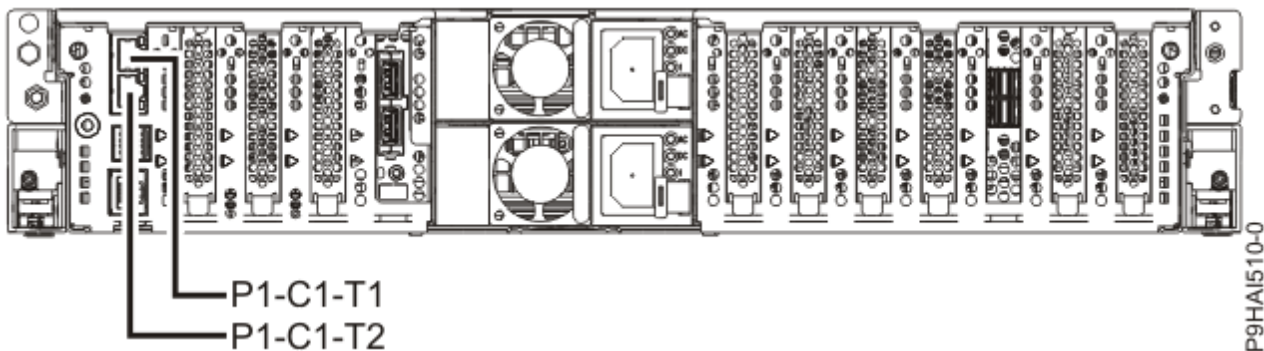


Figura 26. Locais das portas do HMC do 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S

Tabela 39. Locais das portas do HMC do 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H e 9223-22S		
Porta	Código do local físico	Identify LED
Porta 1 do HMC	Un-P1-C1-T1	NÃO
Porta 2 do HMC	Un-P1-C1-T2	Não
Para obter mais informações sobre os locais de porta do HMC no 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H ou 9223-22S, consulte Local da peça e códigos do local para 9008-22L, 9009-22A, 9009-22G, 9223-22H ou 9223-22S .		

Locais da porta do modelo 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S HMC

Use este diagrama e esta tabela para mapear as portas do HMC no 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S.

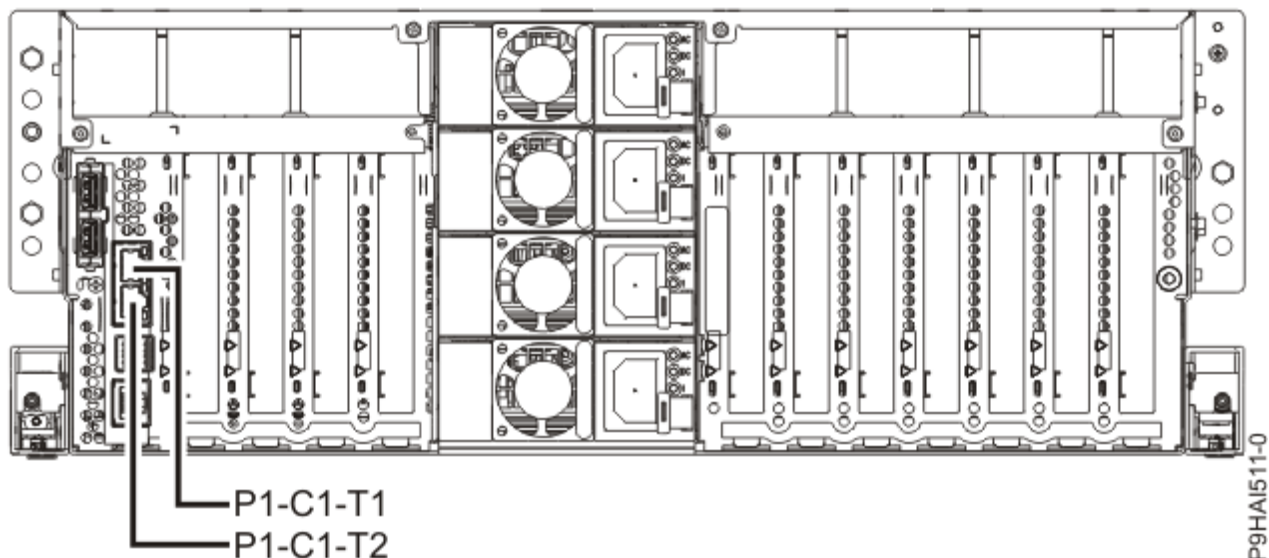


Figura 27. Locais das portas do HMC do 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S

Tabela 40. Locais das portas do HMC do 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H e 9223-42S

Porta	Código do local físico	Identify LED
Porta 1 do HMC	Un-P1-C1-T1	NÃO
Porta 2 do HMC	Un-P1-C1-T2	Não

Para obter mais informações sobre os locais de porta do HMC no 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H ou 9223-42S, consulte [Local da peça e códigos do local para 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H ou 9223-42S](#).

Locais da porta do modelo 9040-MR9 HMC

Use este diagrama e esta tabela para mapear as portas do HMC no 9040-MR9.

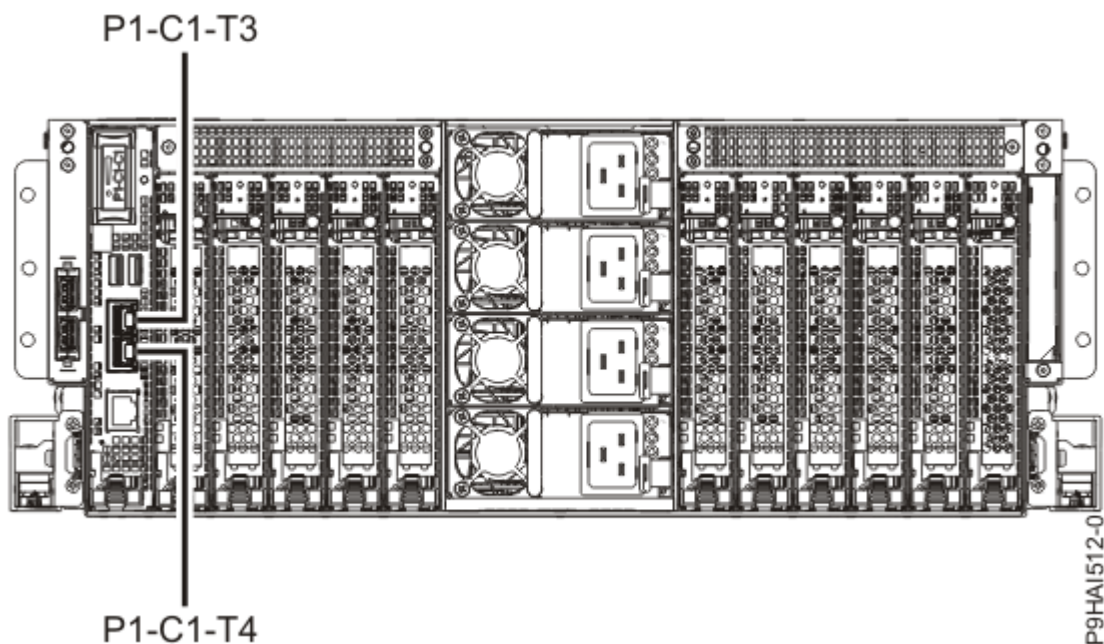


Figura 28. Locais das portas do HMC 9040-MR9

Tabela 41. Locais das portas do HMC 9040-MR9

Porta	Código do local físico	Identify LED
Porta 1 do HMC	Un-P1-C1-T3	NÃO
Porta 2 do HMC	Un-P1-C1-T4	Não

Para obter mais informações sobre os locais da porta do HMC no 9040-MR9, consulte [Local da peça e códigos do local](#).

Locais da porta do modelo 9080-M9S HMC

Use este diagrama e esta tabela para mapear as portas do HMC no 9080-M9S.

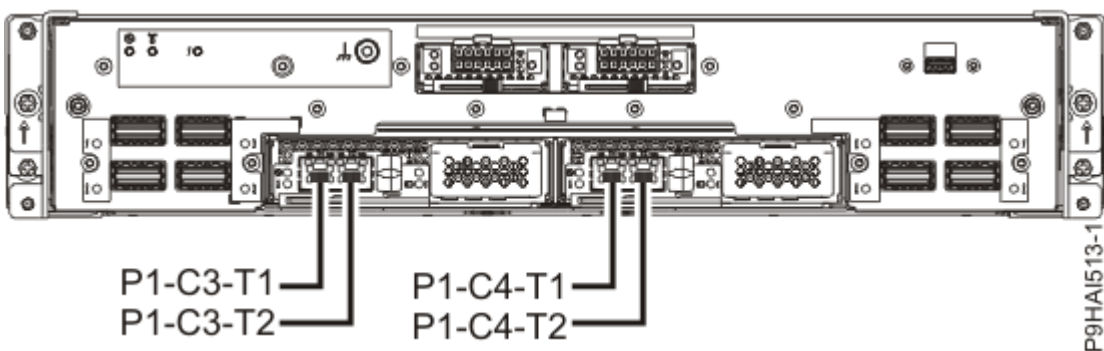


Figura 29. Locais das portas do HMC 9080-M9S

Tabela 42. Locais das portas do HMC 9080-M9S

Porta	Local da porta física	Identify LED
Placa do processador de serviços 1 - Porta 1 do HMC	Un-P1-C3-T1	Não
Placa do processador de serviços 1 - Porta 2 do HMC	Un-P1-C3-T2	NÃO

Tabela 42. Locais das portas do HMC 9080-M9S (continuação)

Porta	Local da porta física	Identify LED
Placa do processador de serviços 2 - Porta 1 do HMC	Un-P1-C4-T1	NÃO
Placa de processador de serviços 2 - Porta 2 do HMC	Un-P1-C4-T2	NÃO
Para obter mais informações sobre os locais da porta do HMC no 9080-M9S, consulte Local da peça e códigos do local .		

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos descritos neste documento. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO LIMITADO ÀS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Todas as referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses Web sites não fazem parte dos materiais desse produto IBM e a utilização desses Web sites é de inteira responsabilidade do Cliente.

A IBM pode usar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os exemplos de clientes e dados de desempenho mencionados são apresentados apenas com propósitos ilustrativos. Os resultados de desempenho reais podem variar, dependendo de configurações e condições operacionais específicas.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a alteração sem aviso prévio. Os preços do revendedor podem variar.

Estas informações foram projetadas apenas com o propósito de planejamento. As informações aqui contidas estão sujeitas a mudanças antes que os produtos descritos estejam disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com pessoas ou empresas reais é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

As ilustrações e especificações contidas aqui não devem ser reproduzidas total ou parcialmente sem a permissão por escrito da IBM.

A IBM preparou essas informações para uso com as máquinas específicas indicadas. A IBM não faz nenhuma representação que esteja de acordo com qualquer outro propósito.

Os sistemas de computador da IBM contêm mecanismos projetados para reduzir a possibilidade de distorção ou perda de dados não detectados. No entanto, esse risco não pode ser eliminado. Os usuários que passam por períodos de inatividades não planejados, falhas de sistema, flutuações ou quedas de energia ou falhas do componente devem verificar a precisão de operações executadas e dados salvos ou transmitidos pelo sistema perto ou no período de inatividade ou falha. Além disso, os usuários devem estabelecer os procedimentos para certificar-se de que há verificação de dados independentes antes de contar com tais dados em operações sensíveis ou críticas. Os usuários devem verificar periodicamente os websites de suporte da IBM para obter informações atualizadas e correções aplicáveis ao sistema e software relacionado.

Instrução de Homologação

Este produto não pode ser certificado em seu país para conexão, por qualquer meio, com as interfaces das redes de telecomunicações públicas. Certificação adicional pode ser requerida por lei antes desse tipo de conexão. Entre em contato com o representante IBM ou o revendedor para qualquer questão.

Recursos de acessibilidade para os servidores IBM Power Systems

Os recursos de acessibilidade ajudam os usuários que têm uma deficiência, tal como mobilidade restrita ou visão limitada, a usar o conteúdo da tecnologia da informação com sucesso.

Visão geral

Os servidores IBM Power Systems incluem os principais recursos de acessibilidade a seguir:

- Operação apenas pelo teclado
- Operações que usam um leitor de tela

Os servidores IBM Power Systems usam o padrão W3C mais recente, [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/), para assegurar a conformidade com [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) e [Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/). Para aproveitar os recursos de acessibilidade, use a versão mais recente do seu leitor de tela e o navegador da web mais recente que é suportado pelos servidores IBM Power Systems.

A documentação do produto on-line dos servidores IBM Power Systems no IBM Knowledge Center está ativada para acessibilidade. Os recursos de acessibilidade do IBM Knowledge Center estão descritos na [seção 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).

Navegação pelo teclado

Este produto usa teclas de navegação padrão.

Informações da interface

As interfaces com o usuário dos servidores IBM Power Systems não possuem conteúdo que pisca de 2 a 55 vezes por segundo.

A interface com o usuário da web dos servidores IBM Power Systems conta com folhas de estilo em cascata para renderizar o conteúdo corretamente e para fornecer uma experiência utilizável. O aplicativo fornece uma maneira equivalente para os usuários com baixa visão para usar as configurações de exibição do sistema, incluindo o modo de alto contraste. É possível controlar o tamanho da fonte usando as configurações do dispositivo ou navegador da web.

A interface com o usuário da web dos servidores IBM Power Systems inclui referências de navegação WAI-ARIA que podem ser usadas para navegar rapidamente para as áreas funcionais no aplicativo.

Software do fornecedor

Os servidores IBM Power Systems incluem determinado software de fornecedor que não é coberto pelo contrato de licença IBM. IBM não faz declarações sobre os recursos de acessibilidade destes produtos. Entre em contato com o fornecedor para obter as informações de acessibilidade sobre seus produtos.

Informações relacionadas de acessibilidade

Além dos websites de help desk e suporte padrão da IBM, a IBM tem um serviço de telefone TTY para uso por clientes surdos ou deficientes auditivos para acessar os serviços de vendas e suporte:

Serviço de TTY
800-IBM-3383 (800-426-3383)
(na América do Norte)

Para obter mais informações sobre o compromisso que a IBM tem com a acessibilidade, veja [IBM Accessibility \(www.ibm.com/able\)](http://www.ibm.com/able).

Considerações sobre política de privacidade

Os produtos de Software IBM, incluindo soluções de software como serviço (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoal identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoais identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoais identificáveis, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, esta Oferta de Software pode usar cookies de sessão que coletam o nome e o endereço IP de cada usuário para propósitos de gerenciamento de sessão. Esses cookies podem ser desativados, mas desativá-los eliminará também a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações pessoais identificáveis dos usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico a respeito de quaisquer leis aplicáveis a esse tipo de coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em <http://www.ibm.com/privacy> e a Declaração de privacidade on-line da IBM em <http://www.ibm.com/privacy/details/us/en/> na seção intitulada “Cookies, web beacons e outras tecnologias”.

Marcas Registradas

IBM, o logotipo IBM e [ibm.com](http://www.ibm.com) são marcas ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser

marcas comerciais da IBM ou outras empresas. Uma lista atual de marcas registradas da IBM está disponível na Web em [Copyright and trademark information](#).

A marca registrada Linux é usada conforme uma sublicença da Linux Foundation, a licenciada exclusiva de Linus Torvalds, proprietário da marca em nível mundial.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph e Gluster são marcas comerciais ou marcas registradas da Red Hat, Inc. ou de suas subsidiárias nos Estados Unidos e em outros países.

Microsoft e Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

Avisos de Emissão Eletrônica

Notas de Classe A

As seguintes instruções de Classe A aplicam-se aos servidores IBM que contêm o processador POWER9 e seus recursos, a menos que designados como Classe B de compatibilidade eletromagnética (EMC) nas informações do recurso.

Quando conectar um monitor ao equipamento, você deve usar o cabo do monitor projetado e quaisquer dispositivos de supressão de interferência fornecidos com o monitor.

Aviso do Canadá

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

Aviso da Comunidade Europeia e do Marrocos

Este produto está em conformidade com os requisitos de proteção da Diretiva 2014/30/EU do Parlamento Europeu e do Conselho sobre a harmonização das leis dos Estados Membros relativas à compatibilidade eletromagnética. A IBM não pode aceitar a responsabilidade por qualquer falha em atender aos requisitos de proteção resultantes de uma modificação não recomendada do produto, incluindo a adaptação de placas opcionais não IBM.

Este produto pode causar interferência se usado em áreas residenciais. Tal utilização deve ser evitada, a menos que o usuário assuma medidas especiais para reduzir as emissões eletromagnéticas para evitar interferência na recepção de transmissões de rádio e televisão.

Aviso: este equipamento é compatível com a classe A do CISPR 32. Em um ambiente residencial, este equipamento pode causar interferência de rádio.

Aviso da 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

e-mail: HalloIBM@de.ibm.com

Generelle Informationen:

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

Aviso do Japan Electronics and Information Technology Industries Association (JEITA)

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値: Knowledge Centerの各製品の
仕様ページ参照

Esta instrução se aplica a produtos menores ou iguais a 20 A por fase.

高調波電流規格 JIS C 61000-3-2 適合品

Essa instrução se aplica a produtos com mais de 20 A, monofásicos.

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、P F C回路付)
- 換算係数 : 0

Esta instrução se aplica aos produtos maiores que 20 A por fase, três fases.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、PFC回路付)
- 換算係数 : 0

Aviso do Japan Voluntary Control Council for Interference (VCCI)

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 da Coreia

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

Aviso da 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 da Rússia

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

Aviso de 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 contato 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 aprovado segundo os critérios estabelecidos para dispositivos digitais Classe A, em conformidade com a Parte 15 das Normas da FCC. Esses critérios têm a finalidade de assegurar um nível adequado de proteção contra interferências prejudiciais, quando o equipamento estiver funcionando em uma instalação comercial. Este equipamento gera, utiliza e pode emitir energia em frequência de rádio e, se não for instalado e utilizado de acordo com o manual de instruções, pode provocar interferência prejudicial em comunicações por rádio. A operação deste equipamento em áreas residenciais pode provocar interferência prejudicial, caso em que o usuário deverá tomar as medidas que forem necessárias às suas próprias custas.

Devem ser utilizados cabos e conectores encapados e aterrados adequadamente, a fim de atender aos critérios de emissão estabelecidos pela FCC. Cabos e conectores adequados estão disponíveis nos revendedores autorizados IBM. A IBM não é responsável por qualquer interferência de rádio ou televisão causada pelo uso de cabos e conectores diferentes dos recomendados ou por mudanças ou modificações não autorizadas neste equipamento. Alterações ou modificações não autorizadas podem cancelar a autorização do usuário para operar o equipamento.

Este dispositivo está em conformidade com a Parte 15 das Normas da FCC. Operation is subject to the following two conditions:

(1) este dispositivo não pode causar interferência danosa e (2) este dispositivo deve aceitar qualquer interferência recebida, incluindo interferência que pode causar operação indesejada.

Parte Responsável:

International Business Machines Corporation
New Orchard Road
CEP 22290-240

Para obter informações somente sobre a conformidade de FCC, entre em contato com
fccinfo@us.ibm.com

Avisos da Classe B

As seguintes declarações da Classe B se aplicam aos recursos designados como Electromagnetic Compatibility (EMC) Classe B nas informações sobre instalação do recurso.

Quando conectar um monitor ao equipamento, você deve usar o cabo do monitor projetado e quaisquer dispositivos de supressão de interferência fornecidos com o monitor.

Aviso do Canadá

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

Aviso da Comunidade Europeia e do Marrocos

Este produto está em conformidade com os requisitos de proteção da Diretiva 2014/30/EU do Parlamento Europeu e do Conselho sobre a harmonização das leis dos Estados Membros relativas à compatibilidade eletromagnética. A IBM não pode aceitar a responsabilidade por qualquer falha em atender aos requisitos de proteção resultantes de uma modificação não recomendada do produto, incluindo a adaptação de placas opcionais não IBM.

Aviso em alemão

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

e-mail: HalloIBM@de.ibm.com

Generelle Informationen:

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

Aviso do Japan Electronics and Information Technology Industries Association (JEITA)

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値: Knowledge Centerの各製品の
仕様ページ参照

Esta instrução se aplica a produtos menores ou iguais a 20 A por fase.

高調波電流規格 JIS C 61000-3-2 適合品

Essa instrução se aplica a produtos com mais de 20 A, monofásicos.

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、P F C回路付)
- 換算係数 : 0

Esta instrução se aplica aos produtos maiores que 20 A por fase, três fases.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、P F C回路付)
- 換算係数 : 0

Aviso do Japan Voluntary Control Council for Interference (VCCI)

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を目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI-B

Aviso de 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 compatível com os limites para um dispositivo digital Classe B, de acordo com a Parte 15 das Normas da FCC. Esses limites são projetados para fornecer proteção razoável contra interferência prejudicial em uma instalação residencial. Este equipamento gera, utiliza e pode emitir energia de frequência de rádio e, se não for instalado e utilizado de acordo com o manual de instruções, pode provocar interferências prejudiciais à comunicação por rádio. Entretanto, não existe nenhuma garantia de que essa interferência não ocorrerá em uma instalação específica. Se esse equipamento realmente provocar interferência prejudicial na recepção de rádio ou televisão, que pode ser determinada ligando e desligando o equipamento, o usuário será encorajado a tentar corrigir a interferência por meio de uma ou mais das medidas a seguir:

- Reoriente ou realocize a antena receptora.
- Aumente a separação entre o equipamento e o receptor.
- Conecte o equipamento em uma tomada em um circuito diferente daquele ao qual o receptor está conectado.
- Consulte um revendedor autorizado IBM ou um representante de serviço para obter ajuda.

Devem ser utilizados cabos e conectores encapados e aterrados adequadamente, a fim de atender aos critérios de emissão estabelecidos pela FCC. Cabos e conectores adequados estão disponíveis nos revendedores autorizados IBM. A IBM não é responsável por qualquer interferência de rádio ou televisão causada pelo uso de cabos e conectores diferentes dos recomendados ou por mudanças ou modificações não autorizadas neste equipamento. Alterações ou modificações não autorizadas podem cancelar a autorização do usuário para operar o equipamento.

Este dispositivo está em conformidade com a Parte 15 das Normas da FCC. Operation is subject to the following two conditions:

(1) este dispositivo não pode causar interferência danosa e (2) este dispositivo deve aceitar qualquer interferência recebida, incluindo interferência que pode causar operação indesejada.

Parte Responsável:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504

Para obter informações somente sobre a conformidade de FCC, entre em contato com
fccinfo@us.ibm.com

Termos e Condições

As permissões para o uso dessas publicações são concedidas sujeitas aos termos e condições a seguir.

Aplicabilidade: Estes termos e condições complementam os termos de uso do website da IBM.

Uso Pessoal: essas publicações podem ser reproduzidas para uso pessoal, não comercial, desde que todos os avisos de propriedade sejam preservados. Não é permitido distribuir, exibir ou fazer trabalhos derivados dessas publicações, ou de qualquer parte delas, sem o consentimento expresso da IBM.

Uso Comercial: é permitido reproduzir, distribuir e expor essas publicações exclusivamente dentro de sua empresa, desde que todos os avisos de propriedade sejam preservados. Não é permitido fazer trabalhos derivados dessas publicações, nem reproduzi-las, distribuí-las ou exibi-las, integral ou parcialmente, fora do âmbito da empresa, sem o consentimento expresso da IBM.

Direitos: Exceto conforme expressamente concedido nesta permissão, nenhuma outra permissão, licença ou direito é concedido, expresso ou implícito, para as publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contida.

A IBM reserva-se o direito de retirar as permissões concedidas neste instrumento sempre que, a seu critério, o uso das publicações for prejudicial a seu interesse ou, conforme determinação da IBM, as instruções anteriores não estejam sendo seguidas adequadamente.

Não é permitido fazer download, exportar ou reexportar estas informações, exceto em total conformidade com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação dos Estados Unidos.

A IBM NÃO DÁ NENHUMA GARANTIA QUANTO AO CONTEÚDO DESSAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM" E SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

